eDoc Workshop

18 April 2007

Brussels, Belgium[1]

[1] This document is the report of the eDoc Workshop organized by the DG Information Society and Media of the European Commission, and held 18 April 2007 in Brussels, Belgium. Although every effort has been made to ensure the accuracy and relevance of the contents, they do not in any way represent the official position or policy of the European Commission

TABLE OF CONTENTS

1. Introduction

1.1. Ministerial declaration[2]

The Ministerial declaration of 24 November 2005, approved unanimously in Manchester UK, focused on delivering clear social and economic benefits to citizens, businesses and governments, through 4 key challenges to governments:

1. No Citizen Left Behind
2. Efficient and Effective Government
3. Delivering High Impact services designed around customer's needs
4. Key enablers for eGovernment (*Simple and Secure access to online public services*)

The declaration identified the implementation and use of eID and the recognition of electronic documents and their electronic archiving as key enablers.

1.2. Signpost document, Building Blocks, Roadmap

The document "Signposts towards eGovernment 2010"[3] published in 2005 by the European Commission Information Society and Media Directorate General, discussed in more detail a number of objectives devised to improve Europe's social and economic development.

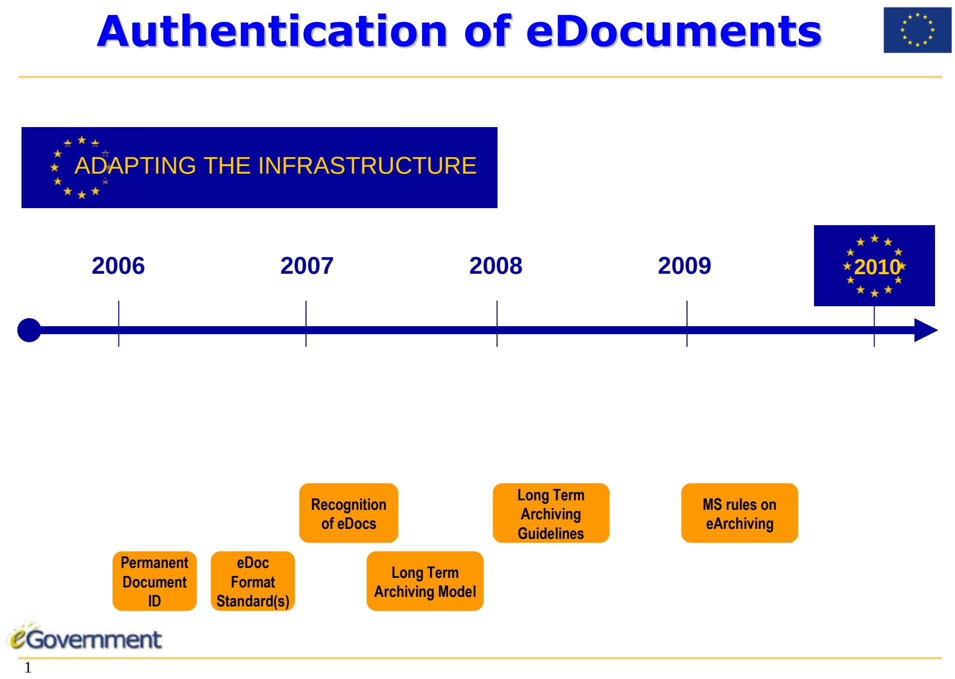
The document points out that as online transactions become more widespread, so will the uses of electronic documents. In particular, it sets out the goal that by 2010 Member States will have agreed a framework for reference to, and use of, authenticated electronic documents across the EU. The Signpost document represents a first step in establishing a roadmap for the achievement of this goal.

The document identified a number of "Building Blocks" laid out in time for efforts related to eID (electronic Identity) and "electronic document authentication" (a.k.a. "eDoc") efforts, which represent areas of activity which need to be conducted during the period leading up to the 2010 target to achieve the desired objectives. The elaboration of these Building Blocks should lead to the establishment of the roadmap for implementation of eDoc.

The context for the use of electronic documents is the delivery of interoperable eServices by EU Member State administrations under the eGovernment program.

