4.5.2010

INFORMAL EXTRACT OF THE

TENDER SPECIFICATIONS

Feasibility study on an electronic identification, authentication and signature policy (*IAS*)

SMART 2010/0008

INFORMAL EXTRACT OF THE TENDER SPECIFICATION

Important disclaimer: the objective of the present call for tenders is to study the feasibility of regulatory framework on electronic identification, authentication, signature and related credentials.

It should not be interpreted as being a commitment of any kind of the European Commission to actually propose such a framework nor of its content, should the Commission decide to propose one.

TABLE OF CONTENTS

PART 1: TECHNICAL DESCRIPTION

1 CONTEXT

1.1 Ground for a policy on identification, authentication, signature and related electronic credentials

Over centuries, mankind has invented concepts enabling citizens to evolve in a society of growing complexity. A keystone concept is the identity of a person. Around it, several means were devised for person identification and for authenticating the claims made by a person. The handwritten signature is probably the most accomplished of these means. Handwritten signatures have a rich symbolic and semantic connotation, univocally linking a person to his/her acts: a signature can express the agreement or commitment of a person, a signature can identify the signatory of a document, the signature can serve as a proof of authenticity and integrity of a document, etc[1]. Mankind has also invented the concept of legal person in addition to natural person. A natural person can sign on behalf of a legal person. Seals or stamps are convenient means used in particular by legal persons to authenticate documents.

This discussion could be further developed but its purpose is simply to remind the Tenderer how much these identification credentials are intrinsically intertwined in the "physical" world. It is deemed sufficient to understand why this ***intertwining*** should also "glue" identification credentials in the information society.

The instruments related to identification, authentication and signature in the "physical" world rely at the same time on technology (ex. pens, seals, identity cards, …) and on legislation. Legislation defines the conditions for the legal recognition of the technological instruments.

It appears as a natural development that all these concepts and instruments would extend to the information society if we want the person to be represented and act in the "electronic" world as in the "physical" world. Since both worlds are not distinct universes but are part of the same whole, identification, authentication and signature instruments should also work in both.

Directive 1999/93/EC on a *Community framework for electronic signatures* (e-signature Directive) is the main EU legal instrument that specifically **addresses such an extension**[2] **and the intimate intertwining between electronic signatures, authentication and identification**. Indeed, its article 1.1 defines an electronic signature *as data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication*; article 1.2 states further that an *'advanced electronic signature' is an electronic signature which is capable of identifying the signatory*.

The Directive links "official"[3] identification to signature through the requirements on qualified certificates for electronic signature (Annex I (c) to the Directive: *Qualified*

---

1 See for instance "Electronic signature in Law", Stephen Manson, Tottel publishing, 2007 for an exhaustive analysis of the meanings of a signature.

2 The data protection, electronic commerce and payment directives are also essential EU legal instruments bridging the "physical" and "electronic" worlds.

3 "Official" identification in the present Tender Specification" means the formal identification data handled by governments in relation to national ID documents or national ID registers.

certificates must contain […] the name of the signatory […]) and rigorous issuance conditions (Annex II (d) to the Directive: *Certification-service-providers must [] verify, by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to which a qualified certificate is issued*).

At the same time, the Directive already takes into account some of the versatility of identification by authorising pseudonyms instead of names[4].

The Directive essentially focuses on concepts and provisions related to the electronic signature; the Directive does not provide details on identification nor authentication. Nine years after the Directive adoption, willing to address the lack of a comprehensive political framework, the European Commission has put forward a first policy initiative in November 2008: *the Action Plan on electronic signatures and electronic identification*[5] which requests to *determine further actions required to enable the effective EU wide usage of eID*.

The electronic signatures framework (Directive 1999/93/EC on a Community framework for electronic signatures) **may thus serve as a starting point to devise a new comprehensive *electronic identification, authentication and signature* (*IAS*) or *electronic credentials* legal framework**.

A new framework would allow proposing solutions to solve remaining e-signature interoperability issues and to address ancillary and related trust services, as well as the related concept of ***electronic seals***. Furthermore, like in the "physical" world there are services for the **registered delivery** of signed documents; similar services are needed to certify the delivery of electronically signed documents.

This scheme would allow a person to create a message, sign it to identify the signatory and authenticate it, and send it in a non disputable way thanks to a certified delivery service. There is an element missing to complete the scheme: the address where to send the message. Therefore, a further element to consider is the feasibility of having EU Member States providing (on a voluntary basis) an "official"[6] ***email address*** for all citizens and legal persons.

> One may actually argue that such an email address may be much more than it appears to be. Because an official email address may combine identity, identification, residence-like information and a unique identifier (i.e. the short but unique string of characters making the e-mail address itself), the official email would actually gather in a compact and easy to handle format most of the elements usually present on an ID card. It could be seen as the *core* element of an identification policy in the information society rather than an ancillary element.

The current situation with electronic identification interoperability is problematic. Indeed, on the grounds of national sovereignty, Member States have followed their own eID plans since

---

4 Directive 1999/93/EC, article 8.3 *Without prejudice to the legal effect given to pseudonyms under national law, Member States shall not prevent certification service providers from indicating in the certificate a pseudonym instead of the signatory's name* and Annex I (c): *Qualified certificates must contain […] the name of the signatory or a pseudonym, which shall be identified as such*

5 Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions on an *Action Plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market*, COM(2008)798 of 28.11.08.

