EU tender for a

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

SMART 2010/0008

Technical, financial and administrative sections

submitted by DLA Piper, Sealed, Timelex, PwC and Studio Notarile Genghini

Table of contents

Executive Summary

This tender is submitted by the law firm DLA Piper UK LLP ("DLA Piper"), following the general invitation to tender of the Directorate-General Information Society and Media, n° SMART N° 2010/008. We understand that the aim of this project is to study the feasibility of a comprehensive EU legal framework for identification-related electronic credentials required to secure electronic transactions (including ancillary services).

Together with its four subcontractors, DLA Piper is convinced to have the required skills and capabilities to address all the needs of this project. Assembling an international and cross-disciplinary team of specialists in the fields of identity management, electronic signatures, data protection and security, the project team has the necessary theoretical and practical experience to tackle the issues addressed in this tender.

Approach

We based our approach on the four tasks specified in the RFP. However, to make sure we deliver our services in an optimal way, we included an upfront Task ("Task 0"), in which we will kick-start the project and ensure optimal mobilisation of all resources involved. Subsequently, we will perform Task 1 (assessment of hypotheses and issues) and Task 2 (stock taking and recommendations) mainly in parallel. During Task 3 (building blocks) we will provide building blocks for a possible pan-European IAS framework. We will reflect about implementation options and combinations of these building blocks to achieve optimal results. Finally, during Task 4, we will provide technical and legal support to the Commission in its interaction with the Stakeholders.

Project Team

To perform the study, the tenderer will set up the following project team:

§ An interdisciplinary and neutral **Core Team** of eight members will be responsible for performing the factual analysis of the issues at stake, and the drafting tasks. It consists of legal, technical and economic experts who each have many years of experience with IAS as a policy challenge and as a tool in the deployment of large-scale projects: Prof. Dr. Patrick Van Eecke, Prof. Dr. Riccardo Genghini, Prof. Dr. Jos Dumortier, Hans Graux, Olivier Delos, Sylvie Lacroix, Marc Sel and Frederic Van Hoorebeke.

  The Core Team will also host a project manager (Maarten Truyens), who will undertake the management tasks in relation to the contract execution.

§ A **Field Experts Team** consisting of ten members will support the Core Expert Team by providing relevant input through performing specified tasks: John Bullard (UK), Claudia Diaz (ES), Marit Hansen (DE), Stephen Kent (US), Chris Reed (UK), Teemu Rissanen (FI), Stefan Santesson (SE), Marc Stern (BE), Eric Verheul (NL) and Jane Winn (US).

  They will review the deliverables of the Core Team, act as a first soundboard for the suggestions and solutions put forward by the Core Team members. Some of them will also draft specific (parts of) deliverables.

- A board of **Stakeholders** will consist of a representative sample of large enterprises, SMEs, universities, governments and consumer organisations. These stakeholders will be consulted for their views, and on the potential solutions proposed by the Core Team. They will allow the Core Team to perform reality checks, investigate the current concerns of information technology players, and evaluate the practical impact of the proposed legal instruments.

Our key strengths

The tenderer is convinced that its project team provides for a balanced structure that guarantees the completeness and overall quality of the deliverables, in accordance with the tender specifications. The key strengths of the team are:

- a **"best-of-breed"** combination of legal and technical expertise from various companies;
- a balanced **international and cross-gender** composition of the project team;
- significant previous **experience with previous projects** for the European Commission, including a significant number that directly relate to IAS;
- significant previous experience in **consensus building**;
- almost the entire Core Team is **based in Brussels**, allowing for low-barrier and cost-efficient meetings with the Commission;
- a **strong and existing network** of contacts and channels for dissemination and testing of preliminary results and ideas;
- **proven legal and technical expertise** in analysing e-signatures and e-authentication (the Core Team contains senior experts with more than fifteen years of experience)

Pricing

Costs	Cost Area	Total
Professional fees	Core Team	270,000 EUR
	Field Experts Team	40,000 EUR
Travel and subsistence expenses	Core Team	11,000 EUR
	Workshops	10,000 EUR
Other expenses	N/A	0
	Total, fixed amount	**331,000 EUR**

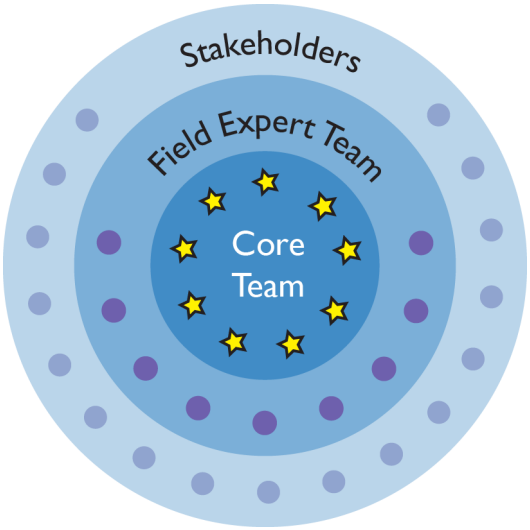
1. Technical Section

1.1 Overview of the proposed team

This Section identifies the tenderer and the subcontractors to perform the required work.

The tenderer proposes a three-layered team:

- **Core Team** – A multi-disciplinary Core Team of eight experts and one project manager will be responsible for performing the main tasks of the project (analysing the current framework, proposing solutions, drafting reports and organising the work-shops).



- **Field Experts Team** – A Field Experts Team of ten international legal and technical experts will perform the quality review of each deliverable, and will provide the Core Team with specific expertise.

- **Stakeholders** – A board of stakeholders will be appointed from industry (SMEs and multinationals), academic circles, consumer protection organisations and governmental agencies. These stakeholders will be consulted for their views on issues, and will particularly be given the opportunity to evaluate the impact and effectiveness of the proposed solutions.

All required justifications for the identification of the tenderer and subcontractors, as well as all detailed curricula vitae, can be found in the annexes.

1.2 Core Team (Circle 1)

1.2.1 Technical, legal and economic

a. Overview

Following the careful study of the tendering specifications, an in-depth analysis of the needs and requirements, the tenderer is convinced that it can offer, through its proposed multidisciplinary Core Team of experts, the guarantee of a strategic partnership that can deliver the best economical results for the European Commission.

The tenderer is proud to present its Core Team, which is composed of renowned experts in their field:

- **Patrick Van Eecke** (DLA Piper), legal expert in the IT field, and in particular in the regulatory framework of e-signatures and ancillary services both a national and international levels;

- **Riccardo Genghini** (Studio Notarile Genghini)**,** expert in the field of standards for e-signatures and ancillary services, and supporter of open standards and technologies. Starting in 1999 with the Protection Profile for Secure Signature Creation Device (CEN CWA 14169), he has spent the last decade in implementing legal rules and principles in technical specifications (and open source code).

- **Jos Dumortier** and **Hans Graux** (Time.lex), both legal experts with a dual profile as practising lawyers and academics, whose expertise specifically covers the EU legal and policy framework with respect to eSignatures and eID interoperability;

- **Olivier Delos** and **Sylvie Lacroix** (SEALED), two experts in eSecurity combining academic, practical (hands on) and demonstrated experience in technical, standardisation, legal, and business implementation aspects of electronic identities, electronic signatures and related ancillary (trusted) services;

- **Marc Sel** and **Frederic Van Hoorebeke** (PwC) are experts in, respectively, the field of eID and Identity Management and in the field of economic strategy. Marc has been involved in numerous identity, access and e-signature projects, both for government and private parties. Frederic has an in-depth experience in developing, reviewing and assessing business plans, both on realism and viability. He has led projects in a private, public and public-private context in, amongst others, technology industry.

b. Characteristics

The Core Team is at the same time **interdisciplinary** (legal, economic and technical expertise), **multilingual** (English, French, Dutch, Italian and German), **international** and **neutral** (no links with enterprises, trade associations or governments). It combines a strong academic leadership with practical expertise, as all experts in the Core Team are experienced in the areas of security, privacy, electronic identities, identity management and electronic signatures.

Moreover, every single member of the Core Team has **participated in multiple large projects** that are similar in scope and subject matter to the current project, not only for several national governments, but also for the European Commission.

All members of the Core Team will be **fully dedicated** to the project: apart from the input of the Field Experts Team and the Stakeholders, no work will be delegated to other persons inside or outside each team member's firm (particularly not to juniors). The members of the Core Team will thus be committed to the project on a day-to-day basis.

As the Core Team is **multilingual**, it can understand and process the vast majority of all reports, legal doctrine and case law in the field of the study.

Finally, it is important to emphasize that instead of proposing a single company to the Commission, a "**best-of-breed**" approach is followed, with a team that is composed of representatives of five different companies. This selection will ensure both a high level of quality and a diverse approach to the problems to be tackled.

c. Strengths

As described above, the Core Team gathers **best in class experience** perfectly fitting the tender specifications, covering in particular the following fields:

§ **A strong and existing network** of contacts and channels for dissemination of preliminary findings, draft reports and final results, collecting feedback and building consensus with key stakeholders and interested parties;

§ **Proven expertise in analysing complex legal aspects of e-signature and e-authentication**, including analysis and interpretation of laws, development of new laws and case laws both at national Member State level and EU level. The three legal expert groups of the Core Team each have more than fifteen years of legal expertise in this area, in particular in the following areas:

- **Setting-up the current eSignatures Directive**, in particular analysing the impact and effect of the eSignatures Directive by serving private sector CSPs, but also through a number of policy support studies for the European Commission.

  *Examples include the 2003 Study on the Legal and Market Aspects of Electronic Signatures and the 2007 and 2009 Preliminary studies (by **Jos Dumortier and Patrick Van Eecke**) on mutual recognition of eSignatures for eGovernment applications. These studies comprehensively described approaches taken in the Member States with respect to eSignatures in eGovernment applications.*

- Analysing **solutions to address eSignatures interoperability**.

  *An example is the 2009 European Federated Validation Service (EFVS) study (undertaken by Siemens, **Time.lex and SEALED**), which examined the feasibility of establishing a federated signature validation tool at the European level, and included a strategy for improving eSignature interoperability in the longer term.*

  *Two other examples are the 2009 Study on electronic documents and electronic delivery for the purpose of the implementation of Art. 8 of the Services Directive, and the 2008 Preliminary Study on the electronic provision of certificates and attestations usually required in public procurement procedures. Core Team member **Hans Graux** was the primary author of both studies.*

- Analysing solutions to **address eID interoperability at the EU level**.

  *An example is the 2007 and 2009 eID Interoperability for PEGS, which examined how electronic identification is being handled in each of the Member States in eGovernment applications. Core Team members **Hans Graux and Jos Dumortier** were the primary authors for both editions (2007 and 2009). Another example is the 2008 report for ENISA on the state of pan-European eIDM initiatives, which provided an overview of all key ongoing initiatives and challenges. The report was authored by **Jos Dumortier and Hans Graux**.*

  Furthermore PwC executed various studies on behalf of clients with regard to eID interoperability e.g. in the context of provision of telecommunication services, as well as in the field of e-invoicing. PwC also assisted DIGIT with aligning their internal ECAS Identity Services with STORK components.

- **Developing national laws on e-signature and e-authentication**.

  *Specifically, **Jos Dumortier and Patrick Van Eecke** were consulted in the drafting of Belgian legislative texts (laws and decrees) on eSignatures, eID and eGovernment in Belgium. **Patrick Van Eecke** was also involved in drafting the Belgian bill on TTP (currently pending).*

§ In-depth knowledge of those legal aspects and their **interrelation with the technical and standardisation related aspects:**

- **Hands-on experience with the technical development and maintenance of e-signature standards**.

  Riccardo Genghini *is the current Chairman of the ETSI ESI (Electronic Signature Infrastructure) technical committee of ETSI in charge of the development and maintenance of ETSI standards related to electronic signatures. He was previously active in CEN for similar standardisation activities.;*

  Patrick van Eecke *conducted a study on ICT standardisation in the EU. The study analysed the current European ICT standardisation policy and the prospective evolution for the forthcoming 10 years, and put forward a set of recommendations for establishing a new European ICT standardisation policy.*

  Sylvie Lacroix and Olivier Delos *have a recognised knowledge of such standardisation activities through their personal involvement in some ETSI Specialist Task Force in charge of developing some of these standards, as a Member of the EESSI Steering Group, through the conduction, with Patrick van Eecke) of the Study on the standardisation aspects of e-signatures, through their involvement in supporting the Commission in writing the Mandate M460 in the field of ICT applied to electronic signatures, and through the conduction of the CROBIES study providing technical input to the Mandate M460.*

  Hans Graux provided legal support to the CROBIES study, including by analysing and providing recommendations on the compatibility of suggested technical solutions with the existing legal framework, and by assisting the European Commission in drafting Commission Decision 2009/767/EC of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the 'points of single contact' under Directive 2006/123/EC; the latter Decision provided a legal basis for the establishment and maintenance of national trusted lists of supervised or accredited CSPs.