[2] Available at: http://archive.cabinetoffice.gov.uk/egov2005conference/documents/proceedings/pdf/051124declaration.pdf

[3] Available at: http://europa.eu.int/information_society/activities/egovernment_research/doc/minconf2005/signposts2005.pdf



Authentication of eDocuments

ADAPTING THE INFRASTRUCTURE

As indicated via the timeline above, the essentials identified via the "Building Blocks" for electronic documents include:

- Permanent identifiers for electronic documents so that they are uniquely identified and identifiable
- Permanence of the electronic documents beyond any specific technology, medium, or platform (format standardization)
- Recognition of authentic electronic documents produced in one EU Member State as being authentic in any other EU Member State
- Long-term storage and archiving of electronic documents across the EU according to an established model & guidelines, and uniform rules

1.3. The eDoc Pilot

The draft CIP workprogramme[4] directly addresses mutual recognition and interoperability of electronic documents as follows:

> *Mutual recognition and interoperability of electronic documents is a pre-requisite and key enabler for many eGovernment services. This will require policies, practices and standards on electronic document format, to establish how electronic documents are identified, authenticated and accessible, and also long term archived. An agreed Framework for electronic documents should ensure permanence beyond any specific technology, medium or platform and shall guarantee availability and allow users to identify which representations of any document are considered authentic by a Member State or associated country and*

[4] Available at: http://ec.europa.eu/information_society/activities/ict_psp/index_en.htm

recognised as such in another. Pilot actions addressing this goal should deliver and test:

- *an agreed framework for reference to, and use of, authenticated electronic documents across the EU. Such documents and the infrastructure supporting them shall be able to include text, picture, audio, and video content;*
- *electronic archives being able to store documents in acceptable formats for as long as is necessary to fulfil specific legal or cultural obligations;*
- *eServices being able to interoperate across the EU, through identifiable and authenticated official electronic documents;*
- *openly available Common specifications, for interoperability of electronic documents.*

The common specifications developed by the pilot shall be publicly available for all Member States or associated countries. Entities responsible for the definition of national standards and systems for electronic documents are expected to exploit the results of the pilot in view of work towards an EU-wide common specification

1.4. The eDoc Workshop

The objectives laid out in the above can become a reality by 2010 if the Member States collectively establish a document recognition framework considered as acceptable throughout the EU, which also takes into consideration technologies that will enable the creation, use and long-term storage of authenticated representations of documents.

This framework is/can be formulated as follows:

1. An EU agreement on electronic document formats (which may include elements of all media types such as: text, picture, audio, and video), recognized by all administrations as equivalent to their physical representations (paper, cassette, etc.)
    - Identifiable and addressable official documents ensuring that they can be authenticated and assert their official and reliable nature.
    - Authenticated electronic documents. This includes interfaces and methods for electronic identification and authentication, in particular the data, security, encryption, authentication and policy issues relating to the proposed eID framework;
    - due attention will be paid to existing standards in the relevant domains, for example from ISO/IEC, CEN, W3C and OASIS
2. An EU agreement on formats and methods deemed acceptable for long-term storage and archiving, whether signed or not.
3. A common understanding within the EU regarding permanent infrastructure to be made available for long-term document storage and authentication.

The complexity of the eDoc area is well recognized, and there is much to be done. As a first step in the development of this framework, a Workshop on electronic documents (eDoc) was held on 18 April 2007 in Brussels, Belgium. Its explicit goal was to collect and discuss opinions on these specific issues.

In order to stimulate reflection on the topics and facilitate the upcoming discussion, a set of questions were formulated in advance of the workshop and distributed to the participants (see Appendix)

The eDoc area is complex, and achievement of the objectives laid out will require concerted effort, by all parties, in multiple areas (legal, organizational, technical, etc.), in parallel, conducted in a very efficient manner.

2. eDoc Workshop Topics

2.1. Introduction

In line with the draft CIP workprogramme, a number of questions were formulated to stimulate reflection and promote the objectives of the workshop set out the key goal of collecting and discussing opinions.