6 "Official" means here "provided by a Member State".

early 2000s without a clear convergence towards interoperable solutions and mutual recognition of these across-borders. eID in nearly every national legislation exists only via reference to the national electronic signature law or as a consequence of the eID card or national register infrastructures but not as a *sui generis* issue. The lack of a legal framework on eIdentification at EU level reflects the situation in most Member States.

The purpose of the present call for tenders is to study the feasibility of a comprehensive EU legal framework that would gather all the identification-related electronic credentials needed to secure electronic transactions as well as the ancillary services needed to use them: **electronic identification, authentication, signature, seals, certified delivery and a** voluntary **official email address.**

The perspective of the legal framework would be to facilitate the smooth working of electronic transactions in the internal market (i.e. the perspective here is not fighting cybercrime). In other words, it would be based on article 114 of the EU Treaty.

In addition to the intrinsic intertwining of the electronic identification-related credentials, it is worth noting that they are essentially **trust building instruments**[7]. Therefore, it is felt that the trust building tools developed for electronic signature in Directive 1999/93/EC may equally be applicable to identification management, authentication and related concepts. Firstly, the trust model is based on trusted third parties, liability and public supervision. Another good example is the application of internal market principles such as the recognition of foreign certification with no need for a local national pre-registration. The Directive also contains specific clauses on data protection and international cooperation. Finally the so-called "new approach"[8] spirit is present in a legal act derived from the Directive (Commission Decision 2003/511/EC) by which a specified security requirement is presumed to be fulfilled by a given system if it complies with a particular standard; this "new approach" spirit would equally be appropriate for eID management.

A positive side effect of using the same kind of tools would allow benefiting from the best practice developed in ten years of operation of the e-signature Directive.

Similar to the equivalence between electronic and handwritten signatures, an e-identification policy should establish the conditions ensuring **equivalence of an electronic identification with identification in the "physical" world** to preserve a coherent legal framework across the Union.

---

7 For a discussion on trusted services, see the last report of "Feasibility study of a European federated e-signature validation service", http://ec.europa.eu/idabc/en/document/7764,

8 The "new approach" was defined by the Council in its Resolution of 7.5.1985 *on a new approach to technical harmonization and standards* (OJC 136 of 4.6.1985). It is based on a few key principles (see http://ec.europa.eu/enterprise/policies/european-standards/documents/harmonised-standards-legislation):

- there is a clear separation between the EU legislation and European standardisation;
- EU legislative harmonisation (e.g. Directives) is limited to the essential requirements (safety requirements of general interest) needed to ensure the free movement of products throughout the Community;
- the Task of drawing up the corresponding technical specifications is entrusted to the standardisation bodies;
- products manufactured in conformity with harmonised standards are presumed to be conformant to the essential legal requirements;
- standards are not mandatory but voluntary Alternate paths are possible but the producer has an obligation to prove that its products conform to the essential requirements;
- standards must offer a guarantee of quality with regard to the essential requirements of the directive;
- public authorities are still responsible for the protection requirements on their territory (e.g. market surveillance);
- safety clauses require Member States to take appropriate measures to withdraw unsafe products from the market.

Finally, another similarity shared by the electronic credentials is that with the currently available **technology**, they rely on the same technology: cryptography and public key infrastructure. Given that an EU policy should be *technology neutral*, this similarity should not be a policy driver. However since the policy should make sense and be feasible, disregarding the means to implement it in the foreseeable future would not be advisable neither. Since compromise is not a solution here, if no technology exists for a given policy element, it would probably be preferable to discard the element in the short/medium term – nothing preventing to update the policy later.

The hypotheses made above require a validation, which is an objective of Task 1 of the feasibility study (see TASK 1 *below).*

2 OBJECTIVES OF THE FEASIBILITY STUDY

2.1 Scope of the work expected from the Contractor

The feasibility study will investigate what should be the elements of an e-identification legal framework which would encompass e-authentication, e-signature and related electronic credentials (*IAS*). The study should address the impact on and **involvement of all parties** (the public sector, the supply and demand sides of the private sector and citizens) with respect to an IAS policy.

The scope of the study is the following:

1. To assess the various hypotheses and issues made below regarding a policy on electronic credentials. See TASK 1.

   The assessment should look at the potential legal impact, technical and operational feasibility aspects, economical viability (macro economic impact for the society and microeconomic impact for service providers/manufacturers) and societal issues (data protection in particular).

2. To identify in past and on-going undertakings supported by the European Commission as well as in major third parties initiatives, as well as in available legislation what are valuable findings and recommendations to use as input material for an *IAS* framework. See TASK 2. TASKS 1 and 2 should mainly be carried out in parallel.

3. Constructing on the e-signature Directive, the study should provide building blocks of a possible pan-European *IAS* framework, including ancillary credentials and services such as seals, registered delivery, e-mail, time-stamping, archiving, etc. See TASK 3. TASK 3 should mainly build on the findings of TASKS 1 and 2.

4. Finally, the Contractor will also provide technical and legal support to the Commission in its interaction with stakeholders. See TASK 4.

2.2 Task 1: Defining the conceptual basis for an *IAS* framework

The first Task of the study will be to identify and assess priority issues that should be addressed by an *IAS* framework and validate working hypotheses. A further detailed assessment with a higher granularity is also expected in Task 3.

2.2.1 Open regulatory and hypotheses issues for a possible IAS framework

This section outlines a number of issues related to identification–related credentials that should be assessed during Task 1. Issues that would be validated as relevant by Task 1 should be further developed in Task 3. The Tenderer may suggest additional issues to be investigated.