- **Proven expertise in cryptography and PKI**. The experts of the Core Team cumulate more than 60 years of expertise in these areas.

  Marc Sel *has a long proven track record of advising clients on cryptography and PKI. This includes areas as diverse as: applications (ERP applications, Adobe and Microsoft); products that include PKI functionality for security reasons (Lotus Notes, internet browsers, mail clients and servers, Microsoft Windows PKI); dedicated PKI hard- and software products (e.g. RSA, Entrust, Cryptomathic, Guardeonic, Utimaco, nCipher); smart card implementations; Certification Authority services (Verisign, Cybertrust/Verizon, Certipost and their competitors); Member State Government bodies responsible for CA accreditation and control; EC-supported PKI services such as for the Digital Tachograph (ERCA – European Root Certification Authority). He has been involved in the Belgian eID card as well as in the deployment of PwC's global PKI solution beTrusted.*

  Sylvie Lacroix *and* ***Olivier Delos*** *started their career by research in cryptography and have several publications in that fields (e.g. CRYPTO'94).*

- **Proven business and economic hands on experience** around the development of e-signature and e-identification products and demonstrated capacity to assess the related economics aspects.

  Between 1998 and 2005, ***Sylvie Lacroix and Olivier Delos*** *have designed, set-up, deployed and managed the development and provision of Belgacom, then Certipost, E-Trust certification services including the provision of qualified certificates, timestamping services, electronic registered mail services as well as the related electronic signatures creation/verification products and devices.*

*Over the last 15 years, **Frederic Van Hoorebeke** has been involved in numerous projects on economic strategy and viability. Recently, he advised Acerta on their e-invoicing business case and assisted DNS (non-profit organization for the registration of the .be domain names) on the development of their strategic business plan. In 2006, Frederic advised Banksys on their pricing strategy and in 2009 he advised the Flemish Government on state aid for the restructuring of two global automotive players and the impact on micro- and macro-economic level. This broad scope and cross-sectoral experience will prove extremely valuable in combination with the in-depth technical experience of the PwC team members.*

§ **Proven consensus building** capability:

*For example, a critical part of the aforementioned EU ICT standardisation study undertaken **by Patrick Van Eecke**, consisted in finding a consensus between the many stakeholders (particularly the ESOs and private consortia). It is interesting to note that this study is reported to have played a significant role in the recent Digital Agenda of the European Commission.*

*In the context of the CROBIES study, when supporting the Commission in the context of the Expert Groups meetings on electronic procedures, **Olivier Delos** and **Hans Graux** demonstrated their capability in building consensus around the Trusted Lists technical specifications and legal provisions of Commission Decision 20009/767/EC.*

*When assessing the options available to PVCYCLE, the sector group for producers of PV modules in Europe, **Frederic Van Hoorebeke** and **PwC** assisted PVCYCLE management in finding consensus amongst dozens of producers all over Europe. For that purpose, amongst others, roadshows and conferences were set-up and moderated by PwC.*

§ Strong knowledge of **EU data protection law**

*Core Team members **Patrick Van Eecke and Maarten Truyens** have undertaken a study on the legal analysis of the EU information society legal framework. One of the most important parts of this study consisted of a critical review of the current data protection legal framework.*

*Similarly, **Jos Dumortier and Hans Graux** conducted a study on behalf of the UK Information Commissioner assessing the effectiveness and impact of the EU Data Protection Directive.*

Both DLA Piper and Time.lex undertake on a daily basis client work in the field of data protection — e.g. conducting international data privacy audits, drafting privacy policies, or assisting clients with binding corporate rules.

1.2.2 Project management

The **project management** will be the responsibility of Maarten Truyens (DLA Piper). As further detailed below, Maarten has ample experience with managing large and interdisciplinary projects, drafting reports and integrating contributions from various parties. Moreover, Maarten worked as a technical consultant before joining the DLA Piper law firm as an IT lawyer. The combination of his legal knowledge and technical background will enable him to tackle the project management from both the legal and the technical side.

1.2.3 Members of the Core Team

a. Patrick Van Eecke (DLA Piper)

Prof. Dr. Patrick Van Eecke is a partner in the IT law Department of DLA Piper in Brussels. Patrick Van Eecke has carried out diverse studies and consultancy assignments in the field of electronic signatures both for public authorities and private clients. He gained his doctoral degree at the K.U.Leuven with a study on the legal aspects of electronic signatures.

He is extensively involved in diverse research and consulting projects for the European Commission and several national governments. For example, Patrick was, together with Jos Dumortier, involved in the first European Commission Study on the legal aspects of electronic signatures (1998), the Study on electronic signature policies (2001), the Study on long term archiving of electronic signatures (2001) and Study on the legal and market aspects of electronic signatures (2003). He was the lead consultant in the study on the future of the ICT standardisation policy, a study on the review of the EU legal framework for the information society, , as well as a study on the creation of an extensive database regarding the Unfair Commercial Practices Directive.

As a national representative, Patrick was involved in the European Council debates on the directive on electronic signatures and the directive on electronic commerce. He was also advising the Economic and Social Committee of the European Communities on these matters. As the legal expert of the EESSI expert team (European Electronic Signature Standardisation Initiative) he was co-author of the first EESSI report and following legal deliverables.

Patrick is a professor at the University of Antwerp, teaching European Information and Communications Law. He is also a guest lecturer at Kings College (London, since 2004) and Queen Mary University (London, since 2004). Patrick is the author of several legal articles and books on computer crime, electronic signatures, electronic contracting and privacy and is a regular speaker on national and international conferences. In 2008 and 2009, he gave more than 50 speeches at national and international events, including appearances on national TV and radio stations and interviews in newspapers. Patrick also has a bi-weekly column on e-business and the law in the leading Belgian IT journal *"IT Professional"*. Patrick is editor of the Belgian *Revue de Droit Commercial* (Larcier), responsible for information technology law. He is also editor of the international *Journal of Internet Law* (Kluwer) responsible for the European internet related legal issues and European correspondent of the international *Digital Evidence Journal* (Pario).

Patrick is member of the Brussels bar and is associate member of the American Bar Association.

b. Jos Dumortier (Time.lex)

Prof. Dr. Jos Dumortier is a professor in Information Technology Law and Legal Informatics at the Faculty of Law, K.U.Leuven since 1989 and Director of the Interdisciplinary Centre for Law and Information Technology (ICRI) since its start in 1990. With this research group he is in charge of the legal guidance of a large number of IT law and IT policy related research and development projects in Belgium, in particular in the context of the Institute for Broadband Technology (www.ibbt.be). As the cabinet advisor to the Minister of Justice between 1995 and 1999, he was also in charge of the transposition of the European data protection directive 95/46/EC into Belgian law. Prof. Dumortier frequently works as an expert for the European Commission, for Belgian and foreign governments and for private organisations. He is a member of several boards and committees in Belgium and abroad. Professor Dumortier published numerous books and articles on

various issues related to information technology law. He is the editor of the International Encyclopaedia of Cyber Law. He is also a partner and co-founder of the law firm Time.lex, which specialises in information and technology law.

c. Riccardo Genghini (Studio Notarile Genghini)

Prof. Dr. Riccardo Genghini is not only one of the best known specialists in the field of electronic signature standards. He is also a respected academic in the field of international corporate law and developer of technologies for the certification of digital data, transactions and identities.

Visiting Professor at the Università Cattolica di Milano for Comparative Commercial Law, in the last 10 years, he has been researching the legal, economic and social impact of digitalisation: the outcome of his research will be published in 2010 under the title "Digital Agreement". His research on the topic began in Germany, involving professionals and academics from Germany, Belgium, Austria, Czech Republic, Italy, whose results have been published with the *"Elektronische Signaturen. Kulturelle Rahmenbedingungen einer technischen Entwícklung"* in 2002.

Since 2010 he is the Chairman of the Electronic Signatures Coordination Group, that coordinates the standardisation effort of CEN and ETSI in the field of electronic signatures, with respect in particular to the implementation of the COM(2008) 798.

Since 2005 he has incorporated a company under Luxembourg law, with the sole scope of creating the technologies needed by notaries for authenticating digital signatures (also at distance), for creating notarial digital public deeds, and for securing emails and for long term preservation of data. In 2008, he was the first notary in Europe to authenticate a fully digital agreement (which has been also filed at the registrar of companies in Milano). Since then he has been authenticating more then one thousand digital notary deeds with customers, like Deutsche Bank, Barclays Bank PLC or ING Direct NV.

Since 2004 Riccardo Genghini is Chairman of the working group on Electronic Signature and Infrastructures (ESI) of ETSI - European Telecommunications Standards Institute.

From 2001 to 2004 he has been Chairman of CEN/ISSS E-Sign Workshop (European Committee for Standardisation - Information Society Standardisation System): under his chairmanship have been approved and updated the three CEN CWA that specify the compliance with the requirements laid down in Annex II f to Directive 1999/93/EC (CWA 14167-1 & 2 regarding the security requirements for trustworthy systems managing certificates for electronic signatures, as well as CWA 14169 on secure signature-creation devices).

He is a strong supporter of open standards, and in this context, he had a significant role in influencing Adobe's strategy with PDF (which has been entrusted to ISO, becoming so an open specification) and its active involvement in the standardisation of PDF signatures as European standards.

In 2003 he performed a study on identity management (*"Identity Management Systems (IMS): Identification and Comparison Study"*) in collaboration with Unabhängiges Landeszentrum für Datenschutz (ULD) Schleswig-Holstein and co-financed by Joint Research Center of Sevilla.

Starting from 2000 Riccardo Genghini has been involved in the law making process in Italy, Austria, Luxembourg and Germany.

Finally, Riccardo Genghini carries out his activity of notary in Milan where in 1990 he founded the Studio Notarile Genghini, one of the most technologically advanced legal offices in Italy and in Europe in working with digital agreements and deeds.

d. Hans Graux (Time.lex)

Hans Graux graduated in Law in 2002, and obtained a complementary degree in IT in 2003 (both at K.U.Leuven, Cum Laude). He then joined the Interdisciplinary Centre for Law and Information Technology, where he did fundamental research on a number of IT law related issues, with a specific focus on electronic identity management through the European ModinisIDM Study.

In May 2005 he joined the IT law department of the Brussels based law firm Lawfort, where he participated in a number of international studies, specifically on the European level. In July 2007, he co-founded the IT law firm Time.lex. His expertise lies mainly in the collection of legal and administrative information in cross border studies, in the analysis of legal frameworks and policy choices, and in formulating specific policy recommendations in this field to eliminate barriers to the correct functioning of the internal market. His recent work for the European Commission has focused specifically on eSignatures, electronic identity management, data protection, eProcurement and the implementation of the Services Directive.

e. Olivier Delos (SEALED)

Olivier Delos (CISSP, CISA) is a recognised expert in Europe in the area of eSignature, eAuthentication and eIdentification (eID cards and ePassports in particular) and their business exploitation and usages, whether in corporate, national or international infrastructure programs. He also has a pretty good experience with regards to the legal & regulatory aspects as well as with the standardization of these techniques.

From a technical background, Olivier has M.S. degree in Computer Science Engineering (Ingénieur civil en Informatique – June 1991). Olivier started his career as research assistant in cryptography at the Université Catholique de Louvain-la-neuve, before moving to Belgacom – the major telecom operator in Belgium – (and then Certipost) were he founded the E-Trust Services (i.e. Trusted Third Party services issuing Qualified Certificates, Electronic Identity Certification, Timestamping services and Electronic Registered Mail). In 2005 he founded his own company, SEALED, together with Sylvie Lacroix.