In addition, as eDoc will be subject to a roadmap which runs in parallel with the roadmap for the introduction of eID, this roadmap will have to be expanded, made operational and validated.

Furthermore, in view of the forthcoming call for proposals, on type B pilot in the context of CIP ICT PSP, the eDoc Workshop participants also sought to identify how such a pilot could support (and be aligned with) the SignPost document & corresponding ministerial declaration.

The eDoc Workshop itself was organized around 6 main sessions dealing with specific topics, and designed to tackle in a comprehensive manner the set of necessary issues:

- Target use-cases of the eDoc framework
- Interoperability requirements
- Mutual recognition
- Archiving and Supporting infrastructure
- The roadmap
- The Pilot

In each session there was key speaker/presenter who outlined the issues to be addressed, followed by a general open discussion of those issues. For each of these sessions is described below the general goal of the session in terms of the subjects to be covered, and any conclusions reached or issues raised during the discussions.

2.2. Target use-cases of the eDoc framework

The key question to be addressed was delimiting the boundaries of which electronic documents are under consideration by the framework. The scope is in general limited to a certain set of selected documents which have official/legal standing within the framework of the provision of eGovernment services to Citizens and Businesses. There could be some relation with PEGS (Pan European Government Services).

Examples of use cases include the presentation of electronic authenticated documents (birth certificate, diplomas, etc.) produced in one member state to a second member state in the framework of requesting some service from the second member state (such as establishment). It was specifically soght to consider and discuss examples taken from existing implementations.

<u>Discussion</u>

For some member states, the scope of coverage could include any document produced by the administration and having legal weight. Administrations must be able to produce all official documents in electronic format and signed electronically by 2010. However, it is foreseen that both worlds (paper and electronic) will be needed.

The example of birth certificate demonstrates perfectly the dimensions of the problem: what if a citizen pays for a digitally signed copy of a birth certificate, stores it on some computer somewhere which is stolen or destroyed? Can he get another copy? Does he have to pay for it? Would he be willing to pay again?

One opinion was that one of the most important use cases is the publication of laws. In one particular Member State, laws are not considered to go into effect until the electronic versions are signed and available. There were divergent opinions on this. In some Member States, every document produced by the administration must be signed; in others signatures on such documents are rarely if ever used.

The question of verification of authenticity was considered an important aspect. With paper, it is quite rare to have a real check on a manual signature - people usually only ask to see a signature and do not verify that it is authentic or valid. The actual European directive does not require verifying electronic signatures; electronic signature verification is a voluntary process. This being said, verification of electronic signatures is a straightforward from the technical perspective. Whether they will be used (in the light of how infrequently existing ones are used) is another matter.

Some participants thought that eDoc could be thought of as another eGovernment service; others felt that the eDoc concept shouldn't be a dumping ground for functionality or conceived of as all-encompassing. Another opinion offered was that eDoc is not about the *use* of documents but rather about the *existence* of electronic documents. These two topics should not be mixed up.

The question is raised that if there are several copies of a birth certificate for a given individual floating around (for example in the central archives of different MS administrations), which is the "key" one? Or which one is considered legally as taking precedence over all others? It appears to be an open question.

2.3. Relevant & applicable interoperability requirements

This session essentially focused on standards and document types, but not on the selection of solutions. A debate on the relative merits of different formats such as PDF, XML or to debate OpenDoc vs. the alternatives was not in the scope; Rather, the focus was on the technical requirements on the standards that would allow eDocs (from the use-cases discussed in the previous session) which were generated in one MS to be used directly in a second member state.

Questions such as how that the integrity and origin of documents in a cross-border context can be ensured were covered. Thought was given to the independence between the document type and the use-case(s) in which it is used.

The context of the interoperability requirements under discussion is both cross-border and cross-sector.

Discussion

Standardization of the digital signatures themselves and their interoperability was a key focus of the discussion, if not the key to achieving interoperability of electronic documents.

It was pointed out that while in previous periods there had been a too diverse set of competing possibilities, current standardization activities are proceeding well. That being said, there are still too many variations possible/in use. It was pointed out that no two implementations of XADES are the same (re: options within blocks).

