Preliminary Study on the electronic provision of certificates and attestations usually required in public procurement procedures

Final report

Strategy and implementation roadmaps

European Commission
Internal Market and Services DG

Brussels

Issued on:.....05/09/2008

This report was prepared by Siemens and Time.lex on behalf of the European Commission, Directorate-General Internal Market and Services under the contract ENTR/05/58-SECURITY/ETD/2006/IM/C1/126.

Table of Contents

Executive summary

Introduction

In this study, the "Preliminary Study on the electronic provision of certificates and attestations in public procurement procedures", we have examined how 32 different European countries (Member States, Candidate Countries and EEA countries) currently manage the use of attestations in procurement procedures, particularly in an eProcurement context. The goal of the study was to identify if and how electronic attestations are currently issued in each of these countries, whether they can be accepted and validated in public procurement procedures across these countries, and if and how their eProcurement systems could be modified or amended to support foreign electronic attestations, thus facilitating cross border economic activities in these countries and contributing to the creation of an internal market for electronic procurements.

As a part of this study, a series of scenarios were created that could be used to build interoperability between existing e-attestation systems, i.e. to ensure that electronic attestations from a tenderer established in one country could be presented to a contracting authority in a different country. These scenarios were then comparatively assessed in order to determine the most efficient or promising ones, and roadmaps were subsequently drafted to implement the most favoured interoperability scenarios. Finally, the study presented a number of recommendations for future actions to gradually improve the availability and usability of electronic attestations in public procurement procedures.

In this executive summary, a brief overview will be provided of the main findings of the study.

Overview of the current status of electronic public procurement in Europe

In the initial stages of this Study, the Study Team examined current practices in 32 European countries in relation to electronic public procurement, examining in particular what types of evidentiary documents were commonly asked for in such proceedings, and if any electronic equivalents of such documents existed. Where no electronic attestations existed, the Study Team inquired what alternative mechanisms were used to replace these documents in electronic procurements; or if no alternatives existed yet, what plans the administrations had to resolve this problem. This information was then systematically analysed, in order to identify common trends, patterns and solution models.

The study showed that the 32 surveyed countries have taken very different approaches to eProcurement and to the role of electronic attestations in the eProcurement process. At one end of the spectrum, we can see eProcurement systems which require only an on-line registration which result in the tenderer receiving a username/password. Using these credentials, the tenderer can submit his offers, relying entirely on conventional file formats and unsigned scans of any additional documents that may be required as supporting evidence. At the other end of the spectrum, we see platforms which support only a small set of PKI signature solutions which can only be obtained after a prior registration. This signature is typically used to sign an offer and a self-declaration form attesting to the tenderer's compliance with the tender specifications, which will then have to be confirmed by submitting original paper certificates to the contracting authority if the bid should prove to be successful.

The same variety is seen with regard to electronic attestations, where eight categories of document types that contracting authorities might commonly ask for in public procurements were examined. These categories included documents showing the absence of criminal convictions (e.g. extracts from judicial records), compliance with fiscal and social obligations (e.g. tax/social security certificates), or adherence to specific standards (e.g. certificates of conformity). Obviously, contracting authorities will only request documentation to be presented if this is required by law or if this is needed to determine the suitability of the bid. In practice, this means that certain document categories (e.g. compliance with environmental standards) are much less commonly encountered than others (e.g. compliance with fiscal obligations).

While the availability of electronic versions of such documents varied from country to country and from document type to document type, the study showed that electronic attestations were generally only rarely available, and even more rarely commonly used in public procurements in the surveyed countries. Broadly speaking, five approaches could be distinguished:

- Countries which have not yet identified a strategy in this regard (15 out of 32 countries; 47%). The vast majority of these countries simply do not yet have any eProcurement infrastructure in place or have not yet implemented an appropriate legal framework. However, there are also a few countries that have not yet made eCertificates a significant part of their eProcurement strategy: eProcurement is possible, but eCertificates are not commonly required.
- Countries which rely on declarations of compliance from the tenderer (10 out of 32 countries; 31%). Such declarations can either serve to postpone the submission of certificates until a winning bid has been chosen, or can replace it entirely.
- Several countries have also implemented a limited trusted third party (TTP) or prequalification system (8 out of 32 countries; 25%), wherein a tenderer may register with a TTP prior to participating in a public procurement, providing certain commonly required evidentiary documents to the TTP.
- Systems where the contracting authority has to obtain the required information itself, if the source is another public sector controlled entity. This approach, consisting of a direct and protected transfer of information from one administration to the next can be found on a limited scale in 5 out of 32 countries (16%).
- Finally, 4 out of 32 countries (12.5%) have reported that administrations can simply issue electronic certificates or attestations which have been signed with a PKI signature. However, in all countries which reported this approach, the systems were largely in a pilot stage, and not yet commonly used in public procurements.

Since the latter category (electronic attestations issued directly by public administrations) does not (yet) occur in eProcurements in practice, it is important to stress that at this time there are thus only three types of electronic attestations to be considered:

- Self-declaration forms, signed by the tenderer using the signature solution permitted by the eProcurement system. However, it is debatable whether these should be considered electronic attestations, since they offer no guarantee other than the candidate's assurance of compliance.
- Direct information exchange between administrations, i.e. the contracting authority will no longer require the tenderer to provide certain information, because it can access them directly from an authentic source. Again, it is debatable whether this should be considered an electronic attestation: while the data transfer perfectly emulates the functionality of a traditional

certificate, the concept is more akin to an explicit mandate given to the administration to make the inquiries that are required to determine compliance with certain tender specifications.

- Declarations of compliance from TTPs in a prequalification system, i.e. the contracting authority is assured by a TTP (which may be a public or private sector entity) that the tenderer meets certain requirements on the basis that the tenderer has undergone a prior registration with the TTP, during which certain evidentiary documents have been provided. However, this again usually does not take the form of an electronic attestation provided to the tenderer by the TTP, but rather a mandate to the contracting authority to request this information from the TTP (a 'pull model'), or an instruction to the TTP to provide this information to the contracting authority (a 'push model').

Examining these approaches, one can only conclude that the main approach used by the surveyed countries to handle the problems related to attestations is to install electronic procedures that eliminate or reduce the need for attestations, either in a paper or electronic form. The creation of new electronic attestations on the other hand is virtually non-existent.

From an interoperability perspective, all of the three models described above – self declaration forms, direct information exchange and prequalification systems – are difficult to extend to foreign users:

- Declaration forms require the tenderer to have access to a supported signature type, and require him to fully comprehend the declaration which he is signing.
- Direct information exchange presently only works on a national level. Information must be provided directly from local databases, and opening such databases to foreign contracting authorities is both legally and politically very sensitive, and presents substantial security and liability risk.
- Finally, prequalification systems are also frequently less accessible to foreign tenderers, because they offer the greatest benefit to tenderers who can easily register with the TTP and who frequently submit offers where the statement from the TTP is used. Both of these factors favour local tenderers over foreign tenderers.

Thus, reliance on these approaches shows substantial benefits, but at the current stage mostly to local tenderers, who see their administrative burden reduced significantly. For foreign tenderers however, it is much more difficult or in some cases even impossible to use these systems, let alone to derive any proportionate benefit from them. Indeed, in practice systems that rely on electronic attestations at this time are rarely accessible to foreign tenderers, with the sole exception being systems which rely on unilateral declarations in instances where the supported signature method is available to foreign bidders, which is a rather rare circumstance.

Solution models – scenarios and potential approaches to the cross border use of e-attestations

Six scenarios that have been elaborated in the course of this study, which aim to resolve these problems by presenting approaches that would allow companies to submit their offers electronically to any public procurement, including foreign ones. However, it is important to keep in mind that the current infrastructure (including from an organisational, legal and technical perspective) does not allow any of these scenarios to be deployed immediately and without an investment of effort. All scenarios will require some degree of reorganisation or modernisation in most or even all countries.

The following scenarios have been created and assessed as a part of this study:

- Unilateral declarations of compliance: in this first scenario, the tenderer uses a standardised electronic form (typically provided by the contracting authority as a part of the tender specifications) to declare his compliance with the applicable procurement requirements, and submits this to the contracting authority using any signature method that is permitted by the contracting authority. This declaration then either replaces the traditional (paper) attestations, or acts as a substitute until the best offer has been selected, at which point, the (provisionally) best tenderer must still submit the traditional paper attestations.
- Non-interventionist information dissemination scenario: in this scenario, Member States would be required to create an informational contact point (e.g. a website) from where they distribute information on their electronic attestation practices, including specific technical information with regard to formats and any electronic signatures being used in electronic attestations (if available). The purpose of this information would be to give aspiring tenderers and administrations a formal information resource that they can consult, and (if desired and possible) to gradually build automatic validation mechanisms into their eProcurement systems.
- Using an electronic attestation package signed by a TTP: here, the tenderer offers a single bundle of attestations (i.e. a single electronic file containing all required attestations), signed by a specific trusted administration in each country. While the contracting authority can still extract the individual attestations from the bundle, validation is only performed on the bundle as a whole; i.e. trust is derived from the fact that the bundle has been signed through a signature belonging to a trusted administration. If the signature on the bundle is valid, the attestations contained in the bundle are also considered to be valid; i.e. trust is 'inherited' from the entire bundle by the individual attestations.
- Decentralised issuance of electronic attestations by the originating administrations: the same administrations keep issuing the same attestations that fall under their competence, but will in the future do so in an electronic form and carrying an electronic signature, without any kind of centralisation (unless this already existed in the present system). From an organisational perspective, this would be considered an electronic continuation of the status quo.
- Single trusted storage point of electronic attestations: in this model, electronic attestations are stored in single storage points, which are either (partially) controlled by a public administration, or which are purely controlled by the tenderer himself. The key element is that the tenderer has a single storage point in which electronic documents can be deposited and kept, and in which the tenderer can authorise third parties (like contracting authorities) to access the storage point to consult all or some of the stored documents. Thus, in this model tenderers no longer provide attestations to contracting authorities, but only limited access to a storage space containing the required information.

- Finally, the sixth scenario is the construction of federated networks to facilitate information exchange between authorised parties. The key objective of this model is to create a network of trusted information sources, between which a consistent direct data exchange approach is implemented. Instead of requesting specific attestations to be provided by the tenderer, contracting authorities will be mandated by the tenderer to obtain information directly at the source, i.e. from the administration(s) which manages the requested information in the tenderer's country of establishment.

In order to determine which of these six scenarios offered the greatest potential for application on a European scale, each of the scenarios was analysed in detail and assessed against a number of criteria, including organisational and technical simplicity; legal, financial and political viability; real interoperability impact and added value. Using a balanced scoring system, each of the models was compared to determine which ones would be the most realistic and offer the greatest added value.

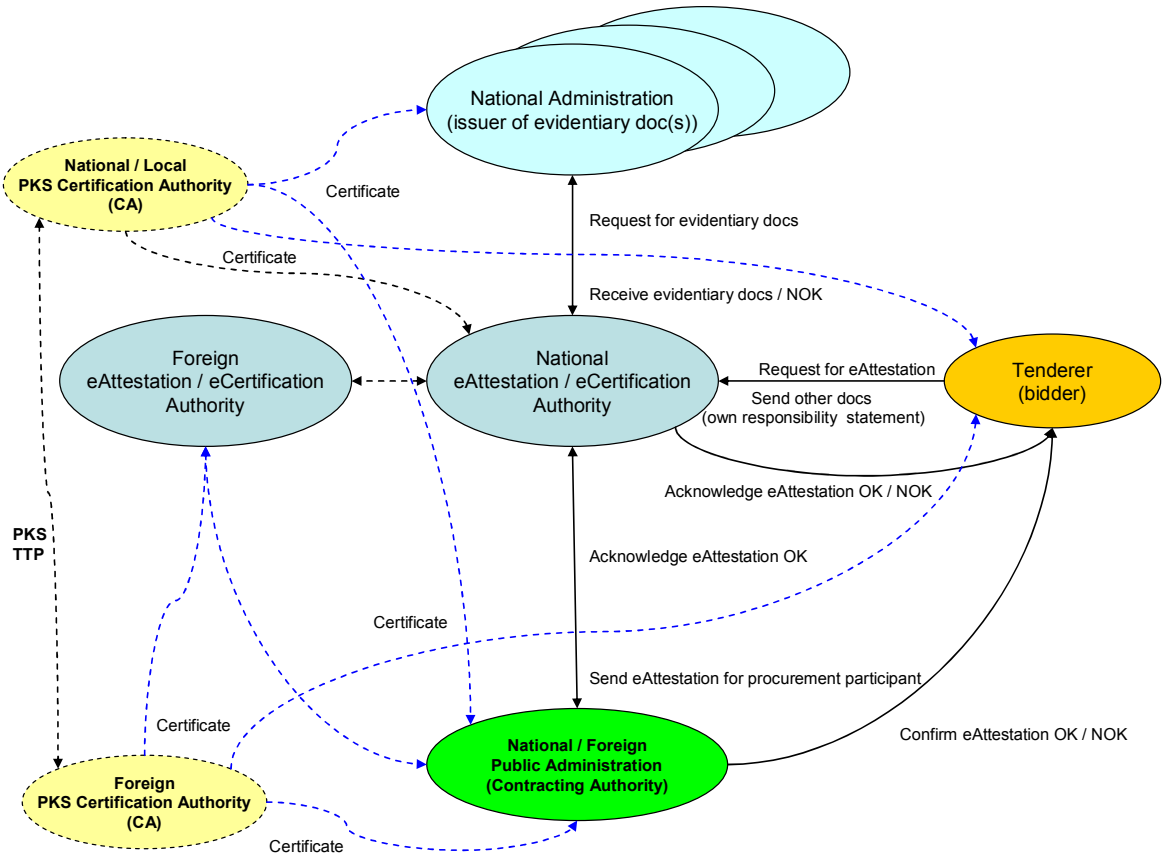
The three highest rated scenarios were the scenarios based on single attestation packages signed by TTP, trusted storage points and federated networks. For each of these scenarios a specific roadmap for its implementation was provided. However, it is even more important to illustrate how these scenarios interrelate, and how progress can be made from a pragmatic perspective. The study handles this question in two different ways: on the one hand by defining an ideal longer term solution, including a number of basic principles to be observed by any solution model in the longer run; and on the other hand by proposing a set of recommendations for gradual progress.

Evolving towards an ideal solution for eProcurement in Europe

The purpose of an Ideal Solution for the implementation of eAttestations /eCertificates is to:

- Create a **theoretical solution** for eAttestations / eCertificates which is built and operated in ideal conditions and which eventually could never be implemented in the real world; this is necessary in order avoid the diversity and complexity of the eAttestations / eCertificates solutions in the real world;
- Allow an easier identification of a **General Strategy** for the set up of such Ideal Solution;
- Define specific **Implementation Roadmaps** for the selected solutions for eAttestations / eCertificates by tailoring the general strategy to the specific context of each selected solution;
- Identify a **Common Set of Elements (a Common Platform)** necessary to:
    - Facilitate the compatibility and interoperability between specific eAttestations / eCertificates solutions;
    - Reduce the complexity of the work performed by the Contracting Authority (the ITT Manager) in processing eAttestations / eCertificates received from national entities or from abroad (mainly the other Members States of EU);
- **Identify Critical Issues and propose ways to improve the key solutions** for eAttestations / eCertificates.

In this document the usage of the Ideal Solution is limited and it is not considered as short term alternative to the selected scenarios. At a high (business) level, the relations and interactions in the envisaged ideal solution can be visualised as follows:



The suggested Ideal Solution consists of:

- A Public (national / foreign) Administration (Contracting Authority) which receives and processes the eAttestations / eCertificates as a first step of an eProcurement processes;
- One or more National Administrations in charge of preparing and issuing the required evidentiary documents;
- One or more national (publicly or privately owned) authority or authorities in charge of:
  - Collecting the documents necessary to issue an eAttestation / eCertificate at the request of an entity / company / physical person interested to participate to an ITT locally or abroad; ideally is that the collected documents are:
    - Based on the recommended evidentiary documents types;
    - Standardized and normalized (national / EU wide); and
    - Available in an electronic format (XML), issued and signed electronically by the national administration responsible;
  - Issuing digitally signing the eAttestations / eCertificates in electronic format (XML);

- Sending the digitally signed eAttestation / eCertificate to the public (national / foreign) administration in charge of the ITT processing (the Contracting Authority);
- The bidder concerned by the eAttestation / eCertificates;
- A National Certification Authority in charge of issuing and management of the certificates containing (among others) the asymmetric key pairs (public + private) for the National eAttestation / eCertificate Authority the National Contracting Authority and eventually for the National Administrations issuing the evidentiary documents (in electronic form);
- A Foreign Certification Authority in charge of issuing and management of the certificates containing (among others) the asymmetric key pairs (public + private) for the Foreign eAttestation / eCertificate Authority or eventually the Foreign Contracting Authority.

The following steps are part of the strategy to implement the eAttestation / eCertificate ideal solution(s) at national and European levels (including EIs level):

1. **Step 1:** European and National political commitment in favour of such an ideal solution for eAttestation / eCertificate as part of the solution for eProcurement, both national and EU wide;
2. **Step 2:** A clear, complete, consistent and compatible legal context is adopted both at the European level (European Directive(s)) and the national level (national laws) for the legal usage as part of the eProcurement process;
3. **Step 3:** Budgets must be made available to finance the eAttestation / eCertificate Ideal solution;
4. **Step 4:** Implement the organizational measures / changes required to perform the eAttestation / eCertificate activities and also the PKI management organisation at national level and European level;
5. **Step 5:** Implement and test the technical solution for the PKI management at national (and European) level;
6. **Step 6:** Implement and test the technical solution for the eAttestation /eCertificate Ideal Solution at national and cross-border level;
7. **Step 7**: Accept and declare the eAttestation / eCertificate solution operational;
8. **Step 8:** Audit the eAttestation / eCertificate system on a regular basis and recommend improvements as part of best practices for IT Governance and also to ensure forward compatibility with the eProcurement process.

The General Strategy for the Ideal Solution described above is considering an ideal context in which there are no blocking or delaying factors (e.g. the budgets required are not approved, there is no national and EU –wide agreement on the standardization / normalization of the evidentiary documents and eAttestations / eCertificates structure and content). For the three key scenarios identified above to be implemented in a real environment, the related roadmaps have taken into account the real world context, identified the critical risks and identified measures to eliminate / reduce these risks.

General conclusions and recommendations

eProcurement and eAttestations / eCertificates in the broader eGovernment context – the need for a common infrastructure and common development

This study focused specifically on the issue of presenting e-attestations to a contracting authority in a public procurement at the E.U. level, and attempted to identify issues and solution strategies for this context. However, the issues and solutions examined in this context are not unique, and recur in almost any eGovernment situation. Key complexities include:

- The cross border submission of electronic documentation, including in situations where only paper original documents exist and no electronic equivalents are readily available;
- The validation of this documentation by the recipient, keeping into account the fact that the original document might be in an unfamiliar language and that even its purpose might not be entirely clear;
- The cross border identification of entities when relying only on electronic resources, keeping unto account that the potential group of entities is vast and that there is no unique identifier that can be universally applied;
- The use of electronic signatures as a mechanism of ensuring the authenticity and integrity of a document, and as a means of linking a document to a specific signatory, especially keeping into account the early stages of deployment of PKI solutions in most countries and the difficulty in determining the legal value and reliability of foreign electronic signatures;
- The creation of trust in foreign entities and the information they provide, either directly or via the intervention of an intermediary;
- The creation of suitable mechanisms for the reliable and trustworthy exchange of information between public authorities and authentic sources without harming national and with full respect of data protection principles.

The list of issues above is a fair approximation of the problems that need to be resolved in virtually any European eGovernment project, and indeed a large number of eGovernment projects are currently underway that already aim to resolve one or more of these issues, including the initiatives surrounding the Services Directive, the STORK and PEPPOL projects, the BRITE project, the ECRIS system and so forth.

While obviously not exhaustive, the list above demonstrates that a large number of projects and initiatives are scheduled or already underway that directly implement some of the aforementioned scenarios in a specific context. This shows that the scenarios are not just theoretical concepts that require fundamental overhauls and redesigning of existing systems simply for the purposes of facilitating electronic procurement; but rather that the scenarios are applications of specific trends that are already underway in the optimisation of public services in general. The results of these initiatives should then be able to logically build on one another, to create a coherent and well functioning infrastructure in which public procurement is simply one more application that the framework can support.

Step by step development – gradual progress towards a 'full service' future

As noted above, it would be quite difficult to realise any of the aforementioned scenarios directly, and this would certainly not be a goal that could be met in the short term. If progress is to be made within a reasonable period, it is recommended to take a step-by-step approach, in which the initial focus is on creating the basic building blocks and providing basic functionalities to as large a group of users as possible. In a second stage, the aforementioned scenarios can be realised for specific document types – in all likelihood one context or document type at a time – with the eventual goal of combining these scenarios into a joint system that can conceptually support any document type, as described in the ideal solution. Below the main operational recommendations in this regard will be summarised.

Short term recommendations – improving information dissemination and encouraging administrative simplification

There are a number of smaller steps that could be taken by the Member States and at the European level in the shorter term (1-2 years) to facilitate further interoperability initiatives. While each of these steps on their own would not bring about a significant amount of interoperability and would not necessarily facilitate the cross border use of electronic attestations, each of them would provide an important piece of the interoperability possible, and jointly they would act as the foundation for further initiatives, including the implementation of the aforementioned scenarios.

A first major step would be to improve the availability of information on (e-)Attestation practices in the Member States, as described in the form of an information dissemination scenario above. To summarise, it is recommended to provide a common platform to the Member States where they would be required to systematically publish detailed information on the attestation types they use, including in an electronic context. One could consider the European Commission to take a guiding role in this respect, by offering the Member States a platform on which they could publish their own information. The Commission would then act as a coordinator for the collection and dissemination of the information, while the Member States would remain responsible for ensuring that the information itself would be accurate and complete. This scenario is not a real model for interoperability, since it only concerns the collection and dissemination of relevant information; and this is the reason why it was not chosen as one of the three preferred scenarios for which roadmaps were created However, the availability of such information is a prerequisite for the efficient execution of all other scenarios. Thus, the creation of such a central information portal could provide a first useful building block in the exchange and acceptance of attestations, both in a traditional and in a paper context.

A second important recommendation is a lesson that can be learned from the activities surrounding the Services Directive, where administrations are also faced with the problem that entities would need to provide documentation via electronic means, when quite frequently no electronic documents are available. However, the Services Directive contains a legal requirement for Member States to minimise requests for original documents, and thus to also accept valid substitutes such as copies, unless an exception applies. Obviously, there is no similar legal obligation in the context of public procurements. None the less, as already noted above, the problem is the same, and there seems to be no reason in principle why Member States would not take the same approach to heart. Formulated pragmatically, one way to reduce the scale of the problem is for Member States to adopt alternative approaches to requesting electronic originals whenever this is viable.

This idea is not revolutionary or even novel: we stressed above that the most common 'solution' to solving the attestation problem (found in 10 out of 32 countries) was to rely on unilateral declarations of compliance from the tenderer. Thus, unilateral declarations of compliance can be seen as a form of administrative simplification, albeit one that seems currently dictated mostly by technical necessity

rather than by a desire to simplify life for the tenderer and the administration. None the less, at least as a provisional mechanism until more reliable scenarios are implemented, approaches which allow the tenderer to submit substitutes for attestations can be considered a good practice.

This recommendation should not be misconstrued as an encouragement to abandon all attestations in favour of unilateral declarations. Rather, the purpose is to show that interoperability problems can be decreased in scale by conducting appropriate risk management exercises to determine what the precise evidentiary needs are in any given procurement. In many cases, such as lower value bids or when sufficient additional verification measures have been taken, the result could well be that unilateral declarations can be an acceptable solution to simplify interoperability issues.

In summary, it is recommended that Member States conduct proper risk management before requesting specific attestations, and that they consider alternative and more flexible options as well.

Recommendations for the medium term - encouraging the uptake and use of electronic attestations at the national level

It was noted above that electronic attestations in the strictest sense (i.e. electronic documents issued directly as evidentiary documentation by the competent administrations) only existed in very few cases, and that their use in public procurements was virtually non-existent. Common attestations such as tax attestations, social security attestations, extracts from criminal registers, attestations of proper conduct, and attestations of non-bankruptcy, generally only exist in a paper form. This is particularly problematic as these are the types of attestations which are requested very frequently in public procurements.

This means that a great deal of progress could be made if these commonly issued public sector attestations were to be issued in an electronic form. For this reason, it is recommended to encourage countries that issue such certificates to make electronic versions available to the public. This refers specifically to the attestation types commonly issued by public administrations and which constitute the bulk of the evidentiary requirements in most procurements, and most notably:

- Extracts from criminal registers or the corresponding court certificates, as the key document to show non-conviction in criminal matters; this also includes attestations of good behaviour in countries which use such documents instead of extracts or court certificates;
- Extracts from commercial registers or court certificates attesting to non-bankruptcy; again this includes attestations of good behaviour in countries which use such documents instead of extracts or court certificates;
- Extracts from commercial registers to show enrolment in a professional register;
- Attestations showing compliance with tax regulations, including VAT legislation if applicable;
- Attestations showing compliance with social security obligations.

The introduction of official electronic substitutes for each of these document types would already provide tenderers with the means to provide official electronic attestations to foreign contracting authorities, even if it would likely remain difficult initially for those authorities to validate such documents in a satisfactory manner. As a way of supporting this process, existing initiatives in countries that already publish such attestations should be published and disseminated as good practices, in order to encourage and support spontaneous harmonisation. This is of course a part of the aforementioned recommendation of publishing and disseminating current attestation practices.

Longer term recommendations – implementation of the scenarios in coordination with existing initiatives

The small steps described above collectively already provide some useful building blocks in solving the eAttestation problem. If applied consistently in all countries, tenderers would be able to provide most types of attestations and documentation in an electronic form to the contracting authority in a majority of procurements. None the less, in order to provide a more satisfactory possibility to contracting authorities, other and more systematic approaches will be needed. While a general uptake of electronic attestations would indeed ensure that tenderers could easily provide their attestations to foreign administrations, this would not resolve all problems.

For this reason, other mechanisms should be considered that are capable of creating trust in attestations even when the actual issuer is unknown to the recipient, and that are capable of working around the restriction that attestations will likely retain their paper form in most countries for the years to come. Such mechanisms should also be able to handle other attestation types than those noted above, and specifically attestations that are not issued by public administrations, such as diplomas, certificates of conformity with specific standards and bank attestations. After all, it must also be possible to submit these documents in an electronic form, even when no electronic originals exist. To solve this problem, the three specific scenarios that have been described above come into play.

It is clear that the scenarios have a different scope and a different application in practice. Without going into details, their main attributes from a pragmatic perspective can be summarised as follows:

- A scenario based on TTPs signing attestation packages can handle any document type equally well, regardless of its origin, since trust in the contents of the package is inherited entirely from the signature of the package itself. Thus, it is conceptually simple. Furthermore, out of the three scenarios, this is the only one that can handle situations where only paper originals exist (by scanning the originals and adding them to the bundle). However, the downside is that it requires a network of TTPs to be set up, which need to provide additional services (beyond simply signing the package) to make their services valuable to the end user. Thus, getting broad adoption could be complicated in practice, especially since only few countries have a tradition in TTP systems.
- A scenario based on trusted storage systems is very flexible, and scales well in the sense that it can start as a simple content management platform (with limited added value) and that it can grow to integrate more reliable information, including from official sources (thus adding substantial added value). However, the scenario struggles to offer added value in cases where no original electronic data is available (i.e. when information cannot be extracted from an official database), since the tenderer can then do little more than simply upload a copy to the system. Thus, the scenario is very useful as a tool to bundle and aggregate information from official and reliable sources. For other information – including most types of information provided by private parties – the scenario will typically not be able to add value, due to the absence of a trusted official electronic resource to exploit.
- Finally, federated networks often the greatest added value, as they allow authentic information to be exchanged directly, thus minimising costs, efforts, and risks of data corruption. However, the scenario can only be implemented when databases containing authentic information are already available, and when this information is already fairly harmonised/standardised, since data exchange requires common standards, formats and semantics. This makes the scenario highly useful to exchange information stored in public databases (as witnessed by the BRITE and ECRIS examples), but almost impossible to apply in cases where databases are unavailable or where the information is not easily comparable.

Summarising the role of the scenarios further, it is clear that federated networks offer an ideal solution, provided that the conditions for its usability (usable electronic database – comparable data – agreements with regard to access and re-use) are met. Furthermore, federated networks offer synergies with the second scenario based on trusted storage systems, as explained above: federated networks offer the possibility of aggregating data regarding an entity directly into its own storage space, thus improving the usability and value of the storage space. Thus, while each of the three scenarios is of course intended to be used as a communication mechanism towards the contracting authority, interactions between different scenarios are possible to a certain degree. This is important, since it also implies that it is not necessary (or even particularly plausible) for one country to choose one scenario for all of its documentation types. It is perfectly possible and even recommended for countries to consider their own preferences and policies when choosing a particular approach for a particular type of electronic evidence. This is a choice that can be left to the Member States themselves.

At the European level, the key recommendation with regard to the scenarios is to monitor and stimulate the linking of these scenarios to existing or planned eGovernment initiatives that lend themselves to extension to public procurement, in order to benefit optimally from potential synergies. However, given the need for further steps to be taken at the national level (as noted in the short term recommendations) and given the current early status of crucial new initiatives in public procurement and beyond (including PEPPOL, BRITE, STORK and others) it does not appear to be beneficial at this stage to initiate separate new initiatives to force the uptake of specific scenarios. Structural support for their take-up in existing initiatives appears to be the more productive option.

1 Documents

1.1 Applicable Documents

[AD3]	Draft First Interim Report within the Preliminary Study on the electronic provision of certificates and attestations in public procurement – national profiles
[AD4]	Draft Second Interim Report – Analysis of European eProcurement Schemes – Comparison and Assessment of eProcurement management solutions interoperability
[AD5]	Draft Third Interim Report - Scenario building, assessment and benchmarking

1.2 Reference Documents

[RD1]	eGovernment in the Member States of the European Union – 5th Edition – May 2006 http://ec.europa.eu/idabc/servlets/Doc?id=24769
[RD2]	Directive 2004/17/EC of the European Parliament and of the Council of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors (30.04.2004) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004L0017:EN:NOT
[RD3]	Directive 2004/18/EC of the European Parliament and of the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts (30.04.2004) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004L0018:EN:NOT
[RD4]	Impact Assessment: Action Plan on electronic Public Procurement - Part 1: Baseline Analysis (December 2004) http://ec.europa.eu/internal_market/publicprocurement/docs/eprocurement/2004-12-impact-external-vol1_en.pdf
[RD5]	Impact Assessment Action Plan on electronic Public Procurement - Part 2: Baseline Scenario (December 2004) http://ec.europa.eu/internal_market/publicprocurement/docs/eprocurement/2004-12-impact-external-vol2_en.pdf
[RD6]	Draft Questionnaire - Application of Art. 45(1) of directive 2004/18/EC (CC/2006/07_rev1 EN)
[RD7]	Action plan for the implementation of the legal framework for electronic public Procurement

	http://ec.europa.eu/internal_market/publicprocurement/docs/eprocurement/actionplan/actionplan_en.pdf
[RD8]	Requirements for conducting public procurement using electronic means under the new public procurement Directives 2004/18/EC and 2004/17/EC http://europa.eu/rapid/pressReleasesAction.do?reference=IP/05/948&format=HTML&aged=0&language=EN&guiLanguage=en
[RD9]	Report on Functional Requirements for conducting e-procurement under the EU framework - external study for the Commission (IDABC programme) http://ec.europa.eu/internal_market/publicprocurement/docs/eprocurement/functional-requirements-vol1_en.pdf http://ec.europa.eu/internal_market/publicprocurement/docs/eprocurement/functional-requirements-vol2_en.pdf
[RD10]	Impact Assessment of the Commission on an Action Plan on electronic public procurement http://ec.europa.eu/internal_market/publicprocurement/docs/eprocurement/2004-12-impact-assessment_en.pdf
[RD11]	State of the Art report - external study for the Commission http://ec.europa.eu/internal_market/publicprocurement/docs/eprocurement/study_vol1_en.pdf http://ec.europa.eu/internal_market/publicprocurement/docs/eprocurement/study_vol2_en.pdf
[RD12]	IDABC Preliminary study on the mutual recognition of eSignatures for eGovernment applications http://ec.europa.eu/idabc/servlets/Doc?id=29484

2 Glossary

2.1 Definitions

In the course of this report, a number of key notions are frequently referred to. To avoid any ambiguity, the following definitions apply to these notions and should also be used by the correspondents.