(1) The **objective** of a possible *IAS* framework would be to **enhance trust in pan-European electronic transactions by fostering cross-border interoperability of electronic credentials and ensuring mutual acceptance**. The framework should result in removing impediments of technical, legal and operational natures**.**

(2) **The following priority areas for e-identification management:** (the *IAS* framework could possibly address in a first step, the non-technical e-identification interoperability issues which are outlined hereafter[9]) should be investigated:

2.1. Options for cross-border **mutual recognition of national eID management systems** (covering of legal persons as well as natural persons).
For instance, should national eID management adhere to a set of voluntary standardised security requirements or no harmonisation and just mutual recognition? If harmonisation is needed, how could it work in practice? Would it require an ***authentication level classification****,* i.e. an agreement on an assessment of the reliability of identification infrastructures.[10] How to ensure the cross-border acceptance of these (mutual recognition)?

2.2. How to deal with **national specific identifiers**. A second issue comes from the wide usage of national specific identifiers*:* identification required for national eGovernment services often if not always, relies on some national specific identifier which is uniquely individualising each and every citizen from his/her fellows (ex. a national register number). These identifiers are rarely granted to foreigners unless they reside in the country. Access is therefore *de facto* denied to residents from other states[11].

2.3. How to ensure **data protection and user empowerment**. User empowerment to control his/her e-identification-related data (e-identification data in the broadest meaning) is a pre-requisite for minimising the potential violation of reasonable expectations regarding the protection of the privacy and identity of individuals (including protection against ID theft) in compliance with the EU data protection and privacy regulations[12]. User-control has to go hand in hand with data proportionality, data minimisation and traceable accountability principles, and with an underlying foundation of the rule of law, including law enforcement and forensics. In a democratic society it is vitally important that citizens are able to make informed judgements and decisions on how to appropriately use their identification data, and on how to balance privacy concerns with the need to obtain services.

Safeguards are insufficient today to ensure that the identification attributes of a

---

9 These priorities are mainly derived from the "Study on mutual recognition of e-signatures for eGovernment applications", http://ec.europa.eu/idabc/en/document/6485.

10 For instance, a given eID scheme could be assessed against (security) standards. A scheme matching or exceeding the requirements of the standards would be declared "qualified" and would be recognised by the other European "qualified" schemes; mutual recognition of non qualified schemes would not be mandatory (this approach in Directive 1999/93/EC lead to the mutual recognition of "qualified" electronic signatures). Another possibility would be to define several standardised levels of reliability to enforce mutual recognition in such a way that a given eID scheme would recognise schemes of the same or higher levels although today, no Member State has a legal basis for multiple reliability level.

11 To address the unique identifier issue, one may think of two alternative models. In the first model, when a citizen of Member State A would like to access a service in Member State B requiring an identification, the eID of Member States A would be used to automatically generate a (transient) identifier in the scheme of Member State B. In the second model, the eID of Member State A would directly be used in Member State B; this second model raises data protection issues and it puts strong requirements on Member States implementations.
NB. To avoid discriminations between EU citizens, the issue of citizens from Member States that do not have an eID system needs also to be addressed.

12 Possibly reinforced.

person remain under his/her control. This is challenging at the cross border level, since all existing challenges that exist at the national level remain including lack of knowledge and awareness of the users, and new challenges are added including language barriers when attempting to obtain informed consent from an end user for an authentication process and the possible clash between national data protection legal regimes. Privacy should not be compromised for sake of cross-border interoperability.

Furthermore, requirements on the transparency on eID tokens (ex. eID cards) should be addressed (ex. the bearer could always have the possibility to verify the content of his/her token; independent trusted third parties could certify that indeed, the eID token does not contain other (hidden) data).

2.4. To reach a consensus on the **data set needed to support identification** in a cross-border interoperability context.

(3) The Contractor should identify which *baseline conditions* could **induce the take-up** of adequate services to manage electronic ID-related credentials and stimulate the development of "***business cases"***. If it is the case, one may expect that a variety of services will be invented to address the undefined but huge set of the possible usages of identification and authentication. These conditions should thus allow an electronic credential business to prosper and at the same time to behave in a responsible manner.

The business case for electronic ID-related credentials services is not clear for the private sector[13] (i.e. how to make profit by offering services managing identification data). Therefore, it is essential that the hypotheses formulated during the study will be successfully matched against micro-economic viability criteria to ensure that the industry would be eager to invest to provide solutions and services.

(4) **Trusted Parties provision (ID data brokers).** The Contractor should investigate if the right business case for e-identification could actually be the avoidance of fines and penalties by identification data consuming businesses due to their risk of mismanaging these private data. For instance, data consuming businesses could be looking for **trusted parties** (on a voluntary basis) to securely handle the private data of their customers.

Therefore, the *Contractor* should investigate the functions that *trusted parties* should fulfil. For instance, how could trusted parties implement the data minimisation principle ("need to know") and the standardised security requirements they would have to match to protect data (ex. requirements on processes such as ISO 27000, on installations, on personnel …)? How could a trusted party be "rewarded" to meet these requirements? Would a legal "***qualification***" as being *trustable* (thus a *Trusted Party)* and a limitation of its responsibilities (liabilities) be stimulating enough? The trust model of the electronic signature regulatory framework relies on the qualification of certification service providers[14]. The Payment Directive[15] also provides examples on the kind of requirements that could be put on trusted parties.