The question of whether only individuals can sign a document or can also organizations sign a document? The example of passports was raised. In the case of a passport, it doesn’t make sense for a person to be signing the document; some participants felt that a physical person must always sign; others felt that the introduction of a concept such as an electronic stamp was warranted.

This leads directly to the subject of qualified signatures. There are differences in implementation in different Member States, and a number of different schemes are in fact possible, but the two key variations discussed were:

- A qualification can be included in the signature (as done in some MS)
- A qualification can be a second signature attesting to the role of the signer

The main point made during the discussions is that it would be practical to define strong requirements for some limited set of elements; that collectively, the EU needs to invest in common formats and common signature schemes. However, the question of the definition of this set of minimum elements, how and by who are beyond the scope of the workshop; however, it is pointed out that:

- Legislative changes could be required for this, although the commission has no plans or discussion on this at this time
- If a list of things to be considered to establish such a list could have a positive impact on moving the pilot forward

It is pointed out that electronic signatures require maintenance (for example changes in encryption technology mandated by changing conditions of relative strength of the algorithms employed), and the concept of the private eNotary service (which would re-certify documents as authentic on a periodic basis, as required) is introduced.

2.4. Mutual recognition of authenticated eDocs

This session focused on business processes and legal provisions required for the aforementioned recognition of authenticated eDocs. Technical issues were not to be addressed (as they were covered in previous sessions). Subtopics in scope included: what do the Member States have to do in order to comply with the EU directives?

This session also sought to identify what is blocking (at both procedural and legal levels) one Member State from recognizing the authenticated electronic documents produced by/in another Member State?

Discussion about the meaning of "authenticated" in this context and the consequent implications were in order.

It was hoped that the discussions would result in enough information or conclusions to produce a detailed explanation of how mutual recognition would work in practical terms.

Discussion

It was pointed out that existing national legal frameworks in many cases are not sufficient.

- The process of translation of EU directives into national legislation across the EU has not yet been completed, and has not lead to uniform results across the EU. The example of a citizen coming in to a government office with some documents on a USB stick, and looking for a stamp of some kind on his document, should be addressed.
- There are practical considerations: government employees and citizens alike need to be able work with what is supplied to them

The context of when/where a document is signed can be important depending on the context, and must be considered independently of the underlying data. In a related point, a document isn't the same as the data it contains; an authentic document coming from a government/administration is an assertion at a specific moment in time.

There is no consensus on what constitutes an authenticated eDoc

- In some MS, when data is put into a "recognized" repository/archive (and from which an eDoc may be extracted), it is considered as "authentic": there is national legislation in force to this effect.
- Today governments are willing to make legally binding decisions on the basis of non-secured paper documents (begging the question as to whether this effort should aim at duplicating the situation as it exists in the paper world – easy – or taking the opportunity to introduce top-down security which may not resemble completely the current way of doing business in such cases)

- In an electronic signature, in many cases it must be possible to retrieve information on the signatory of an official document (name, official position…) for the signature to be considered legally valid, or at least for the document to be considered as acceptable to a relying third party.

- Since it is mandatory to exchange electronic documents between Members States (MS), a practical approach would be to stop trying to solve all the problems at once before acting on the subject. It seems relatively easy to achieve the same level of security as the current paper system (since there is virtually no security) or focus on some specific documents where it would be easy to protect them.

- An actual case was cited in which a judge ruled on the legal requirements with respect to qualified signatures: a document was submitted in evidence, which did not indicate the legal capacity of the signer (the letter did not contain a letter head, organizational stamp, or official title of the signer); it was ruled that this was not enough and the document was rejected.

- In matter of fact however, the present system is not SECURE; it is only pragmatically accepted.