- *Advanced electronic signature*: an electronic signature which meets the following requirements:

  (a) it is uniquely linked to the signatory;

  (b) it is capable of identifying the signatory;

  (c) it is created using means that the signatory can maintain under his sole control; and

  (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

- *Attestation*: any document originating from a party other than the candidate intending to demonstrate a quality or fact pertaining to the candidate. This includes inter alia documents traditionally referred to as certificates, attestations, or declarations. For the purposes of this report and to avoid any confusion, the word 'certificate' is only used in the sense of a certificate attesting to the correctness of certain attributes in a PKI system, with the sole exception being the report's title.

- *eGovernment application*: any interactive public service using electronic means which is offered entirely or partially by or on the authority of a public administration, for the mutual benefit of the end user (which may include citizens, legal persons and/or other administrations) and the public administration. Any form of electronic service (including stand-alone software, web applications, and proprietary interfaces offered locally (e.g. at a local office counter using an electronic device)) can be considered an eGovernment application, provided that a certain degree of interactivity is included. Interactivity requires that a transaction between the parties must be involved; one-way communication by a public administration (such as the publication of standardised forms on a website) does not suffice.

- *Electronic attestation:* any attestation or statement provided in a purely electronic form, whether signed or unsigned, and regardless of format or protocol, which was issued for the use in eProcurement proceedings or which is being used for this purpose.

- *eProcurement or electronic procurement*: public procurements initiated, negotiated and/or concluded using electronic means, i.e. using electronic equipment for the processing and storage of data, in particular through the Internet. For the purposes of this Study, the emphasis is on public procurements where candidates may submit (part of) their offer electronically through the internet. E-Procurement systems which only allow the on-line consultation by candidates of calls are of lesser interest.

- *eSignature or electronic signature*: data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication with regard to this data. Note that this also includes non-PKI solutions.

- *Federated network*: a network consisting of several interconnected nodes between which trust has been established to such a degree that information can be exchanged freely between the nodes, and that an user which has authenticated himself towards one node of the network is also permitted to access resources made accessible through another node.

- *Official registers*: data collections held and maintained by public authorities, in which the identity attributes of a clearly defined subset of entities is managed, and to which a particular legal of factual trust is attached (i.e. which are generally assumed to be correct). This includes National Registers, tax registers, company registers, etc.

- *Public procurement*: a procedure initiated by a government, public authority or public sector body with a view of acquiring goods, services or public works for the fulfilment of its tasks. For the purposes of this Study, the emphasis is on national procedures and practices in the field of public procurement, focusing specifically on public procurement on the national/federal level.

- *Qualified electronic signature*: advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device, as defined in the eSignatures Directive[1].

- *Statement*: any document originating from the candidate intending to demonstrate a quality or fact pertaining to the candidate. This includes inter alia documents traditionally referred to as statements of compliance, declarations under oath, and solemn declarations.

- *Tenderer*: an economic operator (contractor, supplier or service provider) who has submitted a tender, or who has sought an invitation to take part in a restricted or negotiated procedure or a competitive dialogue[2].

- *Validation*: the corroboration of whether an eSignature was valid at the time of signing.

[1] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML

[2] For reasons of simplicity, the Report will only use the notion of “tenderer”, rather than distinguishing between tenderers and candidates, as the Public Procurement Directives do.

2.2 Acronyms

A2A	Administration to Administration
A2B	Administration to Businesses
A2C	Administration to Citizens
CA	Certification Authority
CRL	Certificate Revocation Lists
CSP	Certificate Service Provider
eID	Electronic Identity
eIDM	Electronic Identity Management
IDM	Identity Management
OCSP	Online Certificate Status Protocol
OTP	One-Time Password
PKC	Public-Key Certification
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PKS	Public Key System (public-private key pairs based)
RA	Registration Authority
SHA	Secure Hashing Algorithm
SA	Supervision Authority
SKS	Secret Key System (unique secret key for encryption decryption)
SSCD	Secure Signature Creation Device
USB	Universal Serial Bus
TTP	Trusted Third Party
VA	Validation Authority
XML	eXtensible Markup Language

3 Introduction

3.1 Scope and objectives of the project

The Preliminary Study on the electronic provision of certificates and attestations in public procurement procedures (hereafter referred to as the 'eProcurement Study) aims to examine how different European countries (EU, candidate countries and EEA) currently manage the use of attestations in procurement procedures (hereafter referred to as 'electronic attestations'), particularly in an eProcurement context. The goal of the study is to identify if and how electronic attestations are currently issued, accepted and validated in public procurement procedures across these countries, and if and how their eProcurement systems could be modified or amended to support non-national electronic attestations, thus facilitating cross border economic activities in these countries and contributing to the creation of an internal market for electronic procurements.

The project should conclude with a set of scenarios to build interoperability, and with specific roadmaps to implement the most favoured interoperability scenarios.

3.2 Structure of the project

The eProcurement Study consists of 4 different phases. In a first phase, accurate and up-to-date country reports need to be built for each participating country (27 Member States, 2 Candidate Countries, and 3 EEA Countries). For each of these countries, the national report needs to describe the status of eProcurement in general, the use of attestations in eProcurement procedures in general, and if/how such attestations are available in electronic form for use in eProcurement processes.

In a second phase, this information will be analysed and assessed in order to identify any common patterns or general trends.

In the third stage, the analysed information will be used as a building block to create a series of high level scenarios for the cross border exchange and validation of such electronic attestations.

Finally, a fourth report will provide a more detailed proposal and implementation roadmap for the most viable scenarios identified in stage three.

3.3 Goal of this document

This document ('Final report – Roadmaps for implementation') concerns the fourth and final phase outlined above: it aims to propose roadmaps containing the key building blocks for the three most favoured interoperability scenarios as identified and assessed in the Third Interim Report, namely:

- the scenario based on a single electronic attestation package signed by a TTP, either from the private or public sector;
- the scenario based on a single trusted storage point of electronic attestations; and
- the scenario based on federated networks and national validation points.

These three scenarios were chosen from a group of six as being the most promising from an interoperability perspective, following a systematic assessment and benchmarking in the Third Interim Report, in which their main strengths and weaknesses were gauged (both from a legal/policy and technical/architectural perspective). The purpose of this Final report is to determine how these scenarios could be implemented in practice, and how they can coexist and supplement each other in order to arrive to a European electronic public procurement environment which is conducive to the support of a competitive market.

To accomplish this goal, this document follows a four tiered structure:

- Section 4 will provide a summary of the current status of electronic certificates in European public procurements, including by briefly describing:
    - The main types of solutions being used in electronic procurements in the Member States, EEA Countries and Candidate Countries at this time for the presentation of evidentiary documents, and their main strategies for future plans;
    - The main interoperability problems resulting from current electronic attestation practices, i.e. an overview of the issues in using electronic attestations in a cross border public procurements; and
    - An overview of current practice and expectations for the use of electronic attestations issued directly by administrations.

  It should be noted that these three issues will only be described summarily in this Report, with the main goal being to provide the reader with an overview of current challenges that are handled by the proposed scenarios. For a full description of these and other issues, we refer to the First, Second and Third Interim Reports produced in the course of this Study, which have described these issues in greater detail.

- Section 5 below will contain a high level description of a general vision for European electronic public procurement as the Study team would anticipate in the future. In a sense, this section determines the final goal to which each of the scenarios should be able to contribute, and defines the functionalities which the scenarios collectively should be able to offer in order to be able to interoperate. It will describe how the scenarios (which focus on the cross border use of

electronic attestations) fit into a general European electronic procurement strategy. Section 5 will be split up into two subsections:

- General principles of European electronic public procurement (including the eAttestations /eCertificates phase), which will describe the basic principles that will be of key strategic importance in the development of the cross border market for European public procurements. This section will identify the general interoperability requirements in order for the European electronic public procurement market to become fully accessible and operational.
- The envisaged future operation of cross-border European electronic procurements, including the positioning of the favoured scenarios as one of the main building blocks for such initiatives.

Collectively, section 5 will present **a vision of how a eAttestations / eCertificates system could operate** in the future, **and what role the scenarios should be able to play** in this regard.

- Section 6 will then define **specific roadmaps for each of the three key selected scenarios**, keeping into account the general vision and basic principles defined in section 5. For each of these scenarios, we will provide:
  - A summary overview of general requirements in order for the scenario to be integrated into the general European vision. These requirements have already been presented in an early form in the Third Interim Report, but they will now be re-examined to keep into account the vision and principles outlined in section 5.
  - A definition of the key problems to be overcome in order to meet these requirements and in order for the scenario to function in practice.
  - A description of the key building blocks that need to be put in place within the Member States or at the European level, both from a legal/policy and technical/infrastructural perspective, in order for the scenario to become operational. Broadly speaking, each of the key problems identified above should be overcome by one or more building blocks.
- Finally, section 7 will examine how these scenarios interrelate in practice, and will describe how they can be taken up by the Member States and at the European level to ensure a gradual evolution towards the idealised vision presented in section 5. Specific operational recommendations to forward this goal – both shorter term pragmatic recommendations and longer term strategies – will also be provided.

4 A summary overview of the current status of electronic public procurement in Europe and the role of evidentiary documents

4.1 Introduction

In the initial stages of this Study, the Study Team examined current practices in the Member States, EEA Countries and Candidate Countries in relation to electronic public procurement, examining in particular what types of evidentiary documents were commonly asked for in such proceedings, and if any electronic equivalents of such documents existed. Where no electronic attestations existed, the Study Team inquired what alternative mechanisms were used to replace these documents in electronic procurements; or if no alternatives existed yet, what plans the administrations had to resolve this problem. This was done through the collection of national profiles, in the form of a detailed report for each surveyed country that was drafted by a local expert in the subject. These profiles were bundled in the first deliverable of this Study, the First Interim Report.

In a second stage these national profiles were systematically analysed, in order to identify common trends, patterns and solution models. The resulting document, the Second Interim Report, provided an structured overview that outlined different categories of evidentiary documents and the specific documents that were commonly used in the examined countries, including the availability of electronic versions. In addition, it identified a number of solution models that were being used in the countries to facilitate the delivery of electronic attestations, and which might serve as a model for an international solution to this issue. Finally, the main interoperability challenges to be resolved in a cross border context were identified.

In this section, we will attempt to summarise the main findings of the First and Second Interim Report, to give the reader a basic overview of the current status of electronic attestations along with the issues that will need to be resolved. This will provide a useful background in understanding the proposals and recommendations formulated by this Report. It goes without saying that complete and detailed information can be found in the First and Second Interim Reports themselves.

4.2 The current status of evidentiary documents in electronic public procurements

4.2.1 Approach to electronic public procurement in general

As described in the First and Second Interim Reports, the 32 surveyed countries have taken very different approaches to eProcurement and to the role of electronic attestations in the eProcurement process. There is a great diversity in the stages of sophistication within the surveyed countries, depending on a number of factors, including the general eGovernment status (since eProcurement relies quite heavily on the general 'e-readiness' of public administrations) and on the prevalence of electronic signatures in countries where this is considered an important component of the eProcurement strategy.

A rough distinction can be made between the following categories:

- Countries where no eProcurement portal or system has been implemented yet[3] (14 out of 32 countries (44%). This fairly large number is not surprising, given that the inquiries into legal readiness showed that 7 countries had not yet created a legal framework that was compliant with the Public Procurement Directives. Also, it should be noted that for many countries the development and roll-out of an eProcurement platform or an eProcurement policy is closely related to their national approach to eSignatures, where eSignatures are considered to be one of the building blocks to the deployment of eProcurement applications. Thus, it is not surprising that a relatively large number of countries have not yet established a systematic approach to eProcurement.
- In contrast, 7 out of 32 countries (22%) have implemented a single eProcurement portal, to which certain public administrations can accede for their own procurement needs (e.g. Tenderned in the Netherlands, or EVO in Slovakia). This is thus a relatively common approach, which has the benefit of offering a uniform approach to all public procurements offered in a one-stop-shop model; and which minimises expenses for regional authorities who are not required to create their own eProcurement solutions.
- However, 8 out of 32 countries (25%) offer multiple portals. This is specifically common in countries where there is a larger degree of administrative authority or decentralisation of public procurement competences, including e.g. France, Italy and Spain. While there is a risk of cost duplication, his allows regions the possibility of creating frameworks which are most suitable for their local audiences.
- Finally, 3 out of 32 countries (9%) do not rely on specific portals, but have rather chosen to encourage private sector service providers to develop eProcurement applications (usually also

[3] It should be noted that, for the purposes of this overview, an 'eProcurement portal' is considered to be a website which permits eTendering (i.e. the actual electronic submission of an offer). Strict information dissemination portals where procurement opportunities are published are available in all 32 countries; but these are not considered in this overview unless they also allow the tenderer to submit his offer and any eCertificates along with it; pure announcement portals are irrelevant for the purposes of this study.

portals) which contracting authorities may choose to use. This is inter alia the case in the Czech Republic, Poland and Sweden.

Thus, there is a large diversity in the technical characteristics of the supported solutions and in the resulting security of these systems. At one end of the spectrum, we can then see eProcurement systems which require only an on-line registration which result in the tenderer receiving a username/password (e.g. in Ireland). Using these credentials, the tenderer can submit his offers, relying entirely on conventional file formats and unsigned scans of any additional documents that may be required as supporting evidence. At the other end of the spectrum, we see platforms which support only a small set of PKI signature solutions which can only be obtained after a prior registration (e.g. in the Netherlands). This signature is typically used to sign an offer and a self-declaration form attesting to the tenderer's compliance with the tender specifications, which will then have to be confirmed by submitting original paper certificates to the contracting authority if the bid should prove to be successful.

It is important to be aware of the interoperability implications of this variety. The first approach described above is highly flexible, and ensures easy access to the procurement market. However, it reaches this objective by lowering the bar for security and reliability. The second approach is much more formal and increases security, but de facto leads to an exclusion of a large number of foreign tenderers until a mechanism is found to accept and validate foreign electronic signature solutions and determine their legal value. Meanwhile, the eProcurement approaches are intrinsically incompatible, as tenderers in countries which only offer lower security signature solutions will not be able to meet the security requirements in countries which use higher security solutions.

4.2.2 Approach to electronic attestations in public procurement

The same variety is seen with regard to electronic attestations, as will be show in greater detail in the overview below.

As described in the Second Interim Report, the collected information distinguishes eight categories of document types that contracting authorities might commonly ask for in public procurements. Each category corresponds to a specific need for information that the contracting authority has and that will allow it to determine the most suitable candidate. Obviously, contracting authorities will only request documentation to be presented if this is required by law or if this is needed to determine the suitability of the bid. In practice, this means that certain document categories (e.g. compliance with environmental standards) are much less commonly encountered than others (e.g. compliance with fiscal obligations). Thus, it should be stressed that most public procurements will not require a document to be presented for each of the eight categories enumerated below; exact needs are determined by the scope of the procurement itself.

Below we will provide a short overview of these eight document categories, identifying the documents most commonly asked for in the surveyed countries in each category, the relative commonality of the requirement, and whether or not an electronic substitute was available at this time. At the end of this section, a broader general summary of current electronic attestations practices is provided.

4.2.2.1 Documents with regard to absence of criminal conviction

The overview in the Second Interim Report with regard to this document category showed that:

- The use of official certificates (typically extracts from penal registers or court certificates) was reported in 26 out of 32 countries (81%). In only 5 out of these 26 countries (19%) such certificates were available in electronic form, and 4 out of these 5 used PKI solutions. In the other countries only paper certificates were available;
- For this reason, the success of formal declarations from the tenderer is not surprising, as they can compensate for the absence of formal certificates. Such formal declarations from the tenderer were in use in 15 out of 32 countries (47%), and 7 out of 15 used PKI solutions for this. Legal certainty was generally considered to be sufficient when using self declarations in these countries, since false declarations would render the offer as a whole invalid and would subject the tenderer to criminal sanctions for fraud.
- An interesting problem which was also signalled in a number of countries (see e.g. Portugal) is that criminal liability for legal entities does not exist universally, which leads to the problem that formal certificates or court declarations of non-conviction can only relate to the natural persons who presently manage the legal entity. The adequacy of such certificates or declarations is difficult to determine for the receiving party. In addition, the list of convictions which lead to exclusion do not always map cleanly to the convictions which are potentially listed in the certificate or declaration of non-conviction (i.e. it would theoretically be possible to deliver a certificate showing no conviction, while the tenderer in reality has been convicted for an offense which is simply never included on the certificate). For both of these reasons, declarations are increasingly becoming the preferred solution.
- Apart from these two solutions (official certificates and formal declarations from the tenderer), a third and rare possibility is the use of declarations from a trusted third party. This system was much less common, and was reported in Denmark (where so-called Declarations of Service are delivered by the Commerce and Companies Agency to the contracting authority), and in Romania (where foreign tenderers are required to provide affidavits which have been authenticated by a notary public).
- Finally, two countries reported not using specific documentation in public procurements, namely Norway (where there is no specific document to attest to the requirement; this system is thus quite analogous to an implicit declaration of compliance from the tenderer) and Greece (where the required information is obtained ex officio by the contracting authority itself).

4.2.2.2 Documents with regard to non-bankruptcy and financial status

The overview in the Second Interim Report with regard to this document category showed that:

- The use of official certificates (typically court statements) was reported in 23 out of 32 countries (72%). In only 4 out of these 23 countries (17%) such certificates were available in electronic form, and 3 out of these 4 used PKI solutions. In the other countries only paper certificates were available;
- As with the requirement of non-conviction, formal declarations from the tenderer often replace such formal certificates. Formal declarations from the tenderer were in use in 14 out of 32 countries (43%), and 8 out of 14 used PKI solutions for this. Legal certainty was generally considered to be sufficient when using self declarations, since false declarations would render the offer as a whole invalid and would subject the tenderer to criminal sanctions for fraud.
- It is also noteworthy that a number of countries (including Cyprus and Luxembourg) reported using the same declarations of good behaviour as used in satisfying the prior criterion. As noted above however, criminal liability for legal entities does not exist universally, which leads to the problem that formal certificates or court declarations of non-conviction can only relate to the natural persons who presently manage the legal entity. The adequacy of such certificates or declarations is difficult to determine for the receiving party.
- Apart from these two solutions (official certificates and formal declarations from the tenderer), Denmark again relies on a form of TTP-certifications, through the so-called Declarations of Service from the Commerce and Companies Agency.
- Finally, three countries reported not using specific documentation in public procurements. In Norway and Ireland, no specific documentation was used to show compliance, which is thus quite analogous to an implicit declaration of compliance from the tenderer. In Poland, specific documentation was also not in use for this requirement, because tenderers need to submit current certificates or extracts from relevant trade registers to meet other requirements (see below), and entities enrolled into the National Judiciary Register are obliged to change their names when they enter into the procedure of winding up or bankruptcy (“X in liquidation” or “X in bankruptcy” respectively), whereas other bankrupt entrepreneurs are deleted from the Register of Business Activity. Thus, an additional certificate would be unnecessary.

4.2.2.3 Documents with regard to compliance with fiscal and social obligations

The overview in the Second Interim Report with regard to this document category showed that:

- The use of official certificates (typically court statements) was reported in a vast majority of countries: 28 out of 32 countries (88%). In only 3 out of these 32 countries (9%) such certificates were available in electronic form, all of which were PKI based. However, two out of these three countries (Bulgaria and Italy) indicated that in practice such certificates were virtually unused, leaving only Spain as a user of PKI based electronic attestations at this time;
- Again, formal declarations serve to some extent to solve this lack of electronic certificates, with 8 countries (25%) reporting their use, 4 of which were PKI based. However, it should be noted

that in some of these countries (including e.g. Belgium) this is only a delay, as the winning bid must still provide the formal (paper) certificate; whereas in others (such as France and the Netherlands) the formal declaration is sufficient.

- Again, Denmark again relies on a form of TTP-certifications, through the so-called Declarations of Service from the Commerce and Companies Agency.
- Only the UK reported not using specific documentation for this requirement in public procurements. Also, it is noteworthy that Belgium reported that certificated did not need to be delivered if the contracting authority could obtain the information itself electronically and free of charge, which in practice means that Belgian tenderers often do not need to provide a certificate of compliance with social security obligations.

4.2.2.4 Documents with regard to the suitability to pursue the professional activity

The overview in the Second Interim Report with regard to this document category showed that:

- As is to be expected, attestations and declarations from private entities such as professional organisations are commonly reported (14 out of 32 countries, 44%). However, these are not commonly available in electronic form, and none of the 14 countries reported that they were used in public procurements;
- References to public sector sources (trade registers and such) were less commonly reported: 8 out or 32 countries (25%) reported that public sector certificates or attestations were sometimes used in public procurements, with only 2 out of these 8 being available in electronic form. In addition, 3 countries (9%) referred to publicly accessible public sector databases as a common resource to demonstrating compliance with this requirement (i.e. no certificates were needed, since the database containing the required information was publicly accessible to anyone, including the contracting authority).
- Formal declarations to confirm compliance with this criterion were reported in 7 out of 32 countries (22%), most typically in countries which use such declarations to show compliance with other criteria as well (such as the Czech Republic and the Netherlands).
- Finally, 9 countries out of 32 (28%) stated that specific documentary evidence was rarely if ever required in their country's public procurements.

4.2.2.5 Documents with regard to economic and financial standing

The overview in the Second Interim Report with regard to this document category showed that:

- As was to be expected, there is a large diversity in documentation being used, including mainly:
    - Bank declarations: reported in 15 out of 32 countries (47%);
    - Balance sheets: reported in 29 out of 32 countries (91%);

  - Statements of turnover: reported in 27 out of 32 countries (84%);
  - Professional liability insurance reported in 11 out of 32 countries (34%).
- Also, all countries reported that these were only the most commonly asked for documents, but that any documentation (within reason) could be requested by the contracting authority. Thus, the overview above is certainly not exhaustive.
- The requirement of submitting signed, stamped or otherwise authenticated documents was very rarely reported (the possibility was reported in only 3 out of 32 countries (9%), with only Poland indicating that this requirement was not uncommon). More typically, copies (either on paper or electronically) were permissible.
- Specific approaches were reported in Austria, where tenderers could preregister there information with a central body, ANKÖ, which could thereafter communicate it to contracting authorities; and Belgium, where deposited annual accounts would occasionally (but not commonly) be accessible to the contracting authority electronically and free of charge, thus freeing Belgian tenderers from having to deposit the documentation themselves.
- From an interoperability perspective, this specific requirement presents few difficulties due to the general flexibility in most countries.

4.2.2.6 Documents with regard to technical and/or professional ability

The overview in the Second Interim Report with regard to this document category showed that:

- As was to be expected, there is a large diversity in documentation being used, but official certificates/attestations are quite rare. All 32 profiles follow the description that was presented in the model report, declaring that general documentation in the tender (specifically with regard to specifications, qualifications and product/service descriptions) is usually sufficient, and that more specific documentary evidence is not usually requested.
- Apart from such general information, a minority of countries have signalled that references of past work (6 out of 32 countries, 19%) or diplomas (5 out of 32 countries, 16%) are infrequently requested. It is likely that these requirements indeed occur in all countries, but are uncommon to the point of being generally underreported.
- Furthermore, three countries (Italy, France and the Netherlands) report the use of self-declaration forms to attest to the adequacy of the offered goods or services. This is unsurprising, since the use of such forms is more or less standard practice in these countries to demonstrate compliance with other requirements.
- From an interoperability perspective, this specific requirement seems to present few difficulties, specifically given the relative infrequency with which evidence other than the declarations of the tenderer itself is sought.

4.2.2.7 Documents with regard to quality assurance standards

The overview in the Second Interim Report with regard to this document category showed that:

- As was to be expected, the use of specific certificates is reported as possible but rather unusual in all countries, being limited to procurements with a highly technical nature or high value.
- While all countries comply with European regulations by permitting equivalent certification from foreign bodies, references to national accreditation bodies or national standards are made by the correspondents in 17 out of 32 countries (53%); however, this should not pose substantial interoperability problems, since in these case it would be permissible to provide equivalent foreign certificates.
- All correspondents indicate that original certificates are rarely required, and that copies are usually sufficient. It follows that, in an electronic context, unsigned scans would also be permissible. Indeed, 9 out of 32 countries (28%) explicitly indicate that unsigned scans or unsigned PDF files would also be permissible in most procurements.
- Thus, the use of original certificates is rare, and electronic certificates are equally uncommon. When electronic certificates are used, unsigned copies or unsigned originals are usually permitted, which substantially reduces cross border interoperability difficulties.

4.2.2.8 Documents with regard to environmental management standards

The overview in the Second Interim Report with regard to this document category showed that:

- As anticipated, the situation with environmental standards is highly analogous to that of quality assurance standards: the use of specific certificates is reported as possible but rather unusual in all countries, being limited to procurements with a highly technical nature or high value.
- While all countries comply with European regulations by permitting equivalent certification from foreign bodies, references to national accreditation bodies or national standards are made by the correspondents in 10 out of 32 countries (31%); and 13 out of 32 (41%) reference EMAS and/or ISO 14001 certification. However, references to national frameworks should not pose substantial interoperability problems, since in these case it would be permissible to provide equivalent foreign certificates.
- All correspondents indicate that original certificates are rarely required, and that copies are usually sufficient. It follows that, in an electronic context, unsigned scans would also be permissible. Indeed, 9 out of 32 countries (28%) explicitly indicate that unsigned scans or unsigned PDF files would also be permissible in most procurements.
- Thus, the use of original certificates is rare, and electronic certificates are equally uncommon. When electronic certificates are used, unsigned copies or unsigned originals are usually permitted, which substantially reduces cross border interoperability difficulties.

4.2.2.9 Conclusion with regard to electronic attestations in public procurement processes

The overview above shows that the surveyed countries take different approaches when examining how electronic attestations are provided to prospective tenderers, and that many countries use several approaches depending on the requirement to be covered. Broadly speaking, five approaches can be distinguished:

- Countries which have not yet identified a strategy in this regard (15 out of 32 countries; 47%). The vast majority of these countries simply do not yet have any eProcurement infrastructure in place or have not yet implemented an appropriate legal framework. However, there are also a few countries that have not yet made eCertificates a significant part of their eProcurement strategy, such as e.g. Ireland and Norway, where eProcurement is possible but eCertificates simply are not commonly required.
- Countries which rely on declarations of compliance from the tenderer (10 out of 32 countries; 31%). As noted above, such declarations can either serve to postpone the submission of certificates until a winning bid has been chosen, or can replace it entirely. Either way, the main benefit of this approach is that it eliminates (or postpones) the need to validate separate eCertificates, and allows the contracting authority to limit itself to the validation of the electronic signature method (if any) that has been used by the tenderer itself.
- Several countries have also implemented a limited trusted third party (TTP) or prequalification system (8 out of 32 countries; 25%), wherein a tenderer may register with a TTP prior to participating in a public procurement, providing certain commonly required evidentiary documents to the TTP. This is e.g. the case in Austria (ANKÖ), Slovakia (List of Entrepreneurs), the Czech Republic (List of Approved Economic Operators) and Denmark (Declaration of Service). Upon participation to a procurement, the TTP will then deliver a certificate of compliance to the tenderer, or directly to the contracting authority. This is a highly efficient process for tenderers who frequently participate in public procurements (and who can thus take advantage multiple times of their prequalification); but it is less efficient for occasional tenderers. Also, prequalification can be harder for foreign tenderers, depending on the implementation. It should also be noted that such prequalification systems are of course used in professional registers, where members of specific trade professions need to demonstrate their memberships.
- One of the most efficient models from the tenderers' perspective is of course to require the contracting authority to obtain the required information itself, if the source is another public sector controlled entity. Such a model shifts the burden and expense of demonstrating compliance to the public sector. This approach, consisting of a direct and protected transfer of information from one administration to the next can be found on a limited scale in 5 out of 32 countries (16%), including Belgium, Greece, Slovenia and the Netherlands. However, the current application of these systems is limited, both with regard to the information that administrations can obtain (which must be easily accessible to the contracting authority) and with regard to the beneficiaries (which are exclusively national tenderers). Thus, the disadvantages of this approach are that the tenderer must still provide the information that the administration cannot obtain itself, and that the system introduces a de facto discrimination between national tenderers (which do not need to provide certain information) and foreigners (which have to submit this information themselves).
- Finally, 4 out of 32 countries (12.5%) have reported that administrations can simply issue electronic certificates or attestations which have been signed with a PKI signature, including Italy and Portugal. This is a promising approach due to its flexibility and due to the possibility of treating eProcurement as a generic eSignature application (rather than implementing specific

solutions for this specific sector); but it does present the difficulty that the recipient must be able to not only validate the signature but also to determine the legal capacity of the issuer, i.e. that the signature was placed on behalf of the legal entity which is authorized to issue such certificates. However, in all countries which reported the existence of such PKI signed eCertificates, the correspondents indicated that the systems were largely in a pilot stage, and were not yet commonly used in public procurements. Thus, at the current stage this is primarily a promising future technology.

Since the latter category (electronic attestations issued directly by public administrations) does not (yet) occur in eProcurements in practice, it is important to stress that at this time there are thus only three types of electronic attestations to be considered:

- Self-declaration forms, signed by the tenderer using the signature solution permitted by the eProcurement system. However, it is debatable whether these should be considered electronic attestations, since they offer no guarantee other than the candidate's assurance of compliance; they could therefore be integrated into the offer itself (and this is indeed frequently the case), or even be considered to be an implied part of it (i.e. the submission of an offer is considered to be an implied declaration of compliance).
- Direct information exchange between administrations, i.e. the contracting authority will no longer require the tenderer to provide certain information, because it can access them directly from an authentic source. Again, it is debatable whether this should be considered an electronic attestation: while the data transfer perfectly emulates the functionality of a traditional certificate, the concept is more akin to an explicit mandate given to the administration to make the inquiries that are required to determine compliance with certain tender specifications.
- Declarations of compliance from TTPs in a prequalification system, i.e. the contracting authority is assured by a TTP (which may be a public or private sector entity) that the tenderer meets certain requirements on the basis that the tenderer has undergone a prior registration with the TTP, during which certain evidentiary documents have been provided. However, this again usually does not take the form of an electronic attestation provided to the tenderer by the TTP, but rather a mandate to the contracting authority to request this information from the TTP (a 'pull model'), or an instruction to the TTP to provide this information to the contracting authority (a 'push model').