Olivier has numerous publications and is active speaker in major conferences in Belgium, Europe and beyond. His demonstrated experience acquired through major projects can be illustrated in the various domains related to e-Security, electronic identities, electronic passports and other Machine Readable Travel Documents, electronic signatures and related Trusted Services ranging from concrete business and practical implementations (by the implementation of major projects in e-Security within Belgium and Europe, such as the Belgian eID Cards PKIs, cross-border interoperability of eSignatures, Trusted Lists), consulting projects up to R&D and technical expertise (Olivier published several articles on R&D works related to cryptography and e-Security schemes in the first part of his career, and again recently was co-designer of a digital signature scheme allowing to reconcile citizen identity based eID schemes with business identity needs that is very promising in this era of eID deployment in Europe). He is also active in the context of eSignature standardization as having talking part to the specifications and genesis of the recent European Commission standardization mandate M460 on eSignatures and a recognized and consulted expert in this matter.

f. Sylvie Lacroix (SEALED)

Sylvie Lacroix (CISA) is a recognised expert in Europe in the area of eSignature, eAuthentication and eIdentification (eID cards and ePassports in particular) and their business exploitation and usages, whether in corporate, national or international infrastructure programs. She also has a pretty good experience with regards to the legal & regulatory aspects as well as with the standardization of these techniques.

From a technical background, Sylvie has M.S. degree in Electricity Engineering (Ingénieur civil en Electricité – June 1994). Sylvie started her career as research assistant in cryptography at the Université Catholique de Louvain–la-neuve, before moving to Belgacom – the major telecom operator in Belgium – (and then Certipost) were she was a key person in the foundation of the E-Trust Services (i.e. Trusted Third Party services issuing Qualified Certificates, Electronic Identity Certification, Timestamping services and Electronic Registered Mail). In 2005 she founded her own company, SEALED, together with Olivier Delos.

Sylvie has numerous publications and is active speaker in major conferences in Belgium, Europe and beyond. Her demonstrated experience acquired through major projects can be illustrated in the various domains related to e-Security, electronic identities, electronic passports and other Machine Readable Travel Documents, electronic signatures and related Trusted Services ranging from concrete business and practical implementations (by the implementation of major projects in e-Security within Belgium and Europe, such as the Belgian eID Cards PKIs, cross-border interoperability of eSignatures, Trusted Lists), consulting projects up to R&D and technical expertise (Sylvie published several articles on R&D works related to cryptography and e-Security schemes in the first part of her career, and again recently was co-designer of a digital signature scheme allowing to reconcile citizen identity based eID schemes with business identity needs that is very promising in this era of eID deployment in Europe). She is also active in the context of eSignature standardization as having talking part to the specifications and genesis of the recent European Commission standardization mandate M460 on eSignatures and a recognized and consulted expert in this matter.

g. Marc Sel (PricewaterhouseCoopers)

Marc started his career in 1979 and moved through various positions with Texas Instruments, Alcatel (the former Bell Telephone Manufacturing Company) and Esso. In January 1989 he joined Coopers & Lybrand, where he started as a consultant. After gradually building up more experience by serving international clients, he now takes on the role of Director for the Belgian "Information Protection" group of PwC. He specialises in information security and cryptography, from organisational, managerial and technical perspectives. He has been involved in numerous identity and access projects, as well as e-signature projects, for government and private sector alike.

He holds degrees from Brussels Free University and Royal Holloway University (London, UK). He also holds the CISA certification (1993), CISM (2004) and CGEIT (2008). He is also an accredited ISO/IEC 27001 Lead Assessor, and Prince2 as well as ITIL certified.

He has been assisting the Belgian Ministry of Interior from 2001 to 2003 with the implementation of the Belgian eID card. He has been assisting the Belgian Ministry of Mobility with the implementation of the European digital tachygraph for Belgium. He has been advising clients such as Unified Post with attempting to overcome the constraints that are now present in the internal market

due to Member States imposing their own national requirements on e-Signatures. He advised EC DIGIT with regard to STORK.

h. Frederic Van Hoorebeke (PricewaterhouseCoopers)

Frederic Van Hoorebeke, Master in Law and Master in Business Administration by education, is the head of PwC Belgium's Strategy & Economics department and has extensive experience in leading and conducting economic and strategic studies. He has been involved in numerous studies, transactions and valuation assignments, as well as in business plan assessments and reviews.

He has experience in waste, automotive, technology and infrastructure. He gained this experience advising both public and private clients.

Recently, Frederic was involved in the assessment and critical review of the business plan of two international automotive OEMs, the development of Banksys's business plan and pricing strategy and DNS's business model.

i. Maarten Truyens (DLA Piper)

Maarten Truyens is a qualified lawyer registered with the bar of Brussels, working at DLA Piper Brussels. He specialises in the fields of consumer protection, e-commerce, data protection, telecom, IT contracting, outsourcing and new technologies. His practice includes clients in both the public and the private sector, in Belgium and abroad, with a special attention for SMEs.

Before joining DLA Piper Belgium in 2005, Maarten worked as an IT consultant, in areas such as transactional high-volume websites, database publishing, multimedia and business automation. His clients value his active technical knowledge of internet-related technologies, internet-focused programming languages, database products and Web 2.0 programming frameworks and methodologies), business architectures and general-purpose programming languages (C++, C, C#, Java, Delphi) on multiple platforms.

In his daily practice at DLA Piper, he regularly applies his technical knowledge. This hands-on experience with e-commerce matters, from both a technical and managerial point of view, has rendered him invaluable technical information, which he now combines with his legal knowledge.

Maarten is also a contributing editor of the international Journal for Internet Law (Wolters Kluwer) and is also a regular speaker on seminars regarding electronic document management, ICT law, privacy and corporate governance. He regularly participates in both national and international projects investigating the impact of new IT and telecommunications law. He was also involved in the EU study on technology transfer, and is currently involved in the EU study on the review of the EU information society legal framework.

1.2.4 Companies represented in the Core Team

a. DLA Piper

With more than 3,500 lawyers located in 70 offices in 30 countries, DLA Piper is the largest legal services provider in the world (based on turnover figures).

DLA Piper in Belgium is recognised as one of the fastest growing law firms in Belgium, and is frequently listed and recommended by the yearly Legal 500 editions.

It is a full service law firm, and the expertise of its lawyers includes the following areas of practice: technology, media & commercial matters, banking & finance, business support & restructuring, corporate law, EU and competition, EU regulatory, government affairs, human resources, litigation & arbitration, real estate, administrative law, environmental law and tax.

Currently with a number of 124 lawyers strong (of which 28 partners), DLA is a top-3 full service law firm with offices located in Brussels and Antwerp. Our strength in Belgium is an essential part of our vision to be the leading global business law firm, and an example of how we combine local strength with international capability.

DLA Piper's technology department in Belgium is made up of the firm's specialist IT, IP, telecommunications, media and e-business lawyers. It is one of the largest specialist groups of its sort in Belgium, and is recognized as a leading Belgian practice advising Belgian and international corporations, public entities, IT users and outsourcers.

Our clients include major government departments, some of the world's leading technology and communications companies, national regulatory authorities, major financial institutions, owners of well-known international brands and patents, multinational media and entertainment companies, internet service providers, e-business enterprises, and many more. The reputation of our team is based on the successful synthesis of several crucial qualities: cutting-edge expertise, industry insight and knowledge, the imaginative use of technology and project management skills to facilitate the delivery of services to our clients, a creative approach to costing and budgeting our work and a pragmatic approach to problem-solving, all of which are underpinned by a passionate devotion to client service and relationship management. Consequently, a number of our lawyers are recognized as leaders in their field.

In the technology arena, we have an enviable reputation in IT and business process outsourcing and have extensive experience of acting and advising on innovative technology developments, PPP IT projects, e-commerce, technology procurement, systems implementation and integration projects for a blue chip range of clients. Our work also involves advising on an array of technology issues such as software development and licensing, computer games, data protection, encryption issues and the protection of intellectual property rights.

As the sums of these projects are confidential, these are not included in this document.

b. Studio Notarile Genghini (SNG)

Studio Notarile Genghini (SNG) is a (latin) Notary Public office based in Milan and Rome. It was established in 1990 by Riccardo Genghini and has become probably the most technologically advanced notary office in Europe. It is the only notary office in Europe working on a daily basis with digital contracts and deeds, with large customers, such as banks. It holds in escrow software for multinational companies, it certifies the delivery of e-mails and the content of websites, utilizing technologies specifically developed for such purposes. Therefore Riccardo Genghini has not only a theoretical knowledge of legal issues related with the use of electronic signatures, but has also empirical experience of their utilisation by the stakeholders and of the related barriers to entry.

SNG has been involved in the development of the Italian legislation on digitalization and is currently working in collaboration with several Italian Public Administrations on the changes in C.A.D.

- Codice Amministrazione Digitale (*Digital Administration Code*), which is one of the most advanced in Europe, particularly from the perspective of its effective utilisation not only by the state, but also by stakeholders (2.6 millions of smartcards actually used in Italy; several hundred thousand of registered emails active; etc.).

SNG is an active member of ETSI, Liberty Alliance and several other fora and organisations, that promote digital identities, transactions and documents.

c. Time.lex

Time.lex is a recently founded law firm based in Brussels, specialised in information and technology law in the broadest sense, including privacy protection, data and information management, e-business, intellectual property and telecommunications. Its activities cover all legal issues encountered in the creation, management and exploitation of information and technology, in all of its diverse forms.

While Time.lex itself is still young, having been founded in July 2007 by Prof. Jos Dumortier, Geert Somers and Hans Graux, the team behind it already has an established track record in its field of expertise. Collectively, the founders represent well over 35 years of experience in information and technology law, from an academic, business and policy perspective, spanning every aspect of this discipline. The Time.lex team has extensive experience in most aspects of information and technology law, both from a pragmatic perspective as lawyers at the bar of Brussels, and from a scientific perspective as academics at the Interdisciplinary Centre for Law and ICT of the University of Leuven (K.U.Leuven).

The Time.lex team is specifically known for its European policy studies in a variety of subjects, including electronic signatures, electronic identity management, e-business and e-government, in which they can rely on an extensive network of IT law experts covering all European countries. From a business perspective, Time.lex frequently assists companies in establishing suitable policies and legal frameworks in their data management activities, including with regard to the cross border transfer and processing of personal data, data security and liability management issues. Its clients include private companies and public sector bodies in the IT sector, financial services, e-health, marketing and e-commerce.

d. SEALED

SEALED is the association of the skills and expertise from two senior e-Security & e-Solutions consultants, Sylvie Lacroix (CISA) and Olivier Delos (CISSP, CISA). SEALED has recognised expertise in Europe in the area of PKIs, eSignatures, eIDs and their business exploitation and usages, whether in corporate, national or international infrastructure programs and have significant experience in business representation and exploitation of these techniques, in particular when applied to eIdentification, eAuthentication and eSignatures.

SEALED is member of several e-security professional associations, including the Belgian L-SEC workgroup and EEMA (the independent European Association for e-Identity and Security).

SEALED acts upstream and downstream covering all aspects of IAS, being on one hand consultants for the European Commission on studies aiming to analyse and enhance the existing framework and, on the other hand, advising large organisations or Members States that implement these techniques, *e.g.,* helping them in building their eID or ePassport infrastructure, or support-

ing the related audits. Through SEALED, and previously when heading the E-Trust Solutions department within Belgacom and Certipost, Sylvie and Olivier managed some of the most important projects related to the e-Security in Belgium and beyond and their practical implementations such as the Belgian electronic identity card (eID) PKIs, ID certification services (for the European Commission, Belgian Notaries, Accountants, Revisors, etc.), e-bidding services, electronic registered mail, securing e-invoicing services, as well as the definition and support to set-up of the Electronic Signature Services Infrastructure (ESSI) at the European Commission (DIGIT).

SEALED was also involved as key expert in recent major European studies on eSignature and eAuthentication. In particular, the European Framework for signature Validation Services (EFVS), the European Study on eSignature Standardisations (ESSS) and the Cross-Border Interoperability of eSignatures (CROBIES) studies. This last study not only gave birth to the genesis and technical specification of the European Mandate 460 on reshaping of the eSignatures standardisation landscape, but also to the technical specifications and annex of Commission Decision 2009/767/EC of 16 October 2009. This last achievement clearly shows SEALED Partners ability to build consensus, as it required the agreement of the 27 Member States.

e. PricewaterhouseCoopers

The PricewaterhouseCoopers (PwC) network comprises more than 163,000 people in 151 countries. From within the original audit profession evolved a number of focused specialisations, including information security, encompassing the IAS field.

PwC operates a global network of firms where it invested and continues to invest heavily in all aspects of information security. This allows PwC to combine virtually all possible viewpoints on IAS, ranging from protecting the information of clients, internal responsibility for identity and access management of worldwide staff, as well as the legal context. This is further enhanced by participation in standard organisations and academic involvement.

As part of the Advisory line of service, PwC has global practices dedicated to Security and IAS with over 2,900 professionals combined worldwide. These leading industry practices are dedicated to providing clients world-class security and IAS advice. PwC's security group has become the industry leader through unparalleled experience delivering strategy and IAM implementations at 14 of the Fortune 25 and security assessment and/or implementation at 78% of the Fortune 500.