---

13 The "business case" for the public sector may be clearer because if often stems from legal or social imperative requirements where financial constraints are secondary.

14 Annex II to Directive 1999/93/EC.

15 Directive 2007/64/EC of the European Parliament and of the Council of 13.11.2007 on *payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC*. OJ L 319 , 05/12/2007

Like in the banking and payment sectors, the number and variety of trusted third parties could give the needed freedom to data producers and data users to choose one or several brokers best fulfilling their needs.

In this model, because the personal data of the data subject would be located only with few brokers, he/she would keep the control and easily correct, update or withdraw the data as he/she would deem appropriate. Because the data broker would verify the correctness of data – as deemed appropriate, depending on the nature of the data - the advantage for the data user would be to receive reliable data and to avoid exposure to the risk of data loss. ID theft would become a useless fraud. The model would also offer the adequate structure to define clearly the rights, responsibilities and liabilities of each of the three involved parties[16].

The Contractor should evaluate if such a trusted third parties model could have a positive and significant impact on the management of **"soft"**[17] **identification** (like profiles on the web) because it would create a very appealing incentive for data minimisation.

(5) **Data Protection Provision:** Given the pivotal role of data protection in the context of the management of eID-related data, the Contractor should assess whether the level efficiency of the obligations to protect personal data resulting from the data protection directive[18] matches the requirement of the protection of identification-related personal data (seen as a specific subset of personal data). The Contractor should also assess the need for a stronger harmonisation between EU Member States. In particular, the study should assess the impact of specific requirements for eID-related data breach notification.

(6) The Contractor is also invited to assess the **international dimension** of a European IAS framework. Indeed, the compatibility of third countries electronic identification, authentication and signature frameworks with the European one would favour international transactions.

In summary, The Contractor should analyse and propose recommendations on how to deal with the issues summarised in the table below:

16 **Economic sustainability** of the ID data broker: several models can be imagined (ex. public funding, payment of a fee by the data user, payment of a fee by the data subject or a combination).

17 "soft" identification in opposition to "official" identification.

18 Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Official Journal L281 , 23.11.1995

Essential issues for a possible IAS framework:

1. Mutual recognition of national eID management systems and cross border interoperability
2. Priority areas for e-identification management:
   2.1. cross-border mutual recognition of national eID management systems
   2.2. usage of national specific identifiers
   2.3. data protection and user empowerment
   2.4. common data set for identification in a cross-border context
3. Baseline conditions for the take-up of eID services – Business cases
4. Assessment of a model for "qualified" trusted Parties (ID data brokers).
5. Data protection.
6. International dimension

The Tenderer may also suggest addressing additional issues. Given the imperfect level of understanding of the issues at stake or even the difficulty to formulate the nature of the issues, claiming to look for the comprehensive and final IAS policy would be presumptuous. Therefore the present work ambition should only be to make the first step in an iterative process that will eventually lead to an exhaustive policy in a remote future.

2.2.2 Expansion of the e-signature current framework

The Contractor should assess which provisions of the current e-signature framework established by Directive 1999/93/EC could be **adapted or expanded** to cover wider IAS requirements.

The study should also address specific interoperability shortcomings of the current e-signature framework. An indicative list of issues is given in the table below (NB. Most of the listed issue apply *mutatis mutandis* to IAS). A driving principle for any action in favour of electronic signature should be to **simplify** its usage and implementation.

In addition to the regulatory framework established by Directive 1999/93/EC, an intense standardisation work took place at European level and also deserves attention in the context of the study.

> Some thirty electronic signatures standards have been developed by the European standardisation bodies CEN (European Committee for Standardisation) and ETSI (European Telecommunications Standards Institute) on the basis of the requirements of the Directive.
>
> Annex II(f) and Annex III of the e-signature Directive contain the requirements relating to the security of some electronic signature products. A related list of generally recognised standards has been published in Commission Decision 2003/511/EC. The Action Plan on e-signatures and e-identification COM(2008)798 foresees the update of the Decision.
>
> Electronic signature standards are complex and allow a variety of implementation options. A major **rationalisation of the** existing **electronic signature standardisation**

framework has started in 2010 via a mandate[19] to the European Standardisation Organisations.

Issues to be considered in relation to the e-signature framework[20]

- **Adaptation and/or expansion of the provisions of Directive 1999/93/EC to encompass IAS:**

  Articles 3.2 (accreditation), 3.3 (supervision), 5 (legal effects), 6 (liability), 7 (international aspects), 8 (data protection), Annex I (qualified certificates), Annex II (certification services providers), Article 3.4 and Annex II (hardware requirements).

- **Clarification of the terminology** (ex. the meaning of "*authentication*" in art 2.1 is ambiguous: does it refer to data or person authentication or both?; what is the meaning of "*comply*" in art 4.2, "*application*" and "*additional*" in art 3.7. Does the scope of the Directive cover legal persons?).

- **Options for supervision**:
  1. Minimal common supervision rules between MS (including harmonisation on financial requirements regarding certification service providers);
  2. Relationship between supervision and accreditation;
  3. Publication of trusted lists of certification service providers issuing qualified certificates;
  4. Prior declaration before starting a qualified certification service;
  5. Assessing the feasibility of cross-border supervision (to allow a certification service provider of a Member State to operate in other Member States);
  6. Harmonisation of persons registration requirements.