Examining these approaches, one can only conclude that the main approach used by the surveyed countries to handle the problems related to attestations is to install electronic procedures that eliminate or reduce the need for attestations, either in a paper or electronic form. The creation of new electronic attestations on the other hand (i.e. electronic documents that one might consider as the most obvious example of electronic attestations, such as electronic tax certificates or electronic diplomas) is virtually non-existent. This certificate type that one might expect to commonly encounter, namely an electronic document issued by the same authority that issued the paper documents and signed with an electronic signature, is in fact very rare, and is presently predominantly used in pilot projects in a select number of countries with more mature PKI infrastructures, including Spain and Austria. While these certificates will certainly become much more common in the future as the uptake of PKI in the public and private sector in general increases, the role that they play in eProcurement processes is presently very limited.

4.2.3 Cross border use of electronic attestations

From an interoperability perspective, all of the three models described above – self declaration forms, direct information exchange and prequalification systems – are difficult to extend to foreign users:

- Declaration forms require the tenderer to have access to a supported signature type, and require him to fully comprehend the declaration which he is signing. While the latter element is usually not a significant barrier due to the reality that a tenderer will at any rate need to have at least a basic mastery of the tender's language in order to be able to participate, the former element is significant. In the absence of electronic signatures that can be validly used across borders, foreign tenderers will be required to obtain signatures that are supported by the eProcurement system that they wish to use. In practice, this is usually a disproportionate barrier that makes electronic procurement an entirely unattractive option. As a result, there are currently no systems relying on signed electronic declarations[4] that are commonly used by foreign tenderers.
- Direct information exchange presently only works on a national level. Information must be provided directly from local databases, and opening such databases to foreign contracting authorities is both legally and politically very sensitive, and presents substantial security and liability risk. By way of example, one might refer to a situation where a tenderer from Germany wishes to submit a social security attestation in order to participate in a tender from a Polish commune. In a direct information exchange system, this would require the Polish commune to obtain and use a mandate to access an official database within Germany. This implies that the Polish commune can identify itself to the database controller, that it can demonstrate its mandate, and that it can obtain precisely the information which it needs. These are highly complicated issues, which make such systems harder – though not impossible, as will be shown below – to use in international procurements. As a conclusions, it should be noted that this type of system is currently only beneficial to local tenderers, who no longer need to provide certain information which foreign tenderers will still have to collect and submit themselves. This implies a certain limited market distortion, as local candidates by definition will not have to invest the same time, effort and resources to participate in a bid within their own country.
- Finally, prequalification systems are also frequently less accessible to foreign tenderers, because they offer the greatest benefit to tenderers who can easily register with the TTP and who frequently submit offers where the statement from the TTP is used. Both of these factors favour local tenderers over foreign tenderers, for whom it may be harder to register with a TTP abroad, and who are less likely to frequently submit offers that benefit from the use of prequalification systems.

[4] As noted above, it is possible that a contracting authority would accept unsigned attestations as valid proof, as has been reported to be the case in Ireland. In this situation, there is obviously no interoperability problem. However, this approach seems highly unlikely to become significantly more common, due to the lack of any substantial authenticity guarantees which are considered to be essential in most other legal traditions.

Thus, reliance on these approaches shows substantial benefits, but at the current stage mostly to local tenderers, who see their administrative burden reduced significantly. For foreign tenderers however, it is much more difficult or in some cases even impossible to use these systems, let alone to derive any proportionate benefit from them. Indeed, in practice systems that rely on electronic attestations at this time are rarely accessible to foreign tenderers, with the sole exception being systems which rely on unilateral declarations in instances where the supported signature method is available to foreign bidders, which is a rather rare circumstance. This can have a distorting effect on public procurements, as eProcurement systems presently could result in a de facto competitive advantage for local tenderers, while excluding foreign bids.

The scenarios that will be discussed further below aim to resolve these problems by presenting approaches that would allow companies to submit their offers electronically to any public procurement, including foreign ones. However, it is important to keep in mind that the current infrastructure (including from an organisational, legal and technical perspective) does not allow any of these scenarios to be deployed immediately and without an investment of effort. All scenarios will require some degree of reorganisation or modernisation in most or even all countries. These anticipated efforts will be outlined below.

4.3 Interoperability challenges

It goes without saying that the current status of electronic procurement initiatives in general and electronic attestations in particular causes a number of difficulties for cross border procurements. While a full overview of legal, policy and technical challenges has been provided in the Second Interim Report, we will attempt to provide a brief summary of the main issues to be resolved below. These are of course precisely the questions that any future strategy should be able to respond to, and therefore demarcate the possible solution models that one might consider as valid options for the future.

4.3.1 Early status of initiatives

One of the main difficulties in finding appropriate solution mechanisms is the fact that eProcurement applications have not yet stabilised (or even materialised) in many countries. Specifically for electronic attestations, most countries have not yet implemented mechanisms that permit the use of national electronic attestations in their own applications (apart from unilateral declarations), let alone foreign certificates. Indeed, as referenced above, one of the main trends appears to be the reduction of the need for attestations in the traditional sense, by mimicking their functionality through alternative data exchange mechanisms which relieve tenderers of this administrative burden, rather than reshaping it. Electronic attestations as such (i.e. in the form of electronic documents issued directly by the competent administrations) are still fairly rare, and they remain largely unused in electronic procurements.

Given the relatively early and evolving status of eProcurement initiatives in the surveyed countries, and especially given the lack of a clear approach to the issuance, use and validation of electronic attestations, it is difficult to anticipate a suitable cross border interoperability strategy at the current stage.

Any proposed solution will have to take into account possible evolutions in this regard, and will need to be inherently flexible enough to support new emerging trends.

4.3.2 Multitude of approaches and document sources

As noted above, the surveyed countries are implementing different conceptual models behind current electronic attestation systems, including:

- Replacing electronic attestations by unilateral declarations of compliance from the tenderer (either provisionally or permanently);
- Using limited prequalification systems relying on trusted third parties (TTP) in the public or private sector;
- Exchanging information directly between the contracting authority and the source of the required information (if this source is controlled by another public sector entity); or
- The direct issuing of electronic certificates or attestations which have been signed with a PKI signature by the administrations themselves.

An interoperability model that will work for one of these approaches (e.g. a multi-CSP signature validation platform would work for declarations of compliance) will not necessarily work for another (e.g. such a platform would accomplish little for direct information exchange models). The fundamental issue to be resolved with regard to electronic attestations is that there is no common ground yet between the approaches being taken in the surveyed countries, and that a model needs to be suggested that evens the ground between tenderers using different systems.

In a traditional paper based procurement context, demands for evidentiary documents that cannot be directly met by foreign candidates have traditionally been resolved through policies that allow for a relative degree of flexibility, specifically by allowing tenderers to submit alternative but equivalent documentary evidence, as the contracting authority has the option to contact the tenderer for clarifications in case of ambiguity (a discretion applied within reason, of course). This tradition of flexibility will need to be kept in an electronic context, at least for the near foreseeable future. Unfortunately, this is not what electronic systems do best.

4.3.3 Disconnect between regulatory requirements and market reality

eProcurement applications are in principle required to be open to international competition on a non-discriminatory basis. However, as was noted above, there is presently no commonly accepted solution for the cross-border validation of common electronic signatures on the market. This puts eProcurement application owners in the awkward position of needing in principle to provide an answer to a problem that has not yet been resolved outside of the eGovernment sector. What is observed in practice is that application owners can only opt for a limited number of signature solutions, which are usually not accessible to foreigners.

While the observation above is true for eProcurement in general, the same applies to electronic attestations, where national policies are again usually designed in a way that mostly benefits the vast majority of tenderers, i.e. local ones, rather than all tenderers, i.e. including foreign ones. When considering possible solutions to this problem, it must be taken into account that they should principally aim to eliminate any de facto advantages that local tenderers currently enjoy over their foreign competitors.

4.3.4 eSignatures and electronic attestations

Finally, eSignature approaches currently being used in electronic procurements vary significantly in the surveyed countries, ranging from simple authentication (username/password) systems over advanced signatures to qualified signatures. A spontaneous harmonisation of the approaches does not seem to be likely in the short term. From an interoperability perspective, this means that any proposed solutions would need to keep this full range of diversity into account.

While there is a clear awareness of the need to support non-national tenderers and non-national signature solutions, there appears to be no consensus or clear vision on how to realise this goal. Some countries have opted to eliminate this issue by setting the security bar for electronic procurements relatively low and implementing an eProcurement system which is based solely on prior on-line registration, thus avoiding the difficulties inherent in PKI solutions (albeit by reducing security). Countries which have opted to implement PKI based systems (which is the significant majority of the countries, as noted above) have generally chosen to support a limited range of certificates from private sector CSPs in their national eProcurement portals or in supported eProcurement applications, which at least theoretically allows foreign tenderers to obtain a suitable signature mechanism from one of the supported CSPs. However, in practice mostly national CSPs are supported in such portals and applications, and as a result non-national tenderers thus far have only a limited possibility to obtain valid signature creation mechanisms.

4.4 Expected trends in the issuance and use of electronic attestations within the surveyed countries

In a traditional (paper-based) procurement, a substantial amount of the required evidentiary documentation to be provided by the tenderer typically takes the form of attestations delivered by public authorities. Common examples (as enumerated more extensively above) include tax attestations, social security attestations, extracts from criminal registers, attestations of proper conduct, and attestations of non-bankruptcy. In addition, these are the types of attestations which are requested very frequently in public procurements, while other types of documentation which are often not delivered by public administrations (including diplomas, certificates of conformity with quality/environmental standards, bank declarations) are much less commonly requested. Even when documents from the latter category are requested, copies are often considered acceptable, so that at least in theory electronic copies (e.g. unsigned PDF scans) would typically also be accepted.

This means that a great deal of progress could be made if these commonly issued public sector attestations were to be issued in an electronic form. This is after all a logical continuation of existing processes that does not require extensive organisational changes (since the same administrations remain competent for the issuing of attestations, albeit now in an electronic form), and that would be intuitively familiar to all participants in a bid, including the tenderer himself and the contracting authority. Furthermore, for many tenders the availability of public sector electronic certificates would be a sufficient solution, since additional attestations are only infrequently needed. Thus, the availability of such electronic certificates would be an incomplete but significant step in resolving the attestation problem in electronic procurements.

None the less, the overview above has shown that electronic attestations in the form of signed or unsigned electronic documents issued by the competent administrations have achieved virtually no uptake yet at the present stage. As noted, out of 32 surveyed countries, only 4 reported that administrations could issue electronic certificates or attestations which have been signed with a PKI signature at this time. More remarkably, when looking at their use in public procurements, only a single country – Spain – indicated any use of such certificates in practice; the other countries were still at a pilot stage.

Thus, electronic attestations in their simplest form have not yet seen significant use, for a number of reasons. Inertia in existing government processes – i.e. the reluctance to invest in the required infrastructure and training of the public officials involved – is certainly an important factor, especially when considering that the business case of such attestations so far is still quite limited. In general, in order for the investment to convert paper attestations into electronic ones to be worthwhile, it is essential that this transformation is embedded into a larger e-government context. This means that the electronic attestations should be easy to issue, which includes the possibility of requesting them electronically and at a distance when desired, and above all that they can be broadly used in any context where attestations are required. This implies that such electronic attestations should be usable before any administration that requires them, including other public services and courts. After all, if users need to verify first whether their electronic attestation will be of any use to them, this will certainly be a crippling barrier to their uptake. The creation of added value to the end user is a crucial factor that currently impedes the introduction and uptake of electronic attestations, and this is a barrier that needs to be handled in a broader context than merely that of electronic procurements.

From a practical perspective, most countries will want to rely exclusively on electronic attestations that have been signed by the issuing bodies, to ensure the authenticity and validity of the documents. This also means that the traditional issues related to the use of electronic signatures need to be resolved, which in the current context specifically means that it must be possible to check the validity of the signature at the time of its creation, along with the mandate of the signatory (to ensure that the attestation was indeed issued by an entity authorised to issue such attestations). These issues are

already challenging to resolve at the national level, and in a cross border context this becomes even more complicated due to the larger variety in documents and signatures.

However, it is also important to keep these problems in perspective. It should be remarked that the validity of specific evidentiary documents is determined by the regulatory framework of the country of origin, and not of the country of the contracting authority. This is also true in a paper context (e.g. a country that issues official tax attestations with an official seal cannot reject foreign official attestations if these contain only a signature from the public official that issued them), and there is no reason to change this principle in an electronic context. From a practical perspective, that means that at least a requirement to use specific electronic signatures can in principle not be used to reject evidentiary documents that have been validly issued in a foreign country (e.g. it would not be possible for a country that uses attestations with qualified signatures to reject attestations containing an advanced electronic signature that were validly issued in another country, or at least not on the grounds that the signature type being used is inadequate). This simplifies the problem somewhat, since the main challenge is then in determining if the attestation is authentic, rather than focusing on the characteristics of its implementation.

In addition, it should be noted that the country profiles bundled in the First Interim Report indicated that the validation of foreign paper attestations is generally a rather informal process, where the objective qualities and characteristics of a document (including elements like appearance, letterhead, seals, signatures and stamps) are evaluated on an ad hoc basis, and where subjective appreciations often act as a substitute for any real certainty regarding the legal validity and content of attestations. In short, the factual reliability of paper attestations in cross border procurements should not be overestimated. While it is clear that electronic processes are typically held to higher standards in this regard, it can be expected given this tradition of flexibility that a certain degree of progress could already be made by making such electronic attestations available to tenderers, and by systematically publishing information on the form and technical characteristics of such attestations, which would allow contracting authorities to at least conduct a prima facie verification of foreign attestations. This would bring the process more closely in line with procurement traditions in a paper context, and could thus already act as an enabler for the use of electronic attestations .

For this reason, it is certainly recommended to encourage countries that issue such certificates to make electronic versions available to the public. This refers specifically to the attestation types commonly issued by public administrations and which constitute the bulk of the evidentiary requirements in most procurements, and most notably:

- Extracts from criminal registers or the corresponding court certificates, as the key document to show non-conviction in criminal matters; this also includes attestations of good behaviour in countries which use such documents instead of extracts or court certificates;
- Extracts from commercial registers or court certificates attesting to non-bankruptcy; again this includes attestations of good behaviour in countries which use such documents instead of extracts or court certificates;
- Extracts from commercial registers to show enrolment in a professional register;
- Attestations showing compliance with tax regulations, including VAT legislation if applicable;
- Attestations showing compliance with social security obligations.

The introduction of official electronic substitutes for each of these document types would already provide tenderers with the means to provide official electronic attestations to foreign contracting authorities, even if it would likely remain difficult initially for those authorities to validate such documents in a satisfactory manner. As a way of supporting this process, existing initiatives in

countries that already publish such attestations should be published and disseminated as good practices, in order to encourage and support spontaneous harmonisation.

It goes without saying that this recommendation only applies to countries which already issue such attestations in paper form, and that it should not be misconstrued as a recommendation to start issuing these attestations in countries that have already implemented other means to show compliance with the relevant requirements.

A systematic introduction of electronic attestations could thus already provide a very useful first step. None the less, in order to provide a more satisfactory possibility to contracting authorities, other and more systematic approaches will be needed. While a general uptake of electronic attestations would indeed ensure that tenderers could easily provide their attestations to foreign administrations, this would not resolve all problems. Most notably, foreign administrations might still be unable to validate the signatures used on such attestations, or to determine the identity and legal capacity of the issuer. This is a problem that is difficult to solve, due to the enormous number of administrations that are involved in the issuing of these attestations (e.g. certain attestations might be issued at the commune level), which means that even in a strongly harmonised market there would be a very large variety in document types and signatures being used, making the validation process particularly complicated. In addition, for the same reason it is clear that the general uptake of electronic attestations will not be a quick process: while it is likely to occur at some point in the future, the reality of all administrative bodies (including at the commune level) being capable from a technical and know-how perspective to issue electronic attestations instead of paper ones will simply not materialise in the shorter term.

For this reason, other mechanisms should be considered that are capable of creating trust in attestations even when the actual issuer is unknown to the recipient, and that are capable of working around the restriction that attestations will likely retain their paper form in most countries for the years to come. Such mechanisms should also be able to handle other attestation types than those that were the focus of this paragraph, and specifically attestations that are not issued by public administrations, such as diplomas, certificates of conformity with specific standards and bank attestations. After all, it must also be possible to submit these documents in an electronic form, even when no electronic originals exist. To solve this problem, specific scenarios have been created, which will be identified and discussed below.

4.5 Summary overview and assessment of possible solutions scenarios

A key goal of the present Study, apart from the identification of current electronic attestation practices and interoperability challenges, was the creation of specific high level scenarios that could solve the aforementioned issues by presenting an way in which attestations (or a reasonable facsimile of attestations) could be used in cross border public procurements. Six scenarios were created by the Study team that could conceivable reach this goal. These scenarios were described in the Third Interim Report, along with a comparative assessment aiming to determine which of these scenarios would be most suitable and viable as a solution model on a European scale.

A brief summary of all six scenarios will be presented below, followed by a brief comparative analysis and assessment. For more detailed analysis, we refer to the Third Interim Report.

4.5.1 Unilateral declaration of compliance

This first scenario takes a simple **minimalist approach**: the tenderer uses a standardised electronic form (typically provided by the contracting authority as a part of the tender specifications) to declare his compliance with the applicable procurement requirements, and submits this to the contracting authority using any signature method that is permitted by the contracting authority. This declaration then either:

- Replaces the traditional (paper) attestations unless the contracting authority feels there is a need or reason to request these at a later data; or
- Replaces the traditional (paper) attestations only until the best offer has been selected. At this point, the (provisionally) best tenderer must submit the traditional (paper) attestations, or the procurement opportunity is offered to the tenderer who has submitted the next most suitable offer.

Thus, in this scenario, the **unilateral declaration of compliance replaces the traditionally required evidentiary documents**, typically provisionally or at least conditionally.

One of the main advantages of this approach is the minimum of operational requirements. In order to function adequately, the only real requirement is that the contracting authority must provide a standardised declaration (or at least clarify to the tenderers what they should declare) and a mechanism for submitting it along with the offer. As the practical examples in the analysis above have shown, such a system does not even have to rely on PKI signatures; simple submission through a web portal after authentication or even via e-mail is feasible, provided of course that the contracting authority would deem this to be adequate, which will often not be the case.

The model has the following clear advantages:

- **Operational simplicity** as commented above: infrastructural requirements can be cut down to nearly nothing, since the only requirement is the distribution of standardised electronic declaration forms, or even merely guidance on the information that a declaration should contain;
- **Cost/effort efficiency**: the tenderers do not need to obtain formal attestations from any source. Even if this is only a provisional or conditional exemption, this characteristic at least ensures that expenses and efforts are restricted to the bare minimum.
- **Flexibility**: contracting authorities can provide declarations containing any guarantee that they require, provided that they are compliant with the provisions of the Directives and other binding legal restrictions. Thus, potentially all requirements can be covered. Also, the model can be easily generalised to an international context at a later stage, since standardised declarations could be drafted on a European scale.
- The approach **can be tied in easily to existing eProcurement initiatives**. E.g. a country which has implemented a system relying on specific PKI signatures can simply require that the declaration is signed using the same system, or that it is integrated as part of the offer itself. Thus, the problem of interoperability is reduced to the same complexity as that of eProcurement systems in general: anyone who is capable of using the eProcurement system will also be able to provide the required documentary evidence (i.e. the declaration).
- **Validation is therefore also trivially easy** to the contracting authority, who merely needs to verify whether the requested document is indeed present, and if any applicable signature requirements have been met.

The model has the following clear disadvantages:

- The **declarations as such have limited legal value** since they originate from the tenderer, rather than from a trusted third party as one would expect from documentary evidence. In effect, a virtually equivalent legal effect could be obtained by merely specifying in the tender specifications that the submission of an offer constitutes an implicit declaration of compliance with all requirements (and indeed, this system too is seen in practice in some of the surveyed countries). While the use of a formal declaration from the tenderer is a little more explicit, its legal value remains limited.
- As documents originating from the tenderer rather than from a neutral third party, there is an inherent **risk of false declarations** being submitted, in the sense that the statements being made by the tenderer prove to be false at a later stage. Administrations wishing to use such systems must therefore be aware of the fact that this risk needs to be managed appropriately, in order to mitigate the chances of awarded contracts being legally disputed at a later stage. Strategies to manage this risk encountered in the surveyed countries include:
    - Only allowing declarations as an ‘interim solution’ for eTendering, i.e. the candidate whose bid appears to be best is requested to provide suitable (usually paper) evidence of his qualifications before the bid is definitively assigned (see also directly below);
    - Only allowing declarations from tenderers who have pre-qualified themselves by submitting specific documentation to a trusted third party at an earlier stage; and
    - Notifying tenderers before the submission of the offers that their bids and their general business activities can be made subject to thorough legal scrutiny to identify any

practices related to fiscal or social fraud, money laundering or similar criminal offences (i.e. creating a deterrent for unreliable candidates by using the tendering process as a mandate to audit candidates beyond the limits that would apply outside of tendering procedures; this practice has proven to be efficient in the Netherlands).

- As a result of this risk of falsified documents, these declarations are **only used in current systems as a provisional or conditional replacement of 'real' documentary evidence**, as explained above. Thus, the declaration does not eliminate interoperability problems; it merely postpones them and reduces them in scale, since only the winning candidate can be called upon to provide specific documents. Thus, there is no complete resolution in this model.
- For some countries, the use of eProcurement systems is **only possible when using specific signature types which may not be readily available to foreign candidates**, and which can also be expected to be required for declarations of compliance. However, it should be noted that this is an interoperability problem with regard to eProcurement in general, and not specifically with regard to electronic attestations.
- Finally, **one might also criticise the legal value of a standardised document** which will refer to legal-technical notions and specific legislation in a foreign country, and which is usually only available in a foreign language. A tenderer might dispute that he realistically consented to the statements in the declaration, because their complexity did not allow him to understand the full scope of his actions. On the other hand, this problem should not be overestimated, since the tender specifications as a whole are also often only available in this foreign language, and since cross border procurements can be expected to principally attract candidates with a sufficient degree of professionalism and diligence to consent only to statements that they actually understand. Finally, the contract being concluded after the finalisation of the tendering process will usually also be drafted in the contracting authority's language, so that an adequate familiarity with this language and the key legal concepts is at any rate a prerequisite for successful participation in the public procurement process.

4.5.2 Non-interventionist approach model – information dissemination and national responsibility

This second **minimalist scenario** is based on stressing the national competence of the Member States to govern their own eProcurement policies within the limits of the Public Procurement Directives, and strives to facilitate the creation of interoperability through voluntary action[5].

This model calls for the simple **publication by the Member States of the attestation types they use, including in an electronic context**, and including specific technical information with regard to formats and any electronic signatures being used. The purpose of this information would be to give aspiring tenderers and administrations a formal resource that they can consult to verify the validity of the information that they receive, and (if desired and possible) to gradually build automatic validation mechanisms into their eProcurement systems.

Thus, in this scenario, Member States would be required to create an informational contact point (e.g. a website) from where they distribute information on their electronic attestation practices, giving foreign

[5] An example would be the organization of voluntary interoperability projects between countries with similar legal traditions or similar public procurement approaches, which would allow a more gradual harmonisation of eProcurement practices.

contracting authorities the possibility of obtaining this information and using it to validate foreign evidence.

Again, this is a relatively low-effort system, where the only real operational requirement would be the creation of an official website, preferably in a centralised location (e.g. http://countryname.eprocurement.eu) and in a harmonised format, which is maintained locally (i.e. by a suitably qualified expert in the country itself). By way of example, one could consider the European Commission to take a guiding role in this respect, by offering the Member States a platform on which they could publish their own information. The Commission would then act as a coordinator for the collection and dissemination of the information, while the Member States would remain responsible for ensuring that the information itself would be accurate and complete.

The information collected in the course of this study (specifically the collected country reports, as summarised above) could provide a valuable first input in creating such a portal.

It should be noted that this scenario is not a real model for interoperability, since it only concerns the collection and dissemination of relevant information. However, the availability of such information is a prerequisite for the efficient execution of all other scenarios, as it would be extremely difficult to undertake extensive interoperability initiatives without a detailed and up to date overview of existing practices and choices within the Member States.

The model has the following clear advantages:

- This model too could be implemented in an **operationally simple and relatively inexpensive** way. Infrastructural requirements are limited, being initially limited to the creation of an information portal on the national level, and cheap to maintain.
- **The model can be applied more broadly than only to resolve the specific issue of electronic attestations**, since any relevant country specific public procurement information could be distributed through this central contact point.
- **The model fully respects national autonomy**, both with regard to the administration issuing the attestation and with regard to the administration receiving it. They can take the technical measures that they please and organise their electronic attestation policies in any way they prefer, in accordance with their local preferences and budgetary possibilities.
- **The model is fair**, in the sense that Member States who are already highly flexible in their eProcurement practices and do not suffer from significant interoperability problems are not required to make investments which ultimately offer them comparatively little benefits.
- The model can play a **crucial supporting role for other interoperability initiatives in the field of public procurement,** since the information bundled within such a contact point would at any rate be required to ensure that any proposed interoperability mechanisms are viable and meet the needs of the Member States in their processes.

The model has the following clear disadvantages:

- **This model does not achieve any real interoperability**; it merely makes information that could be used to facilitate later interoperability initiatives more easily available. It could serve as a useful tool for contracting authorities and tenderers to gauge what kind of information they

can be expected to receive or provide in cross border procurements, but actual interoperability is not achieved. This remains a fully national matter.

- **The model assumes that it is administratively feasible to create a single information point per country**. However, given the realities of decentralised competences and the multitude of administrations which can be involved in some of the countries, this may prove to be significantly harder than it seems. However, if the European Commission assumes a centralising role by managing an information portal which houses all the relevant contact points, this problem is significantly simplified.
- Similar to the situation for declarations described above, **linguistic issues can play a negative role**. National contact points will likely only disseminate information in a limited number of languages, which may not be sufficiently accessible to foreign tenderers and/or contracting authorities.
- In addition, **evidentiary requirements can vary strongly** from procurement to procurement, including through the involvement of private sector parties, either as an issuer of documents (e.g. accreditation bodies) or as a provider of eProcurement solutions (e.g. the creator of an application to prepare and submit electronic offers). This variety means that a clear and unambiguous answer to the need for evidentiary requirements often simply does not exist.
- Finally, the **published information must be permanently updated**, whenever evidentiary requirements are added/removed/reformed. This can be particularly cumbersome in cases where there is a large variety in the document types that are commonly used to show compliance with any given requirement. This disadvantage thus partially negates the relatively low expense of this model, since it requires permanent upkeep by a suitably qualified expert in each participating country.

4.5.3 Single electronic attestation package signed by a trusted administration or private sector trusted third party (TTP)

In this first **comprehensive approach** model, rather than providing the contracting authority with a multitude of attestations, the tenderer instead offers **a single bundle of attestations (i.e. a single electronic file containing all required attestations), signed by a specific trusted administration in each country**. While the contracting authority can still extract the individual attestations from the bundle, validation is only performed on the bundle as a whole; i.e. trust is derived from the fact that the bundle has been signed through a signature belonging to a trusted administration. If the signature on the bundle is valid, the attestations contained in the bundle are also considered to be valid; i.e. trust is 'inherited' from the entire bundle by the individual attestations.

Alternatively, the package can be thought of (or even explicitly implemented) as an alternative type of electronic attestation demonstrating compliance with local eProcurement regulations (i.e. a 'procurement compliance attestation'). However, if only a single attestation would be provided rather than a bundle of attestations, the contracting authority would not be able to immediately view the attestations on which the signature of the trusted authority is based. While the trust in the bundle should result from the signature of the trusted administration and this effect is thus largely psychological, at least initially, this seems an unnecessarily large step.

It should be noted that the role of a trusted administration could also be played by a private sector partner (a TTP), such as notaries public or Chambers of Commerce, **in a system that is similar to legalisation of documents for cross border use by notaries public**. This would possibly be a more feasible model, as some Member States might be reluctant to create new administrations or mandate existing ones to act as a TTP. In addition, the reliance on private sector TTPs would allow the

implementation work to draw on existing electronic trust initiatives between the TTPs. Entrusting this role to private sector TTPs that already have a trusted position in certain aspects of public functions, such as notaries public and Chambers of Commerce, might thus be a reasonable compromise between public sector control and private sector initiative. Essentially, this scenario can be seen as a form of 'trust marking', where a trusted party (either a trusted administration or a private sector TTP) attests to the reliability of a specific (electronic) document.

The model can be implemented as a 'pull model', or as a 'push model'. In a 'pull' implementation, a trusted administration/TTP will issue an attestation bundle to the tenderer, who will then deliver the bundle to the contracting authority. Inversely, in a 'push' implementation, the tenderer will no longer be charged with the communication function. Instead, the tenderer will order the trusted administration or TTP to provide the attestation bundle to a contracting authority (i.e. the tenderer will 'push' the attestations to their destination). This choice has only a few implications, which will be outlined below.

As with all comprehensive approaches, this proposal is much more far reaching than the minimalist ones. Its functionality depends on two fundamental requirements:

- Ideally (but not necessarily), a series of electronic attestations to include in the bundle already exists, since this would essentially mean that the bundle can be considered to contain original documents, which would make the model more straightforward from a legal perspective in cases where original attestations are required. However, this is not an absolute requirement, since even in traditional (paper) procurements, administrations frequently indicate that alternative evidentiary documents can be provided (such as formal declarations before a notary public) in the absence of the attestations which are normally required. There seems to be no reason why this same rule could not also be applied in an electronic context, especially since such alternative documents would essentially become trusted through the signature from the trusted administration. For the current model, this would mean that paper attestations that do not (yet) have an electronic equivalent could be scanned by the trusted administration/TTP and added to the bundle in an electronic form. In this way, this model could also be made to function in the absence of original electronic documentation.
- More importantly, the creation and operation of a single trusted administration in each country or the appointment of specific private sector TTPs which would sign these documents after having checked their validity. Additional roles can also be entrusted to this trusted administration/TTP by way of adding value (specifically the collection of some or all of the attestations in the bundle); but these roles are not strictly necessary for the model to function from a trust perspective. In order for the administration to be trusted however, contracting authorities must have the possibility of validating the signatures on the attestation bundles. This can be done either through validation portals (e.g. in an easily identified centralised location (for instance http://countryname.eprocurement.eu), where the contracting authority can upload the received attestation bundle to a web application which verifies the content of the bundle, the identity of the tenderer and the validity of the signature, and which then reports the result to the contracting authority), or as a part of the implementation of a broader trusted signature validation framework for eGovernment applications in general.

Additionally, if a 'push' implementation is chosen, an additional requirement is introduced: the trusted administration/TTP must be able to push the bundle to the contracting authority, i.e. it must know to whom the documentation is to be provided. Depending on the implementation, this can be made trivially easy, e.g. by providing the trusted administration/TTP with an e-mail address to which the signed bundle must be sent. However, that specific implementation would not allow the model to be tied in easily with most existing eProcurement platforms. Therefore, meeting this operational requirement could be more difficult in practice.