1.2.5 Joint expertise of the Core Team

In this section, we provide an overview of the key experience of the members of the Core Team in the field of IAS (organised per topic).

a. eSignatures/eID: standardisation and technical challenges

- **EC Mandate 460 on eSignature** (Riccardo Genghini). In December 2009 Electronic Signature Standardization Mandate (M460) was published. It is a 48 months Mandate and it will mainly be focused on the rationalization of the present framework and on providing guidelines for implementing electronic signature interoperability. ETSI and CEN are the two ESOs that will implement EC Mandate 460. The ETSI ESI Members are the widest, most active and most long standing community of ES experts not only in Europe, but also from global per-

spective: ETSI ESI's role in the implementation of the Mandate will be certainly very relevant. Since 2004 Riccardo Genghini is Chairman of the working group on Electronic Signature and Infrastructures (ESI) of ETSI - European Telecommunications Standards Institute.

On the other hand, SEALED was also involved as key expert in the Cross-Border Interoperability of eSignatures (CROBIES) studies that gave birth to the genesis and technical specification of this European Mandate 460 on reshaping of the eSignatures standardisation landscape.

§ **Cross-Border Interoperability of eSignatures (CROBIES)** study, (SEALED, Time.lex) consulting for the European Commission (DG INFSO). SEALED, together with Siemens and Time.lex, performed a study for the European Commission analysing the actions necessary to a truly interoperable cross-border use of Qualified Electronic Signatures. The results of the Study shall be taken into account as input for the Mandate M460 from the EC to CEN, CENELEC and ETSI in the field of Information and Communication Technologies applied to electronic signatures, 7 January 2010. The study contributed significantly to the technical specifications and annex of Commission Decision 2009/767/EC. This study had strong liaison with the **European Framework for signature Validation Services (EFVS)** study, for which SEALED partners were also key experts.

§ **European Commission Study on Standardisation Aspects of electronic Signatures** (DLA Piper and SEALED). Based on the effective use of eSignatures and related EU standards, this study analysed the "legal requirements / standardisation" model proposed by the Directive and provided the information and assessment needed for a possible review of the needs for standardisation in this context and to design new standardisation tasks that will serve in future to establishing trust in e-transactions/e-services. Recommendations have been made in terms of legal, standardization and marketing tasks, as well as quick-wins for the effective mutual recognition of Qualified Electronic Signatures.

§ **QUALISIGN** (2000-2001): SNG together with the A-SIT (the Austrian Government Centre for IT Security) has made a study aimed at defining the technical properties needed by electronic signatures, in order to fulfil their function as alternative to handwritten documents.

§ **EC study on the legal aspects of electronic signatures** (1998, Jos Dumurtier and Patrick Van Eecke). The study was in 1997 awarded by the European Commission in response to its tender on the n°XV/96/51/E invitation to tender *"The Legal Aspects of Digital Signatures"* and has been finalised in September 1998. The study gave an overview of concepts, general legal issues, practical usage, policies and regulations concerning electronic signatures. The study described and analysed the legal situation in the different EU member states and the main contracting countries regarding the use, the implementation and the legal acceptance of electronic signatures and related services. Furthermore, the study defined the legal obstacles to the Internal Market, and proposed an outset for a European legal initiative.

§ **European Electronic Signature Standardization Initiative** (EESSI, 1999). The EESSI initiative aims at elaborating a first set of standards that will help in the implementation of the directive on electronic signatures. The initiative is carried out by the European Committee for Standardization (CEN) and the European Telecommunications Standards Institute (ETSI) under the auspices of the European Commission. Patrick Van Eecke participated as expert in the elaboration of the EESSI preliminary study and undertook a consulting role in the respective standardization projects.

b. eSignatures/eID: legal implementation and market challenges

- **Study on the Legal and Market Aspects of Electronic Signatures**, conducted for DG INFSO. The authors of this groundbreaking study included Patrick Van Eecke (DLA) and Jos Dumortier (Time.lex). The study assessed the implementation of the Directive in the Member States, and the operation of the eSignatures services market at the time. Key interoperability challenges were flagged, which served as inputs to subsequent studies organised by the Commission.

- **UNCITRAL: Cross-border acceptance of electronic signatures** (DLA Piper)**.** Patrick Van Eecke has been asked as an expert on legal aspects of electronic signatures to provide UNCITRAL with the necessary input to draft a new model law on the cross-border use of electronic signatures. Although many countries have implemented electronic signature related legislation, the practical use of electronic signatures on a cross-border level seem to be underdeveloped. UNCITRAL is investigating the need for new model legislation on this issue.

- SEALED Partners had the opportunity to **comment on the Belgian bill on e-signatures**, at the moment of its transposition of the 1999/93/EC Directive in 2001, in quality of e-Security and PKI experts. SEALED Partners were also consulted in quality of experts in the framework of the establishment of a new legislation aiming to rules services applicable to e-signatures (such as timestamping, electronic registered mail, long term archiving, etc.), completing the 9th of July 2001 Belgian law on electronic signatures implementing the eSignatures Directive.

c. eSignatures/eID as building blocks for eGovernment services

- **FEDICT: electronic identity cards and alternative identities** (DLA Piper)**.** Patrick Van Eecke provides legal assistance to the Belgian government (Fedict) on the creation of a sound legal framework relating to electronic identity cards and alternative forms of identity. He drafted related legislation (a.o. on labelling of card readers and eID applications) and licenses (e.g. open source license for eID middleware).

- While heading the E-Trust services, Sylvie Lacroix and Olivier Delos were managing the delivery of the **PKI certification services for the Belgian eID**.

- **European Federated Validation Service (EFVS) study** (2009). Building on the 2007 Preliminary study mentioned above, the EFVS study examined the feasibility of establishing a federated signature validation tool at the European level. Information was collected on several key eSignature validation solutions operated in Europe and beyond, in each case examining the technical and legal approach. Building on the analysis of these solution mechanisms, a tentative strategy was proposed for improving eSignature interoperability in the longer term. The study was drafted for IDABC by Siemens, Time.lex and SEALED, with authors including Hans Graux, Olivier Delos, and Sylvie Lacroix. The outputs of the study have also served as an input to the CROBIES study mentioned above.

- **Preliminary studies on mutual recognition of eSignatures for eGovernment applications** (2007 and 2009). These studies were conducted for IDABC by Siemens and Time.lex, with Hans Graux and Jos Dumortier being primary authors for both editions (2007 and 2009) of the study. Each edition of the study required information to be collected on the status of eSignatures and eSignature interoperability in eGovernment applications in the Member

States, EEA countries and candidate countries. Interoperability challenges were identified, along with possible solution strategies.

- **eID Interoperability for PEGS studies** (2007 and 2009). These studies were conducted for IDABC in parallel with the aforementioned eSignatures studies, with Hans Graux and Jos Dumortier again being primary authors for both editions (2007 and 2009). These studies examined how electronic identification was being handled in each of the Member States in eGovernment applications (including the role of eSignatures as a technology enabling reliable identification in some countries), and serve as a baseline of knowledge on this topic today.

d. eSignatures/eID and their role in the information society

- **Elektronische Signaturen** (1999-2000). Jos Dumortier and Riccardo Genghini worked together in a project of the Europäische Akademie (a German No-Profit organisation), involving a dozen of academics and professionals from Austria, Belgium, Check Republic, Germany and Italy, aimed at defining the possible socio-economic benefits and risks of digitalisation through electronic signatures.
- **Study on Identity Management Systems** (IMS) (Riccardo Genghini) In 2003, Riccardo Genghini participated in a project on the Identity Management. The study titled: "Identity Management Systems (IMS): Identification and Comparison Study" was developed in collaboration with Landeszentrums für Datenschutz (ULD) Schleswig-Holsteint and co-financed by Joint Research Center of Sevilla.
- **Report for ENISA on the state of pan-European eIDM initiatives** (2008), which provided an overview of all key ongoing initiatives and challenges in the field of eID, focusing specifically on the Commission's eID Roadmap, the STORK project and the implementation of the Services Directive. The report was authored by Jos Dumortier and Hans Graux, and serves as a quick overview of EU eID policies at the time.

e. eSignatures/eID in specific application areas

- In 2008 and 2009, SEALED provided **eSignatures expertise in the context of the EU-CHINA Information Society Project** with the aim to provide advices on successful and interoperable eSignature implementation models.
- 2009 **Study on electronic documents and electronic delivery for the purpose of the implementation of Art. 8 of the Services Directive**. This study examined how Member States were planning to address the implementation of the Services Directive, including the challenge of exchanging authentic electronic information between Member States in a sufficiently secure manner (involving the use of eSignatures in many Member States). Solution models were developed by Siemens/Time.lex to assist the Member States in overcoming interoperability challenges.
- **Preliminary Study on the electronic provision of certificates and attestations usually required in public procurement procedures** (2008). Through this study, information was collected on the use of authentic electronic attestations, certificates and declarations in electronic public procurements within the Member States. Again, the use of eSignatures to safe-

guard the authenticity of such documents was examined, including the identification of interoperability challenges. Hans Graux was the primary author of this study.

§ Definition of the **Electronic Signature Services Infrastructure (ESSI)** (SEALED, Time.lex) for the European Commission, Directorate Informatics (DIGIT). Establishment of the detailed specifications for the ESSI Platform and advices for the eProcurement process and refinement of the specifications (both aspects of PKI certification and related services and on the required centralized eSignature creation and validation services are covered by the ESSI Platform).

§ Consulting in the context of the writing and issuing of RFPs related to the provision of PKI-based certification services in the support of **electronic identity cards and ICAO compliant Machine Readable Travel Documents (MRTDs)** (two European governments, SEALED) and support to both countries in the implementations of the related infrastructures. Consulting in the context of specifying the PKI-based certification services in the support of ICAO compliant Machine Readable Travel Documents (MRTDs) to **a non-European governmental.**

§ Consulting for the DG MARKT in order to provide a study on a **User identification and authentication methods in e-payments** (SEALED, Time.lex), In particular, the market evolution and new perspectives around such techniques, is at the heart of the study.

§ While heading the E-Trust services, Sylvie and Olivier (SEALED) were managing some of the most important projects and certification services provisioning related to the e-Security in Belgium and their **practical implementations** such as the **PKI certification services for the Belgian eID**, ID and Bridge certification services for the European Commission through the IDABC programme, certification services provisioning for Belgian Notaries, Accountants, Revisors, HealthCare (Carenet) and for eGovernment solutions requiring implementation of electronic signatures, and related trusted services.

§ **Luxtrust** (2003-2004): DLA Piper advised the Government of Luxembourg and 9 banks on setting up a national PKI scheme, including digital identity cards.

§ **National Bank of Romania** (2003-2004): DLA Piper offered legal assistance on the implementation of a national interbanking payment system making use of PKI in Romania.

§ **Belgian Social Security Administration** (2002): DLA Piper advised on the implementation of electronic signature solutions for employers' declarations on employees' social security data.

f. ICT policy in general

§ **EU Study on the specific policy needs for ICT standardisation** (DLA Piper). Patrick Van Eecke was leading a multidisciplinary, international team of researchers advising the European Commission on ICT standardisation policy issues. The study analysed the current European ICT standardisation policy and the prospective evolution in ICT services, products and applications for the coming 10 years. The study subsequently identified the evolving needs of a European ICT standardisation policy that is required to serve the needs of industry, societal requirements and public authority expectations. The study also put forward a set of recommendations for establishing a new European ICT standardisation policy. See also *www.ictstandardisation.eu*

- **Study on the legal analysis of a single market for an information society** (DLA Piper). The aim of this study, commissioned by the European Commission (DG Infosoc), is to review the "acquis communautaire" on online services and markets, in order to identify its benefits, gaps, lack of future proofing and implementation hurdles. It covers a broad range of topics, including e-commerce practices, services, data protection, consumer protection, applicable law and jurisdiction, e-payments, illegal and harmful content, protection of minors, security, taxation and e-procurements. This project's website is available at www.euinternetlaw.eu.

- **ENISA Legal study** (DLA Piper). Patrick Van Eecke was appointed as member of the expert group "Working-group on Regulatory Aspects of Network and Information Security". The aim of the study was collect regulatory information related to Network Information Security and to consider appropriate regulatory principles of existing regulation. The study addressed EU regulations and legislation that has become available and which is within the scope of the technical and organisational measures associated with electronic transactions in the Internal Market. Patrick was co-author of the deliverable "Mapping the regulatory NIS activities of Europe: ENISA publishing inventory & assessment report on EU regulatory activity in NIS."