- **Possible derogation for public services** (current art 3.7):
  1. Need for and possibly clarification of the use of public services derogations (art 3.7)
  2. Excessive use of art 3.7 and consequent potential internal market barriers (ex. compulsory accreditation required to issue qualified certificate to be used for eGovernment applications).

- **Need to clarify/lay down security requirements**:
  1. Certification when Designated Bodies (art 3.4) do not exist in a Member State.
  2. Certification of signature applications.
  3. Cryptographic algorithms for electronic signature (and authentication).
  4. Clarification of security concepts: ex. *sole control* in art 2.2, *verification* in Annex IV, rules on key pairs, rules on interfacing secure signature creation devices (API), use of different keys for authentication and signature.
  5. Mapping of the legal security requirements with standards and giving a legal effect as a reward of compliance to standards.
  6. What should be the boundaries of signature components? (ex. clarifications on end-to-end security requirements for signature equipment).

- **Issues to be considered in relation to qualified certificate profiles** (Directive's Annex 1):
  1. Efficiency and need of financial limitations in the qualified certificate (with an impact on automated processing or on the evaluation of the risk of a certification service provider).
  2. Impact of the provision of the same key pairs in two different certificates issued to the same person and contemporaneously.

[19] Mandate m460, http://ec.europa.eu/information_society/policy/esignature/eu_legislation/standardisation

[20] The references point to articles and annexes of Directive 1999/93/EC or to its related Decisions 2003/511/EC and 2000/709/EC.

3. Need to tackle differences between national provisions for qualified certificate profiles including the lack of a "qualification" marker.

- **Issues linked to the classification of credentials** according to their security quality:
  1. Clarification on the status of *advanced* e-signatures[21] and especially of lower security signatures,
  2. Assessment on the usefulness of a "super qualified" signature of higher security than the "*qualified*" e-signature[22] by setting requirements on the end-to-end security (ex. for signatures requiring a very high level of reliability such as for transactions requiring the intermediary of a notary).
- **Signature validation:**
  1. Definition of third party services offering **signature verification**:
     - Legal effect of the verification;
     - Liability of the service provider.
  2. How to ensure that the legal value of an electronic signature (i.e. equivalence or lack of equivalence to a handwritten signature) is explicit in the verification process..
- Issue of the impact of the multiplicity of **signature formats** on interoperability.
- Clarification of the liability of a "Bridge Certification Authority" (Bridge CA) – when this solution is used for cross-border interoperability.
- Options for the coverage of signature creation devices for **mass signature**.
- Options for the coverage of mobile devices (ex. for **mobile signature**).

The Tenderer may also suggest addressing additional interoperability issues.

The Contractor will also assess the impact of the following issues on related credentials and services (e-seals, certified delivery, official delivery address) and ancillary services to e-signature as listed in the table below:
:

Issues linked to the use of identification-related credentials and services; ancillary services to e-signature

- Coverage of **delegation of power,** i.e. natural persons authorised to sign on behalf of another natural or legal person (ex. power of attorney, tutor of a minor).
- (Qualified) **electronic stamps or seals,** i.e. an e-stamp would be a proof of authenticity but not a signature.
- **Ancillary services to signature** like time stamping or long term archiving
- **Registered electronic documents delivery** (including proof of delivery):
- **Official delivery address** for each citizen and legal person (on a voluntary basis).

The Tenderer may also suggest addressing additional similar issues.

The resulting assessments as well as recommendations on elements to be considered for further elaboration will be the object of **Deliverable 1.** Deliverable 1 will be presented and debated during a **public workshop** (1st public workshop – see Task 4). The elements retained for further elaboration in Deliverable 1, version 1b (final) will be developed in Task 3.

---

21 Art. 2.2 of Directive 1999/93/EC.

22 Art. 5.1 of Directive 1999/93/EC.

Deliverable 1, Version 1: Assessment as well as recommendations on elements to be considered for elaboration in Task 3 [M4].

Deliverable 1, Version 1b (final): Update of version 1 after the 1st public workshop [M6].

2.3 Task 2: Stock taking

The objective of this task is twofold:

1. Firstly, the Contractor will perform a critical review of existing legislation as well as past and ongoing initiatives related to electronic credential to identify.

   The Tenderer should select for analysis (and justify its selection), the most relevant legislations and initiatives, be they national, European, international, or emanating from non-EU countries.

2. Secondly, from this review, the Contractor will identify results worth to be "re-used" directly or indirectly by an *IAS* regulatory framework.

   Examples of direct re-use would be copying provisions of an existing law in a Member State or re-using definitions of concepts. An example of indirect re-use would be to identify an existing standard that could potentially be referred to by the framework with a "new approach" spirit. Another kind of relevant usage of results would be to identify a technology (ex. a protocol, a pilot) that could demonstrate that some legal provisions can indeed be implemented.

For each selected legislation or initiative, the Contractor will identify and analyse the issues with relevance to the study. Then, the Contractor will provide a synthesis, which may be used as an input to Task 3.

The Commission Services at the kick-off meeting may provide supplementary input information, other than those identified by the Tenderer, to be analysed as part of Task 3.

NB. In particular, the Institute for Prospective Technological Studies (IPTS), an entity of the European Commission's Joint Research Centre, plans to launch, in close cooperation with DG Information Society & Media, the "**eID Compass**". It will be an observatory of the scientific work taking place on e-identification with the objective to "distil" the gathered information into a consolidated eID management concept. The Contractor is expected to exchange information with the eID Compass.