The model has the following clear advantages:

- **Conceptual simplicity behind the trust structure**: there is a single trusted administration or TTP that signs to ensure that the provided attestations are valid. The trust model is simple, and requires only the validation of one signature on the electronic attestation bundle (in addition to that of the tenderer). When this is made possible through a simple national validation portal (e.g. the contracting authority can upload the received bundle to a web application which verifies the content of the bundle, the identity of the tenderer and the validity of the signature, and which then reports the result to the contracting authority) the implementation can be done relatively cheaply and effectively.
- Through the use of a attestation bundle, **the contracting authority receiving the package still has the possibility of viewing the underlying attestations and ask for clarifications** if it deems this necessary. This means that the system will be inherently more familiar and intuitively more trusted than a system in which this possibility would no longer exist.
- **Member States can choose to minimise the responsibilities** of the trusted administrations/TTPs by asking the tenderer to collect all required information himself and then to submit it to the trusted administration/TTP for trusted signing. However, to improve user friendliness to the tenderer, administrations/TTPs could also choose to offer further services, specifically by directly collecting some or all of the required attestations. This would be a significant advantage for the tenderer, and could also allow the Member States/TTPs to build a business model around this service by charging a suitable and proportionate fee.
- **This model fits in with existing trends in a number of countries**, specifically those which have already begun allowing administrations to issue PKI signed attestations, and those which have already assumed the responsibility of collecting some of the required formal attestations on behalf of the tenderer.
- If the role of trusted organisation is given to private sector TTPs, one of the key advantages is **that TTP models already exist in some states** through the involvement of notaries public.
- Furthermore, **this model does not require the pre-existence of electronic attestations**, since it is the TTP's signature from which trust originates and not just the document itself. There is little objection against a TTP e.g. making scans of paper attestations and signing these, when no electronic attestation is available. In short, the model is flexible.
- Finally, if a 'push' implementation is chosen, the fact that information is directly 'pushed' by the trusted administration/TTP rather than by the tenderer himself has an **immediate beneficial effect on trust**, since it shortens the trust chain, thereby removing a potential weakness. Also, the model then offers a small additional benefit to the tenderer, since he is no longer charged with communicating the resulting package himself to the contracting authority, which removes a possibility for error.

The model has the following clear disadvantages:

- **If trusted administrations are chosen instead of private sector TTPs, the model relies on the creation and operation of unique trusted administrations in each country**. These will have to be created specifically for this purpose in most countries, which results in an additional investment. However, it should be noted that any trustworthy interaction between the Member States using PKI infrastructure would inevitably involve the establishment of trust between certain parties and/or administrations, so that this should not be perceived as a real disadvantage of this model. Choosing private sector TTPs would avoid this problem, although

in this case the creation of trust might be more complicated, since contracting authorities would then essentially grant private sector signatures the same trust as public sector documents.

- **The economical viability and appeal of the model relies largely on the added value that the trusted administrations/TTPs can offer.** As noted above, these trusted authorities could also just limit their services to the trusted signing of documents provided by the tenderer; but then it would be unlikely that tenderers would want to use their services. After all, tenderers would then have the choice between collection all documentation and submitting a paper bid as they are used to; or collecting all documentation, visiting a trusted authority and submitting an electronic bid. If this is indeed the choice a tenderer must make, most tenderers will likely prefer to use paper bids instead, since it requires less effort and likely lower cost. In practice, if the services of the trusted administrations/TTPs are to find any uptake, they need to offer added value beyond their trusted signature. As noted above, collection of certain documents on behalf of the tenderer seems to be the obvious model.
- **These trusted administrations/TTPs derive their trust from the fact that they are expected to validate the attestations, which is a function that currently does not exist** in the surveyed countries. This is a non-trivial burden, since this means that for the large variety of documentary evidence in existence, the trusted administration/TTP would have to conduct a prima facie validation. However, it should be noted that a prima facie validation (rather than an extensive and in depth validation) appears to be enough, since essentially this is the same process that these documents would otherwise undergo in foreign administrations: prima facie validation, with a request for additional information in case of ambiguities. It does not seem necessary or proportionate to impose a higher burden in this regard on national trusted administrations/TTPs than on contracting authorities.
- **The model benefits significantly from the existence of electronic attestations which can be bundled together, since these can be considered originals. However, the existence of electronic attestations is still rather rare.** The model can compensate for this through the fact that the trusted administration can vouch for the correctness of the information being offered, i.e. when an electronic attestation is unavailable and an alternative document is provided (in compliance with the tender specifications), the trusted administration/TTP can assure that the replacement is necessary because no electronic attestation is available. However, this does require that the trusted authority has a clear overview of available attestations within its borders. This is not as trivial as it seems, given the possibility of private sector involvement (such as ISO certifications, extracts from professional organisation registers, Chambers of Commerce etc.).
- When a bid is submitted by multiple tenderers, the model becomes slightly more complicated if the tenderers originate from different countries. In this case, multiple bundles may need to be provided, each of which is signed by the applicable trusted administration/TTP.
- Finally, if a 'push' implementation is chosen, **the trusted administration/TTP needs to be able to communicate with the contracting authority**, either directly or via its counterpart in the contracting authority's country (i.e. the local trusted administration/TTP).

4.5.4 Decentralised issuance of electronic attestations by the originating administrations

The second **comprehensive approach** model is essentially an **electronic emulation of the status quo: the same administrations keep issuing the same attestations that fall under their competence, but will in the future do so in an electronic form and carrying an electronic signature**, without any kind of centralisation (unless this already existed in the present system). As was already described in section 4.4 above, the main difficulty, apart from validation of the electronic signatures applied to the electronic attestations, would be the determination and validation of the quality and competence of the signatory.

The proposal's functionality depends on a number of operational requirements, most notably:

- Administrations must be willing and able to use PKI signature systems when issuing attestations. This requires that the necessary infrastructure is in place to create electronic attestations, and that public officials have the required infrastructure and knowledge to add their electronic signatures to these.
- The necessary infrastructure must be put in place to validate the issued electronic attestations, including their scope and legal capacity of the issuer. This can be done through national validation portals where the contracting authority can upload the specific electronic attestations that it has received to have their validity checked, or via a broader eSignature validation model (although the latter will not allow the contracting authority to conclusively determine whether the issuer was indeed legally competent to issue the relevant electronic attestation, unless this functionality is specifically built in).

The model has the following clear advantages:

- The model is **highly intuitive for all parties**, since it is nothing more than an electronic rendition of traditional attestation processes: the tenderer must still obtain them from whichever administration has been appointed as competent, and provide them to the contracting authority, which is charged with validation.
- **No competence changes are required** at the Member State level, since the same administrations remain in charge and no central authority or contact point is technically required. Of course, the technical infrastructure and required know-how will have to be imparted on the public officials in charge of issuing electronic attestations, but this would have to be done as a part of any e-government modernisation process.
- **The legal infrastructure is largely in place**, since the Member States already had to implement the eSignatures Directive. Member States would only have to review whether their local regulations have requirements with regard to attestations that explicitly impose the use of paper, stamps or other formal requirements which may need to be abolished or reformed.
- **The system can be easily tied in with the existing trend in many Member States of providing electronic means of communication to citizens and enterprises**, e.g. by allowing them to electronically request certain documents or services. The same system could be applied to request electronic attestations, which would cut down on administrative burdens.

The model has the following clear disadvantages:

- **The model relies on administrations being willing and able to issue PKI signed electronic attestations.** While it can certainly be expected that this will increasingly become a reality in the future, presently such official PKI signed electronic attestations are still very rare, at least in an eProcurement context. Thus, the model would likely see less short term uptake, until e-government modernisation projects have advanced to a further stage.
- **The cross border validation of the signatures on the electronic attestations is complex**, and there is no infrastructure yet that can do so at this time. It is conceivable that authentication portals could be created where foreign contracting authorities could upload received electronic attestations in order to have them validated, but this type of solution is also not yet commonly used in any of the surveyed countries. Alternatively, a broader cross border eSignature validation mechanism could be implemented that would be applicable outside an eProcurement context, but such initiatives are equally still at an early stage.
- There is also **the problem of validating the competence of the issuing authority**. While the scope of this problem should not be overestimated (since it has not been conclusively resolved in an offline context either), any implementation of this model should still strive to provide a mechanism to determine the capacity of the person or entity who signed the electronic attestation. This could be integrated into a national validation portal, where the outcome of the validation would not only be a conclusion with regard to the validity of the signature and the status of the signature certificate used to sign the electronic attestation, but also a summary description of the entity on whose authority the signature was added.
- The model also **retains the downsides of traditional paper attestations**: like their paper counterparts, the scope of electronic attestations would still be difficult to assess by a foreign contracting authority, because of the inherent language barrier. The user of validation portals however could diminish this problem, since such portals could also provide a summary description of the contents and scope of the electronic attestation.
- Finally, it should be noted that this model offers **limited added value in comparison to other models** presented in report: the tenderer still has to get the attestation himself and deliver it himself, and the contracting authority must still assess its contents, validity and suitability in accordance with its own standards. While this is still a valid interoperability model, it mainly aims to re-form traditional procedures in an electronic context, rather than unlocking additional potential in modernisation efforts.

4.5.5 Single trusted storage point of electronic attestations

In this third **comprehensive approach** model, electronic attestations are stored in single storage points, which are either (partially) controlled by a public administration, or which are purely controlled by the tenderer himself. The key element is that the tenderer has a single storage point in which electronic documents can be deposited and kept, and in which the tenderer can authorise third parties (like contracting authorities) to access the storage point to consult all or some of the stored documents.

In a model where the storage space is hosted by a public administration, it would be possible to no longer issue specific electronic attestations to the tenderer, either singularly or as a bundle. Instead, **the Member States offer protected storage spaces for registered entities, where information related to the entity can be stored both by authorised public administrations and by the entity itself**. These storage spaces could be designed so that they could contain confirmations by the

competent national administrations of the tenderer's compliance with procurement requirements, either in the form of signed documents, or simply as links to distributed databases which could confirm compliance with certain criteria. Alternatively, the model could also simply be implemented as a system where tenderers have the possibility of storing any electronic attestations that might be available in their country[6].

Rather than providing their electronic attestations to the contracting authorities, tenderers in this system would provide contracting authorities with an authorisation to access the protected storage space, where the contracting authorities can confirm directly what the status of the tenderer is. This would no longer require 'attestations' in the strictest sense (i.e. specific documents), but could also be implemented through a mechanism of assertions of compliance, which would replace attestations.

Alternatively, the storage space could also simply be hosted by the tenderer himself, giving him full control over any electronic information published within the space. However, this has clear trust implications: since public administrations can no longer exert any influence over the information stored within the space, it essentially offers very limited advantages. For this reason, this second implementation possibility will not be examined further, and the analysis in this section will only focus on the aforementioned possibility, where the storage space is at least partially controlled by public authorities.

The proposal's functionality depends on a number of operational requirements, most notably:

The creation and availability of protected storage spaces (e.g. http://companyname.tenderplatform.cc) where electronic attestations can be bundled together, or where as a minimum a contracting authority can see if the tenderer meets the requirements of the tender specifications. This platform would need to make a distinction between information which is provided by the public administrations (social security attestations, declarations of non-conviction, etc.) and information which is added by the tenderer (self declarations, and information from third parties such as trade register extracts or ISO certifications). This distinction is necessary to allow the contracting authority to determine if the information in the storage page is official, i.e. provided by a public authority (and therefore trusted).

- The protected storage spaces must be made accessible only with the tenderer's permission. This can be done in relatively simple ways, e.g. by allowing the tenderer to automatically generate complex pseudorandom links (e.g. http://ED86b!àçeNCFéz.companyname.tenderplatform.cc) which would lead the contracting authority to the information stored on his platform for a limited duration, or by a simple username/password system. More advanced and secure systems can also be envisaged, but would require a more complicated trust structure and additional expenses.
- Finally, the protected storage space must allow the contracting authority to verify compliance with the tender specifications. This can either be done by providing electronic attestations, or by merely setting 'compliance flags' when no electronic attestation is available (e.g. a country that does not issue electronic attestations to show compliance with tax regulations could simply list the attribute 'Tax compliance', and mark this as 'OK' or 'not OK'). Thus, the use of electronic attestations as such is not strictly necessary in this model.

[6] In this form, the system is already being used in a number of countries, including France. See e.g. the public procurement platform of the Bourgogne region, https://www.e-bourgogne.fr/; the platform offered by the Ministry of Defence, http://www.achats.defense.gouv.fr/; and the general site mon.service-public.fr/

The model has the following clear advantages:

- **Conceptual simplicity behind the trust structure**: there is a single storage space where information is made available, and it is the tenderer himself who can grant access to this storage space. In this space, information is separated into information added by the tenderer (self declarations and documents from private sector parties) and information added by public administrations (e.g. official attestations). This allows a contracting authority to determine easily whether information originates from an official source and can therefore be considered reliable, or whether it is merely a confirmation from a private party.
- At least with regard to official documents, **validation can be kept simple**, since official information can be added directly by public administrations. I.e. if information from a public source is provided, then this is by definition reliable.
- **The model can be tied in with existing initiatives**, since a number of countries are already experimenting with MyPage-type models. This would be an intuitive extension of this evolution.
- **The model can be made to evolve easily**. For instance, in the initial stage, a tenderer could be asked to provide all documents himself, and the only role of public administrations would be to provide a storage point. In this case, there is less trust in the documentation (since it all originates from the tenderer), but the cost would also be limited. In a second phase, public administrations could start adding certain information themselves, if and when they have decided to make the necessary investments to do so. In a third stage information could be added 'live', i.e. as the information is being requested. For instance, social security compliance is checked when the space is accessed. This would mean that the information is never out of date, and the contracting authority always has the most current information instead of attestations which may be months old and contain information which may have become entirely incorrect. In this way, the system would provide a real added value to contracting authorities. Finally, in a fourth stage the validation process could be fully automated, i.e. rather than clicking a link and visiting the company portal, an application could automatically access it and validate the provided information without further human intervention. However, this latter evolution requires significant effort on the semantic field, as well as with regard to data formats and communication protocols.
- **The system is very user centric**, in that it allows the tenderer to manage access to the information on the trusted space. If desired, the tenderer can even be allowed to limit the information that he provides based on the entity trying to access it (e.g. when contracting authority x tries to access the space he will see all documents; but authority y will only see documents a, b, and c, and not documents d and e which are confidential and/or irrelevant for authority y). Furthermore, this flexibility allows the model to be useful outside of an eProcurement context as well, since business may frequently be asked to provide certain information to third parties such as private sector business partners. Using this system, they could do so in a fairly user friendly way.

The model has the following clear disadvantages:

- **The model relies on the creation and operation of company spaces in each country**. These will have to be created specifically for this purpose in most countries, which results in an additional investment. Also, companies have to be willing to use them, which will likely require significant awareness raising campaigns.
- In order for the company spaces to be useful from an electronic attestation perspective, some of the information needs to be provided by public administrations, to allow contracting

authorities to trust in these (inversely, if all information is simply provided by the tenderer, the company space has little added value when compared to a simple e-mail sent by the tenderer to the contracting authority). This mean that **unlocking the full potential of this model will require gradual added investment and modernisation initiatives**.

- The implementation of a system that allows tenderers to grant **access to their information to foreign contracting authorities** could be considered politically complex, especially in cases where this information is subject to specific legal protection (e.g. declarations of non-conviction, which authorities might be reluctant to share with foreign bodies).
- In addition, **language barriers** can become a concern, especially in implementations where the 'look and feel' of storage spaces is determined at the national level, so that foreign contracting authorities have no simple way of identifying which documents they require, and what these documents mean. However, this problem could be alleviated through European level standardisation of the storage platforms, to ensure that information is presented in a coherent fashion.

4.5.6 Federated networks and national validation points

This fourth and last **comprehensive approach** model is the most complicated, but also offers the greatest potential benefits. The key objective of this model is to create a network of trusted information sources, between which a consistent direct data exchange approach is implemented. **Instead of requesting specific attestations to be provided by the tenderer, contracting authorities will be mandated by the tenderer to obtain information directly at the source, i.e. from the administration(s) which manages the requested information in the tenderer's country of establishment.**

Thus, this last solution tries to recreate and improve the functionality provided by the requirement of providing specific attestations, while eliminating the burden of requiring that the tenderer does so.

The model has a complex set of operational requirements, including most notably:

- The availability of the data sources that are used in the tenderer's country of origin to demonstrate compliance with specific formal requirements. This does not imply that the contracting authority can directly access the underlying databases on the information contained therein; but rather than the contracting authority has a contact point which it can address in any given country which it can query to obtain a confirmation of compliance. For example, a contracting authority would not need to access tax registers, or even to receive a tax attestation, if it can simply receive a reliable assertion that tax obligations are met. Thus, a first requirement is the availability of electronic data sources for (at a minimum) the principal requirements to show compliance with the tender specifications. It should be noted that it would be possible to implement this vertically rather than horizontally, i.e. in the form of context specific data exchange networks. One might imagine e.g. that a network could be formed between tax administrations (for the exchange of tax compliance information), next to a network between social security administrations (who perform the same function in their sector). In this regard, reference can be made to the ECRIS system (European Criminal Records Information System), described in section 4.7.3.6. below, which is already being used to facilitate the electronic exchange of judicial records between criminal authorities in certain Member States.

- Secondly, there must be a clear and unambiguous way for the contracting authority to be mandated by the tenderer to obtain this information from the data source. This requires (1) that the contracting authority has a way to uniquely and unambiguously identify the tenderer when requesting information; and (2) that the data source can validate whether a mandate actually has been given. Neither problem is easy to resolve. For instance, the use of VAT numbers is a good solution to problem (1) in most cases, but not all tenderers will have a VAT number, so that it is not sufficient. Problem (2) could be resolved by allowing tenderers to issue specific passwords or pseudorandom URLs to contracting authorities, similar to the solution that was already described above; but all Member States may not be willing to make specific information available on the sole basis of these mechanisms, for reasons of data protection and confidentiality.
- Finally, in order for information to be reliably exchanged between data sources and contracting authorities, a series of standards needs to be embraced with regard to semantics, file formats and communication protocols. Furthermore, the provided information needs to be signed by the data source in a manner that allows the contracting authority to validate it and its origin.

One additional aspect that should be stressed is the possibility of using this model only within specific sectors, i.e. by interconnecting only related administrations. Common examples might include interconnecting business registers in order to exchange valid and authentic business identification information; interconnecting tax administrations in order to exchange information about tax compliance; or interconnecting criminal registers to check for evidence of non-conviction. For such document types in particular, a federated model is very suitable, especially keeping into account the fact that such networks are typically usable in a much broader context than public procurement alone.

The model has the following clear advantages:

- Firstly, **it is the most user friendly and economical model for the tenderers themselves**, whose principal responsibility would be to provide the contracting authority with the necessary credentials to allow them to access the required information to demonstrate compliance with the tender specifications. It would thus reduce the tenderer's cost of demonstrating compliance significantly, encouraging the participation in public procurements.
- **The model has a strong focus on functionality over formality**: the goal of the system is to ensure that reliable information (regardless of its form) is made available to the contracting authority, rather than in merely recreating electronic versions of traditional formalities.
- **Since the information is obtained directly from the source, it is always up to date**. Thus, for the contracting authority one of the main benefits of this model is that there is no significant risk of discrepancies due to delays anymore.

The model has the following clear disadvantages:

- **It is the most complicated and expensive for the public administrations of all the models presented in this study**. It requires administrations to make their official information sources available to foreign contracting authorities, while the country surveys show that many countries are still struggling to make this information electronically available on a national scale. Thus, it would require great investments of time and effort in many countries, and will also require substantial regulatory changes.

- **The direct exchange of information is highly complicated**, and requires a clear consensus on semantics, standards and protocols between all participants.
- **The establishment of trust is a complicated matter**. The only pragmatic way of allowing this model to operate is by creating a central contact point for each country which a foreign contracting authority could contact to obtain the required information. This central contact point would then obtain the required information from the correct sources, sign it, and pass it back to the requesting authority.
- **Privacy issues and confidentiality become a greater concern,** since the model essentially entails a free data exchange between administrations with only a limited intervention of the tenderer. Furthermore, while the contracting authority is mandated by the tenderer to access the information, it difficult to implement a mechanism to ensure that the requesting (and mandated) party is indeed a public authority, rather than a private sector entity. While this openness could also be perceived as an opportunity (since this allows the system to be used in private sector relations as well), it may be politically difficult to introduce it, and may have difficulty in achieving trust among the potential tenderers.
- An additional problem is that **the model assumes that a central contact point could access the required information.** While this is at least conceivably true for databases controlled by public authorities, **this will likely not be the case for private sector issued documents** (such as extracts from professional registers or declarations from Chambers of Commerce). While these private sector documents could in principle also be integrated into a federated network, in practice this will be difficult due to the large variety of documents seen in practice, and due to the fact that additional documents or sources can be created at any time. Thus, the system is unlikely to ever become complete (i.e. able to provide all requested information).

4.5.7 Comparative assessment of the scenarios – selection of three key scenarios for further analysis

In order to determine which of the aforementioned scenarios offers the greatest potential for application on a European cross border scale, each of the scenarios was assessed against a number of criteria in the Third Interim Report. These criteria included:

- Organisational simplicity, i.e. the efforts involved in creating, organising and maintaining the necessary bodies to support the scenario;
- Technical simplicity, i.e. the efforts involved in ensuring the technical functioning of the scenario, including file formats, communication protocols and standards;
- Legal viability, i.e. the likelihood that the scenario could function on a European scale with limited legal difficulties;
- Financial viability, i.e. the expected costs resulting from the adoption of the scenario;
- Political viability, i.e. the likelihood that the proposed scenario would be considered acceptable as an interoperability solution by the Member States;
- Real interoperability impact, i.e. the scenario's ability to resolve the main interoperability issues surrounding the use of e-Attestations in electronic procurements;
- Extensibility and added value, i.e. the scenario's ability to grow in the future to offer additional benefits to the end user, thus making electronic procurements an attractive option.

For each of these criteria, the models received a score ranging from 1 to 5, with 1 being considered the most negative, and 5 the most positive, along with a justification of the score given. Furthermore, each scenario was assessed in the same way to determine its suitability for each of the eight[7] aforementioned document types. Finally, a global score was calculated.

Without going into the details and justifications for the assessments (which can be found in the Third Interim Report, the assessments can be summarised by the following table:

NR	Scenario	Score 1	Score 2	Total Score	Recommendations
1	Unilateral declaration of compliance	3.43	2.71	6.14	This scenario has a relative high score due to its simplicity. It is recommendable mostly as a temporary short term solution.
2	Non-interventionist approach model – information dissemination and national responsibility	3.00	3.50	6.50	This scenario has also a relatively good score, basically due to its added value as a complement to each of the other scenarios. It is recommended to be implemented in any case as a useful tool to disseminate national (e)Attestations practices and evolutions.
3	Single electronic attestation package signed by a trusted administration or private sector trusted third party (TTP)	3.00	4.00	7.00	This scenario has the second highest score due to its ability to integrate any specific evidentiary documents required to issue (e)Attestations, and also because can be integrated in the medium-long term within an EU-wide PKI system.
4	Decentralised issuance of electronic attestations by the originating administrations	2.71	3.00	5.71	This scenario obtained the lowest total score among all scenarios analysed in this document mainly due to its lack of flexibility and difficulty to integrate with private sector issued attestations within a reasonable timeframe.
5	Single trusted storage point of electronic attestations	3.86	3.43	7.29	This scenario obtained the highest score because it is built on the premise of a gradual migration to an integrated PKI solution over a longer period of time, while medium term quick wins are also possible.
6	Federated networks and national validation points	3.14	3.72	6.86	This scenario obtained a relatively high score due mainly to its long term potential, but lost points due to its organisational and technical complexity in the shorter term.

[7] However, it should be noted that categories 7 and 8 (requirements with regard to environmental standards and quality assurance) will be handled collectively in this overview, as the issues surrounding these two categories are essentially identical.

The table above shows that most of the scenarios show different but relatively close degrees of feasibility, and that that their applicability needs to consider the short, medium and long term keeping in mind the need for an integrated solution for eProcurement based on state of the art technologies.

The three highest rated scenarios – single attestation packages signed by TTP, trusted storage points and federated networks – will be analysed in greater detail below, and specific roadmaps will be provided for these scenarios. Furthermore, operational recommendations to ensure gradual but steady progress in this field will also be formulated.

5 General vision for eAttestations / eCertificates solutions in EU

5.1 General principles of eAttestations / eCertificates / eProcurement in EU

Before attempting to define an ideal scenario for electronic public procurement in Europe, it is important to establish the main goals to be achieved by such a scenario, and the general principles that would need to be observed to ensure that the scenario could be used in practice by the Member States.

As with the individual scenario assessments described in the Third Interim Report, the envisaged ideal solution for electronic public procurement in Europe should be able to satisfy a set of success criteria that determine its general usability. The main criteria to be considered for this purpose are identical to those retained for the assessment of individual scenarios, and specifically:

- Organisational simplicity, i.e. the efforts involved in creating, organising and maintaining the necessary bodies to support the ideal solution;
- Technical simplicity, i.e. the efforts involved in ensuring the technical functioning of the ideal solution, including file formats, communication protocols and standards;
- Legal viability, i.e. the likelihood that the ideal solution could function on a European scale with limited legal difficulties;
- Financial viability, i.e. the expected costs resulting from the adoption of the ideal solution;
- Political viability, i.e. the likelihood that the proposed ideal solution would be considered acceptable as an interoperability solution by the Member States;
- Real interoperability impact, i.e. the ideal solution's ability to resolve the interoperability issues surrounding electronic procurements;
- Extensibility and added value, i.e. the ideal solution's ability to evolve in the future to offer significant benefits to the end user, thus making electronic procurements an attractive option.

It goes without saying that the success of the ideal solution is not measured by the absence of any problems for all of these criteria, but rather by its ability to provide a suitable answer to any problem arising for each of these criteria.

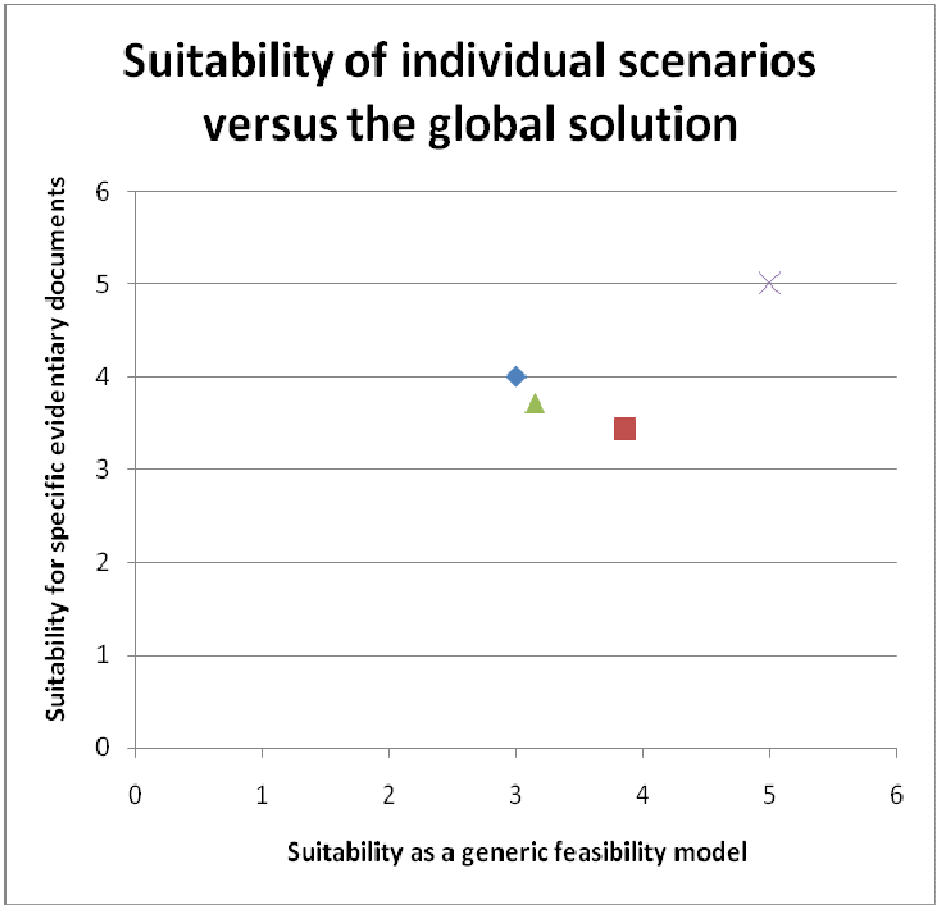
Furthermore, since the goal of this Study is to ensure that electronic attestations can be freely used on a European scale, the proposed ideal solution should also be capable of handling each of the document categories described in the earlier reports as also summarised above, and specifically:

- Requirements with regard to absence of conviction, i.e. attestations which are in the vast majority of cases (81%) issued by public authorities, typically by courts (extracts from criminal registers) or by administrative bodies (declarations of sound behaviour);
- Requirements with regard to non-bankruptcy and financial status; again, in the vast majority of cases (72%) attestations issued by public authorities are used, typically court certificates or business register extracts;

- Requirements with regard to compliance with fiscal and social obligations, where almost universally (88%) attestations issued by public authorities are used, typically court certificates or declarations from administrative bodies (tax and social security administrations);
- Requirements with regard to the suitability to pursue the professional activity, where there is a very large variety in documents within the countries, with declarations or attestations from private sector bodies being the most common (41%), with secondary roles for public sector registers (25%) and unilateral declarations of compliance from the tenderer (22%);
- Requirements with regard to economic and financial standing, most notably balance sheets (91%), statements of turnover (84%), bank declarations (47%) and liability insurance (34%). While other documents can also be asked, the common thread is that they typically originate from private sector bodies;
- Requirements with regard to technical and/or professional ability, most notably CVs, references, diplomas, available manpower and/or production capacity, or descriptions of products/facilities/equipment. Information is usually simply included in the offer; when documentation is required, it is usually issued by private sector bodies (mostly educational facilities or accreditation bodies);
- Requirements with regard to quality assurance and environmental standards, where documentation (if required) is usually issued by private sector bodies, most notably certification/auditing bodies.

Again, the ideal solution should be conceptually capable of handling all of these document types, regardless of whether they are issued by public sector bodies or private entities.

Graphically, the current situation and the goals of the scenarios can be depicted as follows:



Legenda

♦: Single electronic attestation package signed by a TTP

▲: The single trusted storage point of electronic attestations

■: Federated networks and national validation points

X: Envisaged ideal solution

In this diagram, the position of the three coloured symbols depict the individual scenarios' capability of meeting all requirements of an idealised electronic public procurement system as assessed in the Third Interim Report, i.e. based on:

- Their suitability as a generic feasibility model (scored on the horizontal axis with a rating from 1 to 5, with 1 being worst and 5 being optimal); and
- Their suitability to handle the specific evidentiary document categories identified above (scored on the vertical axis, again with a rating from 1 to 5, with 1 being worst and 5 being optimal).

The ideal solution is marked by an X, and shows a situation which meets all aforementioned success criteria and which can handle any document type, i.e. scoring an optimal 5 on both axes. The distance between the coloured symbols and the X then depicts the gap that needs to be bridged between the individual scenarios and the ideal solution.

It goes without saying that the gradual evolution towards the envisaged ideal solution will be more burdensome for some countries than for others. As was analysed in the Second Interim Report, the surveyed countries are at vastly different stages of design/implementation of their eProcurement solutions. While most countries have implemented some form of public procurement portal site, the level of interactivity of such sites still varies quite widely, with some sites acting purely as information dissemination portals focusing on the publication of public procurement opportunities, and others allowing the actual submission of bids. This is a factor which will need to be taken into account when considering the content and the timing of the Roadmaps below.