1.3 Field Experts Team (Circle 2)

The Field Experts Team will consist of ten international experts, who will both review the deliverables of the Core Team and act as a first soundboard for the suggestions and solutions put forward by the Core Team members. Some of them will also draft specific (parts of) deliverables.

a. John Bullard (UK)

John Bullard is the Global Ambassador of IdenTrust, the global leader in trusted identity solutions, used by global financial institutions, government agencies and corporations around the world. IdenTrust specialises in managing the risks associated with identity authentication, achieving interoperably with countries around the world, minimising investment in creating local policies and legal frameworks, and deploying a spectrum of products insuring trust, smarter, faster, and more cost effectively.

John Bullard has a background of over 20 years in banking- with Barclays in the UK, US (California 1980's & Wall Street 1990's), and Europe and Asia. His responsibilities centred primarily around relationship management for Financial Institutions and larger Corporates for Barclays – especially in periods of change (e.g. deregulation in the London markets); from this he became Director at Group Operational Risk (eCommerce) at Barclays corporate HQ in London.

From this role, John was selected to join IdenTrust at its original foundation in 1999 as a bank consortium, and has managed much of the worldwide (mainly non US) external-facing issues. Now, as the Company's Global Ambassador, he brings a wealth of experience and insight particularly from the banking and the end-Customer perspective about what is needed in managing operational risk, including Supply Chain, for Corporates, the Public Sector, and ultimately the Citizen, in the era of the global "Networked Economy".

John is based out of IdenTrust's offices in London with a team focused on successful partnering and collaborative working with Corporates, Governments and Banks as IdenTrust helps to address their challenges in the eID space.

b. Claudia Diaz (ES)

Since 2006, Claudia is a postdoctoral researcher at the COSIC research group of the Department of Electrical Engineering (ESAT) at the K.U.Leuven. She defended her doctoral thesis entitled "Anonymity and Privacy in Electronic Services" in December 2005. Before that, she obtained in 2000 het Master's degree in Telecommunications Engineering at the University of Vigo (Spain). Between January and March 2009, she was a research visitor at the Computer Lab Security Group in Cambridge (UK). Since October 2009, she is funded by a post-doctoral research grant from the National Fund for Scientific Research in Flanders (FWO).

For many years, she worked in close collaboration with the lawyers at the Interdisciplinary Centre for Law and ICT (ICRI), as well as with researchers of the DistriNet group at the Dept. of Computer Science, in the context of the APES and ADAPID projects. Between 2004 and 2009 she was actively involved with the FP6 FIDIS Network of Excellence.

She is an Associate Editor of the multidisciplinary Journal on Identity in the Information Society (IDIS), and a member of the Scientific Committee of the Computers, Privacy and Data Protection Conference (CPDP), whose aim is to create a bridge between policymakers, academics, practitioners and activists.

Her research is focused on Privacy Enhancing Technologies, and she published many research papers in collaboration with different co-authors. The research questions she is most interested in are formalization, modeling and quantification of privacy properties (such as anonymity, unlinkability, unobservability and deniability). The goal of this line of work is to define models that provide a better understanding of what is meant by privacy, and metrics that are useful to assess the level of privacy protection provided by different systems. One of her main research contributions has been the proposal of information-theoretic anonymity metrics.

Another research area consists of the design and analysis of privacy preserving systems. A big part of her work in this area has dealt with anonymous communication systems to preserve the confidentiality of communication relationships.

c. Marit Hansen (DE)

Marit Hansen (formerly known as Marit Köhntopp) has a diploma in computer science in 1995. Since then, she is head of the "Privacy Enhancing Technologies (PET)" section at the Independent Centre for Privacy Protection, Schleswig-Holstein, Germany. Her work is focused on security and privacy aspects, especially concerning the Internet, anonymity, pseudonymity, identity management, biometrics, multilateral security, and e-privacy from both the technical and the legal perspectives.

Since 2002 she chairs the Special Interest Group (SIG) on PET of the German Society for Computer Science (GI). Marit Hansen is member of W3C's P3P (Platform for Privacy Preferences) Working Groups and of IBM Advisory Board on Privacy. She has been involved in the preparation of EU proposals on the project "PRIME—Privacy and Identity Management for Europe" and the Network of Excellence "FIDIS—Future of Identity in the Information Society" and has worked on the "Identity Management Systems (IMS): Identification and Comparison Study", initiated by JRC Seville, IPTS. Manifold publications on privacy and privacy technology.

d. Stephen Kent (US)

Dr Kent's R&D activities have included the design and development of user authentication and access control systems, network layer encryption and access control systems, secure transport layer protocols secure e-mail technology, multi-level secure (X.500) directory systems, public-key certification authority systems, and key recovery systems. His most recent work focuses on public-key certification infrastructures for government and commercial applications, security mechanisms and associated infrastructure for Internet routing (BGP), high speed (>10Gb/s) network security devices, and high assurance cryptographic modules.

He has acted as system architect in the design and development of network security systems for the US Department of Defense and served as principal investigator on a number of network security R&D projects for over 25 years. In his capacity as Director of the GTE Internetworking Security Practice Center, Dr Kent monitored all security related aspects of the service offerings of GTE Internetworking. As CTO for CyberTrust Solutions, Dr Kent provided strategic direction for this certification authority's product and service business, reporting to the President of CyberTrust.

Dr Kent served as a member of the Internet Architecture Board (1983-1994), and chaired the Privacy and Security Research Group of the Internet Research Task Force (1985-1998), both now under the auspices of the Internet Society. He chaired the Privacy Enhanced Mail (PEM) working group of the Internet Engineering Task Force (IETF) from 1990-1995 and currently co-chairs the Public Key Infrastructure Working Group (1995-). He is an active participant in several security-related Internet standards working groups in the IETF.

Dr Kent was a charter member of the Board of the International Association of Cryptologic Research (1982-89) and served on the editorial board for the Journal of Telecommunication Networks (1982-1984). He served on the editorial board of the Journal of Computer Security (1995-2001) and on the board of the Security Research Alliance, a consortium of leading information security companies. Dr Kent serves on the Canada Research Chairs board (2002-), which evaluates applications for chaired faculty positions at universities in Canada. In 2004 he was appointed to the External Advisory Committee for the National Center for Advanced Secure Systems Research, and in 2005 he was appointed to the International Scientific Advisory Board for MITACS (Mathematics of Information Technology and Complex Systems), a Canadian institution.

Dr Kent chaired the committee on Authentication Technologies and Their Privacy Implications, for the Computer Science and Telecommunications Board (CSTB) of the National Research Council (NRC). Dr Kent also served (2005-2008) on the Intelligence Science Board, reporting to the Director of National Intelligence (DNI). The Secretary of Commerce appointed Dr Kent as chair of the Federal Advisory Committee to Develop a FIPS for Federal Key Management Infrastructure (1996-98). The output of that committee forms the underpinning for a FIPS on Key Recovery. He previously served on the Presidential SKIPJACK Review panel (1993-1994).

He chaired the steering committee for the Symposium on Network and Distributed System Security (1990-1998) and was General Chair of the IEEE Symposium on Security and Privacy (1996-97). He has appeared as an invited speaker at security conferences throughout the U.S., Europe, Asia and Africa.

e. Chris Reed (UK)

Prof. Chris Reed is Professor of Electronic Commerce Law at the Centre for Commercial Law Studies of Queen Mary university (London). He has published widely on many aspects of com-

puter law and research in which he was involved led to the EU directives on electronic signatures and on electronic commerce. From 1997-2000, Chris was Joint Chairman of the Society for Computers and Law, and in 1997-8 he acted as Specialist Adviser to the House of Lords Select Committee on Science and Technology. Chris participated as an Expert at the European Commission/Danish Government Copenhagen Hearing on Digital Signatures, represented the UK Government at the Hague Conference on Private International Law and has been an invited speaker at OECD and G8 international conferences. He is a former Director of CCLS, and from 2004 to 2009 was Academic Dean of the Faculty of Law & Social Sciences.

f. Teemu Rissanen (FI)

Teemu Rissanen (Security Consultant and Managing Director of Conseils Oy SimplySecure) has been working for Conseils Oy since 2001. His expertise covers the areas of trust and security solutions, consultancy services and security studies. He has designed and carried out concepts and systems for paperless processes, secured infrastructure applications and transactions requiring strong authentication and digital signature, compliant with European legislation and standards. Rissanen has also carried out studies and participated in R&D projects in the area of eHealth and eSignatures.

Rissanen has carried out National digital signature and identity management interoperability studies for the EU IDABC programme, the legal framework interoperability study for eHealth, for the EU CEC DGINFSO, and he is involved with numerous other digital signature and identity management studies and projects for national and EU institutions.

As project manager he has lead the consortium in charge of the manufacturing and personalisation the next generation FINEID organisation certificate smartcards in Finland. Teemu Rissanen has a strong expertise in smartcard technology implementation for various business fields. Currently Teemu Rissanen is involved in an EU project where he provides consultancy and expert services on identity management and secure data sharing for providing outpatient eHealth services.

He is a frequent speaker in several international PKI, smartcard and identity management focused conferences, including the Porvoo Group (EU), European Forum for Digital Signatures and PKI (PL), World eID (FR), Omicard (DE), Cartes et Identification (FR), Security Document World (UK), Med-e-Tel (LU), and Net-ID (DE), all between 2006 and 2010.

g. Stefan Santesson (SE)

Stefan Santesson, independent expert consultant and CISSP, is chairman of the Public Key Infrastructure group (PKIX) in the Internet Engineering Task Force (IETF), member of the IETF Security Area Directorate and manager/owner of the consultancy company 3xA Security. Stefan has 25 years of experience with Information Security, ranging from crypto algorithm development to managing an international security organization. Stefan has been responsible for development of several core standards, in ETSI as well as in the IETF, which influence current implementation of electronic signatures.

Most notably Stefan is the co author of RFC 5280 which is the main standard for implementation of Public Key Infrastructure technology around the world. Stefan was also the lead editor of both the international IETF standard for Qualified Certificates (RFC 3739) and the European profile for

Qualified Certificates (ETSI TS 101 862), profiling RFC 3739). In total, Stefan is the author or co author of 12 IETF RFC documents spanning several different security areas.

During the years 2003-2009 Stefan worked as Senior Program Manager for Microsoft Windows Security where he was responsible for several Microsoft engagements within Internet security protocol development.

Since 2009 Stefan is acting as independent consultant with a continued engagements in international development within internet security, electronic signatures and identity management.

h. Marc Stern (BE)

Marc Stern is Senior Consultant at Approach. He is an expert in Information Systems Security, and in Systems and Network Architecture, with an impressive personal track record in Public Key Infrastructures and smart card-based systems for eID applications. He is also one of the European leaders in the field of Web applications protection. During the last years, Marc Stern worked within the private sector (financial market, manufacturing industries) and within the public sector (Belgian Government, Belgian Social Security, European Commission, NATO) where he played a major role in shaping the new security landscape.

Marc Stern is deeply involved in the STORK project on the implementation of a EU wide interoperable system for recognition of eID and authentication that will enable citizens to use their national electronic identities in any Member State. This competency is of particular interest in the context of the IAS study.

i. Eric Verheul (NL)

Prof. Dr. Eric Verheul is both a Senior Manager at PwC and part-time professor at the University of Nijmegen (Digital Security group). At PwC he is consulting both to government and private sector clients. At the University of Nijmegen he holds the special chair "*Mathematical applications in Information Security*"'. This activity includes providing education and doing research on the subject of information security and its relation with mathematics.

He obtained his Masters in Mathematics (1987) as well as his PhD in Mathematics (1991) at the Free University Amsterdam. He is also the holder of two cryptographic patents.

Other qualifications of Eric include Lead auditor qualification by the Dutch national accreditation body (RvA) for performing audits against ETSI 101456 and ISO 27001/ISO 27002; qualification "IT Auditor PKI" and "Expert PKI" by the Luxembourg national accreditation OLAS; and Certified Information System Auditor (CISA) as well as Certified Information Systems Security Professional (CISSP).

j. Jane Winn (US)

Jane K. Winn is Charles I. Stone Professor and a director of the Law, Technology and Arts Group at University of Washington School of Law in Seattle, Washington where she teaches commercial, comparative, technology and trade law courses, including European Union Law. She received a B.Sc. (Econ) First Class Honours from Queen Mary College, University of London and a J.D. (cum laude) from Harvard Law School.