- As touched on in previous sessions, authenticity is also concerned with qualification of signatures with regard to their origin. In technical terms (and relating explicitly, directly to the use of digital signatures) there are (roughly speaking) two solutions (or more accurately “major approaches”) to the problem of determining the legal capacity of the creator of qualified signatures :

    - Object identifiers (embedded in certificates)

    - “Organizational stamps” (a second certificate linking the signer and the document signed in the signer’s capacity)

- Another example given in the context of a courtroom: a document submitted by one party and accepted by both parties and by the judge as authentic becomes authentic

- Another example given in the context of reply to public tenders: currently it is often required that a tendering company submits an attestation of compliance with some regulations in force (such as social security contributions); instead of supplying a signed certificate (either paper or electronic) a real alternative is for access to be given to the beneficiary to lookup the information for themselves in the relevant government/MS database(s); For some MS this appears to already be the case, for others there continues to be a formal separation. This highlighted the different approaches followed in different member states, deriving from their different legal traditions (for example, the distinction between “common law” vs “roman law” systems; or the distinction between more formalized western and central European legal systems, and generally more flexible Scandinavian systems)

The evolution in the field of eDoc is slow but is proceeding. Some of the barriers known at this time include:

- There is no way to easily know the capacity of the signatory at the time the document is signed.

- The directive is not about signatures but about certificates. There is a need for a new legislation.

- On an EU-wide scale, documents signed in one country will not be recognized in another country since there is no infrastructure to do so. There is a clear need to have some application (centralized or one application per country) accessible to the public to verify the electronic signatures. This application(s) should be offered by the government(s). We are not talking here about full interoperability but rather a step-by-step approach starting with verifying a signature of a particular country publicly.

- In order for MS A to be prepared to accept documents from MS B as authentic, they will want to know about the procedures behind the signatures, and the system behind it, such as the infrastructure, business realities, etc. The absence of an established agreed framework on these procedures providing a "circle of trust" constitutes a significant barrier to mutual recognition of electronic documents.

- Infrastructure is the main/most important barrier (for validation); in particular, often when we are presented with an eDoc that is supposed to be authentic, we don't know how to validate; it would be very helpful if MS's could develop/offer applications to validate specific signed documents (not ALL eDocs but a specific small set); Different solutions to this problem were presented:

One MS offers a public service application for verifying documents; In other MS, it is the signed document itself that "tells" (or provides the means via hyperlinks) where / how the document/signature can be validated. It is not a global solution that is being sought, as there will always be a need for specific signature types for specific documents and applications, and hence different validations.

The first step of validation is to verify if a document is valid where it was produced ; it is only at later/ 2nd step where on is concerned with whether its acceptable for a given usage

It was pointed out that there is a distinction between the validity of a particular electronic document, and the validity of the data it contains (from a business or specific application perspective); this distinction was more pronounced in some MS than in others

There was some disagreement on the question of "term of validity", for which some documents such as passports or other ID papers, have fixed terms (with good reason); Some participants felt that eDoc is not about the application-specific handling of documents. In the end this was merely a misunderstanding over terminology; the conclusions that can be drawn are that:

- Due to the requirements of certain eDocs, such as identity papers, period of validity must be an optional attribute of eDocs (not all eDocs need to have a validity period, expiration date, etc.)

- The impact of this optional attribute on how the document is processed/used/not used/etc. is entirely application-specific and is not a part of the eDoc effort or specification
- A document that is signed remains (in perpetuity, or for the life of the document itself, whichever is shorter) signed, as the electronic object which constitutes the electronic signature continues to exist;
- An electronic signature on an eDoc can be revoked or nullified (in a variety of ways, for example as the revocation of a certificate), but this adds to the eDoc, additional objects and does not remove the original signature object

2.5. Requirements for supporting infrastructure, architecture, etc.

This session was intended to cover a variety of miscellaneous topics, including architecture, requirements for supporting infrastructure, long term archiving of authenticated eDocs, etc. Provided that a well defined and agreed set of eDocs are implemented, are mutually recognized, and comply with agreed EU technical interoperability requirements, the question is: what else is needed to support the use-cases in terms of supporting infrastructure, what kind of architecture would/could the solution have, what networking infrastructure to provide for secure transport of eDocs between entities (MS, …), would be required, and what centralized components or MS-located components in a common infrastructure should be put in place? The infrastructure subject also particularly focuses on the important issue of the long-term storage/archiving of eDocs, repositories, etc.

<u>Discussion</u>

Many historical documents that will end up being stored in such archives will be scanned representations of physical documents, stored as image files. They present specific challenges for organization, storage and retrieval.