Broadly speaking, a distinction can be made between three categories of countries:

- Early stage countries, i.e. countries which have not yet done substantial implementation work in the creation of an electronic public procurement system and/or which lack any mechanism to allow the electronic submission of any attestations in the course of electronic public procurements. These are countries which require the greatest effort, as not even the most basic building blocks for electronic public procurement have been put into place. The upside however is that there is no legacy technology or regulations to take into account.
- Middle stage countries, i.e. countries which have made some progress in providing an electronic public procurement system allowing the basic submission of electronic bids by their own nationals, even if this option is not (yet) available for all procurements and even if no systematic solution has been found or chosen for the electronic submission of attestations. For these countries, which constitute the majority of the surveyed group, there is already a basic infrastructure and organisational framework in place, which means that implementation activities will typically need to focus on refining the existing systems.
- Advanced stage countries, i.e. countries which already use electronic public procurement systems in practice on a wider scale and which allow the electronic submission of some attestations through these systems. As was noted in the Second Interim Report, systems which are fully functional in the sense that they are accessible and usable to all E.U. foreigners and that any attestation can also be provided electronically are virtually non-existent at this point; however, the main characteristic in these countries is the existence of a coherent eProcurement vision which encompasses the submission of electronic documents. The main difficulty for these countries will likely be the need to update existing technology or regulations to accommodate E.U. wide functionality.

While obviously archetypical, this distinction is none the less useful as a reminder of the multitude of difficulties that the Roadmaps will need to be able to handle.

5.2 General principles for eAttestation / eCertificate implementations

These general principles described below are applicable for:

- The eAttestations / eCertificates solutions but also for more general eProcurement solutions
- The defined strategy but also for the implementation roadmaps

and must be considered having as reference the ideal solution for eAttestations / eCertificates described later in this document.

5.2.1 The Principle of Convergence

The Principle of Convergence requires that:

- all MSs and EIs converge in time to the ideal solution regardless of their current situation or the scenario identified by the benchmarking and picked up as the best (intermediary) solutions
- each MS and EI ensures the convergence of measures taken from political, legal, financial, organizational and technical viewpoints in order to implement the ideal solution in long term.

5.2.2 The Principle of Shared Synergies

The Principle of Shared Synergies means that the MSs and EIs should share positive but also negative experiences concerning the implementation of eAttestations / eCertificates at:

- the national level, i.e. by sharing synergies between national public administrations
- the European level, i.e. by sharing synergies between equivalent public administration(s) but cross-borders)
- the private sector level, i.e. by sharing positive and negative user experiences to improve general usability.

5.2.3 The Principle of Compatibility

The Principle of Compatibility refers to the need to prioritise:

- The compatibility between the eAttestation / eCertificate solutions implemented by different national / European public administrations at the national and cross border level
- The compatibility of a eAttestation / eCertificate solution, both backward (with previously implemented (e)Attestation / (e)Certification solutions) and forward (with future better eAttestation / eCertificate solutions);
- Generally, the compatibility of the eAttestation / eCertificate solution with the past, present and future eProcurement solution(s).

5.2.4 The Principle of Interoperability

The Principle of Interoperability means that the eAttestation / eCertificate solutions implemented by the national public administrations should be compatible with each other at the technical level, thus creating the ability to exchange eAttestations / eCertificates at national and cross-border levels.

The Interoperability is mainly technical and covers the following aspects:

- With regard to the evidentiary documents used to produce the (e)Attestations / (e)Certifications
    - Types / Categories (as summarised in section 4.1)
    - Structure (standardized and normalized at national / EU level)
    - Form (paper / electronic)
- With regard to the (e)Attestation /(e) Certification itself:
    - Structure (standardized and normalized at national / EU level) including the related attributes
- With regard to the mechanism(s) used to deliver the evidentiary docs and (e)Attestations / (e)Certifications
    - Physical delivery (postal mail)
    - Electronic delivery (e-mail or any other equivalent electronic mechanism)

5.2.5 The Principle of Standardization and Normalization

The Standardization and Normalization Principle apply mainly at the following levels:

- The evidentiary documents and (e)Attestation / (e)Certification level: it means that all national public administrations from all EU MSs plus the EIs :
    - will have to consistently use and accept the same types of evidentiary documents as mentioned above (section 4.1)
    - will use standardized and normalized documents for each type of evidentiary document and (e)Attestation / (e)Certification, which are perfectly equivalent in all official EU languages
- The delivery mechanism level: it means that the delivery mechanisms should be developed based on the same technical standards in order to ensure their compatibility and interoperability.

5.2.6 The Principle of Consistency and Compliance

The Principle of Consistency and Compliance refers to the requirement that all measures taken at the national public administration / national / EU level to implement the strategy need to be:

- Internally consistent from a political, legal, financial, organizational and technical viewpoint. Any anomaly could delay or even jeopardize the implementation and eventually success of the strategy;
- Compliant with the laws, rules, regulations, policies and standards agreed between concerned entities at national and EU levels.

5.2.7 The Principle of Inclusion and Non-discrimination

The Principle of Inclusion and non-discrimination refers to the requirement that the ideal solution should be accessible to all European users interested in participating in public procurements. This implies that:

- The ideal solution should not rely on requirements that cannot be met by any given tenderer;
- Member States should be assisted to ensure that their solutions evolve towards a European ideal solution in the shortest possible timeframe;
- In the ideal solution, requirements for using eProcurement solutions in cross border procurements should not be prohibitively complex or expensive, or otherwise result in a de facto discrimination against foreign tenderers.

5.2.8 The Principle of Legal Equivalence

The Principle of Legal Equivalence refers to the requirement that a systematic and as far as possible automated approach is taken when judging the equivalence of foreign evidentiary documents with locally requirements. While this principle already exists in the Public Procurement Directives, the ideal solution should ensure that it can be observed more easily and consistently, preferably to a system of automated verifications.

5.3 Definition of an Ideal Solution for eAttestations / eCertificates

5.3.1 Purpose and Scope

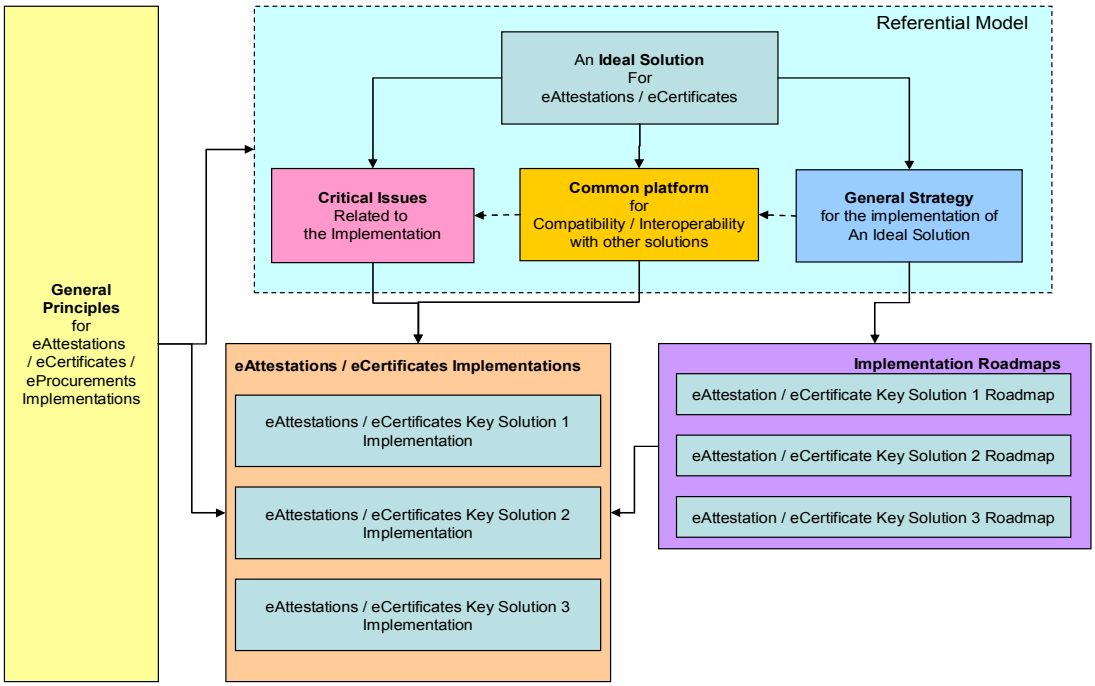
The purpose of an Ideal Solution for the implementation of eAttestations /eCertificates is to:

- Create a **theoretical solution** for eAttestations / eCertificates which is built and operated in ideal conditions and which eventually could never be implemented in the real world; this is necessary in order avoid the diversity and complexity of the eAttestations / eCertificates solutions in the real world;
- Allow an easier identification of a **General Strategy** for the set up of such Ideal Solution;
- Define specific **Implementation Roadmaps** for the selected solutions for eAttestations / eCertificates by tailoring the general strategy to the specific context of each selected solution;
- Identify a **Common Set of Elements (a Common Platform)** necessary to:
    - Facilitate the compatibility and interoperability between specific eAttestations / eCertificates solutions;
    - Reduce the complexity of the work performed by the Contracting Authority (the ITT Manager) in processing eAttestations / eCertificates received from national entities or from abroad (mainly the other Members States of EU);
- **Identify Critical Issues and propose ways to improve the key solutions** for eAttestations / eCertificates;

In this document the usage of the Ideal Solution is limited and it is not considered as short term alternative to the selected solutions for eAttestations / eCertificates.

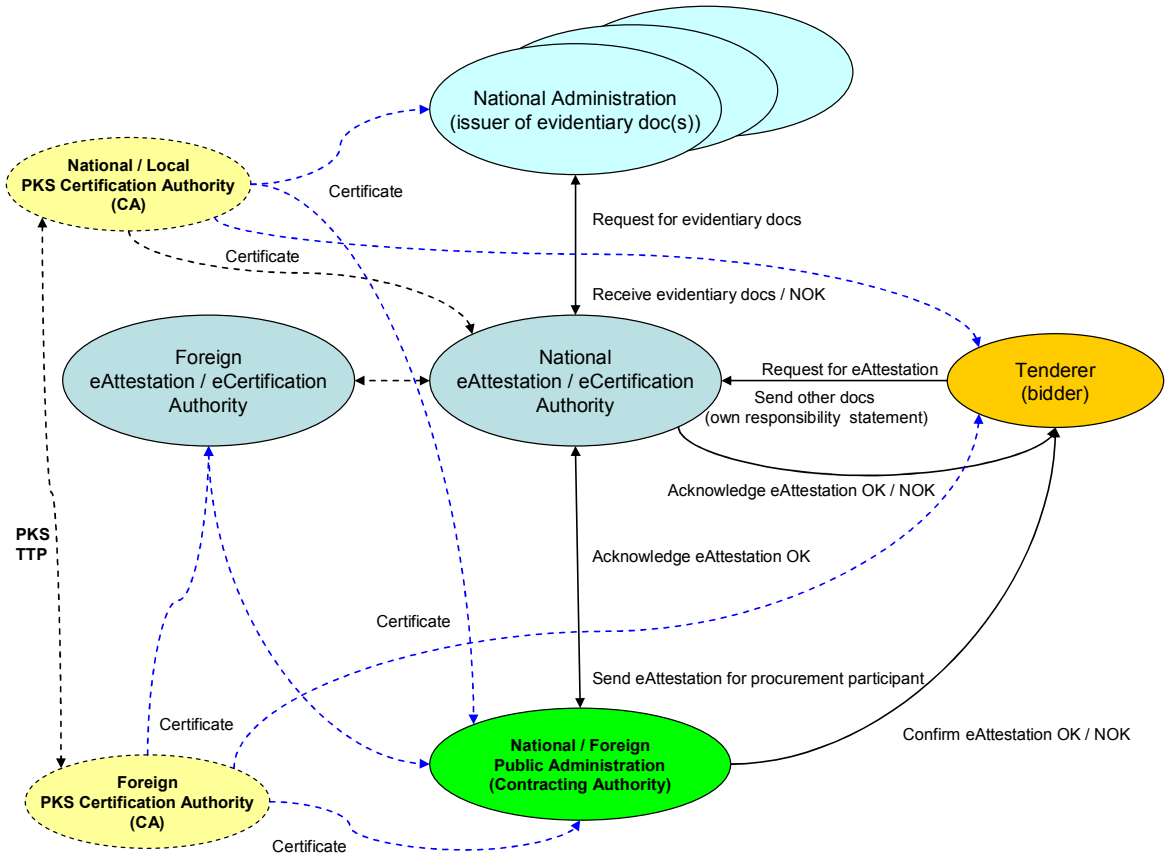
Nevertheless the Ideal Solution should be considered as a referential not only in the context of eAttestations / eCertifications or eProcurement applications but also in the larger context of eGovernement initiatives as it defines a feasible basis for eGovernement services and solutions.

The following diagram shows, at a methodological level, how an Ideal Solution is used in the process of identifying the roadmaps for the eAttestations / eCertificates key solutions and the effective implementations of these solutions and its positioning towards other relevant stakeholders.



5.3.2 General Approach

At a higher (business) level, the relations and interactions in the envisaged ideal solution can be visualised as follows:



The suggested Ideal Solution consists in

- A Public (national / foreign) Administration (Contracting Authority) which receives and processes the eAttestations / eCertificates as a first step of an eProcurement processes
- One or more National Administrations in charge of preparing and issuing the required evidentiary documents
- One or more national (publicly or privately owned) authority or authorities in charge of:
  - Collecting the documents necessary to issue an eAttestation / eCertificate at the request of an entity / company / physical person interested to participate to an ITT locally or abroad; ideally is that the collected documents are:
    - Based on the recommended evidentiary documents types
    - Standardized and normalized (national / EU wide) and

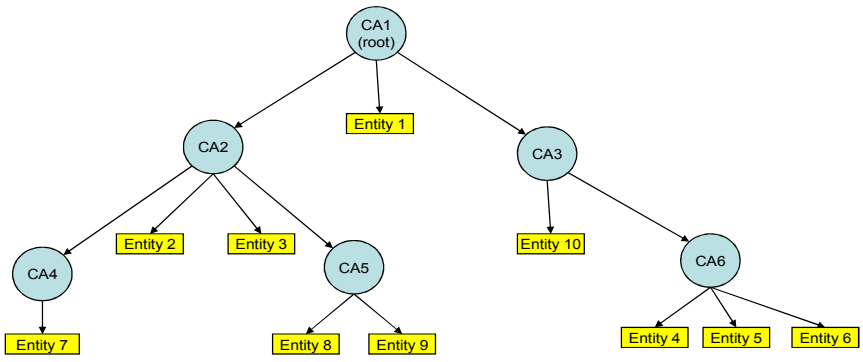
  - Available in an electronic format (XML), issued and signed electronically by the national administration responsible

- Issuing digitally signing the eAttestations / eCertificates in electronic format (XML)
- Sending the digitally signed eAttestation / eCertificate to the public (national / foreign) administration in charge of the ITT processing (the Contracting Authority).
- The bidder concerned by the eAttestation / eCertificates
- A National Certification Authority in charge of issuing and management of the certificates containing (among others) the asymmetric key pairs (public + private) for the National eAttestation / eCertificate Authority the National Contracting Authority and eventually for the National Administrations issuing the evidentiary documents (in electronic form)
- A Foreign Certification Authority in charge of issuing and management of the certificates containing (among others) the asymmetric key pairs (public + private) for the Foreign eAttestation / eCertificate Authority or eventually the Foreign Contracting Authority

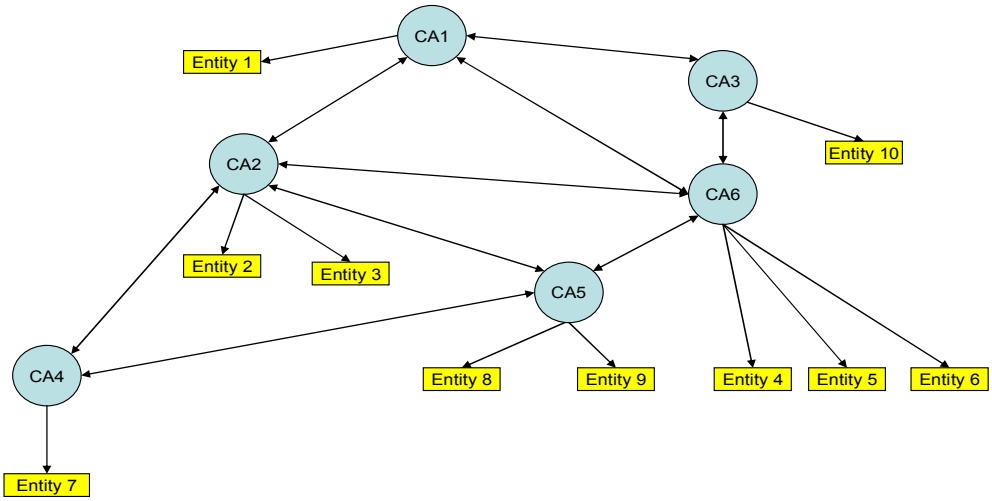
In general the PKI organization on which the National / Foreign Certification Authority is based is independent of the eAttestation / eCertification Authorities related organization as it can serve a wider list of clients and applications. Of the cornerstone importance in this situation is that Certification Authorities involved in the process mutually trust each other.

In order to use digital signatures, suitable PKIs need to be established at the national level in the country of the bidder (whose attestations need to be electronically signed) and of the ITT organizer or Contracting Authority (who needs to be able to validate the digital signatures). The architecture of each national PKI depends on the relationship between different Certification Authorities which may exist in any given country, but it can generally be one of the following:

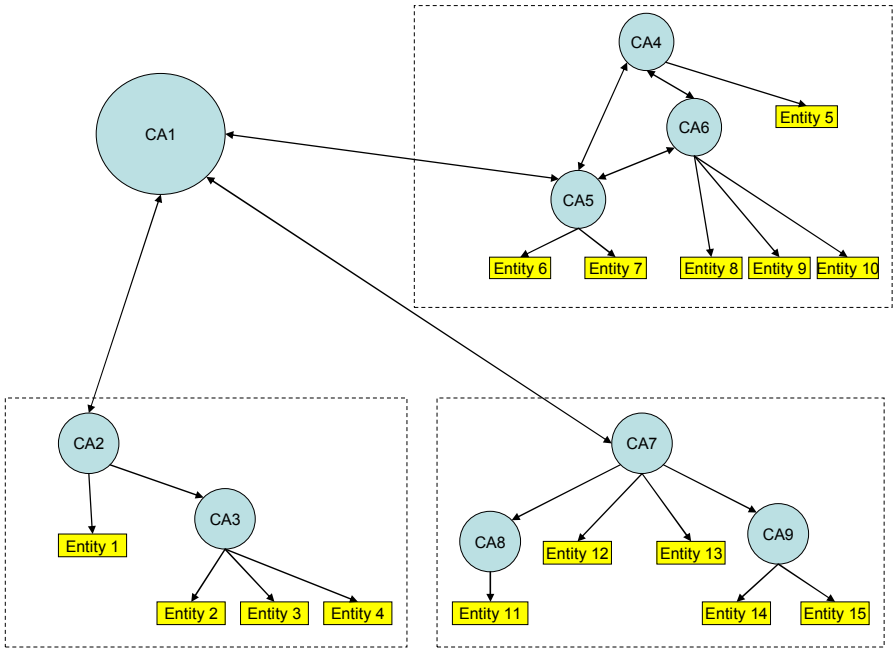
- **Hierarchical PKI Architecture** – the CAs are organized hierarchically, with a root CA and one or more main CA branches. Each CA issues certificates to CAs and Entities (users) located below it. A certificate is verified by checking the path of certificates from the root CA.



- **Mesh PKI Architecture** – the characteristic of this PKI architecture is that independent CAs cross-certify each other in a mesh of CAs.



- **Bridge PKI Architecture** – this PKI architecture includes a bridge CA concept certified to Enterprise PKIs (like the root CA in stand alone Hierarchical PKI Architectures or to relevant (principal)CAs in the Mesh PKI Architectures)



The organizational structure put in place at national level to implement and support the eAttestation / eCertificate services could be completely separated from the national PKI architecture (i.e. the administrations involved in issuing eAttestations/eCertificates do not need to be involved in any CA activity). What is required is that the CA issuing the public-private key pairs for the eAttestation / eCertificate Authority (national or local level) is trusted by the CA of the ITT owner.

5.3.3 Political Aspects

Consistent and convergent political measures are required at national and EU levels to:

- Adopt and implement the necessary laws;
- Define and adopt the necessary budgets (see financial aspects);
- Take to executive decisions regarding the organizational issues, specifically regarding the identification of suitable CAs and administrations to play the aforementioned roles.

5.3.4 Legal Aspects

National and European regulations will have to be reviewed and possibly amended to ensure that:

- EU directives have been translated accurately into national legislation;
- National legislations are compatible and support the aforementioned model, specifically taking into account:
    - the usage of eAttestations / eCertificates in eProcurements, keeping into account that such eAttestations / eCertificates will possibly not be originals in the sense that they are signed by the competent administration;
    - the need for mutual recognition of eAttestations / eCertificates, specifically including electronic signatures applied to these, and the different requirements that Member States may have put in place with regard to electronic signatures in public procurements;
    - Finally, privacy protection / data protection issues must also be considered, specifically taking into account the involvement of additional parties in the aforementioned ideal situation and the risk of data leaks.

5.3.5 Financial Aspects

The realisation of the Ideal Solution is a long term goal which could require significant financial resources. Therefore:

- Budgets should be made available especially for technical and organizational efforts including the set up, implementation, support and operation aspects at national and EU levels;
- The budgets should be distributed in time and related to the expected results;

- Co-financing of eAttestation / eCertificate / eProcurement projects by EU and MSs should be considered when necessary;
- The breakdown structure of the costs for an eventual implementation of the Ideal Solution will be related to the General Strategy defined later in this document and it will be analyzed for each of the key scenarios selected in [AD5].

5.3.6 Organizational Aspects

In order to ensure that the aforementioned ideal solution could be realised, Member States should:

- Adapt current national public / private organizations to cope with eAttestations / eCertificates / digital signatures / PKI;
- Set up new national public / private organization(s) to cope with eAttestations / eCertificates / digital signatures / PKI (probably different organizational infrastructures for managing eAttestations / eCertificates and PKI);
- PKI architectures at national level and cross-border relationship between CAs authorized issue public – private key pairs to the national eAttestation / eCertificate entities in charge of issuing eAttestation / eCertificate at national / cross-border level;
- Interface with relevant professional organizations in the private sector (e.g. accreditation bodies).

5.3.7 Technical Aspects

The following technical aspects will have to be sorted out in order to ensure compatible and interoperable solutions national and European wide:

- **Standardized and normalized evidentiary documents and eAttestation / eCertificate** - each type of the evidentiary documents based on which the eAttestations / eCertificates are issued by the eAttestations / eCertificates Authorities (National or European level) will have to:
    - Be simplified (e.g. clear multiple choices and less free text);
    - Contain the same fields and in the same order;
    - Have a similar layout, with the exception of fields identifying uniquely the issuing organization (e.g: logos, signatures);

  The standardization and normalization of the evidentiary documents will simplify (eventually):
    - Their (automatic) translation from the language of issuer;
    - Their translation in an electronic format, XML based (see below);
- **Electronic forms for evidentiary docs based on XML** – the existence of the standardized and normalized evidentiary documents in an electronic format such as XML will facilitate:
    - Their easy and automatic translation from one language to another;
    - Their electronic signature using the public key of the electronic document issuer (see below);

Implementing electronic evidentiary documents (XML based) in standard format for all Member States and European Institutions will facilitate in long term:

- The implementation of the paperless administrations;
- The exchange of electronic documents instead of paper docs;
- The efficiency of work performed;

- **Compatible PKS (for digital signatures and hash functions) and SKS (for data encryption / decryption)** – the technical implementations required and necessary to use digital signature and data encryption / decryption at national level to manage eAttestations / eCertificates need to be :
  - Common hash functions used;
  - Secure enough (key lengths);
  - Compatible with other Member States and European Institutions implementations in order to ensure interoperability and compatibility.;
- **PKI (CA, VA, …) and possible architectures at national and EU level** – the implemented PKIs and organizations / authorities running them at national and European levels need to be mutually certified (their CAs are mutually certified as TTP) in order to allow the eAttestation / eCertificate Authorities at local, national and european level to exchange digitally signed (and eventually encrypted) eAttestations / eCertificates;
- **eAttestations / eCertificate delivery / transport mechanisms compatibility and interoperability** – once issued by the eAttestation / eCertificate National / European Authority the eAttestations / eCertificates need to be delivered to the Requester (bidder) or to the Public Administration in charge of screening the bidders using a electronic transport mechanisms in a safe and timely manner such as an e-mail system (SMTP based); the e-mail containing the eAttestation / eCertificate should be digitally signed by an authorized person representing the eAttestation / eCertificate issuer Authority and it should be configured to send back delivery and read acknowledgments from the recipient side and ensure the authentication of the sender and non-repudiation of the recipient.

5.4 Strategy to implement the Ideal Solution for eAttestation / eCertificate

The following steps are part of the strategy to implement the eAttestation / eCertificate ideal solution(s) at national and European levels (including EIs level):

1. **Step 1:** European and National political commitment in favour of such an ideal solution for eAttestation / eCertificate as part of the solution for eProcurement national and European wide;
2. **Step 2:** A clear, complete, consistent and compatible legal context is adopted both at the European level (European Directive(s)) and the national level (national laws) for the legal usage as part of the eProcurement process of:
   - The standardized and normalized evidentiary documents (in electronic form);
   - The eAttestation / eCertificates (standard format and content but also mutual recognition of eAttesttations / eCertificates);
   - The digital signature (public – private key pairs, hash functions) – in order to ensure the legal compatibility of digital signature solutions across Europe;

- The encryption of data (precise legal conditions under which the encryption of data can be performed, encryption algorithms, secret key length, encrypted data transmission conditions, …);
- The privacy of data (data protection aspects);

3. **Step 3:** Budgets must be made available to finance the eAttestation / eCertificate Ideal solution aspects related to:
   - The set up and operation of the organizational aspects of the eAttestation / eCertificate Authorities at national and European levels;
   - The set up and operation of the IT aspects of the eAttestation / eCertificate Ideal Solution such as:
     - The eAttestation / eCertificate database;
     - The evidentiary documents database;
     - The (eAttestation / eCertificate) data transmission mechanisms (e-mail system) to / from eAttestation / eCertificate requester and PKI CAs;
     - The security management software (encryption / decryption, digital signature, hash functions) in order to implement specific security services: data integrity, data confidentiality, availability, authentication, non-repudiation.
4. **Step 4:** Implement the organizational measures / changes required to perform the eAttestation / eCertificate activities and also the PKI management organisation at national level and European level;
5. **Step 5:** Implement and test the technical solution for the PKI management at national (and European) level;
6. **Step 6:** Implement and test the technical solution for the eAttestation /eCertificate Ideal Solution at national and cross-border level;
7. **Step 7**: Accept and declare the eAttestation / eCertificate solution operational;
8. **Step 8:** Audit the eAttestation / eCertificate system on a regular basis and recommend improvements as part of best practices for IT Governance and also to ensure forward compatibility with the eProcurement process.

The General Strategy for the Ideal Solution described above is considering an ideal context in which there are no blocking or delaying factors (e.g. the budgets required are not approved, there is no national and EU –wide agreement on the standardization / normalization of the evidentiary documents and eAttestations / eCertificates structure and content). For the key scenarios, to be implemented in a real environment, the related roadmaps will take into account the real world context, identify the critical risks and identify measures to eliminate / reduce these risks.

5.5 Cost Breakdown Structure for an Ideal Solution

The purpose of this section is to identify the main cost elements for the implementation of an Ideal Solution taking into account the General Strategy defined above. This Cost Breakdown Structure will be used together with the roadmaps defined for each key scenario to provide short qualitative analysis for each key scenario.

The following main costs have been identified:

- Organizational Costs
  - Set up new organization or adapt existing one (one shot)
  - Operation costs (recurrent)
- Technical Costs
  - For eAttestation / eCerticate solution
    - Development and set up costs (one shot) – including the costs related to tests
    - Operation and maintenance costs (recurrent)
  - For PKI solution
    - Development and set up costs (one shot)
    - Operation and maintenance costs (recurrent)
- Audit and Continuous Improvement Costs: cover mainly the costs of the internal and external audits organized by each entity (e.g. eAttestation / eCertificate Authority, Contracting Authority, Certification Authority, Public Administrations) and costs related the implementation of the recommendations resulted from the internal / external audits

This Costs Breakdown Structure identified for the Ideal Solution will be adapted and qualitatively analyzed for the key scenarios.

6 Roadmaps for key scenarios

6.1 General principles of the roadmaps

As a guideline to their implementation, in this section we will provide roadmaps for specific recommended scenarios identified in the Third Interim Report, as noted above, and which should help the Member States in reaching the objective of the aforementioned ideal solution. The roadmaps aim to address any issues to be resolved at the national and European level in order to arrive at this objective, including both legal/policy issues and technical/infrastructural questions.

The roadmaps will focus specifically on the three scenarios assessed as being the most promising in the Third Interim Report, notably:

- The **single electronic attestation package signed by a trusted administration or private sector trusted third party (TTP)**;
- The **single trusted storage point** of eAttestations / eCertificates; and
- **Federated networks** and national validation points.

For each of these three scenarios, the roadmaps below will identify the general operational requirements, the key problems to be overcome both from a technical/infrastructural perspective and from a legal/policy perspective, and the building blocks which need to be put in place to solve these problems. The relation of each scenario to general e-government initiatives and existing projects will also be briefly explored to clarify the existing context and efforts required. Finally, an overview will be added that provides a logical chronological order to these building blocks and which can be used as a guideline for the implementation of these roadmaps.

Collectively, the roadmaps can be considered as high-level medium - long term plans towards the implementation of the scenarios using the strategy to implement the Ideal Solution for eAttestations / eCertificates as reference and adapting it to allow the three chosen scenarios to move closer to the Ideal Solution by implementing the elements which will ensure their compatibility and interoperability and also allowing the Member States and European Institutions to implement the most convenient solution and evolution path.

6.2 Roadmap for the scenario based on a single electronic attestation package signed by a TTP

6.2.1 General requirements

As was noted in the Third Interim Report and as summarised above, in this scenario the tenderer offers the contracting authority **a single bundle of attestations (i.e. a single electronic file containing all required attestations), signed by a specific trusted administration or private sector entity (a TTP) in each country**. While the contracting authority can still extract the individual attestations from the bundle, validation is only performed on the bundle as a whole; i.e. trust is derived from the fact that the bundle has been signed through a signature belonging to a trusted administration. If the signature on the bundle is valid, the attestations contained in the bundle are also considered to be valid; i.e. trust is 'inherited' from the entire bundle by the individual attestations.

Its functionality depends on three fundamental requirements:

- Ideally (but not necessarily), a series of electronic attestations to include in the bundle already exists, since this would essentially mean that the bundle can be considered to contain original documents, which would make the model more straightforward from a legal perspective in cases where original attestations are required. However, this is not an absolute requirement, since paper attestations that do not (yet) have an electronic equivalent could be scanned by the TTP and added to the bundle in an electronic form. In this way, this model could also be made to function in the absence of original electronic documentation.
- More importantly, the creation and operation of a (group of) TTPs in each country which would sign these documents after having checked their validity. By definition, these TTPs should be trusted by the (foreign) contracting authorities that wish to rely on their services. Additional roles can also be entrusted to this TTP by way of adding value (specifically the collection of some or all of the attestations in the bundle); but these roles are not strictly necessary for the model to function from a trust perspective.
- In order for the administration to be trusted, contracting authorities must have the possibility of validating the signatures on the attestation bundles. This can be done either through validation portals (e.g. in an easily identified centralised location (for instance http://countryname.eprocurement.eu), where the contracting authority can upload the received attestation bundle to a web application which verifies the content of the bundle, the identity of the tenderer and the validity of the signature, and which then reports the result to the contracting authority), or as a part of the implementation of a broader trusted signature validation framework for eGovernment applications in general.