The resulting analysis and recommendations on elements to be considered as valid input for an *IAS* framework will be the object of **Deliverable 2.** Deliverable 2 will be presented and debated during a **public workshop** (1st public workshop – see Task 4).

Deliverable 2, Version 1:	Result of the analysis and recommendations on external elements to be considered as input for an IAS regulatory framework [M4].
Deliverable 2, Version 1b:	Update of version 1 after the 1st workshop (see Task 4) [M6].
Deliverable 2, Version 2:	Update of version 1 (to take into account developments of the analysed legislations and initiatives – and possibly new ones) [M16].
Deliverable 2, Version 2b (final):	Update of version 2 after the 2nd workshop (see Task 4) [M18].

2.4 Tasks 3: Defining building blocks for IAS

Based on the approach in Directive 1999/93/EC, the Contractor is expected to elaborate building blocks for a legal framework on electronic identification-related credentials (e-identification, e-authentication, e-signature, ancillary credential, ancillary services) with a view to removing interoperability barriers and facilitating the usage of these credentials.

The elements to be considered for Task 3 are those retained in Task 1 as well as relevant input from legislation and undertakings identified in Task 2.

The Contractor is expected to formulate proposals for policy options including for each option:

- Legal definitions, impact and rationale;
- Technical aspects – including standardisation;
- Operational aspects – including standardisation;
- Business issues (macro economic impact for the society and microeconomic impact for service providers/manufacturers);
- Societal issues (data protection in particular).

In particular, under this perspective,

- The Contractor is expected to formulate proposals for policy options on **electronic identification and authentication policy** expanding appropriate existing provisions of the e-signature legal framework. The expansion of existing provisions may also include, where necessary, improving these provisions to create more legal certainty and to avoid cross-border interoperability barriers. For issues where no provisions currently exist (or which need to be clarified), the Contractor should formulate proposals for new (original) provisions.
- The Contractor is expected to perform a gap analysis on **e-identification standards** and define the requirements that should be addressed in standards to be developed in the future (NB. standards development is outside the scope of the study).
- The Contractor is expected to formulate proposals for policy options on **ancillary credentials and services** related to electronic identification, such as electronic stamps/seals, delegation of power, certified delivery of e-mail and official e-mail address.

- For issues specific to e-signatures, the Contractor is expected to formulate proposals to improve the current **e-signature legal framework** with a view of removing interoperability barriers and to facilitate the usage of e-signatures
- The Contractor is expected to formulate proposals for policy options on **ancillary services to e-signature** such as time-stamping, (long term) archiving and authorisation/role management.

The result of this work will be the object of Deliverable 3:

Deliverable 3, Version 1:	Building blocks and Recommendations [M11].
Deliverable 3, Version 2:	Update of version 1 (reflecting the progress of the work since the previous version of the document) [M16].
Deliverable 3, Version 2b (final):	Update of version 2 after the 2nd workshop (see Task 4) [M18].

2.5 Task 4: Synthesis, workshops and support

Task 4's activities will be the following:

1. The results of Tasks 1 and 2 will be presented in a **first public workshop** in order to be scrutinised and debated by interested stakeholders, in the 6th month of the contract.

2. The Contractor will **compile** the results of the Tasks 1, 2 and 3 in a coherent document (the draft final study report).

3. The draft final study report will be presented in a **second public workshop** in order to be scrutinised and debated by interested stakeholders, in the 17th month of the contract.

4. Lastly, the Contractor is also expected to follow up developments in standardisation and implementation of electronic identification, authentication, signature and related credentials, and further develop any requirements identified in this process for the progress of the definition of the IAS framework.

   The Contractor will **support** Commission services in interacting with Member States, European Standardisation Organisations, and the various stakeholders to discuss IAS issues and for the further development of e-signature framework, in particular in implementing the Action Plan on e-signature and e-identification COM(2008)798, the M460 mandate[23] and the revision process of Commission Decision 2003/511/EC. Additionally, on-the-spot operational and technical support and advice should be foreseen.

   The Contractor should note that this support required in this paragraph is likely to be requested from the very beginning of the study, especially for e-signature (see also "Specialised ad hoc meetings" in section 4.2 below).

[23] See http://ec.europa.eu/information_society/policy/esignature/eu_legislation/standardisation

The result of this work will be the object of the following Deliverables:

Deliverable 4.1:	1st Workshop report [M6].
Deliverable 4.2, Version 1:	Draft final study report) [M16].
Deliverable 4.2, Version 1b (final):	Final study report (update of version1 after the 2nd workshop) [M18].
Deliverable 4.3:	2nd Workshop report [M18].
Deliverables 4.4:	Specialised ad hoc meeting reports (see §4.2 below)

3 DURATION

Duration of the Tasks must not exceed **18 months** and is subject to the provisions of Art. I.2.3 of the contract.

4 DELIVERABLES, MEETINGS AND TIMETABLE

4.1 Deliverables

All work will be carried out in English. Fluency in written and spoken English is required. All deliverables will be in English.

Unless explicitly indicated hereafter, all deliverables will be submitted in an editable electronic format (ex. Word) and in PDF format suitable for web posting and printing. No delivery on paper is requested (NB. the Contractor will nevertheless be free to deliver a reference paper copy if it so desires).

The Contractor must ensure the **quality of the style** of the draft and final deliverables as well as the **correctness of the English language** (ex. if the author(s) of a deliverable does not sufficiently master the English written language, deliverables should be submitted to a professional translator or native English speaker before submission to the Commission). The Commission may decide to post on its website any deliverable in draft or final format.