Winn is a co-author of the Law of Electronic Commerce (4th edition 2001, supplemented through 2010), a leading reference work on electronic commerce law issues under U.S. Law as well as a student textbook on electronic commerce law. She has published many articles and book on commercial law, comparative law, technology law and trade law issues.

Her current research interests include electronic commerce law developments in the United States, the European Union, and China. In 2008, she received a Fulbright Research Grant to support her research on electronic commerce in China. She is affiliated with the EU Centre of Excellence at the University of Washington, and has received research and travel grants from the Centre, and has also participated in EU funded research in the past.

In addition to participating in law reform projects, Jane Winn is also a member of standard setting organizations. She was an advisor to the American Law Institute's Principles of Software Contracts and is co-chair of an American Bar Association Task Force on legal issues of Federated Identity Management. As a member of the Liberty Alliance/Kantara Initiative, she has served on the ICT Standards Board since 2008. She speaks frequently at academic and professional conference on topics related to electronic commerce and information security including the annual RSA Information Security Conference.

1.4 Stakeholders (Circle 3)

In order to achieve a wide collection of data and objective scrutiny, and in order to integrate a balanced view of the interests, concerns and comments of stakeholders, we will set up:

- A **wide network of stakeholders and interested parties** with regards to regulation in the context of e-signatures and e-identification.
- A board of **key stakeholders**. This board will consist of a representative sample of large enterprises, SME's, universities, governments and consumer organisations who will be consulted for their views on the information society issues encountered throughout the project.

The Stakeholders will be consulted for their views on the information society issues encountered throughout the project, and on the potential solutions proposed by the Core Team. They will allow the Core Team to perform reality checks, investigate the current concerns of information technology players, and evaluate the practical impact of the proposed legal instruments.

The final list of Stakeholders will be determined in cooperation with the Commission, but provisionally the project team can propose a list of experts and organisations that it aims to consult in the execution of the project. An example list is set forth in the table below.

Please note that participation in the project by the stakeholders will take place on a strictly voluntary basis and free of charge. The Circle 3 Stakeholders do not have any formal tasks under the current proposal, and are therefore not to be considered as subcontractors within the present proposal. This also means that additional stakeholders can be added to Circle 3 after the initiation of the project, so that we can cover a large group of interested parties.

Organisation	Description — examples	Area
A selection of certification service providers listed in EU Member States Trusted Lists	Certification Service Providers issuing qualified certificates listed in the Member States Trusted Lists will be specifically addressed. At least one such CSP per Member State, when applicable, will be liaised as key stakeholder (e.g., for Belgium, *Certipost*).	Industry
EU Member States official representatives with regards to eSignature and eIdentification regulation	Member States *Examples:* § *AT (R. Posch), DE (A. Reisen), FR (Martine Schiavo), UK (Richard Trevorah), IT (Adriano Rossi), SK (Peter Rybar), EE (Tarvi Martens), ES (Miguel Alvarez Rodriguez), SE, PL (Marcin Fijalkowski), BE (F. Leyman, JF Petit)*	Government
Supervisory, Accreditation and Designated Bodies	Member States *Examples:* § *FESA* § *AT (H. Leitold), DE (J. Schwemmer), FR, UK, IT (S. Arbia), SK, EE, ES, EL, SE, PL, BE (Jean-François Petit)*	Government
Zetes	Ronny Depoortere	Industry
Smart card industry	*Examples:* § Gemplus § Gemalto (Lorenzo Gaston), § G&D (Jan Van Eenoo)	Industry
Eurochambres	Vicent Tilman	Business
Eurosmart	Jacques Seneca	
Consumer Associations	E.g., *German consumer association*	Public interest
Civil liberties associations	E.g., *German consumer association*	Public interest
Microsoft	Stefan Brands	Industry
Adobe	Marc Straat	Industry
Banking and payment sector	Banking and payment sector. *Examples:* § *EPC (Marijke Desoete)* § *Swift (Jacques Hagelstein)* § *Dexia Group - Global Security Officer (Stéphane Hurtaud)*	Industry

1.5 Technical proposal

1.5.1 Setting the scene

a. IAS as a subject: what is IAS?

The main aim of the study is to examine the feasibility of an electronic identification, authentication and signature (IAS) policy for the European Union, as well as electronic credentials in general. These concepts are not uniformly defined at the European level, and their interaction is not yet well understood. It is however clear – as is also demonstrated by the technical specifications – that the notion of an identity plays an interconnecting role between them, as is even reflected in the existing regulatory framework for electronic signatures, Directive 1999/93/EC (the eSignatures Directive).

This Directive defines the notion of a certificate as "an electronic attestation which links signature-verification data to a person and confirms the identity of that person". Similarly, CSPs issuing qualified signature certificates to the public are required via Annex II to the Directive to "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". This supporting role for identities in a framework which was created to harmonise the Internal Market for eSignature services is born out of necessity: without the ability to determine the identity and/or relevant attributes pertaining to the signatory, the value of the signature is likely to be limited.

Keeping this in mind, it is perhaps surprising to observe that no common policy framework to address IAS issues comprehensively exists at the European level. While the eSignatures Directive uses the identity concept as a building block and even imposes an obligation for certain CSPs in Annex II to verify the identity of qualified certificate holders, it conspicuously requires that this verification is done 'by appropriate means in accordance with national law'.

Thus, while eSignatures have benefited from significant policy attention in recent years, IAS as a whole – including questions of identity, attribute management and authorisations – has not been handled in the same way. In the absence of a comprehensive policy framework, Member States and CSPs have retained the competence and freedom to address this issue in line with their local traditions and business/policy preferences. As we will illustrate in the sections below, this situation may lead to a suboptimal situation by allowing barriers to exist for the cross border deployment of IAS services, both in the public and private sector.

b. IAS within the broader authentication context

To correctly assess the importance of IAS, it is important to examine the different contexts in which IAS processes play a role. When doing so, it becomes clear that IAS must be considered *as an authentication service*, intrinsically linked to a number of other authentication services, i.e. services which aim to ensure that certain information may be relied upon within a certain context.

The identification of entities is an obvious example of this type of service, as the main goal here is to demonstrate that one or more specific attributes pertaining to an identity are authentic and sufficiently unique to identify that entity within a well defined group of similar entities. Identification (or perhaps more appropriately **entity authentication**) can **apply to natural persons**, but also to **legal persons or even information systems**.

It is however not always necessary for an entity to be uniquely identified within a specific context. In some cases, it may be entirely sufficient to corroborate specific attributes related to an entity, such as e.g. its legal status or the allocation of specific authorisations. **Attribute authentication** is a key feature in practice, especially when considering *what* an entity is, rather than *who* it is.

It is clear that these questions (who and what are the entity?) are important to determine the value of **eSignatures** as well. This is one of the main challenges in the existing European eSignatures framework today: the Directive itself does not concern itself with the question of who or what the signatory is. As a result, Member States address this issue in different ways: while most Member States hold that qualified eSignatures can only be created by natural persons, some also accept that they can be created by legal persons, leading to discussions in practice on the legal meaning and value of such signatures. If the issue of entity authentication had been addressed consistently, it would also have been possible to address the concept of eSignatures in a more nuanced way, e.g. by unambiguously distinguishing eSignatures (created by natural persons), **company seals** (by legal persons) and **system seals** (by information systems).

In turn, other authentication services build on these IAS services as well, including:

- Time stamping services
- Electronic archiving / long term validity services
- Conversion from paper to electronic form
- Registered e-mail / official e-mail services
- IAS validation services

In practical terms, these services build upon each other and extend each other: e.g. long term validity assurance requires the use of time stamping and eSignatures, which in turn require reliable identification services to determine who the signatory is. Yet, only the signature component of the IAS service package has been partially addressed at the EU level.

c. IAS as an internal market issue

IAS is not just an authentication service, it is a *market service.* Currently, only the eSignatures component of IAS is duly recognised as such through a Directive which aims to harmonise the internal market for eSignature services, whereas other IAS components related to identity (and also the ancillary services briefly referenced above) have not received the same treatment at the European level.

None the less, the 4th recital of the eSignatures Directive could be applied directly to identification services as well, merely by substituting "identification" for "signatures", as marked in italics here:

> "Electronic communication and commerce necessitate " electronic *identification*" and related services allowing data authentication; divergent rules with respect to legal recognition of electronic *identification* and the accreditation of certification-service providers in the Member States may create a significant barrier to the use of electronic communications and electronic commerce; on the other hand, a clear Community framework regarding the conditions applying to electronic *identification* will strengthen confidence in, and general acceptance of, the new technologies; legislation in the Member States should not hinder the free movement of goods and services in the internal market."

This is not merely a theoretical consideration. In the absence of a European approach, authentication policies have been created at the Member State level and by private sector service providers which aim to define specific reliability requirements for identification services, often linked directly to the eSignatures context. This leads to market barriers between the Member States in practice, as these authentication policies are redefined on a case by case basis, meaning that they cannot be applied consistently at the European level. As a result, the internal market for identification services is fragmented.

d. IAS as a societal issue

It is important to recognise that the identification component of IAS services also implies societal concerns which are not present to the same extent for other authentication services. The ability to be uniquely identified in a specific context is certainly useful and even necessary in an information society, but also requires that certain safeguards are put in place to avoid abuses. Specifically with respect to questions of data protection, unique identifiers (identification numbers and biometric data) and user control, any policy framework to be developed at the European level needs to be sufficiently robust (combining legal requirements with a privacy-by-design approach) to address these issues.

This issue has been explored already to a significant extent via existing EU initiatives, including through the FIDIS Network of Excellence (www.fidis.net), and the PRIME (www.prime-project.eu) and PrimeLife (www.primelife.eu) research projects, which have examined models and approaches for managing identities in an electronic environment in innovative ways that optimally safeguard the privacy of participating subjects. However, these initiatives are still largely academic exercises which have so far had a limited impact on electronic identity management deployments in practice.

This is an important realisation, since current EU initiatives (such as notably the large scale pilot STORK - www.eid-stork.eu) aim to make robust IAS solutions a reality for European citizens and enterprises in the medium term. One of the key challenges of the envisaged feasibility study will be to identify the steps that would be needed to ensure the practical viability and sustainability of IAS models such as those being developed through STORK or other initiatives, while integrating the innovative and pro-active data protection approaches that have been pioneered through the aforementioned projects.

Before IAS services can expect to see significant take-up in practice, a clear perspective needs to be available on the trustworthiness of such services, including particularly their impact on the privacy of end users. This implies a clear legal framework for the responsibilities of IAS service providers with respect to data protection, in line with the principles established by the Data Protection Directive 95/46/EC and with EU citizens' fundamental rights, as well as a clear definition of the rights and safeguards for European citizens. Thus, any consensus to be developed on a future European IAS policy framework need to take into account the expected and desired societal impact of IAS services.

1.5.2 Current IAS approach at the EU level

The overview above has shown that the IAS approach at the European level is still at an embryonic stage and highly fragmented. Several useful building blocks have been put in place that can (and must) be leveraged and built upon to create a future IAS policy:

- Obviously, the eSignatures Directive acts as a legal framework for one specific type of IAS services. It is important to recognise that this Directive has not just established a legal context for such services, but that it is also backed by standardisation efforts and by a trust infrastructure at the national level. Due to the importance of the Directive as a key regulatory building block, we will analyse its impact (including benefits and shortcomings) in greater detail in the sections below.
- Considering the privacy impact of identification services, the Data Protection Directive (Directive 95/46/EC) must also receive due credit, as it establishes a baseline of obligations to be observed when processing personal data. The correct application of this Directive in the context of IAS services will undoubtedly prove to be an important enabler for establishing trust in European IAS service providers.
- Several European studies have already charted the key challenges for the establishment of IAS services, including many of those referenced above (e.g. the Study on Standardisation Aspects of electronic Signatures, the EFVS Study, the IDABC studies on eSignature and eID interoperability, etc; all of these were conducted by the project team). This means that the problems and challenges for IAS policies are well known and understood.
- The EU has been forward thinking in bringing together and stimulating the development of top expertise on the societal and privacy impacts of identity management in the information society, including through projects such as FIDIS, PRIME, and PrimeLife. The EU can fall back on leading know-how in this area.
- Potential ways forward are also already being explored, including through the aforementioned CROBIES study (also conducted by the project team) and large scale pilots such as STORK. This means that high level visions on developing IAS policies already exist, albeit typically still in a trial form and without much consensus at the EU level yet. None the less, IAS efforts in the EU have surpassed the strict 'problem definition' stage, and are moving gradually towards formulating solutions.