The implementation of this scenario requires that a number of problems are overcome, as will be explained below.

6.2.2 Complexities and solutions for bids submitted by consortia or other multi-party groupings

In a scenario based on a single electronic attestation package signed by a TTP, the participation of multiple entities in a single bid does not present insurmountable difficulties. Essentially, the following situations can be distinguished:

- The grouping constitutes a new legal entity (e.g. a temporary limited liability organisation), or can be represented by a single participant in the grouping (e.g. in the case of subcontracting under one lead participant, or in consortia where the tender specifications require one of the partners to take the lead and the responsibility towards the contracting authority). In each of these cases, there is only one entity that needs to present evidentiary documentation, irrespective of whether the procurement is traditional (paper based) or electronic. As a result, the scenario does not suffer any additional complexities.
- Several or all members of the grouping need to present evidentiary documents, either because they constitute a consortium of equal partners, or because the tender specifications require this for other reasons. In this case, each partner would ideally present a certificate package of its own, signed by a TTP established in its own country. In cases where multiple or all members of a consortium are established in the same country and where the same TTP could be competent, there is no objection to the integration of the certificates of these members into a single attestation package to further decrease expenses. For the contracting authority, the presentation of multiple attestation packages (e.g. one per partner of the grouping) should not present additional complexities, since the scenario is at any rate dependent on the possibility of validating certificate packages from foreign TTPs.
- However, a complexity can arise when one or more partners of a grouping cannot present a certificate package of their own because there is no TTP system in place within its country (i.e. its country has not adopted a TTP scenario). In this case, there are several possible solutions:
    - The first solution would be to allow TTPs to create certificate packages for foreign tenderers as well. This would be unlikely to function well in practice without further supporting measures, since it would in principle require TTPs to validate foreign evidentiary documentation and to sign for its validity (e.g. a Dutch TTP might have to validate and sign documentary evidence from a Bulgarian candidate). It is highly unlikely that such a system could be implemented in a cost-effective manner, unless additional measures were taken.
    - One additional measure that could make this process more manageable would be to extend the TTP system to include trusted authorities who do not operate electronically themselves, but who would be able to collaborate with other TTPs. To continue the example above, it would be conceivable that a trusted authority (such as a notary public) in Bulgaria would perform the validation in Bulgaria, and then provide a statement to his colleague in the Netherlands attesting to the compliance of the Bulgarian evidentiary documentation. The Dutch TTP could then integrate this declaration along with the Bulgarian attestations in a certificate bundle. However, this process would likely be cumbersome in practice, as it would require a further interaction between two trusted parties as a part of tendering processes. Furthermore, it would require further measures to be taken to ensure that the Dutch TTP can establish the legal value and trustworthiness of his Bulgarian counterpart, further complicating the process and the resulting expenses. For this reason, other options should be considered.

- The main possibility to be considered in this regard is the reliance on other scenarios that might be supported in the country that has not implemented a TTP system, and which may include:
  - The decentralised delivery of electronic attestations by the competent administrations directly to the tenderer (see section 4.5.4. above);
  - The use of trusted storage points which could contain the required certificates (see section 4.5.5. above);
  - The use of federated networks, insofar as a federation would exist between the tenderer's country of establishment and the contracting authority's country in relation to the documents concerned (see section 4.5.6. above).

  In all of these cases, compliance with the ideal solution in section 5 will facilitate interoperability and cross border use.

Of course, it is also conceivable that one of the partners of a grouping is established in a country which has not chosen to implement any of the scenarios above. In this case, the valid electronic submission of attestations will likely be impossible. In this case, the problem is of course caused by the absence of any functioning electronic administration, and the only solution therefore is the systematic deployment of one or more solution models presented in this report, so that electronic resources are made available that can be used for the purposes of electronic procurement.

6.2.3 Relation of the scenario to existing eGovernment initiatives – pre-existing initiatives and know-how

This first scenario relies on national TTPs, which is a concept that does have some prior history in public administration.

As already noted above, notaries public have traditionally played the role of trust providers for the validation of foreign documents. One example is the use of apostilles, as recognised by the 1961 Hague Convention Abolishing the Requirement of Legalization for Foreign Public Documents. This mechanism allows notaries public to add apostilles (essentially certificates of authenticity) to notarised documents, thus granting them legal validity in countries which are signatories to the aforementioned Hague Convention.

Initiatives have been underway for several years now to implement an electronic equivalent of this system, most notably within the activities of the Hague Conference on International Private Law (see http://www.e-app.info/, and http://www.nationalnotary.org/intlforum/index.cfm?text=ifEapp). While these initiatives are currently still at a pilot stage and no large scale implementations exist yet, all indications are that such models could see significant take-up in the future. Since the approach relies on a pre-existing trusted network of notaries public and on a legal framework (namely the Hague Convention) that has been found to be sufficiently flexible to allow the creation and use of electronic apostilles, the integration of the aforementioned model is such a mechanism would not require undue effort or investment.

Similarly, the currently running BRITE project.(see http://www.briteproject.net) aims at connecting national business registers to ensure that certain business information can be exchanged across borders in a standardised and interoperable manner. While this approach is inherently more similar to a direct data exchange mechanism in a federated model as described below, it is clear that the proper functioning of this project will require a network of trust to be set up between the participating national managers of business registers. It is not inconceivable that, once these parties have established

sufficient trust to exchange national business register information, they could play a similar role for other types of information as well.

It should be stressed that these initiatives are currently still in an early pilot stage. However, they do show that the creation of networks of trusted administrations or TTPs is not an effort that would necessarily have to start from scratch, and that at least conceptually such models are sound.

Thus, the use of TTPs for this type of mechanism has some precedent in the public sector. Its use as proposed in this particular scenario – validation of attestations, creation of packages and signing them as a trust creating mechanism – is however fairly novel, and is still at an experimental stage. For this reason, the system might be difficult to set up in practice.

From a broader eGovernment perspective, it goes without saying that such a TTP infrastructure, once established, has much broader applications that merely public procurement. In effect, once the system has been set up there is no limitation to the variety of documents that could be exchanged and validated across borders, with applications including the submission of foreign legal documents to courts, the submission of administrative certificates issued by communes (such as birth certificates and marriage declarations), or simply the transfer of authentic private sector documents such as contracts that were deposited into escrow. In effect, the TTP system can be extended to cover any transfer of official documentation.

6.2.4 Key issues and building blocks

In order to implement this scenario, a number of issues need to be overcome, mostly related to the choice and responsibilities of TTPs in each of the Member States, which is the unique characteristic and basic requirement of this scenario. However, this presents a number of unique challenges that will be briefly described below.

6.2.4.1 Legal/policy challenges

- As a first step, Member States would need to agree at the European level on the abstract minimum requirements to be met by TTPs, related specifically to their credentials (including their legal status (e.g. public service administrations or certain private sector service providers), formal training and experience), and to their responsibility/liability. These requirements must be sufficient to ensure that all Member States will accept statements from foreign TTPs as legally valid. A legal instrument must be created at the national level within each country to formalise this consensus. As has been noted above, some countries already have limited experience with TTPs that deliver general statements of compliance to tenderers (e.g. in Denmark and Austria), so that only limited changes would be needed in such countries. However, in the majority of countries there is no such system in place, and the selection of appropriate TTPs might be more complicated. Even in countries that have notaries public and/or chambers of commerce in place, it could be difficult to extend their roles to meet the requirements of this specific scenario.

  → Key building blocks: **Common European list of minimum requirements for TTPs**; **Legal acceptance of this list of minimum requirements**.

- A consensus must also be found on the types of signatures to be used by the TTPs, in relation to their legal status according to the eSignatures Directive, and/or in relation to the security/reliability guarantees of these signatures, which may include direct references to specific standards to be supported and guidelines for their implementation. Again, a legal instrument must be created at the national level within each country to formalise this consensus. It is uncertain to which extent Member States might consider this requirement to be strictly necessary, given that they have no authority to dictate formal aspects of attestations in a paper context (e.g. a country would not be able to reject an official tax attestation on the grounds that it lacked a seal, if such seals were simply not used in the country of origin). Similarly, it could be considered acceptable that national administrations themselves would have complete authority in determining the technical characteristics (including any electronic signatures) of electronic attestations.

  → Key building blocks: **Common European set of minimum requirements for electronic signatures applied to attestation packages**; **Legal acceptance of this set of minimum requirements**.

- Thirdly, Member States must designate appropriate TTPs within their borders; these TTPs must at a minimum meet the aforementioned requirements, and appropriate legal agreements must be put into place governing the scope of the TTPs services and their responsibilities. Again, this will be easier in countries that already have limited TTP systems in place (e.g. Austria and Denmark) or which already have a history of extended trust in certain administrative service providers such as notaries public or chambers of commerce. However, in countries where this is not the case, or inversely where there are a larger number of potential service providers (e.g. notaries and chambers would both be candidates), choosing appropriate candidates for this role could be politically very sensitive.

  → Key building blocks: **Choice of suitable TTPs at the national level**; **Legal agreements detailing the tasks and responsibilities of TTPs**

- From a policy perspective, a viable business model for the TTPs must be found; this implies firstly that localised offices of TTPs are established (to avoid that users have only one single office they can go to in their country), and that TTPs offer additional services to their customers beyond attesting to authenticity (since otherwise, paper submission is likely to be easier and cheaper to the end user). This is an essential step at the national level: the use of TTPs must offer a sufficient advantage to the user, which would not be the case if TTPs merely served to bundle and sign attestations that were already collected by the tenderer. After all, in that case the tenderer could simply submit the collected attestations himself. Realistically, TTPs will likely need to be involved in the collection of suitable attestations on behalf of the tenderers; otherwise, the added value is likely to be perceived as too limited.

  → Key building block: **Defining a viable business model for TTP services at the national level**

- Legal screening exercises will need to be conducted at the national and European level to ensure that attestation bundles from TTPs are legally valid and capable of meeting the requirements imposed by the applicable legal framework; if this is not the case, the legal frameworks need to be updated to support the model. More specifically, the key element to be verified is whether or not national frameworks have been implemented in a sufficiently pragmatic way to allow attestation bundles as permissible evidence. This could be done by ensuring that the already existing legal clauses that permit alternative documents to be provided are extended to cover attestation bundles. E.g. currently the legal frameworks often

require the production of a specific attestation, but if this is not available, then alternative documents such as attestations from notaries public, court declarations or similar documents can be provided by the tenderer. It would be sufficient if these exception rules are formulated sufficiently broadly to also allow attestations from TTPs meeting specific requirements (as outlined in the first bullet point above), at least in electronic procurements and only when no electronic attestations are available in the tenderer's country of origin.

→ Key building blocks: **Screening of national and European legal frameworks to ensure the model is legally viable; Updating of legal frameworks if necessary**

- The content of the attestation bundle must be recognisable to some degree, so that contracting authorities who receive a bundle are capable of identifying the nature and purpose of each attestation included within the bundle. This can be achieved through the systematic publication of information surrounding commonly used attestations (as described in section 2.5.2.), at least for most procurements. From the Member States' perspective, this means that they should strive to provide accurate and up to date information to such an information dissemination mechanism as was described in section 2.5.2., to facilitate cross border recognisability.

  → Key building block: **European information dissemination on the structure and contents of the attestation bundle**

- Finally, in the longer term it is recommended to harmonise the content of the attestations at the European level (insofar as reasonably possible keeping into account the large diversity in attestations), so that contracting authorities can more easily determine the content of the attestations irrespective of language barriers, and so that automated processing of these attestations becomes possible.

  → Key building blocks: **Standardisation of electronic attestations themselves**

6.2.4.2 Technical/infrastructural challenges

- At the most basic level, the implementation of the scenario requires a consensus on technical standards/formats to be used by the TTPs, including with regard to electronic signatures, the attestation bundle as a whole, and each attestation within.

  → Key building blocks: **Standardisation of attestation bundle format; Standardisation of attestations; and Standardisation of signature solutions**

- Contracting authorities must be able to call upon the necessary infrastructure to validate the signature applied to the attestation bundle. Thus, suitable validation mechanisms need to be made available, either in the form of purely national validation portal sites, or in the more complicated form of international validation platforms. At the initial stages, only the former goal will likely be achievable.

  → Key building block: **Creation of suitable validation mechanisms to support contracting authorities**

- The necessary infrastructure must be made available to the national TTPs to create electronic signatures. This might require specific assistance in some countries (e.g. related to financing, training and awareness, etc.).

  → Key building blocks: **Structural support of TTPs at the national level**

6.2.5 Roadmap description

The roadmap below takes the strategy defined for the Ideal Solution for eAttestations / eCertificates and for each step identifies the specific issues to be implemented in order to make the **single electronic attestation package signed by a trusted administration or private sector trusted third party (TTP)** solution evolve to a better version. Among others, this roadmap facilitates interoperability and compatibility with other eAttestations / eCertificates solutions (the recommended solutions plus the Ideal Solution) implemented by other Public Administration(s), Member State(s) or at cross-border

Step nr.	Step Description	Comments
1.	**A political statement and commitment** in favour of this solution needs to be secured as the concept of a "bundle of eAttestations / eCertificates" is difficult to accept / implement due to significant (legal, technical) challenges which need to be solved.	
2.	The legal context required to use the bundle of eAttestations / eCertificates need to be in place at the following levels: • The bundle of eAttestations / eCertifications (structure, content, standardization, normalization) • Each of the eAttestations / eCertificates which are included in the bundle • The legal documents (in electronic form?) required for each eAttestation / eCertificate part of the bundle	The bundle of eAttestations / eCertifications concept is much more complex than the simple eAttestation / eCertificate concept and requires much more resources and time to implement the legal context.
3.	The budgets required to implement this solution need to be committed in advance and be preceded by a study in order to estimate accurately size of the budgets for a successful implementation taking into account the specific risks	The financial feasibility study of the planned implementation is highly recommended in the early stages of the decision process.
4.	The organizational changes required in this case are complex especially concerning the roles and responsibilities of each of the organizations issuing at least one of the eAttestations / eCertificates in the bundle and for bundle itself: the digital signature of the bundle and of each of the eAttestations / eCertificates in the bundle should be considered from	

	PKI / PKS management viewpoint	
5.	The PKI required to support this solution needs to be designed taken into account the specificity and complexity of the bundle of eAttestations / eCertifications concept. For the already available PKI, it needs to be analyzed to see if it supports the bundle of eAttestations / eCertificates concept and to see how difficult is to adapt it accordingly.	
6.	Implementation of this solution is straight forward although it requires special attention to the bundle of eAttestations / eCertificates concept and standardization & normalization of the electronic (XML) templates for the bundle, each eAttestation / eCertificates and eventually the related evidentiary documents. The test of this solution should take into account, if possible, the local, national and cross-border levels with public administrations using the same type of eAttestation / eCertificate solution or a different one Using an SMTP based e-mail system to transport the bundle of eAttestations / eCertifications is the recommend approach for this solution.	The interoperability tests with other eAttestations / eCertificates solutions types will probably require extra-development for these systems in order to handle the bundle of eAttestations / eCertifications without human intervention.
7.	Once this solution is declared operational it will be able to interact with any eAttestations / eCertifications solution capable to handle the bundle of eAttestations / eCertifications	The interaction of the KPIs in support of the interacting eAttestation / eCertificates solutions should also be considered for compatibility and interoperability aspects
8.	The audit of a eAttestations /eCertifications solution based on the bundle of eAttestations / eCertifications concept should be done on a regular an ad-hoc issues in order to identify any anomaly and take the necessary measures to improvement as part of the continuous improvement process	

6.2.6 Costs Analysis

The Cost Analysis for this key solution is based on the Cost Breakdown Structure defined for the Ideal Solution customized in line with the **Single electronic attestation package signed by a trusted administration or private sector trusted third party (TTP) solution** specific issues.

Main Category	Specific Item	Costs Level	Comments
Organizational Costs	Set up new organization or adapt existing one (one shot) mainly for the eAttestation / eCertificate Authority and the Contracting Authority	Medium ->High	**Medium costs** to be considered in a case and existing organization is adapted in order to cope with the single electronic attestation package (uses current infrastructure and most of the staff) **Higher costs** to be considered if a new organization will be put in place (e.g. new infrastructure + new staff) for the eAttestations / eCertificates Authority, Contracting Authority and / or for a brand new PKI organization at national / local level
	Operation costs (recurrent) mainly for the eAttestation / eCertificate Authority and the Contracting Authority	Low -> Medium	**Low recurrent costs** are foreseen when the existing organizations and infrastructures are used.
Technical Costs	**For eAttestation / eCertificate solution:** - Development and set up costs (one shot) – including the costs related to tests; they apply mainly for the eAttestation / eCertificate Authority and the Contracting Authority	Medium	**Medium development / implementation costs** are foreseen for this key solution but the costs can be drastically reduced if the Common Platform elements are considered and if a customisation and / or extension of a previously successfully implemented solution for eAttestations / eCertificates / eProcurements is used (the shared synergies principle)
	For eAttestation / eCertificate solution: - Operation and maintenance costs (recurrent) mainly for the	Low	**In principle the costs for the operation and maintenance of the eAttestation / eCertificate solution are low** if all bugs

	eAttestation / eCertificate Authority and the Contracting Authority		have been identified and solutions implemented before the eAttestation / eCertificate solution is accepted by the (national) / foreign) eAttestation / eCertification Authority. The costs could raise in case replacement of the faulty IT equipment is required.
	For PKI solution: - Development and set up costs (one shot) mainly for the eAttestation / eCertificate Authority and the Contracting Authority	Medium	**The costs for the PKI solution are considered medium** because in the majority of the situations it covers only the integration and customization of an existing PKI solution available from a specialized provider for the eAttestation / eCertificate Authority and the Contracting Authority; The costs could raise if other stakeholders (such as the evidentiary documents providers) will have to sent them electronically signed to the single eAttestation / eCertificate Authority
	For PKI solution: - Operation and maintenance costs (recurrent) mainly for the eAttestation / eCertificate Authority and the Contracting Authority	Low -> Medium	They consists mainly in the operation of the PKI related to the maintenance of the asymmetric key pairs used to digitally sign the eAttestations / eCerticates issued by the unique eAttestations /eCertificates Authority and addressed to the Contracting Authority. It also includes the asymmetric keys pair maintenance for the Contracting Authority. If other stakeholders (such as the evidentiary documents issuers) will have to sent electronically digitally signed docs they will have to use their own pairs of keys and thus the overall costs could increase significantly.
Audit and Continuous Improvement	Audit Costs mainly for the eAttestation / eCertificate Authority and the Contracting Authority	Medium	It will depend basically on the number and type of audit performed. In principle one

Costs			general (IT governance) audit and one security audit per year for the unique eAttestation / eCertificate Issuer and for the Contracting Authority are considered in the scope of this costs estimation.
	Continuous Improvement Costs mainly for the eAttestation / eCertificate Authority and the Contracting Authority	Medium -> Low	The Costs related to the continuous improvement process are in principle more important in the beginning and lower after the whole eAttestation / eCertificate solution has been optimized.

Taking into account all elements of costs briefly assessed in the table above,an overall Medium Costs Level is assigned for the **single electronic attestation package signed by a trusted administration or private sector trusted third party (TTP)** solution. The set up and operation costs could increase dramatically if they are build from scratch and the number of stakeholders increases.

Nevertheless costs reductions for this solution would be easily reached by, for example,

- Outsourcing some of elements such as the PKI organisation and operation to private (national) bodies; or
- Making the eAttestations / eCertificate service payable by the requester (normally the tenderer).

6.3 Roadmap for the scenario based on a single trusted storage point of electronic attestations

6.3.1 General requirements

As noted above, in this model, electronic attestations are stored in single storage points, which are either (partially) controlled by a public administration, or which are purely controlled by the tenderer himself. The key element is that the tenderer has a single storage point in which electronic documents can be deposited and kept, and in which the tenderer can authorise third parties (like contracting authorities) to access the storage point to consult all or some of the stored documents.

In a model where the storage space is hosted by a public administration, it would be possible to no longer issue specific electronic attestations to the tenderer, either singularly or as a bundle. Instead, **the Member States offer protected storage spaces for registered entities, where information related to the entity can be stored both by authorised public administrations and by the entity itself**. These storage spaces could be designed so that they could contain confirmations by the competent national administrations of the tenderer's compliance with procurement requirements, either in the form of signed documents, or simply as links to distributed databases which could confirm compliance with certain criteria. Alternatively, the model could also simply be implemented as a system

where tenderers have the possibility of storing any electronic attestations that might be available in their country.

Rather than providing their electronic attestations to the contracting authorities, tenderers in this system would provide contracting authorities with an authorisation to access the protected storage space, where the contracting authorities can confirm directly what the status of the tenderer is. This would no longer require 'attestations' in the strictest sense (i.e. specific documents), but could also be implemented through a mechanism of assertions of compliance, which would replace attestations.

The proposal's functionality depends on a number of operational requirements, most notably:

- The creation and availability of protected storage spaces (e.g. http://companyname.tenderplatform.cc) where electronic attestations can be bundled together, or where as a minimum a contracting authority can see if the tenderer meets the requirements of the tender specifications. This platform would need to make a distinction between information which is provided by the public administrations (social security attestations, declarations of non-conviction, etc.) and information which is added by the tenderer (self declarations, and information from third parties such as trade register extracts or ISO certifications). This distinction is necessary to allow the contracting authority to determine if the information in the storage page is official, i.e. provided by a public authority (and therefore trusted).
- The protected storage spaces must be made accessible only with the tenderer's permission. This can be done in relatively simple ways, e.g. by allowing the tenderer to automatically generate complex pseudorandom links (e.g. http://ED86b!àçeNCFéz.companyname.tenderplatform.cc) which would lead the contracting authority to the information stored on his platform for a limited duration, or by a simple username/password system. More advanced and secure systems can also be envisaged, but would require a more complicated trust structure and additional expenses.
- Finally, the protected storage space must allow the contracting authority to verify compliance with the tender specifications. This can either be done by providing electronic attestations, or by merely setting 'compliance flags' when no electronic attestation is available (e.g. a country that does not issue electronic attestations to show compliance with tax regulations could simply list the attribute 'Tax compliance', and mark this as 'OK' or 'not OK'). Thus, the use of electronic attestations as such is not strictly necessary in this model.

6.3.2 Complexities and solutions for bids submitted by consortia or other multi-party groupings (consortium)

A key characteristic of this scenario is its inherently individual nature: while it might be envisaged that a TTP could create a bundle containing attestations of several tenderers (as described in the previous scenario), in this second scenario the very nature of individual storage spaces make the bundling of information pertaining to several members of a grouping less suitable. After all, in a TTP scenario, trust is derived from the TTP itself, regardless of the legal entities involved. In a single storage space, trust is derived from the fact that information regarding a specific legal entity can be added directly to a portal by the competent administrations. This trust does not 'spill over' onto other entities.

As a matter of nuance, a contracting authority might still find some value in situations where attestations from other members of a grouping are collected within the storage space of the lead contractor with regard to his subcontractors, or by the head partner of a consortium with regard to the other members. In these cases, the inclusion of attestations pertaining to other entities than the owner

of the storage space can be considered an implied declaration on behalf of the owner that it has checked these attestations for their accuracy. Obviously, the legal value and reliability of such a practice would be limited, since it is not fundamentally different from a lead partner's submission of unverified copies related to his consortium members, at least from the perspective of the contracting authority. In short, the inclusion of attestations or declarations from other entities on the trusted storage space of a third party has limited added value.

Thus, when a grouping wishes to participate in a public procurement where trusted storage spaces will be used, ideally each of the partners would have its own storage space within its own country containing the required information. In these cases, it is a relatively simple matter to provide the contracting authority with the required permissions to access the different storage spaces belonging to each member of the grouping.

As with the scenario above however, complications arise when one or more partners of a grouping cannot or do not use protected storage spaces, for instance because such systems are not operational within its country. Again, the main possibility to be considered in this regard is the reliance on other scenarios that might be supported in the country that has not implemented a storage space system, and which may include:

- The use of attestation packages signed by TTPs (see section 4.5.3. above);
- The decentralised delivery of electronic attestations by the competent administrations directly to the tenderer (see section 4.5.4. above);
- The use of federated networks, insofar as a federation would exist between the tenderer's country of establishment and the contracting authority's country in relation to the documents concerned (see section 4.5.6. above).

In all of these cases, compliance with the ideal solution in section 5 will facilitate interoperability and cross border use.

Again, it remains possible that one of the partners of a grouping is established in a country which has not chosen to implement any of the scenarios above, and in which electronic resources are entirely absent. In this case, the valid electronic submission of attestations will likely be impossible (unless, as noted above, the contracting authority would be satisfied with only one partner using a trusted storage space, and other partners publishing their attestations on this portal). In this case, the only solution is the systematic deployment of one or more solution models presented in this report, so that electronic resources are made available that can be used for the purposes of electronic procurement.

6.3.3 Relation of the scenario to existing eGovernment initiatives – pre-existing initiatives and know-how

The scenario based on trusted storage spaces draws most of its utility from the circumstance that official information (i.e. information from official databases that is considered as being correct ex officio) can be made directly available to third parties, in the case of public procurements to contracting authorities. For instance, a contracting authority could access the trusted storage space and find tax information provided directly from fiscal databases (potentially simply by setting and showing a 'compliance flag' as being positive or negative). Information that is not available from official databases can of course also be published by the entity who owns the portal space, but such information would come without any other guarantees than the assurance of the owner. Thus, while any document type

could be integrated into the system, the actual utility will be much greater for public sector issued documents which can draw upon authoritative sources.

Two related projects that should be mentioned in this context are the CIP ICT PSP pilots STORK and PEPPOL. The STORK project (**S**ecure Iden**t**ity Acr**o**ss Bo**r**ders Ac**k**nowledged) is an initiative guided by DG INFSO which aims to further the development of interoperable identity management and signature solutions by developing specific working European scale pilot applications in a variety of e-government fields. One of the work packages within STORK will likely also focus on eProcurement and electronic attestations, through a specific eProcurement project. However, specific details are not yet available, as the consortium partners are currently still negotiating their tasks and responsibilities.

The PEPPOL project (**P**ublic **e-P**rocurement **P**ilot **O**n-**L**ine; see http://www.schemaworks.com/20070926ArchitectureforaEuropeanSOIf.pdf) focuses only on electronic procurement. One of the pillars of the project (WP2) is the creation and use of a Virtual Company Dossier, which is conceptually similar to an advanced version of the proposed centralized storage scenario, where information is made available 'on the fly' by utilising company information already registered in public sector databases. However, the project is still in its early stages, as it is scheduled to run between 2007 and 2013, so that a more detailed comparison is presently not yet possible.

As was already mentioned above, embryonic implementations of this scenario already exist at the national level, in the form of portals where tenderers have the possibility of storing any electronic attestations that might be available in their country, such as the French examples of the public procurement platform of the Bourgogne region, https://www.e-bourgogne.fr/; the platform offered by the Ministry of Defence, http://www.achats.defense.gouv.fr/; and the general site mon.service-public.fr/.

If such initiatives were to be deployed at an international level (i.e. similar individual portal systems would be made available in all Member States), this could provide for very interesting synergies with other projects. By way of a simple example:

- Early implementations could focus exclusively on providing storage spaces that tenderers could use to upload specific documents. In this embryonic form, the model amounts to little more than a simplified content management system, and the added value for procurement is very limited. However, deployment can be fairly simple and cheap.
- In a second phase, the system can be enriched with identity information derived from official databases, i.e. each portal would contain official information such as the name, legal form, official address, registry number/VAT number etc. for each entity. This could be done entirely on the national level, or could benefit from the outputs from the BRITE project, which is after all designed to make such information accessible at the European level. With this addition, at least identity information related to the entity has been validated, which already offers some added security, and thus added benefit.
- In a third phase (and any number of successive phases), other databases could be integrated into such a system, with the aforementioned ECRIS project being an example of a potential avenue. As noted above, the ECRIS system (European Criminal Records Information System) is currently aimed at improving collaboration between European criminal investigators by enabling the exchange of information extracted from the criminal record. In principle, there is no technical reason why such a system could not also be extended to automatically feed information about criminal convictions into a protected storage space controlled by its owner, provided of course that the policy and privacy objections could be overcome, which is no trivial barrier. In this way, the owner of the storage space could authorise third parties (including contracting authorities) to access the storage space and directly verify the status of any criminal history from the most authoritative source. This would provide a very significant direct benefit and added value to all parties concerned.

While the example above is far from trivial to implement and is likely to see some opposition for reasons of data protection, the concept itself is sound and shows how a trusted storage space can be used to benefit all parties concerned by gradually extending its functionality and reliability. The example of ECRIS above could of course also be applied to any other electronic cross border network that aims at exchanging relevant information, which might well include tax information and social security status in the future.

This scalability and extensibility however could also be said to constitute something of a weakness, in the sense that trusted storage spaces can only reach their full potential by making all information accessible through such a portal. An earlier implementation which only confirms identity information is of little value, and even the addition of criminal record information only solves the problems related to one specific attestation type. For any additional attestation type, similar initiatives would be needed. This is in contrast to the aforementioned TTP solution, where the creation of a functioning TTP network would be adequate to handle any attestation type, or indeed any type of documentation in general. Thus, in order to get the full benefit out of protected storage spaces, a consistent choice and continued development is necessary in order to ensure that the storage space includes as many different types of documents as possible.

As with the TTP scenario above, it is clear that protected storage spaces have ample applications outside of eProcurement, as they can be used in any situation where a legal entity wishes to provide reliable information to a third party, either within the public sector or beyond. For instance, one could easily imagine that such a system could be used to provide information to a professional organisation abroad in order to obtain a license to offer one's service in that country (as required by the Services Directive). Or even more broadly, the mechanism could be used to submit commercial offers (including entirely unofficial information such as product/service catalogues) or introductory information to specific business partners. In this way, storage spaces could gradually evolve to reliable communication mechanisms with broad applications in business traffic in general.

6.3.4 Key issues and building blocks

The scenario can present a multitude of difficulties, depending on the complexity of the chosen implementation. However, irrespective of the details of the implementation, the key issues related to this scenario concern the deployment of storage spaces and the creation/adoption of suitable security policies, specifically in relation to managing the identification of the users and the authorisation of contracting authorities who attempt to gain access to the storage space. The unique challenges related to this scenario will be briefly described below.

6.3.4.1 Legal/policy challenges

- As a first step, Member States must agree on requirements in relation to the security of the storage spaces, including registration and access requirements (i.e. how does a prospective tenderer open a storage space, who can access it and on which conditions), hosting (i.e. will the storage space be hosted by a private party or by a public administration), logging etc. This agreement must be formalised in a suitable legal instrument. It is important to have a European consensus on the requirements for such storage spaces before any instruments are created at the national level, since Member States must first agree among each other on the guarantees that such a system should offer.