For the moment, the most advanced archiving systems have limited scope in terms of the type of electronic documents stored there, the types of formats expected and the interface/controls.

Some key characteristics of an advanced system as implemented by the AT administration were reviewed:

- There is an implicit trust between the government and lawyers for the exchange of old documents that are not electronically signed. The state of mind is that a document is considered as an original until it is proved as not being one.
- The AT archival system that was described only covers a subset of eDoc's produced by the AT administration, namely: land registry and judicial/court records; access to these documents is unrestricted, all are public; in the future will be implemented access controls which will allow only the "filing person" to access/retrieve any given document, or another duly authorized to do so by this person.

The delivery of eDocs is an important subject that until now was not discussed in sufficient detail; in the EU for the moment cross-border exchanges are very much ad-hoc bilateral affairs.

It was pointed out that archiving has to be built into the eService/eGovernment processes, so that we are sure that in 10 years documents used today will still be available.

Concerning the topic of a (centralized) repository of authenticated documents, it is not sure whether this is needed since there are not a lot of electronically authenticated documents and that usually a document is created and authenticated when it is required (for example, a criminal record summary for a citizen is created/signed when asked for from the information in the databases and not stored authenticated in a repository). In any case, if such a repository is created, access must be guaranteed for all MS.

2.6. Towards an actionable eDoc Roadmap

The intention was to gather sufficient information to begin the process of "fleshing-out" the eDoc roadmap into a viable and actionable plan. As the "Building Blocks" are not described in detail, it was hoped to gather some details, or at least to better visualize the path (specific steps to be taken, specific information to be gathered) to an actionable roadmap and eventually to a workable global plan. The starting point is the current understandings of the "Building Blocks", and the desired endpoint is a common understanding thereof, at a level of detail including: activities encompassed, their inputs, expected outputs, etc.

The results of the previous sessions will need to be evaluated, reviewed, and synthesized in light of this objective.

Discussion

A first proposal for an eDoc roadmap based on the Building blocks agreed/provided in the Signposts 2010 paper, and using the roadmap established for the parallel eID-related efforts as template/starting point for discussion was given

It was noted that there were a number of overlaps with the eID (first by presenter then by some in the audience); (as well as common activities relevant to both efforts, perhaps in varying ways and to varying degrees) it was noted explicitly that there were dependency links and common activities between the two efforts, some of which are obvious, some still remaining to be discovered but that all would have to be explored in much more detail and documented as input to a subsequent draft of the eDoc roadmap

It is mentioned that IDABC is already working on some of the presented topics and that work should not be redone. There is a need to talk with other workgroups to make sure that similar topics are not reworked.

Since the eID project has been developed further, eDoc should focus on what eID does not do. Knowledge from eID must be reused. It should be made clear what the core items for eDoc are.

The issues of scope and funding for eDoc are raised. Reference was made to the ICT PSP draft work program, where eDoc funding was included for type B pilots.

An updated version of the roadmap with a clear definition of the basic blocks will be made available. It will then be presented to the MS for further review.

2.7. Achieving an eDoc Roadmap through potential Pilots

The goal of the session is to identify/catalog explicit links between pilot activities and roadmap/building-blocks elements and also to consider how selected use cases for a pilot would enable verification of eDoc functionalities.

The draft CIP workprogramme defines the scope of these activities.

Discussion

The ICT-PST draft workprgramme for 2007 sets out clearly the requirements of the eDoc (*Mutual recognition and interoperability of electronic documents)* pilot (Type B). These are also fully in line with the text for a framework on interoperable and mutually recognizable electronic document for eGovernment services, in the Manchester eGovernment Ministerial Declaration in 2005 and the i2010 eGovernment action plan. In this respect, any pilot on eDoc should ensure that Member States have a key role in the implementation, and also on common specifications for the eDoc. The potential wider impact of eDoc cannot be achieved without such commitment from the Member States. However, it is clear and well known that technology expertise lies with the industries, and effective co-operation between the industries, Member States and the Standardization bodies would be key to success of a pilot on eDoc. It has also been noted that the use cases chosen for the pilot should ensure that the different functionalities of the eDoc should be tested and verifiable through them.