Thus, a few important steps have already been taken, which already suggest some of the core concepts for a future EU IAS framework. However, these are only building blocks, and vital challenges still remain. These will be explored below.

1.5.3 Key preliminary building block for an IAS policy: the eSignatures Directive

The eSignatures Directive can already be seen as the embryo of the future IAS framework, as noted in the tender specifications. Not only because it rightly declares the fact that an eSignature must allow the identification of the signatory, but also thanks to its business model that could theoretically be extended to a generic and comprehensive IAS framework. Indeed, as shown in the next section, the eSignatures Directive, from a certain perspective, was a success.

However, for different reasons – briefly summarised in the next section as well, with more details developed by the project team in the CROBIES study – it also faced some difficulties in sustaining a sound and interoperable deployment of eSignatures in the market. The challenge for the future IAS framework will be to maintain the elements that can be seen as success factors of the eSignature Directive, while avoiding its pitfalls. The Commission will need to present to the Member States an IAS framework based on a clear and consistent success story, while precluding the possible (expectable) criticisms frequently heard with regards to the eSignatures directive:

- While claiming to be technologically neutral, the Directive *de facto* imposes and relies on one single specific technology (PKI). If a new framework is to be designed, one must insure that there is at least one existing technology to sustain it, and that the legal framework can be easily translated into specific requirements related to the underlying technology.

  As an example, in the current framework, harmonisation of supervision and accreditation criteria (between Member States) is not a legal obligation and this is an issue.

- The businesses cases for eSignatures are not clearly identified.
- There are too many missing links in the eSignatures Directive (*e.g.,* no requirements on Secure Creation or Verification Applications).
- The mapping between the Directive and the paper world is not straightforward, due to the mixing of the legal concept of a signature and the technological process of a signature. In the paper world, there is no signature *"per se"* and the signatures are not specifically linked to the data to which they refer.

Clearly, it would be desirable to use the past eleven years of experience with the eSignature Directive to support evidence-based policy making for IAS.

1.5.4 Assessment of the Directive's impact on IAS services: does it fall short?

When assessing the impact of the eSignatures Directive on IAS services, it must first be recognised that the basic conceptual approach of the Directive with respect to eSignatures appears to be sound, and conducive to enabling an interoperable eSignatures market. The following positive characteristics should be recognised in particular:

- **Principle of technological neutrality**: the eSignatures Directive is in principle technologically neutral, as it defines its basic concepts (notably electronic signatures and advanced electronic signatures) in terms which do not explicitly refer to any specific technology. While other concepts (certificate, qualified certificate, signature creation device and SSCD) are clearly biased towards a PKI environment, the basic scope of applicability of the Directive is linked to the neutral concept of an electronic signature. This approach is fundamentally sound, as it ensures that the Directive focuses on a function rather than on a technology.

- **Legal equivalence / legal value**: the Directive establishes two tiers in the legal value of an electronic signature: for the basic concept of an electronic signature, only a non-discrimination principle applies, and the legal value in any proceedings will therefore need to be assessed on a case by case basis. However, for advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device (so called qualified signatures - QES) the legal value is determined by an equivalence rule, declaring such qualified signatures to be legally equivalent to hand written signatures and by definition admissible as evidence in legal proceedings. Thus, the basic approach is to define a qualified level of the signature, for which specific requirements need to be met, and to which a clear legal value is assigned. This is a positive approach, as it in principle allows similar qualified signatures to benefit from a uniform value across the internal market.

- **Approach to standardisation**: the Directive only defines specific technical requirements at a high and generic level through its Annexes. Details must be fleshed out outside of the legislative process via standardisation procedures, which must then be affirmed and given legal

value through a Commission Decision. The fact that technical standards are not integrated into the Directive means that there is greater flexibility in keeping these standards up to date, and ensures that such details can be determined by experts in the field, which should ensure that they are more clearly aligned with the technical state of the art.

§ **Supervision and voluntary accreditation**: the Directive ensures the trustworthiness of certain signatures via the mandatory supervision of CSPs issuing qualified certificates to the public, and by permitting the introduction of voluntary accreditation schemes. The mandatory supervision scheme is crucial: by ensuring that equivalent supervision schemes are available in each Member States, CSPs issuing such qualified certificates can offer their services from any Member State and in principle be confident that their services will be equally acceptable across the EU. The voluntary accreditation schemes offer Member States to establish separate quality requirements which can further ensure the trustworthiness of specific signature solutions.

§ **Market access and internal market provisions**: the Directive aims to ensure that CSPs can freely establish in any Member State and offer their services throughout the internal market, most notably by explicitly forbidding prior authorization schemes. This ensures that the market cannot be artificially limited or distorted through the introduction of national rules that exclude foreign service providers. This should favour competition, thus leading to improved quality of services and/or lower prices.

§ **Liability**: to ensure that the qualified service level offers real guarantees to relying parties, article 6 of the Directive includes specific liability rules that apply notably to CSPs issuing such certificates to the public, thus ensuring that certain errors linked to the usage of such certificates lead to the liability of a more clearly identifiable party that must assume responsibility for these errors (namely the CSP), rather than allowing all liability to be shifted to a party that may be practically impossible to identify or hold responsible (the signatory). This benefits the trustworthiness of such signatures, and provides the necessary incentive for such CSPs to establish the required processes to ensure the actual reliability of their certificates.

Nonetheless, and despite all of these positive characteristics, with respect to IAS as a whole, the impact of the Directive is limited. This is not surprising, as the Directive was not intended to provide a comprehensive framework for any IAS services. By focusing on eSignatures, it targets only one component of the IAS landscape.

As such, the Directive (and current EU policy in this area as a whole) is unable to address a number of key questions with respect to IAS services. The main challenges relate to:

§ The existence of key issues which are unresolved with respect to eSignatures, despite the fact that this is the core IAS component addressed by the Directive. As examined by the CROBIES study, these include notably:

- The unclear status of qualified signatures created by legal persons. The Directive defines a signatory as 'a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents' (Article 2.3). In practice, most Member States take this to mean that only natural persons can be signatories, whereas others allow also legal persons to play this role. This leads to a very unclear situation, since a qualified signature created by a legal person may be considered a normal phenomenon in Member State A, whereas the same concept is meaningless and has no legal value in Member State B;

- Whether or not there is a requirement to obtain formal conformity assessments with respect to SSCDs. The Directive clearly states that *"(t)he conformity of secure signature-creation-devices with the requirements laid down in Annex III shall be determined by appropriate public or private bodies designated by Member States"* (Article 3.4). However, it does not state whether such an assessment is necessary before a signature creation device can legally be considered an SSCD, or whether the assessment merely serves to eliminate any doubt on this point. In practice, Member States interpret this question differently, so that the concept of an SSCD is not unequivocally understood in the EU;
- The delineation of the SSCD concept. Recital 15 to the Directive notes that *"Annex III covers requirements for secure signature-creation devices to ensure the functionality of advanced electronic signatures; it does not cover the entire system environment in which such devices operate"*. However, this legal approach is difficult to apply in practice, and the standardisation framework tends to take a broader approach than the Directive. In practice, it is not always clear how far conformity assessment bodies should go (or are allowed to go) to assess SSCDs;
- The meaning of the public sector clause (article 3.7); this provision allows Member States to *"make the use of electronic signatures in the public sector subject to possible additional requirements. Such requirements shall be objective, transparent, proportionate and non-discriminatory and shall relate only to the specific characteristics of the application concerned. Such requirements may not constitute an obstacle to cross-border services for citizens."* In practice, it is not clear at all when such additional requirements may be lawfully imposed, and what the meaning and impact of the public sector clause is. Given an excessively broad reading, the clause could be interpreted to significantly harm the interoperability of eSignatures in an eGovernment context, which could include such vital areas as eHealth and eProcurement;
- The incomplete trust model (no common supervision requirements). The Directive requires Member States to implement *"an appropriate system that allows for supervision of certification-service-providers which are established on its territory and issue qualified certificates to the public"* (article 3.3). This gives Member States a very substantial amount of leeway to determine what they consider to be appropriate, leading to some divergences in the quality of supervision schemes. While this is not a legal problem, excessive differences can negatively impact the trustworthiness of eSignatures, as CSPs might be inclined to 'forum shop' for the least demanding supervision scheme.
- No European common way of unambiguously identifying a person (the signatory). As noted above, identification is governed by national law. Thus, despite the fact that identity is a key building block to determine the meaning and legal value of an eSignature, it is not impacted by the eSignatures Directive as such.

§ Other challenges exist as well, which can partially be addressed within the current framework, as examined within CROBIES. E.g. the standardisation framework is currently being updated and rationalised, which should also result in clearer implementation guidelines. However, the challenges mentioned above may require a deeper recasting of the legal framework.

- The scope of the Directive is almost entirely limited to eSignatures. Ancillary services such as those discussed above are not covered in any meaningful way. There is no common definition or understanding of these services, of their requirements, or of their legal value (if any).

- With respect to the concept of identity, the Directive simply refers to the legal notions of "physical person" and "legal entity" provided by national legislation. Often there is no comprehensive (or scientifically proved) notion of identity in the national legislation.

- Ensuring a clear and uniform market impact, including the practical effect and enforcement of the equivalence and non-discrimination rules of the Directive. The business case for eSignatures remains hard to determine in this environment.

- Lack of a clear model and guidance with regard to responsibility and liability. This is further aggravated by the fact that it is unclear where to complain in practice, e.g. in the case of a particular Memberstate denying the legal value of electronic signatures created by the National eID card of another Member State.

All of these elements point to the conclusion also embodied in the tender specifications: it seems that there is a need for a comprehensive EU policy framework for IAS and ancillary services, and the eSignatures Directive does not appear adequate to play this role without being extended on the basis of its basic principles which are sound and on the basis of which an IAS policy could be build.

1.6 Objectives of the Study: building towards an IAS framework

1.6.1 What needs to be addressed by a European IAS framework?

Conceptually, there are a number of ways in which a European IAS framework can be established, with the model of the eSignatures Directive mentioned above being only one possible approach. However, irrespective of the approach taken, a European IAS framework requires a legal component, a **technical** component, and a **trust** component.

The **legal** component refers to the need to have a framework that provides a common definition of key IAS services. In each case, this definition should be tied to common requirements imposed on service providers and the related responsibilities/liabilities, linked to a clear legal value of the services, and supported by internal market provisions.

The **technical** component refers to a need for a common standardisation framework, supported by practice-oriented implementation guidelines, which are in line with the state of the art on the market. Furthermore, there must be a clear plan to keep the standardisation framework up to date, taking into account the progress of technology, as well as the increasing need to align European approaches with developments at the international level.

Finally, the **trust** component refers to the need for a framework that ensures that relying parties can determine the reliability and value of IAS services in practice, in a way that provides them with sufficient guarantees in case of later disputes.

It goes without saying that these components interact and must be well aligned:

- The legal framework must also provide the basis for common European standards and trust;
- The technical framework needs to allow stakeholders to automatically check compliance with legal requirements and the status of the IAS service in the trust framework;
- The trust framework must check compliance with the legal framework and serve as a trust anchor for technical implementation.
- A clear mapping between the legal and standardisation (technical) framework is crucial and could rely on an extension of CD 2003/511/EC.
- A clear model for responsibility and liability.

Finally, whatever IAS framework is ultimately adopted, it must have a clear market orientation. The IAS framework must be built taking into account best practices within the current market, and must also be sufficiently pragmatic to allow IAS service providers to easily comply with the framework to the extent that they desire.

Flexibility of the regulatory model should also be searched in order to cover any component certification service as well as any future service, e.g. build upon a combination of existing basic component services.

1.6.2 Building on the approach taken in the eSignatures Directive

eSignatures approach – The tender specifications state that the eSignatures Directive may *"serve as a starting point to devise a new comprehensive electronic identification, authentication*

and signature (IAS) or electronic credentials legal framework". Based on the advantages of the eSignatures Directive, this is indeed an attractive premise:

- The eSignatures Directive already provides a model for a basic **legal** framework that could be modified to be applied to IAS and other authentication services as well. The Directive's approach meets the basic requirements above: it defines key concepts, outlines responsibilities and liabilities, contains a reusable approach to define legal value based on the distinction between qualified and nonqualified services, and provides internal market provisions.

- The eSignatures Directive is complemented by a **technical** framework, in the form of standards which are given a formal status through a Commission Decision.

- The eSignatures Directive established a **trust** framework based on a regime of national supervision for qualified services.