→ Key building block: **Common European security policy in relation to the creation and management of storage spaces.**

- Secondly, national and European legal frameworks must be screened and amended if needed to ensure that information provided via a storage space is legally valid (especially in a more advanced stage of implementation, where so-called 'compliance flags' might be used instead of attestations in any real sense of the word). Since no fully functional storage spaces as described above are currently operational yet, it is likely that all Member States wishing to rely on such systems will need to amend their legal frameworks. It should also be noted that legal changes will be needed in all countries, and not only in the countries that wish to offer protected storage facilities to their citizens and companies. After all, the crucial factor in the operation of such storage spaces for public procurement purposes is precisely that foreign contracting authorities must be willing and able to access a tenderer's storage space and accept the information stored therein as legally valid. This may be the greatest legal and operational barrier to the functioning of this scenario.

  → Key building blocks: **Screening of national and European legal frameworks to ensure the model is legally viable; updating of legal frameworks if necessary**

- If information can be added to the storage space by any other party than the tenderer (e.g. by the competent public administration, but other possibilities exist depending on the choices made in the aforementioned security policy), this implies the need for additional liability arrangements (beyond those that already fall upon the tenderer himself). In other words, if other parties than the tenderer can add information to the storage space, they must assume responsibility for this. This is an aspect that can be implemented at the national level, although it is clear that key arrangements and guarantees also need to be foreseen at the European level. This will after all be one of the conditions for accepting the use of attestations provided through storage spaces of foreign tenderers: sufficient guarantees need to be present with regard to the accuracy and reliability of the provided information.

  → Key building block: **Consensus on and implementation of a suitable responsibility/liability model for any information added by third parties**

- The content of the storage spaces must be standardised to some degree at the European level, so that contracting authorities who gain access to a foreign storage space are capable of identifying the nature and purpose of each attestation included within the space.

  → Key building block: **European agreements on the structure and contents of the storage space**

- In the longer term it is recommended to harmonise the content of the attestations at the European level (insofar as reasonably possible keeping into account the large diversity in attestations), so that contracting authorities can more easily determine the content of the attestations irrespective of language barriers, and so that automated processing of these attestations becomes possible.

  → Key building blocks: **Standardisation of electronic attestations themselves**

- Finally, a European consensus must be sought on the privacy aspects of such a system and on the scope to which it can be extended. Storage spaces allow tenderers much greater

freedom in managing their own information, including potentially in relation to information which is traditionally stored in (closed) public sector databases (e.g. the aforementioned criminal register extracts, social security declarations etc.). Member States must agree on the general usability of such a system, and on whether it is reconcilable with their legal frameworks and policy preferences. As noted above, this will require an extensive private debate if the mechanism is to function across Europe, rather than in a selected number of countries.

→ Key building blocks: **European agreement on the privacy aspects and general permissibility of such a system**

6.3.4.2 Technical/infrastructural challenges

- Appropriate standards and guidelines need to be put in place to assist in the implementation of storage spaces at the national level; assistance can also consist in the development of a standardised implementation at the European level which can be copied at the national level.

  → Key building blocks: **Structural support of the development and deployment of storage spaces at the national level**

- An acceptable identification/mandate management model needs to be implemented. This includes agreements on how the tenderers themselves can access their portals and add information, but also on how tenderers can grant third parties (such as contracting authorities) limited access to the portal.

  → Key building blocks: **Structural support of the development and deployment of storage spaces at the national level**

- At the most basic level, the implementation of the scenario requires a consensus on technical standards/formats to be used for each attestation stored within the storage space.

  → Key building blocks: **Standardisation of attestation formats**

- [Optional: ideally administrations should be capable of adding information directly to the storage space; or at a later stage to simply set compliance flags (i.e. Criminal convictions: OK/not OK). In this case, a mechanism must be included that allows foreign contracting authorities to determine if the information is authentic. This can be done in a relatively simple manner, e.g. by splitting the storage space into two sections, one of which can only be edited by the competent authority but not by the tenderer. However, even such a simplified system requires European consensus to ensure that the mechanism is recognised throughout the E.U.]

  → Key building blocks: **European agreement on validation mechanisms if/when information is added directly by the competent administrations.**

- [Optional: if the storage space relies on PKI based signatures, a consensus is needed on the technical standards/formats to be used for attestations within the storage space with regard to electronic signatures. Furthermore, contracting authorities must be able to call upon the

necessary infrastructure to validate the signature. Thus, suitable validation mechanisms need to be made available, either in the form of purely national validation portal sites, or in the more complicated form of international validation platforms.

→ Key building blocks: **Standardisation of signature solutions; Creation of suitable validation mechanisms to support contracting authorities**

6.3.5 Roadmap description

The roadmap below takes the strategy defined for the Ideal Solution for eAttestation / eCertificates and for each step identifies the specific issues to be implemented in order to implement and improve the **roadmap for the scenario based on a single trusted storage point of electronic attestations solution** by allowing interoperability and making it compatible with other eAttestation / eCertificates solutions (the recommended solutions plus the Ideal Solution) implemented by other Public Admin, Member States or at cross-border:

Step nr.	Step Description	Comments
1.	The political commitment in the case of this scenario is absolutely essential due to its complexity and the number of stakeholders involved. Regular consultations with the private sector are also essential as the tenderers (usually coming from the private sector and from all sectors of activities!) will have to commit on building, maintaining and operating the single storage points for eAttestations / eCertificates	Political support should be expressed in general for all tenderers but specifically for those for which building and maintaining such as single point of storage is a burden from organisational, technical and financially viewpoints.
2.	The legal context required by the implementation of the single storage point of eAttestations / eCertificates should be carefully assessed and the necessary laws should be in place before any solution based on the single storage point of eAttestations / eCertifications implementation. The security of the storage site (information, access) and the usage of the PKI in this context should also be carefully analyzed and covered by specific laws. The standardization and normalization of the eAttestation / eCertificates will need to be covered as well as the usage and management of digital signature and encryption / decryption technologies.	The laws required to create a valid legal context for the implementation and usage of the single storage points of eAttestations and eCertifications should also provide the possibilities of grouping the storage points by economical sectors and be managed by authorized legal entities such as professional associations to simplify the whole model at a national scale.
3.	Financing the implementation of the single storage point of eAttestations / eCertificates concept will require: • Public financing – to allow the public administrations to implement mechanisms to generate eAttestations / eCertificates and send / upload them in the single storage point • Private financing – to allow the tenderers the setting up, operation and maintenance of the	In order to be successful, the single storage point of eAttestations / eCertificates, specific financial mechanisms will have to be defined in order to stimulate small players, with limited financial resources, to implement such solutions or joint similar initiatives (e.g. economic sector single storage point variant)

	single storage point plus	
4.	The organizational measures required to make this solution work will have to be defined and implemented for each single storage point of eAttestations / eCertificates. The organizational measures will impact not only the tenderers but also the public administrations as issuers of eAttestations / eCertificates and the PKI management entities. Without taking advantage of eventual synergies the implementation of the single storage points of eAttestations / eCertificates will be very complex from organizational viewpoint.	Some potential synergies able to reduce the organizational complexity: • Use economical sector level (or similar) for single storage point instead of each tenderer • If available, use existing PKIs
5.	In the case of the single storage point the usage of the PKI should be based on existing systems. If a new system will have to be set up, it will have to take into account specific architecture and design foreseen for the single storage point concept at national level and eventually cross-border. It will have to address the public-private keys pairs management for the public administrations but also for other (private) entities (tenderers, professional organizations or alike) entitled to issue eAttestations / eCertificates or evidentiary documents as input for eAttestations / eCertificates	The tests of the PKI and public – private (asymmetric) key pairs should start small (local level) and evolve wider to national and eventually (if possible) cross-border
6.	The implementation and testing of the technical solution for the single storage point of eAttestations / eCertificates requires that the following technical points are solved in order to ensure compatibility and interoperability with other eAttestations / eCertificates / eProcurement solutions (Ideal Solution or the recommended scenarios): • Standardization and normalization of the eAttestations / eCertificates and their corresponding evidentiary documents but also of the bundle concept at national and European levels • The availability of the electronic versions for the docs mentioned in the previous point; strongly recommended is the XML usage; • The design and implementation of a secure database able to store the eAttestations / eCertificates / eBundles[8] and related evidentiary documents • The interface with the corresponding PKI managing the asymmetric keys and eventually the secret keys of various single	The technical solution briefly mentioned here will allow the compatibility and interoperability with the other recommended scenarios and eventually, in long term with implementations of the Ideal Solution, if any.

[8] An eBundle represents the electronic version of a bundle of eAttestations / eCertificates and eventually the related electronic versions of the evidentiary docs.

	storage point stakeholders. • Well defined and secure mechanisms able to o Send / receive the eDocuments[9] stored in the secure database representing the single storage point (front-end e-mail application serving the secure database) o And / or to allow the upload / download of the eDocuments stored in the secure database (e.g. front-end web portal serving the single storage point of eAttestations / eCertificates / eBundels)	
7.	Once the technical solution implemented and tested successfully, the single storage point is declared operational and able the support the eAttestation / eCertification / eProcurement processes at national and European level. The compatibility and interoperability with other eAttestation / eCertification implementations will depend on their compliance to the general principles mentioned in section 4.2 and their implementation for recommended key scenarios or the Ideal solution.	Additional work will be required in order maintain • the information in the secure database including the eAttestations / eCertifications / eBundles and related evidentiary docs; • the users authorized to have access to the information and their access profiles.
8.	The single storage point should be audited on a regular and ad-hoc basis in order to detect anomalies at organizational, technical and security levels and suggest measures for continuous improvement	

6.3.6 Costs Analysis

The Cost Analysis for this key solution is based on the Cost Breakdown Structure defined for the Ideal Solution customized in line with the **Single trusted storage point of electronic attestations solution** specific issues.

Main Category	Specific Item	Costs Level	Comments
Organizational Costs	Set up new organization or adapt existing one (one shot) for the public administration and / or	Low - Medium	The related organizational set up costs could be low if each entity (tenderer) sets up its own storage space or medium if a public

[9] eDocuments covers all docs in electronic versions including eAttestations, eCertificates and eBundles but also evidentiary documents.

	the private entity in order to (electronically) store the evidentiary documents and / or the eAttestations / eCertificates		administration / entity sets up storage spaces for all entities requesting it at national or local level. Again the costs are lower if an existing organization is adapted to cover the service and they are higher if a brand new organization (including infrastructure) is defined for this purpose. Medium costs are also estimated for the Contracting Authority in order to retrive itself the eAttestations / eCertificates and / or evidentiary documents for all tenderers or al least a part of them if mixed eAtttestations / eCertificats solutions are implemented national / EU wide.
	Operation costs (recurrent)	Low -Medium	The recurrent organizational costs when adapting an existing organization are probably lower that the ones when a new organization is in place and considered medium. Also, in principle, due to the fact that the Contracting Authority will have to retrieve itself the eAttestations /eCertificates and / or the evidentiary document from the storage space hosted by a public administration / private entity (tenderer) for all or a part of the tenderers, more people will be involved in these activities and thus more recurrent operational costs will occur. The gathering of such information will be also time consuming for the Contracting Authority.
Technical Costs	**For eAttestation / eCertificate solution:** - Development and set up costs (one shot) – including the costs related to tests	Low -Medium	If the eAttestations / eCertifcates and / or evidentiary documents are stored in a (virtual) space protected by a login and password the set up of such a space are considered low for the private entity (tenderer) and medium for the public administration (due to the quantity of data stored and restricted access control mechanisms to be put in place depending on the autorization

			level and related access rights.
	For eAttestation / eCertificate solution: - Operation and maintenance costs (recurrent)	Low - Medium	The operation and maintenance costs for this key solution are considered low if each private entity (tenderer) stores in a protected space its own data uploaded by the stakeholders concerned (eAttestations / eCertificates and / or evidentiary documents issuers) but it can become non-trivial (medium level) is the storage space hosts documents for national / cross-border entities (tenderers) updated by authorized public administrations and / private parties. Thus is due to the volume of information handled, number of stakeholders and security measures required to restrict the access to the information stored.
	For PKI solution: - Development and set up costs (one shot)	Low (0) - Medium	The costs are considered low if no PKI solution is implemented and medium if PKI solution is implemented in order to check the data integrity and stored eAttestations / eCertificates and / or evidentiary documents authenticity. Nevertheless, without the digital signature (PKI based) the (virtual) storage space will not be able to guarantee the data integrity and the authentication of the issuer of the stored eAttestation / eCertificates and / or related evidentiary documents. Which implies a non-trivial risk for the Contracting Authority using the information.
	For PKI solution: - Operation and maintenance costs (recurrent)	Low (0) - Medium	The recurrent operating costs are low (zero) if no PKI solution is integrated and medium if a PKI based solution is used due basically to the asymmetric key pairs maintenance (renewal included) for all stakeholders (public administrations, others) using PKI to digitally sign their documents (eAttestations / eCertificates and / or evidentiary documents) uploaded in the

			storage space.
Audit and Continuous Improvement Costs	Audit Costs	Medium	The relevant types of audits for this key solution will have to include all critical stakeholders and concentrate mainly on the security aspects especially if no PKI solution is integrated to check data integrity and authentication aspects.
	Continuous Improvement Costs	Low - Medium	The costs are low for each private entity (tenderer) storing its own eAttestations / eCertificates and / or evidentiary documents uploaded by the rightful issuers. The costs implied by the continuous improvement of this key solution are medium if there is a national / european level (public or private) entity storing national / european eAttestations / eCertificates and / or evidentiary docs of the national / european tenderers and uploaded by national / european public administrations or private entities (tenderers). The costs for the improvement / optimization of such as complex database could evolve to higher levels even.

Taking into account all elements of costs briefly assessed in the table above, an overall Low -Medium Costs Level is assigned for the **Single trusted storage point of electronic attestations solution**. When the private entity (tenderer hosts it own storage point the set up and operation costs for each private entity (tenderer) are low but the overhead induced to the eAttestations / eCertificates Authorities, evidentiary documents issuers and Contracting Authorities is high and human resources consuming. The set up and usage of the PKI will imply additional costs but ensure the integrity and authenticity of the data stored.

As for the first key solution, costs reductions for this solution are possible, for example, by:

- Outsourcing the set up and operation of the storage space to a national / European public / private body trusted by all stakeholders, and by
- Making this service payable by the requester (normally the tenderer).

Unfortunately, the costs reductions suggested above cannot solve the overhead induced to the Contracting Authorities and eventually to the eAttestations / eCertificates and / or evidentiary documents issuers if an integrated solution is not implemented.

6.4 Roadmap for the scenario based on federated networks and national validation points

6.4.1 General requirements

The key objective of this model is to create a network of trusted information sources, between which a consistent direct data exchange approach is implemented. **Instead of requesting specific attestations to be provided by the tenderer, contracting authorities will be mandated by the tenderer to obtain information directly at the source, i.e. from the administration(s) which manages the requested information in the tenderer's country of establishment.**

Thus, this last solution tries to recreate and improve the functionality provided by the requirement of providing specific attestations, while eliminating the burden of requiring that the tenderer does so.

The model has a complex set of operational requirements, including most notably:

- The availability of the data sources that are used in the tenderer's country of origin to demonstrate compliance with specific formal requirements. This does not imply that the contracting authority can directly access the underlying databases on the information contained therein; but rather than the contracting authority has a contact point which it can address in any given country which it can query to obtain a confirmation of compliance. For example, a contracting authority would not need to access tax registers, or even to receive a tax attestation, if it can simply receive a reliable assertion that tax obligations are met. Thus, a first requirement is the availability of electronic data sources for (at a minimum) the principal requirements to show compliance with the tender specifications. It should be noted that it would be possible to implement this vertically rather than horizontally, i.e. in the form of context specific data exchange networks. One might imagine e.g. that a network could be formed between tax administrations (for the exchange of tax compliance information), next to a network between social security administrations (who perform the same function in their sector).
- Secondly, there must be a clear and unambiguous way for the contracting authority to be mandated by the tenderer to obtain this information from the data source. This requires (1) that the contracting authority has a way to uniquely and unambiguously identify the tenderer when requesting information; and (2) that the data source can validate whether a mandate actually has been given. Neither problem is easy to resolve. For instance, the use of VAT numbers is a good solution to problem (1) in most cases, but not all tenderers will have a VAT number, so that it is not sufficient. Problem (2) could be resolved by allowing tenderers to issue specific passwords or pseudorandom URLs to contracting authorities, similar to the solution that was already described above; but all Member States may not be willing to make specific information available on the sole basis of these mechanisms, for reasons of data protection and confidentiality.
- Finally, in order for information to be reliably exchanged between data sources and contracting authorities, a series of standards needs to be embraced with regard to semantics, file formats and communication protocols. Furthermore, the provided information needs to be signed by the data source in a manner that allows the contracting authority to validate it and its origin.

6.4.2 Complexities and solutions for bids submitted by consortia or other multi-party groupings

More than the earlier two scenarios described above, federated networks are binary in their operation: they either work perfectly for any given entity, or they do not work at all. The involvement of additional parties in a procurement does not change this fact. When a bid is jointly submitted by a grouping of entities, then a federated solution will be capable of providing the contracting authority with the required information for all parties in the bid which are established in a country that is a member of the federated network, and it will fail for any others.

When a member of a grouping is not established in a country that is a part of the federation, the main solution is once again the reliance on other scenarios that might be supported in its country, and which may include:

- The use of attestation packages signed by TTPs (see section 4.5.3. above);
- The decentralised delivery of electronic attestations by the competent administrations directly to the tenderer (see section 4.5.4. above);
- The use of trusted storage spaces to provide the information that other members of the grouping are providing through federated networks (see section 4.5.5. above).

In all of these cases, compliance with the ideal solution in section 5 will facilitate interoperability and cross border use.

Again, it remains possible that one of the partners of a grouping is established in a country which has not chosen to implement any of the scenarios above, and in which electronic resources are entirely absent. In this case, the valid electronic submission of attestations will likely be impossible. In this case, the only solution is the systematic deployment of one or more solution models presented in this report, so that electronic resources are made available that can be used for the purposes of electronic procurement.

6.4.3 Relation of the scenario to existing eGovernment initiatives – pre-existing initiatives and know-how

This specific scenario knows only a limited application in eGovernment situations at this time, mostly due to its technical complexity and the need for interoperable national infrastructure, which implies that information sources at the national level must be aligned quite substantially. For this reason, it is easier to apply this scenario in a system that is being created from scratch (i.e. where even national databases do not exist yet) than in cases where national databases have already been implemented in accordance with whatever policies a country deemed optimal, and where harmonisation and interoperability thus require greater effort.

None the less, in a limited number of specific sectors the model is already operational and functioning in practice. The Schengen Information System could be considered an implementation of such a structure, as it consists of a series of national databases interconnected by a specific interface that allows law enforcement officials to more easily exchange and obtain information on persons or items under suspicion.

Another logical continuation of this model is the aforementioned BRITE project (see http://www.briteproject.net), which aims at connecting national business registers to ensure that certain business information can be exchanged across borders in a standardised and interoperable manner. This is a clear application of the federated model, which could be usable in any number of contexts.

Similarly, the ECRIS system was already mentioned above as a pilot project looking to facilitate the electronic exchange of judicial records between criminal authorities in the Member States, including through the ECRIS system (European Criminal Records Information System). This initiative is currently aimed at improving collaboration between European criminal investigators, as described in Council Decision 2005/876/JHA of 21 November 2005 on the exchange of information extracted from the criminal record[10]. However, as the infrastructure has already been established and is currently being used by six Member States to improve their judicial collaboration.

As all of these examples illustrate, federated networks tend to function only within specific sectors, i.e. by interconnecting only related administrations which store comparable information. For such document types in particular, a federated model is very suitable. Of course, this also requires that the federated system covers all (or at least a larger number of) Member States, and that a sufficient common political ground can be found between the Member States to use such federated systems also for eProcurement purposes. This means that sufficient privacy safeguards need to be built in, to ensure that e.g. in the case of ECRIS, the electronic exchange of judicial records would only be possible with the consent of the tenderer, thus minimising the risk of excessive intrusion into the tenderer's private sphere. The legal basis for the current ECRIS system will be extended through a new Framework Decision on the organisation and content of the exchange of information extracted from criminal records between Member States, to be formalised in the course of 2008. However, this framework decision mainly entails the extension of the system to all Member States and the clarification of the Member States' obligations. Its potential use for public procurement purposes will likely not be covered, and will require separate agreements to be put in place.

Thus, it is clear that extended collaboration between functionally related administrations in the Member States is a possible avenue for realistically and gradually developing federated models. As the examples above have shown, such systems are generally created to improve cross border collaboration in general, and eProcurement is just one of the application domains that could benefit from federated networks.

6.4.4 Key issues and building blocks

The main element of complexity in this scenario relates to the choice of contexts in which information will be directly exchanged, the creation of a functioning legal and technical framework to accompany this exchange, and above all the fundamental need to harmonise/standardise existing information sources and information exchange sources. This means that for each context in which the scenario will be applied, agreements need to be put in place regarding the precise content of each attestation, and regarding the exact semantics behind each data element within an attestation. The unique challenges related to this scenario will be briefly described below.

[10] See also http://europa.eu/scadplus/leg/en/lvb/l14500.htm, and related initiatives such as the establishment of Eurojust as a way of reinforcing the fight against serious crime at the European level (see http://europa.eu/scadplus/leg/en/lvb/l33188.htm).

6.4.4.1 Legal/policy challenges

- It is clear that a federated model is not practically usable for all document types, as the system favours relatively uniform attestations which are issued and managed by a small number of competent administrations; a greater variety in documents and/or issuers (e.g. diplomas issued by private sector educational organisations) complicates the model considerably. Member States must therefore agree on the formation of federations within specific contexts on a case by case basis. This implies the creation of legal instruments formalising a consensus on responsibilities and liabilities for all members of the federated network.

  → Key building blocks: **Legal instruments formalising the creation of a federated network within a specific context; Legal framework determining the responsibilities and liabilities of the federated network's members**

- Furthermore, the privacy aspects will need to be stringently assessed and monitored, since the scenario implies the cross border exchange of personal data which is potentially of a highly sensitive nature (as is e.g. the case for extracts from criminal registers). Member States must come to a consensus on the general usability of such a system within a specific context, and on whether it is reconcilable with their legal frameworks and policy preferences.

  → Key building blocks: **European agreement on the privacy aspects and general permissibility of such a system for each context**

- Legal screening exercises will need to be conducted at the national and European level to ensure that information obtained directly from the source through a federated network is legally valid and capable of meeting the requirements imposed by the applicable legal framework; if this is not the case, the legal frameworks need to be updated to support the model.

  → Key building blocks: **Screening of national and European legal frameworks to ensure the model is legally viable; Updating of legal frameworks if necessary**

- The content of the attestations must be semantically aligned to a very large degree. Unlike the two scenarios above, for the current scenario this is an absolute necessity, since information cannot otherwise be exchanged. This may also imply that regulations and policies determining which/how information in a specific context is stored and transmitted must be aligned at the European level.

  → Key building block: **Semantic alignment of the content of the electronic attestations**

6.4.4.2 Technical/infrastructural challenges

- In order for the model to function, the participating administrations must update their available infrastructures in order to be able to electronically exchange information with foreign administrations and to validate the information they receive via national contact points. In some cases, this will mean that electronic databases will need to be created, or at least reorganised to make them accessible.

→ Key building block: **Structural support of administrations at the national level to ensure that the required infrastructure can be created**

- A full consensus is needed on standards / formats for the structuring of all exchanged information in electronic attestations, so that they can be processed automatically without regard to linguistic barriers. This implies extensive standardisation with regard to semantics, and will typically require the drafting of detailed vocabularies.

  → Key building blocks: **Semantic standardisation of existing attestations; Creation of context specific vocabularies**

- Additionally, a consensus is needed between participating administrations on communication protocols and standards to ensure that the exchange of information is technically possible

  → Key building blocks: **Agreements on communication mechanisms between administrations within a federation**

- An acceptable identification/mandate management model needs to be implemented, so that administrations within a given federation can recognise and trust each other; and so that tenderers can give foreign administrations in the federation permission to retrieve information from their counterpart in the tenderer's country. This also implies the availability of functioning identification means that can be used to uniquely identify the tenderer.

  → Key building blocks: **Creation of a mechanism to identify/authorise administrations within a federation; Creation of a mechanism to identify the tenderer to whom information requests pertain.**

6.4.5 Roadmap description

The roadmap below takes the strategy defined for the Ideal Solution for eAttestation / eCertificates and for each step identifies the specific issues to be implemented in order to improve the **Federated networks and national validation points solution. It** allows interoperability and compatibility with other eAttestation / eCertificates scenarios (the recommended key scenarios plus the Ideal Solution) implemented by other Public Admin, Member States or eventually at European level:

Step nr.	Step Description	Comments
1.	The national and local political commitment is required in order to adopt the concept of federated networks and national validation points As multiple public administrations are required to collaborate to put in place the federated networks but also the national validation point(s) a political agreement and consensus on the roles and responsibilities of each stakeholder are of cornerstone importance in order to ensure convergence and stability in long term.	
2.	The European Directives covering the eAttestations /	

	eCertificates / eProcurement will have to include references to the legal aspects of using the federated networks and national validation points Specific laws will have to be defined and adopted at national level (based on the European Directives) in order to allow the implementation and usage of the federated networks and the national validation points (see 5.4.2.1 section above). Additionally, legal context covering • the usage and management of the digital signature and encryption / decryption of data • sensitive data exchange issues • standardization and normalization of eAttestation / eCertifications and their usage in a standard electronic format (e.g. XML) • security services issues (data integrity, data confidentiality, data availability, authentication and non-repudiation) related to the specificity of this key scenario	
3.	Setting up and operation of the federated networks and single validation point model requires a lot of work and resources, more specifically financial resources. To estimate accurately the budgets necessary, a feasibility study should be run first to identify the current situation and afterwards to estimate the most suitable solution and in consequence the budget required to implement it.	As each member of a federated network has the freedom to implement its preferred recommended key scenario (or even the Ideal Solution), the financial effort required to interconnect them will have to be considered.
4.	The implementation of the federated networks and national validation points scenario requires • Changes in the organizational structure of each member of the federated network in order to allow these organizations (e.g. public administrations) to collaborate efficiently. • The set up of the organization supporting the national validation points and the interactions with the members of the federated networks • Clear definition of the roles and responsibilities between various stakeholders (members of federated networks, national validation points, PKI organization)	The organizational changes required to implement the federated networks and national validation points are disturbing for the personnel, could destabilize the organization itself and should be processed carefully.
5.	The technical solution for PKI will have to be adapted to the specificity of the federated networks and national validation points solution to be implemented, more specifically to the corresponding organizational structure and the roles and responsibilities assigned to each organization and to critical stakeholders within each organization.	The testing of the technical PKI solution should cover first one member of the federated networks and eventually one national validation point and if successful add new members and new validation points.

	The testing of the technical PKI solution will have to start small and evolve to all critical stakeholders in order to eliminate / reduce as much as possible the potential risks (configuration, security)	
6.	Implementation of the technical solution for the federated networks and national validation points should be planned carefully by including first the critical members (eAttestations / eCertifications and corresponding evidentiary documents issuers) of the federated networks and relevant national validation points. Special attention should be paid to the interaction with the PKI (asymmetric keys and secret key issuing, distribution and management) and in general to the security aspects. The testing should also follow the implementation phases in order to verify the new elements introduced but also to check backward validity of the solution implemented. This scenario is very heavy from the beginning but it could become even more complex with the increasing number of members and national validation points.	The technical solution for the federated networks and national validation points will have to include support for standardized and normalized eAttestations / eCertifications / eBundles but also for the evidentiary documents. The usage of the electronic versions available in XML is highly recommended. In order to facilitate the exchange of information, an e-mail (SMTP based) transport mechanism should be used • By the members of the federated networks • By the national validation points. • By the CAs and TTPs
7.	Once the technical solution implemented and tested successfully, the federated networks and national validation points solution is declared operational and able the support the eAttestation / eCertificate / eProcurement processes at national and European level. The compatibility and interoperability with other eAttestation / eCertificate implementations (e.g. by other members of the federated networks) will depend on their compliance to the general principles mentioned in section 4.2 and their implementation for recommended key scenarios or the Ideal solution	
8.	The auditing of the federated networks and national validation points is more complex than the ones for the other recommended key scenarios but it is absolutely necessary periodically or on an ad-hoc basis in order to identify anomalies and recommend measures to resynchronize various elements involved and improve their performance.	

6.4.6 Costs Analysis

The Cost Analysis for this key solution is based on the Cost Breakdown Structure defined for the Ideal Solution customized in line with the **Federated networks and national validation points solution** specific issues.

Main Category	Specific Item	Costs Level	Comments
Organizational Costs	Set up new organization or adapt existing one (one shot) for each member of the federated networks plus the Contracting Authorities	High	The High Costs Level is due to the number and complexity of the member networks. Adapting each network organization implies more reduce costs but at the "federated" lavel a new organization is required in order to coordinate the member networks. In exchange, for the Contracting Authorities, a national validation point implies more efficiency and hides the organizational and technical complexity of the federated networks.
	Operation costs (recurrent) for each member of the federated networks plus the Contracting Authorities	High	The higher the number of the member networks and their complexity the higher the recurrent costs of operations from organisational viewpoint. In exchange, for the Contracting Authorities recurrent operational costs from organizational viewpoint are reduced due to the single national validation point.
Technical Costs	**For eAttestation / eCertificate solution:** - Development and set up costs (one shot) – including the costs related to tests for each member of the federated networks plus the Contracting Authorities	High	The costs for the development and set up of the this eAttestations / eCertificates solution is high due to the costs for each member network plus the complexity in integrating them. Without adopting a common platform to facilitate their compatibility and interoperability, this solution could prove very

			complex and costly.
	For eAttestation / eCertificate solution: - Operation and maintenance costs (recurrent) for each member of the federated networks plus the Contracting Authorities	High	The operation and maintenance costs are high and represents mainly the sum of the operation and maintenance costs for each member network plus the operation and maintenance costs for the integrated / federated layer. Reducing the member network types by standardizing them and using a common platform to facilitate their compatibility and interoperability could reduce considerably the operation and maintenance costs.
	For PKI solution: - Development and set up costs (one shot) for each member of the federated networks plus the Contracting Authorities	Medium - High	If this key solution uses an existing PKI organization the costs will be reduced to the integration of the PKS to the eAttestations / eCertificates implementation at the level of each member network, federated layer (single validation point) and Contracting Authority. Nevertheless, the costs are considered high due to the number and complexity of the member networks.
	For PKI solution: - Operation and maintenance costs (recurrent)	Medium - High	The more complex the PKI solution adopted and number and diversity of the member networks the higher the recurring operation and maintenance costs will be.
Audit and Continuous Improvement Costs	Audit Costs	High	The Auditing costs are high as they cover the corresponding costs for auditing each of the member networks plus the federated layer. Separated or coordinated security audits imply also additional costs.
	Continuous Improvement Costs	High	The costs due the

			continuous improvements are high and sustainable for a relatively long period of time due to the implicit complexity of the federated networks solution. In order to reduce the costs the improvements should reduce the complexity of this solution by implementing the common platform and improving the compatibility and interoperability between the member networks, between the member networks and the federated layer and between federated layer and the Contracting Authorities and tenderers

Taking into account all elements of costs briefly assessed in the table above, an overall **High Costs Level** is assigned for the **Federated networks and national validation points solution**. To reduce the development and set up costs it is necessary to design this solution from the beginning with a reduced degree of complexity by using standard solution(s) or if not possible due to legacy applications in place , by using a common platform able to reduce or hidden the complexity of each member network and its differences compared with the other member networks. The operation and maintenance costs could be reduced in long term by using shared synergies between member networks and federated layer based continuous improvement activities.