3. Conclusions

3.1. Use cases

- There has been general agreement that birth certificates and education diplomas are within the scope of eDoc; a number of other documents produced by administrations for the use of citizens and businesses generally are also considered in scope
- Verification of signatures is important and needs to addressed in the resulting framework
- Originality of eDocs (if multiple versions of a document exist in electronic form, in different locations, possibly in different countries, which is considered as the "original"?) needs to addressed in the resulting framework

3.2. Relevant & applicable interoperability requirements

- Standardization of the digital signatures themselves and their interoperability is a key aspect of these "interoperability requirements"; while progress is good, there are still too many variations possible; One practical approach could be to define strong requirements for some limited set of elements; another approach could involve a gateway/translator between implementations
- Collectively, the EU could benefit substantially by investing in common formats and common signature schemes
- The final conceptual model must address the question of the identity of "signers" (individuals vs. organizations), as well as the closely related question of "qualification" of signatures (legal capacity of the signer); a number of different basic schemes are possible, and some are already in use in some Member States
- From a technological standpoint, electronic signatures require maintenance (to preserve the "authentication strength"); different approaches are possible, including the use of a private sector "eNotary" service, but this is an archiving issue (see section 3.4 below)

3.3. Mutual recognition of authenticated eDocs

- There are inconsistencies in the translation of (relevant) EU directives into national legislation across the EU, and the results have not been uniform
- Consensus needs to be reached on what constitutes an authenticated eDoc
- Distinction can be made between the authenticity of a signed document and the authenticity of the data it contains
- Current paper-based rules do not provide a high level of security but are widely accepted; whether the same level of security is acceptable for electronic based transactions (some of which can take place online, remotely/at a distance) is an important question to be considered; it is a question of risk
- There are several distinct (culturally based) legal approaches or philosophies underlying national approaches (legal, organizational, environmental) in the EU, which could present barriers to interoperability and mutual recognition if not adequately considered
- The establishment of trust is a key goal, and will require concerted and coherent efforts in a number of areas in parallel; it is not just a technical issue
- Validation of the authenticity of eDocs and the signatures in particular is a key element of the framework
- Electronic documents can have terms of validity (in scope of the framework), but may be *processed* differently depending on when they are presented, delivered, etc. (not in scope of the framework)

- Signatures can never be removed from an eDoc, but their validity can be revoked

3.4. Requirements for supporting infrastructure, architecture, etc.

- The framework has to address the following aspects:
    - Data protection of the data contained in the eDocs in the archive(s);
    - Access to the documents stored within the archive(s);
    - Searching (and possibly indexing of) the archive(s);
    - Architecture of the archive(s) (centralized/decentralized, sector-specific or other schemes for subdivisions, or by doc type, etc.);
    - The definition and implementation of adequate handling rules allowing for the fulfillment of the maintenance requirements on the eDoc archive(s), including strength of authentication/signatures (see section 3.2 above)
- There are a variety of practical considerations, including the loading of older, originally paper-based documents directly into archives (such as: different level of verification of their authenticity; who is their owner when all parties are deceased, etc.)
- Archiving systems currently in use while highly successful are limited in terms of the amount and variety of documents they handle, and in terms of the length of time they have been in operation (eDoc archives are intended to be in operation indefinitely); There is limited experience with handling of the amount and variety of documents understood to be in the scope of the archiving framework to-be

3.5. Towards an actionable eDoc Roadmap

- The Commission activities had already achieved significant progress in some of the areas impacting or relating to eDoc
- More detailed elaboration of the eDoc Building Block related activities needs to take place, on an accelerated basis
- There are a number of overlaps with eID related efforts, as well as dependencies between eID and eDoc related efforts, which will have to be considered during the 2 pilots and during the periodic review of the eID and eDoc roadmaps
- An updated version of the roadmap with a clear definition of the basic blocks will be made available. It will then be presented to the MS for further review.