Deliverables to be discussed at the workshops have to be delivered to the Commission one month before the workshop and forwarded to the workshop attendees at the latest seven calendar days before the workshop but after prior authorisation from the Commission.

The deliverables listed below must be provided by the Contractor:

Deliverable	Version	Description	Due date
D0.1		Inception report	Week 2
D0.2		Management reports (technical reports)	M6 M12 M18
D0.3		Draft webpage of the project	M1
D1	v1 v1b	Assessment as well as recommendations on elements to be considered for elaboration in Task 3	M4 M6
D2	v1 v1b v2 v2b	Result of the analysis and recommendations on external elements to be considered for a possible IAS policy. *D2 v2: to be presented as an annex to D4.2 v1*	M4 M6 M16 M18
D3	v1 v2 v2b	Building blocks and recommendations *D3 v2: to be presented as an annex to D4.2 v1*	M11 M16 M18
D4.1		1st Workshop report	M6
D4.2	v1 v1b	Draft final study report Final study report	M16 M18
D4.3		2nd Workshop report	M18
D4.43		Draft minutes of specialised meetings.	as needed

List of deliverables

- **Inception report (D0.1)**, specifying the methodology, resources and objectives provided in the tender in accordance with the indications provided by the Commission during the inception meeting. The report should contain the tables of contents for Deliverables 1, 2 and 3. The report should also include the detailed list of initiatives and legislations to be analysed during Task 2.

- **1st Interim study report** which will cover Task 1 and Task 2 and be made of **D1 and D2 versions 1.** The 1st interim study report shall be made available to the Commission's services within **4** months after the signature of the contract and will serve as a basis for the 1st public workshop (see §4.2). The report will be updated to take into account the conclusions of the public workshop (**versions 1b**).

- **2nd Interim study report** which will cover Task 3 and contain **D3 version 1.** The 2nd interim study report shall be made available to the Commission's services within **11** months.

- ***Final study report (D4.2),*** including the following parts:
  1. Executive summary
  2. Annexes:
     - Glossary
     - D1 version 1b,
     - D2 version 2 (i.e. the simple update of D2, version 1b)
     - D3 version 2

  The draft final study (**D4.2, version 1**) report will mainly be an updated compilation of the work done with an executive summary. The draft final study report shall be made available to the Commission's services within **16** months and will serve as a basis for the

2nd public workshop (see §4.2). The report will be updated to take into account the conclusion of the 2nd public workshop (**D4.2, version 1b final**).

- Workshops reports (D4.1 and D4.3),

Reporting on the 1st and 2nd workshops. Due five working days after each workshop.

*- **Management reports (Technical reports D0.2),***

Reporting on the work done, the attendance to meetings and events. Reporting on problems and risks. The reports will include time-sheets on man/days consumption, detailed travel information, use of consumables, etc.

*- **Draft minutes of specialised meetings*** (**D4.4)** (see §4.2)

The Contractor may be asked by the Commission to draft minutes of these meetings. When requested, draft minutes should be submitted within two working days after the meeting.

*- **Draft webpage of the study*** (**D0.3)**

The Contractor will provide the Commission with draft simple webpage(s) presenting the project and its progress. This (these) page(s) will serve as input for the Commission to update its website. A first delivery is expected within **1** month after the signature of the contract and update should be delivered as necessary to keep the website up-to-date and informative.

4.2 Meetings and workshops

For all meetings:

- Travel expenses will be borne by the Contractor for its own staff,
- Hotel and subsistence expenses will be borne by the Contractor for its own staff.

If deemed appropriate, the Contractor and the Commission may agree to anticipate, postpone or cancel any of the foreseen meetings.

Inception meeting

An inception meeting will be organised by the Commission's services at the Commission's premises in Brussels within **two weeks** after signature of the contract by the last contracting party. The Contractor will have to finalise the inception report on the basis of the outcome of the inception meeting within five working days after the meeting.

Progress meetings (management meetings)

Progress meetings will be held every **six months** with the Commission at the Commission's premises in Brussels. Minutes of the meetings will be submitted to the Commission within five working days after each meeting.

First workshop

An interim meeting during which the Contractor will present D1 and D2, versions 1 will be held within **5** months after signature of the contract by the last contracting party. The Contractor will have to finalise the interim study report on the basis of the outcome of the interim meeting.

One hundred persons are foreseen to attend the workshop. The Contractor may be requested to suggest names of attendees to the Commission. The Contractor will organise the workshop, including sending the invitations after Commission approval. In particular, the Contractor will suggest names of persons able to represent the undertakings which were analysed during Task 2. The civil society should also well be represented in the workshop.

For the workshop, the Contractor will invite at least five representatives from the civil society (ex. consumers associations, NGOs active on civil liberties, fundamental rights or protection of privacy). Travel expenses of these representatives including hotel and subsistence expenses, will be borne by the Contractor,

The Commission will provide at no costs for the Contractor, the premises for the workshop (including coffee and meal).

Final Workshop (2nd public workshop)

The draft final study report below will be presented by the Contractor during a final workshop to be held within **17** months after signature of the contract by the last contracting party. The Contractor is expected to provide a senior member of staff having worked on the contract to deliver a presentation on the main findings. The workshop will be organised by the Contractor in Brussels and will last one day. The draft final report will then be updated to take into account the feedback provided by the attendees.