As for the first two key solutions, other costs reductions for this solution are possible, for example, by making this service payable by the requester (normally the tenderer).

7 Conclusions and recommendations

7.1 eProcurement and eAttestations / eCertificates in the broader eGovernment context – the need for a common infrastructure and common development

This Final Report and the preceding Interim Reports focused specifically on the issue of presenting documentary evidence in an electronic form (eAttestations / eCertificates) to a contracting authority in a public procurement at the E.U. level, and attempted to identify issues and solution strategies for this context. However, the issues and solutions examined in this context are not unique, and recur in almost any eGovernment situation. Key complexities include:

- The cross border submission of electronic documentation, including in situations where only paper original documents exist and no electronic equivalents are readily available;
- The validation of this documentation by the recipient, keeping into account the fact that the original document might be in an unfamiliar language and that even its purpose might not be entirely clear;
- The cross border identification of entities when relying only on electronic resources, keeping unto account that the potential group of entities is vast and that there is no unique identifier that can be universally applied;
- The use of electronic signatures as a mechanism of ensuring the authenticity and integrity of a document, and as a means of linking a document to a specific signatory, especially keeping into account the early stages of deployment of PKI solutions in most countries and the difficulty in determining the legal value and reliability of foreign electronic signatures;
- The creation of trust in foreign entities and the information they provide, either directly or via the intervention of an intermediary;
- The creation of suitable mechanisms for the reliable and trustworthy exchange of information between public authorities and authentic sources without harming national and with full respect of data protection principles.

The list of issues above is a fair approximation of the problems that need to be resolved in virtually any European eGovernment project. While the focus of the current study is eProcurement (or rather, the use of eAttestations / eCertificates in eProcurement), the list of problems above is strikingly similar to the issues the Member States need to face in the implementation of the Services Directive[11], as recently studied[12]. This Directive inter alia requires the Member States to implement electronic points of single contact where service providers covered by the Directive, both national and from other

[11] Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market („Services Directive"); see http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0123:EN:NOT

[12] See the recent DG Markt Study on electronic procedures as foreseen under Art. 8 of the Services Directive, as published on http://ec.europa.eu/idabc/en/document/7667/5644

Member States, can electronically complete all procedures and formalities in order to be allowed to start or exercise an service activity in that Member State (article 8 of the Services Directive).

Obviously, the problems that the Member States face in meeting this requirement are largely the same as in the context of public procurement: after identifying themselves electronically, service providers need to present specific documentary evidence (such as attestations, declarations, diplomas etc.) to the point of single contact, so that a valid decision can be made. However, while this information is to be submitted electronically, original documentation is often only available in a paper format – much as attestations in a public procurement context, where electronic equivalents are also often lacking. Thus, it is clear that these two contexts – public procurement and access to the services market – will share similar solutions.

None the less, it is also important to keep the differences between the two contexts in mind. Central among these is the requirement that Member States must meet their obligations under the Services Directive (including the implementation of functioning points of single contact) by 31 December 2009. It is clear that none of the three scenarios described above could be realised by that deadline, even under the most optimistic assessment of circumstances. For this reason, the aforementioned Study regarding the implementation of the Services Directive advocates a more pragmatic approach that favours the increased uptake of a limited number of electronic signatures – preferably qualified or at least based on qualified certificates – as an interim solution to facilitating the legally valid exchange of electronic documentation. While the Study acknowledged that this approach will certainly not resolve all problems in this field, it was considered to be an optimal strategy towards making considerable progress in meeting the deadlines of the Directive, while the eventual outcome could be refined once an initial basic infrastructure would be in place.

The current Study however does not limit itself to the perspective of what is feasible within the next few years, which is why the scenarios proposed above are more far reaching and ambitious than the recommendations in the Services Directive Study. However, one of the principal lessons remains the same: steady progress requires changes to be made in small steps, as these are more likely to be effective than attempting to make giant strides. For this reason, the recommendations provided below do not focus exclusively on the scenarios as defined above, but will also take a look at some smaller steps that can be taken, keeping into account the expectations with regard to the implementation activities surrounding the Services Directive.

The similarities between eAttestations and the Services Directive play out mostly at the horizontal level, in the sense that both deal with the same issues in a different context. But apart from that, it is also possible and even essential to look for similarities at the vertical level, i.e. by seeing which approaches and projects can be tied into the aforementioned scenarios and recommendations in general, and where the possibilities of synergies lie.

Most of the possible synergies have already been outlined in the findings above, but it is worth reiterating them here, if only to emphasise how the scenarios above – which may seem overly ambitious and unrealistic at first – actually have efforts underway already which could significantly facilitate their uptake in practice. Key projects and outputs in this regard include:

- The aforementioned activities regarding the implementation of the Services Directive[13], which are taking place mostly at the national level right now, with support from the Commission. Current efforts are focusing inter alia on improving eSignature interoperability between countries, by focusing provisionally on a smaller number of higher security signature solutions (most notably qualified signatures and signatures based on qualified certificates). These initiatives and the resulting infrastructures could provide a crucial building block to the

[13] See the recent DG Markt Study on electronic procedures as foreseen under Art. 8 of the Services Directive, as published on http://ec.europa.eu/idabc/en/document/7667/5644

development of any of the scenarios above, and specifically of scenarios with a stronger reliance on PKI signature technology, such as the TTP based scenario.

- At a (slightly) broader level, recent studies in the field of eSignature interoperability[14] have called for the creation of validation platforms which could be used for the validation of any electronic signature type, rather than only the higher security solutions targeted by the Services Directive Study. This approach is more complex, but might be more broadly applicable since it could theoretically validate any type of signature being used by public administrations. Private sector initiatives to develop such validation platforms are currently already underway[15].
- Apart from electronic signatures, separate study activities have also been conducted to examine the issues and potential solutions for the electronic cross border identification of entities[16], which is a problem that is only summarily dealt with by the other initiatives. Specific proposals to create federated identity infrastructures have been proposed in this regard, and the aforementioned STORK project (**S**ecure Iden**t**ity Acr**o**ss Bo**r**ders Ac**k**nowledged) will be a logical continuation of this that aims to develop specific European scale pilot applications in a variety of e-government fields. The outcome of this initiative could be a crucial building block in facilitating the identification of entities in a public procurement context, regardless of the scenarios chosen.
- The aforementioned PEPPOL project (**P**ublic **e-P**rocurement **P**ilot **O**n-**L**ine; see http://www.schemaworks.com/20070926ArchitectureforaEuropeanSOIf.pdf) focuses only on electronic procurement. One of the pillars of the project (WP2) is the creation and use of a Virtual Company Dossier, which is conceptually similar to an advanced version of the proposed trusted storage space scenario
- The currently running BRITE project (see http://www.briteproject.net) aims at connecting national business registers to ensure that certain business information can be exchanged across borders in a standardised and interoperable manner. This is essentially a functioning example of the federated network scenario as described above, in which identity information can made available 'on the fly' by utilising company information already registered in public sector databases. It goes without saying that this information can be coupled with other approaches, e.g. by integrating it into protected storage spaces (as e.g. in the Virtual Company Dossier of the PEPPOL project) to immediately add value and exploit synergies.
- In precisely the same way as the BRITE project, the ECRIS system (European Criminal Records Information System) is currently aimed at improving collaboration between European criminal investigators by enabling the exchange of information extracted from the criminal record. In principle, there is no technical reason why such a system could not also be extended to automatically feed information about criminal convictions into a protected storage space controlled by its owner, provided of course that the policy and privacy objections could be overcome, which is no trivial barrier. However, this is another example of a federated network that could be connected to other scenarios.
- With regard to the TTP scenario, the use of apostilles can be considered as an application that already functions in a paper environment (as recognised by the 1961 Hague Convention Abolishing the Requirement of Legalization for Foreign Public Documents), and which has electronic equivalents at the pilot stage. The Convention allows notaries public to add

[14] See the IDABC Preliminary study on mutual recognition of eSignatures for eGovernment applications, http://ec.europa.eu/idabc/en/document/6485.

[15] See e.g. the DNV Validation Authority Service - http://www.dnv.com/services/verification/vas/

[16] See the IDABC Study on eID Interoperability for PEGS, http://ec.europa.eu/idabc/en/document/6484/5644

apostilles (essentially certificates of authenticity) to notarised documents, thus granting them legal validity in countries which are signatories to the aforementioned Hague Convention. Initiatives have been underway for several years now to implement an electronic equivalent of this system, most notably within the activities of the Hague Conference on International Private Law (see http://www.e-app.info/, and http://www.nationalnotary.org/intlforum/index.cfm?text=ifEapp). While these initiatives are currently still at a pilot stage and no large scale implementations exist yet, all indications are that such models could see significant take-up in the future.

- Finally, other initiatives could similarly lend themselves to a TTP approach, including the IDABC IMI (Internal Market Information) System (see http://ec.europa.eu/idabc/en/document/5378/5637). The IMI is conceived as an on-line database and communications system, controlled by the European Commission, that Member State administrations can use for mutual assistance and information exchange, including the validation of specific documents through national contact points. One of the options currently being explored is the possibility to use the IMI system as a support for the purposes of information exchange and validation in the context of the Services Directive. While this is not a clear example of a TTP infrastructure as described in the scenario above (due to a lack of any signed attestation package), it is clear that the concept behind it – the creation of a network of trusted partners – is broadly the same.

While obviously not exhaustive, the list above demonstrates that a large number of projects and initiatives are scheduled or already underway that directly implement some of the aforementioned scenarios in a specific context. This shows that the scenarios are not just theoretical concepts that require fundamental overhauls and redesigning of existing systems simply for the purposes of facilitating electronic procurement; but rather that the scenarios are applications of specific trends that are already underway in the optimisation of public services in general.

This does not mean that the scenarios will be easy or trivial to realise; a sensible balance is needed between simpler short term measures and more complicated initiatives, as will be shown in the recommendations below. However, it is clear that a large number of European eGovernment initiatives in general – including outside of the public procurement contexts – are looking to resolve broadly similar problems in broadly the same way. The results of these initiatives should then be able to logically build on one another, to create a coherent and well functioning infrastructure in which public procurement is simply one more application that the framework can support.

7.2 Step by step development – gradual progress towards a 'full service' future

As noted above, it would be quite difficult to realise any of the aforementioned scenarios directly, and this would certainly not be a goal that could be met in the short term. If progress is to be made within a reasonable period, it is recommended to take a step-by-step approach, in which the initial focus is on creating the basic building blocks and providing basic functionalities to as large a group of users as possible. In a second stage, the aforementioned scenarios can be realised for specific document types – in all likelihood one context or document type at a time – with the eventual goal of combining these scenarios into a joint system that can conceptually support any document type, as described in the ideal solution.

In the meantime, it is highly recommended that the Contracting Authorities in the Member States or European Institutions implementing eAttestation / e Certification solutions at European, national or local levels:

- Keep a backward compatibility with paper based systems (national, local and cross-border): to allow equal chances for tenderers having access to eAttestations / eCertificates services and those having access only to paper based services.
- Encourage the mutual recognition of (e)Attestations / (e)Certificates but also of the related evidentiary documents in order to allow (eProcurement) business continuity regardless of the status of the negotiations concerning the standardization and normalization of the documents used; the legal considerations should be further investigated to better assess the feasibility and applicability in short – medium term.

Below we will provide the main operational recommendations in this regard.

7.2.1 Short term recommendations – improving information dissemination, encouraging administrative simplification, and encouraging the uptake and use of electronic attestations at the national level

As noted above in the description of interoperability challenges to be resolved (section 4.3), there are a number of smaller steps that could be taken by the Member States and at the European level in the shorter term (1-2 years) to facilitate further interoperability initiatives. While each of these steps on their own would not bring about a significant amount of interoperability and would not necessarily facilitate the cross border use of electronic attestations, each of them would provide an important piece of the interoperability possible, and jointly they would act as the foundation for further initiatives, including the implementation of the aforementioned scenarios.

7.2.1.1 Enhancing information dissemination and the spread of good practices

A first major step would be to improve the availability of information on (e-)Attestation practices in the Member States, as described in the form of a minimalist scenario in section 4.5.2. above. To summarise, it is recommended to provide a common platform to the Member States where they would be required to systematically publish detailed information on the attestation types they use, including in an electronic context. This information would include the competent authority for delivering the attestation, content of the attestation (including a specimen sample to show its appearance), its purpose, and specific technical information with regard to formats and any electronic signatures being used in the case of electronic attestations. The purpose of this information would be to give aspiring tenderers and administrations a formal resource that they can consult to verify the validity of the information that they receive, and to gradually build validation mechanisms into new eProcurement initiatives (including in the implementation of the three scenarios described in the roadmaps).

One could consider the European Commission to take a guiding role in this respect, by offering the Member States a platform on which they could publish their own information. The Commission would then act as a coordinator for the collection and dissemination of the information, while the Member States would remain responsible for ensuring that the information itself would be accurate and complete.

The information collected in the course of this study (specifically the collected country reports, as summarised above) could provide a valuable first input in creating such a portal.

As has already been stressed above, this scenario is not a real model for interoperability, since it only concerns the collection and dissemination of relevant information; and this is the reason why it was not chosen as one of the three preferred scenarios for which roadmaps were created However, the availability of such information is a prerequisite for the efficient execution of all other scenarios, as it would be extremely difficult to undertake extensive interoperability initiatives without a detailed and up to date overview of existing practices and choices within the Member States.

Thus, the creation of such a central information portal could provide a first useful building block in the exchange and acceptance of attestations, both in a traditional and in a paper context.

7.2.1.2 Encouraging administrative simplification and systematic risk assessment

A second important recommendation is a lesson that can be learned from the activities surrounding the Services Directive, where roughly similar problems are being addressed. Here too, administrations are faced with the problem that entities would need to provide documentation via electronic means, when quite frequently no electronic documents are available. Obviously this creates a substantial problem: it is not possible to provide an electronic original document (i.e. a document bearing a signature, seal or similar means of authentication) when only a paper original exists.

However, in the case of the Services Directive, this problem has been foreseen and replied to in the Directive itself. As was also described in the aforementioned Services Study[17], Article 5 of the Directive deals specifically with the simplification of existing procedures. This article requires Member States to

[17] Again, see the recent DG Markt Study on electronic procedures as foreseen under Art. 8 of the Services Directive, as published on http://ec.europa.eu/idabc/en/document/7667/5644

„examine the procedures and formalities applicable to access to a service activity and to the exercise thereof" , and to simplify them whenever appropriate.

The article is particularly important with regard to its provisions on documentary evidence. Article 5.3 declares that Member States „may not require a document from another Member State to be produced in its original form, or as a certified copy or as a certified translation, save in the cases provided for in other Community instruments or where such a requirement is justified by an overriding reason relating to the public interest, including public order and security." This article is thus an explicit requirement for Member States to eliminate the need for original documentation, unless a specific and well defined justification exists.

In short, the Services Directive contains a legal requirement for Member States to minimise requests for original documents, and thus to also accept valid substitutes such as copies, unless an exception applies. Obviously, there is no similar legal obligation in the context of public procurements. None the less, as already noted above, the problem is the same, and there seems to be no reason in principle why Member States would not take the same approach to heart. Formulated pragmatically, one way to reduce the scale of the problem is for Member States to adopt alternative approaches to requesting electronic originals whenever this is viable.

This idea is not revolutionary or even novel; in fact it is already being broadly applied in practice, as was shown in section 4.2 above. Specifically, we stressed in section 4.2 that the most common 'solution' to solving the attestation problem (found in 10 out of 32 countries) was to rely on unilateral declarations of compliance from the tenderer. This approach is usually taken either as a way to postpone the submission of attestations until a winning bid has been chosen, or it can replace it entirely. Either way, the main benefit of this approach is that it eliminates (or postpones) the need to validate separate eAttestations, thus allowing the contracting authority to limit itself to the validation of the electronic signature method (if any) that has been used on the declaration itself.

Thus, unilateral declarations of compliance can be seen as a form of administrative simplification, albeit one that seems currently dictated mostly by technical necessity rather than by a desire to simplify life for the tenderer and the administration. None the less, at least as a provisional mechanism until more reliable scenarios are implemented, approaches which allow the tenderer to submit substitutes for attestations can be considered a good practice.

Obviously, a caveat is in order here. It is clear that for many public procurements it would not be deemed acceptable to simply submit a unilateral declaration of compliance. As a document originating from the tenderer rather than from a neutral third party, there is an inherent risk of false declarations being submitted, in the sense that the statements being made by the tenderer prove to be false at a later stage. Administrations wishing to use such systems must therefore be aware of the fact that this risk needs to be managed appropriately, in order to mitigate the chances of awarded contracts being legally disputed at a later stage. Strategies currently used to manage this risk in the surveyed countries include:

- Only allowing declarations as an 'interim solution' for eTendering, i.e. the candidate whose bid appears to be best is requested to provide suitable (usually paper) evidence of his qualifications before the bid is definitively assigned (see also directly below);
- Only allowing declarations from tenderers who have pre-qualified themselves by submitting specific documentation to a trusted third party at an earlier stage; and
- Notifying tenderers before the submission of the offers that their bids and their general business activities can be made subject to thorough legal scrutiny to identify any practices related to fiscal or social fraud, money laundering or similar criminal offences (i.e. creating a deterrent for unreliable candidates by using the tendering process as a mandate to audit

candidates beyond the limits that would apply outside of tendering procedures; this practice has proven to be efficient in the Netherlands).

Thus, the recommendation should not be misconstrued as an encouragement to abandon all attestations in favour of unilateral declarations. Rather, the purpose is to show that interoperability problems can be decreased in scale by conducting appropriate risk management exercises to determine what the precise evidentiary needs are in any given procurement. In many cases, such as lower value bids or when sufficient additional verification measures have been taken, the result could well be that unilateral declarations can be an acceptable solution to simplify interoperability issues.

In summary, it is recommended that Member States conduct proper risk management before requesting specific attestations, and that they consider alternative and more flexible options as well.

7.2.1.3 Encouraging the uptake and use of electronic attestations at the national level

Finally, it was noted in section 4.4. above that electronic attestations in the strictest sense (i.e. electronic documents issued directly as evidentiary documentation by the competent administrations) only existed in very few cases, and that their use in public procurements was virtually non-existent. Common attestations such as tax attestations, social security attestations, extracts from criminal registers, attestations of proper conduct, and attestations of non-bankruptcy, generally only exist in a paper form. This is particularly problematic as these are the types of attestations which are requested very frequently in public procurements.

As noted above, "[t]his means that a great deal of progress could be made if these commonly issued public sector attestations were to be issued in an electronic form. This is after all a logical continuation of existing processes that does not require extensive organisational changes (since the same administrations remain competent for the issuing of attestations, albeit now in an electronic form), and that would be intuitively familiar to all participants in a bid, including the tenderer himself and the contracting authority. Furthermore, for many tenders the availability of public sector electronic certificates would be a sufficient solution, since additional attestations are only infrequently needed. Thus, the availability of such electronic certificates would be an incomplete but significant step in resolving the attestation problem in electronic procurements.

From a practical perspective, most countries will want to rely exclusively on electronic attestations that have been signed by the issuing bodies, to ensure the authenticity and validity of the documents. This also means that the traditional issues related to the use of electronic signatures would need to be resolved, which in the current context specifically means that it must be possible to check the validity of the signature at the time of its creation, along with the mandate of the signatory (to ensure that the attestation was indeed issued by an entity authorised to issue such attestations). These issues are already challenging to resolve at the national level, and in a cross border context this becomes even more complicated due to the larger variety in documents and signatures.

However, it is also important to keep these problems in perspective. It should be remarked that the validity of specific evidentiary documents is determined by the regulatory framework of the country of origin, and not of the country of the contracting authority. This is also true in a paper context (e.g. a country that issues official tax attestations with an official seal cannot reject foreign official attestations if these contain only a signature from the public official that issued them), and there is no reason to change this principle in an electronic context. From a practical perspective, that means that at least a requirement to use specific electronic signatures can in principle not be used to reject evidentiary documents that have been validly issued in a foreign country (e.g. it would not be possible for a country

that uses attestations with qualified signatures to reject attestations containing an advanced electronic signature that were validly issued in another country, or at least not on the grounds that the signature type being used is inadequate). This simplifies the problem somewhat, since the main challenge is then in determining if the attestation is authentic, rather than focusing on the characteristics of its implementation.

In addition, it should be noted that the country profiles bundled in the First Interim Report indicated that the validation of foreign paper attestations is generally a rather informal process, where the objective qualities and characteristics of a document (including elements like appearance, letterhead, seals, signatures and stamps) are evaluated on an ad hoc basis, and where subjective appreciations often act as a substitute for any real certainty regarding the legal validity and content of attestations. In short, the factual reliability of paper attestations in cross border procurements should not be overestimated. While it is clear that electronic processes are typically held to higher standards in this regard, it can be expected given this tradition of flexibility that a certain degree of progress could already be made by making such electronic attestations available to tenderers, and by systematically publishing information on the form and technical characteristics of such attestations, as was recommended above, which would allow contracting authorities to at least conduct a prima facie verification of foreign attestations. This would bring the process more closely in line with procurement traditions in a paper context, and could thus already act as an enabler for the use of electronic attestations .

For this reason, it is recommended to encourage countries that issue such certificates to make electronic versions available to the public. This refers specifically to the attestation types commonly issued by public administrations and which constitute the bulk of the evidentiary requirements in most procurements, and most notably:

- Extracts from criminal registers or the corresponding court certificates, as the key document to show non-conviction in criminal matters; this also includes attestations of good behaviour in countries which use such documents instead of extracts or court certificates;
- Extracts from commercial registers or court certificates attesting to non-bankruptcy; again this includes attestations of good behaviour in countries which use such documents instead of extracts or court certificates;
- Extracts from commercial registers to show enrolment in a professional register;
- Attestations showing compliance with tax regulations, including VAT legislation if applicable;
- Attestations showing compliance with social security obligations.

It goes without saying that this recommendation only applies to countries which already issue such attestations in paper form, and that it should not be misconstrued as a recommendation to start issuing these attestations in countries that have already implemented other means to show compliance with the relevant requirements.

The introduction of official electronic substitutes for each of these document types would already provide tenderers with the means to provide official electronic attestations to foreign contracting authorities, even if it would likely remain difficult initially for those authorities to validate such documents in a satisfactory manner. As a way of supporting this process, existing initiatives in countries that already publish such attestations should be published and disseminated as good practices, in order to encourage and support spontaneous harmonisation. This is of course a part of the aforementioned recommendation of publishing and disseminating current attestation practices (section 7.1.2.1 above).

7.2.2 Longer term recommendations – implementation of the scenarios in coordination with existing initiatives

The small steps described above collectively already provide some useful building blocks in solving the eAttestation problem. If applied consistently in all countries, tenderers would be able to provide most types of attestations and documentation in an electronic form to the contracting authority in a majority of procurements. None the less, in order to provide a more satisfactory possibility to contracting authorities, other and more systematic approaches will be needed. While a general uptake of electronic attestations would indeed ensure that tenderers could easily provide their attestations to foreign administrations, this would not resolve all problems.

Most notably, foreign administrations might still be unable to validate the signatures used on such attestations, or to determine the identity and legal capacity of the issuer. This is a problem that is difficult to solve, due to the enormous number of administrations that are involved in the issuing of these attestations (e.g. certain attestations might be issued at the commune level), which means that even in a strongly harmonised market there would be a very large variety in document types and signatures being used, making the validation process particularly complicated. In addition, for the same reason it is clear that the general uptake of electronic attestations will not be a quick process: while it is likely to occur at some point in the future, the reality of all administrative bodies (including at the commune level) being capable from a technical and know-how perspective to issue electronic attestations instead of paper ones will simply not materialise in the shorter term.

For this reason, other mechanisms should be considered that are capable of creating trust in attestations even when the actual issuer is unknown to the recipient, and that are capable of working around the restriction that attestations will likely retain their paper form in most countries for the years to come. Such mechanisms should also be able to handle other attestation types than those noted above, and specifically attestations that are not issued by public administrations, such as diplomas, certificates of conformity with specific standards and bank attestations. After all, it must also be possible to submit these documents in an electronic form, even when no electronic originals exist. To solve this problem, the three specific scenarios that have been described above come into play.

It is clear that the scenarios have a different scope and a different application in practice. Without going back to a full description of their characteristics, strengths and weaknesses (all of which have been summarised in section 4.5, and in greater detail in the Third Interim Report), their main attributes from a pragmatic perspective can be summarised as follows:

- A scenario based on TTPs signing attestation packages can handle any document type equally well, regardless of its origin, since trust in the contents of the package is inherited entirely from the signature of the package itself. Thus, it is conceptually simple. Furthermore, out of the three scenarios, this is the only one that can handle situations where only paper originals exist (by scanning the originals and adding them to the bundle). However, the downside is that it requires a network of TTPs to be set up, which need to provide additional services (beyond simply signing the package) to make their services valuable to the end user. Thus, getting broad adoption could be complicated in practice, especially since only few countries have a tradition in TTP systems.
- A scenario based on trusted storage systems is very flexible, and scales well in the sense that it can start as a simple content management platform (with limited added value) and that it can grow to integrate more reliable information, including from official sources (thus adding substantial added value). However, the scenario struggles to offer added value in cases where no original electronic data is available (i.e. when information cannot be extracted from an

official database), since the tenderer can then do little more than simply upload a copy to the system. Thus, the scenario is very useful as a tool to bundle and aggregate information from official and reliable sources. For other information – including most types of information provided by private parties – the scenario will typically not be able to add value, due to the absence of a trusted official electronic resource to exploit.

- Finally, federated networks often the greatest added value, as they allow authentic information to be exchanged directly, thus minimising costs, efforts, and risks of data corruption. However, the scenario can only be implemented when databases containing authentic information are already available, and when this information is already fairly harmonised/standardised, since data exchange requires common standards, formats and semantics. This makes the scenario highly useful to exchange information stored in public databases (as witnessed by the BRITE and ECRIS examples), but almost impossible to apply in cases where databases are unavailable or where the information is not easily comparable.

Summarising the role of the scenarios further, it is clear that federated networks offer an ideal solution, provided that the conditions for its usability (usable electronic database – comparable data – agreements with regard to access and re-use) are met. Furthermore, federated networks offer synergies with the second scenario based on trusted storage systems, as explained above: federated networks offer the possibility of aggregating data regarding an entity directly into its own storage space, thus improving the usability and value of the storage space.

Thus, while each of the three scenarios is of course intended to be used as a communication mechanism towards the contracting authority, interactions between different scenarios are possible to a certain degree, as shown in the table below.

Data exchange from/to	**TTP**	**Storage space**	**Federated network**
TTP	N.A.	Yes: signed packages can be uploaded to the storage space	No. Federated networks only use trusted internal sources
Storage space	Yes: the TTP can obtain information published on the storage space and sign it	N.A.	No. Federated networks only use trusted internal sources
Federated network	Yes: the TTP could contact a national/regional contact point of the network and obtain information there	Yes: data from the network can be aggregated through the storage space	N.A.

It is thus possible for the scenarios to interact to a certain degree. This is important, since it also implies that it is not necessary (or even particularly plausible) for one country to choose one scenario for all of its documentation types. It is perfectly possible and even recommended for countries to consider their own preferences and policies when choosing a particular approach for a particular type of electronic evidence. This is a choice that can be left to the Member States themselves.

At the European level, the key recommendation with regard to the scenarios is to monitor and stimulate the linking of these scenarios to existing or planned eGovernment initiatives that lend themselves to extension to public procurement, in order to benefit optimally from potential synergies. However, given the need for further steps to be taken at the national level (as noted in the short term recommendations) and given the current early status of crucial new initiatives in public procurement and beyond (including PEPPOL, BRITE, STORK and others) it does not appear to be beneficial at this stage to initiate separate new initiatives to force the uptake of specific scenarios. Structural support for their take-up in existing initiatives appears to be the more productive option.

With regard to the future of specific scenarios at the European level, as noted above, federated networks can be considered as something of an end point, due to the significant added value and simplification that they offer, at least in cases where their implementation is possible. The BRITE and ECRIS projects are good examples of this, and it is conceivable that similar projects could be established at some point in other sectors. Possible examples of this would be federated networks related to income/corporate taxation, solvency and social security, allowing the respective attestations to be replaced. Thus, future initiatives in these sectors should be monitored for possibility of integration into the broader public procurement ambitions.

The development of the other two scenarios (TTPs and trusted storage spaces) and the need for further initiatives at the European level to stimulate this depends largely on the experiences that will be gained in currently ongoing projects, including PEPPOL, the IMI system and e-Apostille projects. These projects and initiatives can be expected to show the possible business case for these approaches, and whether or not specific additional efforts are desirable to further encourage their uptake.

7.2.3 Conclusions of the Key Solutions Costs Analysis

The following conclusions came out from the Costs Analysis made for the eAttestations / eCertificates Key Solutions:

- **The Federated networks and national validation points solution** is expensive from development, set up, operation and maintenance viewpoint for the eAttestations / eCertificates Authorities and evidentiary document issuers. Nevertheless the Contracting Authorities are advantages by this solution from financial view point
- **The Single trusted storage point of electronic attestations solution** is more costs affordable from private entity (tenderer) viewpoint but creates a work overhead (and thus additional costs) for the Contracting Authorities and eAttestations / eCertificates and evidentiary documents issuers perspective as they need to upload / download the documents hosted by the store space.
- The estimated costs for **the single electronic attestation package signed by a trusted administration or private sector trusted third party (TTP) solution** are between the costs of the other two key solutions but they can be reduced in short – medium term

7.3 Longer term goals - Coordination between the scenarios – roles and potential evolutions

As each Member State has the freedom to implement the most suitable solution taking into account the current situation, ideal solution and other specific factors (political, organizational, financial and technical), sharing synergies between national or cross-border eAttestation / eCertification projects in order to ensure their compatibility, interoperability and convergence is of critical importance.

The roadmaps described for each of the recommended key scenarios and based on the strategy defined for the Ideal Solution show that it is possible to simplify the work of the contracting authority and in the same time have a certain level of compatibility between various stakeholders especially at the level of

- eAttestations / eCetificates /eBundles and related evidentiary documents standardization and normalization and their availability in electronic form;
- a common transport mechanism able to facilitate the exchange of eDocuments regardless of the Attestations / eCertificates applications used by the information exchanging parties.

Nevertheless, this improved compatibility and interoperability does not mean that one can move from one recommended key scenario to another easily. Such a decision should be taken, eventually, after a study on the impact of such move will have on the continuity of the eAttestations / eCertifications service and on the end-users.

In order to take an educated decision, some mechanisms able to help sharing synergies are shortly described below:

1. One simple mechanism to collect and disseminate information about various national or cross-border eAttestation / eCertificate / eProcurement initiatives is to set up **a eAttestations / eCertificates / eProcurement information web site** able to collect and publish useful information about successful / unsuccessful eAttestations / eCertificates / eProcurement past projects but also about current and future initiatives in this domain. The web site could be run and maintained by the European Commission or be outsourced to an external contractor and run and maintained on behalf of the Commission;
2. Set up **an eAttestations / eCertificates / eProcurement expert working group** in charge of
   - identifying all new initiatives in the domain
   - gathering information about them
   - publishing the information about the eAttestations / eCertificates / eProcurement projects including analysis about the positive and negative lessons learned
3. Facilitate the implementation of eAttestation / eCertificate / eProcurement solutions by improving their financing mechanisms or their access to cheap financial sources. For example the implementation of an eAttestations / eCertificates solution at national or cross-border levels can be stimulated by co-financing it from national and European funds.