3.6. Achieving an eDoc Roadmap through potential Pilots

- In this respect, any pilot on eDoc should ensure that Member States have a key role in the implementation, and also on common specifications for the eDoc.
- The potential wider impact of eDoc cannot be achieved without such commitment from the Member States.
- It is clear and well known that technology expertise lies with the industries
- Effective co-operation between the industries, Member States and the Standardization bodies would be key to success of a pilot on eDoc.
- It has also been noted that the use cases chosen for the pilot should ensure that the different functionalities of the eDoc should be tested and verifiable through them.

4. Participants

Name	*Organization*
Anneli ANDRESSON-BOURGEY	European Commission
Antony BISCH	European Commission
Martin BOTTERMAN	GNKS Consult
Baudouin DESONIS	eu-forum.org
Aitor ELORZA	European Commission, SG/B3
Hans GRAUX	Lawfort
Marco GRISPIGNI	European Commission
Mike KULBICKAS	TRASYS, S.A.
Jean-Severin LAIR	Ministry EFI/DGME France
Mireille LEVY	Home Office, UK
Christine MAHIEU	Strategic Cell, eGov Belgium
Tarvi MARTENS	Estonian Adminisrtation (AS Sertifitseerimiskeskus)
Gzim OCAKOGLU	European Commission, DIGIT 01, IDABC
Tadgh O'LEARY	CMOD (Technology Policy Division), Ireland
Eric PICHON	European Commission, SG/B3
Dr Reinhard POSCH	CIO, Austrian Administration
Olli-Pekka RISSANEN	Finish Ministry of Finance, State IT Management Unit
Marc STRAAT	Adobe, S.A.
Dr Aniyan VARGHESE	European Commission, DG-INFSO
Désirée VESCHETTI-HOLMGREN	Verva, Swedish Administrative Development Agency
Luc WIJNS	Sun Microsystems
Anja ZISAK	Austria – Federal Ministry of Justice

5. Annex

5.1. Questions used for reflection at the workshop

To stimulate reflection on the intended framework, a number of questions were formulated in advance of the workshop for reflection and consideration by a team of experts and representatives gathered from across the EU, from positions in government administrations, the private sector (including industry associations), and from different standardization bodies. The questions included:

- How can the general framework for interoperability between administrations be described, e.g., in terms of specific restrictions in force in different areas such as legal restrictions, language differences, formal requirements, or other de-facto restrictions?
- What (if any) approaches are there already in use with respect to interoperability? Are there any contradictions or problems already noted?
- What constitutes an “original” document in the electronic world?
- What are the valid sets of transformations that can be applied to electronic documents (which may or may not include translation between national/official languages, document format, presentation/display via style sheets, fonts, etc.)?
- What is the potential for “standardization” of certificates representing specific electronic documents such as birth certificates, diplomas etc. that would allow for automatic processing to take place?
- What could be a common model of validity (encompassing such items as duration/lifetime/validity period of an electronic document, possibility/frequency/process for renewal, requirements on the digital signature, etc.)?
- What are the target use-cases of the framework for electronic documents, i.e., does it (or does it not) include such items as (and what else could it include):
  - attestations such as birth/death certificates, compliance with Social Security obligations, lack of criminal record;
  - education diplomas,
  - tax returns,
  - Other official documents such as e-votes, e-invoices, etc.
- What is required by industry and governments for such a framework to be of practical usefulness?
- What is the definition of an authenticated electronic document? Should we plan for several standardized levels of authentication of electronic documents, depending on the context? What could be the characteristics of these authentication levels?

- How is the framework of eDoc linked with eID-related efforts? Examples of the kind of scenarios where dependencies can arise and should therefore be considered include:
    - Sometimes it is necessary that a specific, duly mandated, physical person signs a document, other times this is not the case, such as a company "stamp".
    - In some specific situations, it may be important to deliver a large amount of officially recognized documents in a short period of time (e.g. a university signing thousands of attestations/diplomas).
- We expect that should be used whenever possible. What are the minimum essential requirements informing the selection of standards for electronic document formats, including standards based on existing/open standards?
- What are key aspects of the framework that could be supported by the pilot type B project and how could they be linked to the roadmap?