One hundred persons are foreseen to attend the workshop. The Contractor may be requested to suggest names of attendees to the Commission. The Contractor will organise the workshop, including sending the invitations after Commission approval. The civil society should also well be represented in the workshop. The Commission will provide at no costs for the Contractor, the premises for the workshop (including coffee and meal).

For the workshop, the Contractor will invite at least five representatives from the civil society (ex. consumers associations, NGOs active on civil liberties, fundamental rights or protection of privacy). Travel expenses of these representatives including hotel and subsistence expenses, will be borne by the Contractor,

The Contractor will have to finalise the final study report on the basis of the outcome of the final workshop.

Specialised ad hoc meetings

The Contractor will often be asked to accompany the Commission, in an adviser capacity, to meetings with stakeholders (ex. meetings with standardisation bodies, meetings with technical committees…). An average frequency of one meeting per month should be foreseen. Most meetings will not exceed one day. Most meetings will take place in Brussels but the Contractor should foresee three two days meetings taking place in other cities in Europe.

Additionally, the Contractor should be ready to attend on a short notice, internal Commission meetings to advise the Commission on specific detailed issues regarding the subjects of this study. For instance, these meetings could be the preparation of larger meetings with the stakeholders; in that case, the preparation meeting would take place the day before the stakeholder meeting. An average frequency of one meeting per month should be foreseen. Most meetings will take place in Brussels. These meetings will not exceed one day.

In particular, for each of the two public workshops, a preparation meeting will be organised (most probably the day before) and a debriefing meeting will be organised (most probably the same day or the day after).

The Tenderer should thus foresee a budget for an average of **36 missions** to attend these ad hoc meetings. Usually meetings will not start before 10:00 and finish not later than 16:30 allowing travelling the same day back and forth to Brussels from most European cities.
The Contractor may be asked by the Commission to draft minutes of these meetings. Draft minutes should then be submitted within two working days after the meeting (set of deliverables D4.4).

4.3 Timetable

Deliverable	**Meeting**	**Month**																	
↓	↓	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
Inception report D0.1	Inception meeting																		
1st interim study report																			
	1st public workshop																		
2nd interim study report																			
Draft final study report D4.2																			
	2nd public workshop																		
Final study report D4.2																			

Schematic indicative timetable

5 TERMS OF APPROVAL OF DELIVERABLES

NB. Deliverables that do not have a style allowing for easy reading or written in incorrect English will be rejected.

5.1 Study report(s)

After reception of each deliverable included in section 4.1 above, the Commission will have **forty-five** calendar days in which:

- to approve it,
- to reject it and request a new report.

If the Commission does not react within this period, the report shall be deemed to be approved.

Where the Commission requests a new report because the one previously submitted has been rejected, this must be submitted within **thirty** calendar days. The new report shall likewise be subject to the above provisions.

5.2 Technical reports (management reports)

The Commission shall have **forty-five** days from receipt to approve or reject the technical reports, and the Contractor shall have **twenty** calendar days in which to submit additional information or a new report.]

6 RELATIVE DOCUMENTATION

Interested parties may consider useful consulting the following indicative list of documents and initiatives related to the subjects of the study.

- Directive 1999/93/EC of the European Parliament and the Council of 13.12.1999 on a Community framework for electronic signatures
- Decision 2003/511/EC of 14.7.2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council
- Commission Decision 2000/709/EC of 6.11.2000 on the minimum criteria to be taken into account by MS when designating bodies in accordance with Article 3(4) of Directive 1999/93/EC of the European Parliament and Council on a Community framework for electronic signatures.
- *Action Plan on e-signatures and e-identification to facilitate the provision of cross-border public services in the Single Market, COM(2008)798 of 28.11.2008*
  http://eur-ex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52008DC0798:EN:NOT
- *Commission Decision 2009/767/EC* of 16.10.09 on «Trusted Lists» of qualified signature certificate providers
  http://ec.europa.eu/information_society/policy/esignature/eu_legislation/trusted_list
- Mandate M460 to Standardisation organisations,
  http://ec.europa.eu/information_society/policy/esignature/eu_legislation/standardisation/index_en.htm
- IDABC studies:
  - Study on mutual recognition of e-signatures for eGovernment applications: http://ec.europa.eu/idabc/en/document/6485
  - Feasibility study of a European federated e-signature validation service: http://ec.europa.eu/idabc/en/document/7764
  - eID Interoperability for pan-European government services: http://ec.europa.eu/idabc/en/document/7768
- Regulating a European eID. A preliminary study on a regulatory framework for entity authentication and a pan European Electronic ID for the Porvoo e-ID Group, 31 January 2005, Thomas Myhr, http://porvoo9.gov.si/Thomas_Myhr_report.pdf
- Relevant IST PSP projects (ex. STORK, PEPPOL, SPOCS):
  http://ec.europa.eu/information_society/activities/ict_psp/index_en.htm
- Relevant MS (or form third countries) laws on eID, e-signature, certified email, time stamping, (long term) archiving, electronic seals (or stamps), official email addresses for legal and/or natural persons, delegation of power.
- RISEPTIS report: http://www.think-trust.eu/riseptis.html
  Relevant ENISA documents: http://www.enisa.europa.eu
- Liberty alliance initiative: http://www.projectliberty.org
- Kantara initiative: http://kantarainitiative.org/
- The OpenID Foundation: http://openid.net/foundation
- OASIS standards: www.oasis-open.org
- Etc.