- The Trust framework main tool is the Trusted List specifications and regime are stated in CD 2009/767/EC

Furthermore, reusing this approach would allow the Commission to correct the weaknesses of the current framework as identified above, and ensure that IAS services are properly framed within the broader context of authentication services in general. Thus, the appeal of the eSignatures model to address IAS challenges in Europe is clear.

Alternative approach – Nonetheless, it should be recognised that this is only *one* possible way to address the lack of an IAS framework. While the approach is clearly very appealing, one of the core tasks of the feasibility study will also be to liaise with stakeholders (including CSPs and policy experts) to determine whether they consider this approach to be a viable and desirable option. Before establishing an IAS framework based on the eSignature Directive's model, it must be ensured that such an approach would be welcomed by practitioners. The current (lack of) maturity of certain authentication service markets and technologies is an important factor to be considered, for example the question whether these areas are sufficiently stable to make regulation a favourable option. Another factor to be considered is the known criticism against the eSignatures Directive — it needs to be investigated whether a re-cast and broadened version of the Directive will address these concerns.

For these reasons, there are several clear components to the feasibility study, which corresponds to the tasks defined in the tender specifications:

- A conceptual model must be found for defining a European IAS framework. The eSignatures Directive provides one option, but we will need to explore other options as well (**Task 1**: Defining a conceptual basis).

- This will need to be done taking into account the state of the art, especially in Member States which have already tried to define their own IAS framework. Experiences from leading countries outside the EU are also relevant, given the importance of having an internationally scalable approach (**Task 2**: Stock taking).

- The conceptual model needs to be developed into a first proposal for a European IAS framework. This proposal must contain all the crucial elements to allow the Commission to present it to the Member States and (if desired) to bring it to a final stage of maturity (**Task 3**: Defining building blocks, and **Task 4**: Support).

§ Finally, interactions with key stakeholders (within the Commission, Member States, policy experts and service providers) will need to be organised on an ongoing basis in order to validate whether the conceptual model meets existing concerns, and whether it is an appropriate way forward in the European internal market. Consensus on the proposed model will need to be developed and cultivated (**Task 4**: Synthesis, workshops).

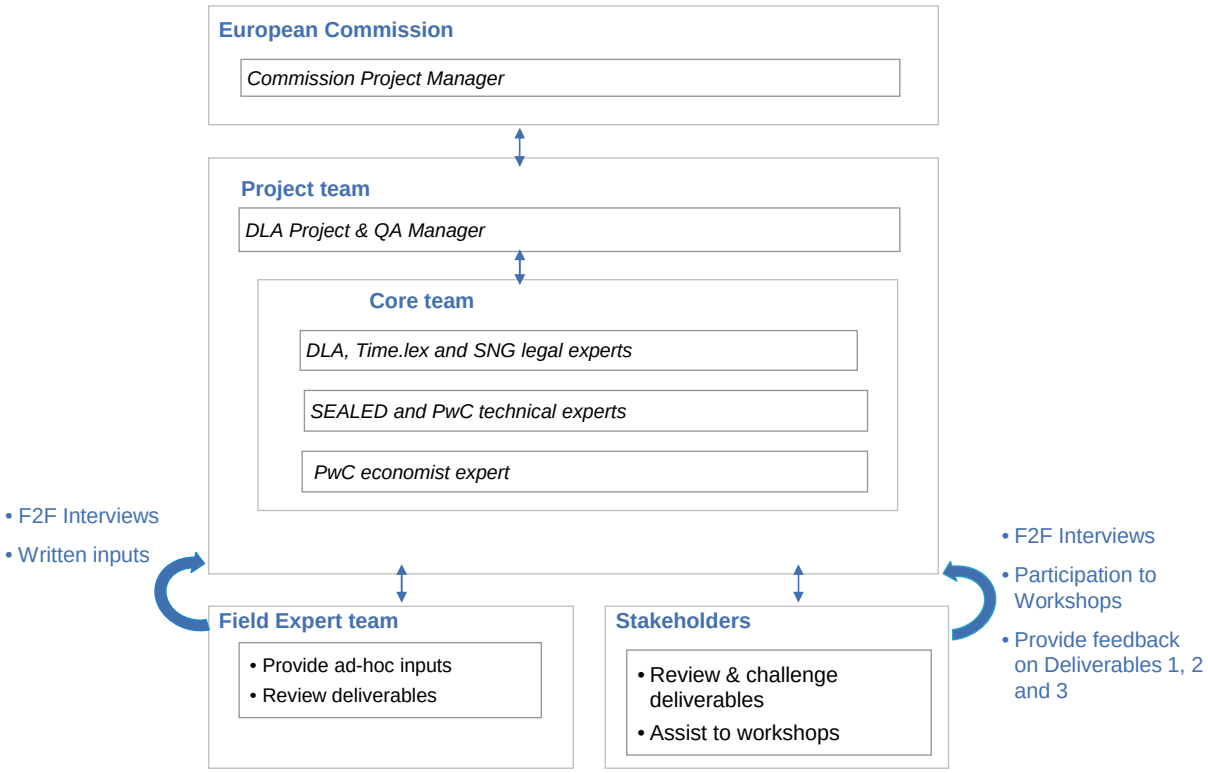
In the sections below, we will develop our methodology for implementing each of these tasks.

1.7 Methodology for the Study

1.7.1 Distribution across the Core Team, Field Experts Team and stakeholders

To guarantee a smooth delivery of quality content, we propose a method of working that is based on extensive research by the Core Team and continuous input delivered by the Field Experts Team.

Project organisation



The distribution described below is, of course, provisional and open for discussion at the kick-off meeting that will be held at the beginning of the project.

a. Core Team: neutral, multilingual, cross-country and interdisciplinary approach

The Core Team will undertake the core tasks regarding the study, analysis and assessment of the issues discussed in this tender and the preparation of the required deliverables. More in particular, this will entail:

- analysing the technical and legal aspects of the issues within the scope of the tender;
- exchanging views, opinions and background material with the stakeholders;
- performing a gap analysis and opportunity search for Europe with regard to these issues;
- contacting stakeholders and external experts to participate in the workshop;
- drafting the deliverables;
- sending the deliverables to the Field Experts Team for quality control;
- preparing the dissemination of the results of the project through the Commission's website.

Within the Core Team, each member will have specific tasks, which will be linked to his/her area of expertise. However, the team will liaise continuously (both in person and through conference calls and web meetings) and will review each individual member's contributions.

At the inception meeting, the representatives of the Core Team and the Commission will discuss the methodology, resources and objectives of the study and make the necessary practical arrangements.

b. The Project Manager: ensuring co-ordination and managerial support

To ensure the smooth interaction between the working teams, as well as the timely and consistent submission of deliverables, we have determined specific management tasks for the overall project's duration. For better work efficacy, we have entrusted this managerial and co-ordination role to one individual of the Core Team (Maarten Truyens), who has both legal and technical skills.

Project managerial responsibilities will primarily include:

- consolidating the roadmap and determining actions to be achieved by each project member (Core Team and the Field Experts Team);
- ensuring consistency of the deliverables (wording, formatting, etc.) developed by each individual project member;
- ensuring quality control *(see section 1.11 below)*
- ensuring that timelines for submission of deliverables are respected by each team member;
- assisting in the organisation of the workshop (sending invitations, correspondence with attendees, etc.);
- ensuring appropriate monitoring of meetings' content and outcome;
- serving as the project's contact point for the different teams and external parties.

c. Field Experts Team

The Field Experts Team will support the activities of the Core Team. In particular, this will entail:

- conducting quality control on the deliverables;
- providing input to the Core Team on the legal aspects of the issues within the scope of the tender;
- supporting the analysis of gaps and opportunities for European industry and policy makers;
- exchanging views and opinions with the Core Team;

d. Stakeholders

As a significant part of the success of the project will depend on finding a consensus among the various stakeholders, we will approach a diverse selection of stakeholders in order to test our ideas and proposals before they are tested "in the wild".

The members of the Core Team will conduct interviews by telephone and – where possible (taking into account travel and lodging expenses, remote location of stakeholders, time availability, etc.) – *in personam*. The stakeholders will be individually solicited for comments and their position on the aspects covered by the execution of the study. In addition, the entire set of stakeholders will be consulted at major milestones of the execution of the study (e.g. through the organisation of two workshops).

e. Added value of the proposed approach for the Commission

The approach presented by the project team will allow the European Commission to choose an appropriate and evidence based approach to developing an IAS policy at the level which is best suited to the IAS state of the art.

The composition of the project team and their past experiences in the IAS domain (including policy support to the Commission and practical support to stakeholders) ensure that the Commission's resources will be optimally spent, as each member of the team is already highly familiar with the state of the IAS debate at the European and national level. The project team is well aware of existing IAS challenges and of potential ways forward.

Furthermore, the approach based on three circles of participants (Core team, Field Experts and Stakeholders) ensures that any approach developed by the project team will be grounded in reality and will reflect a consensus insofar as realistically feasible. In this way, the Commission can avoid wasting time on re-validating the work of the project team with stakeholders, since this task is already integrated in the proposed approach.

The project team therefore believes that the methodology it proposes will create a real and significant added value for the Commission's IAS ambitions.

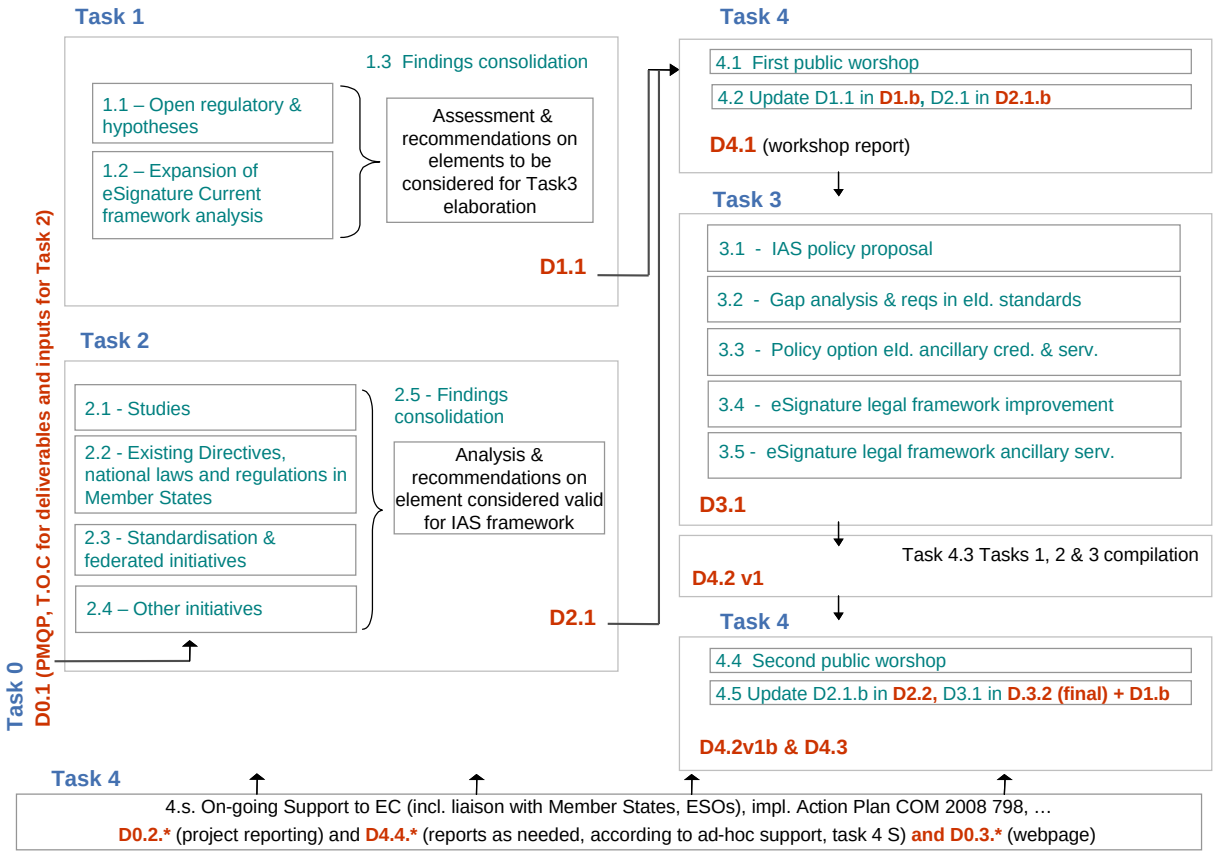
1.8 Tasks and deliverables

The deliverables of the project will be progressively issued and fined-tuned as result of the different tasks to be performed, according the an ad-hoc working method presented in the next sections.

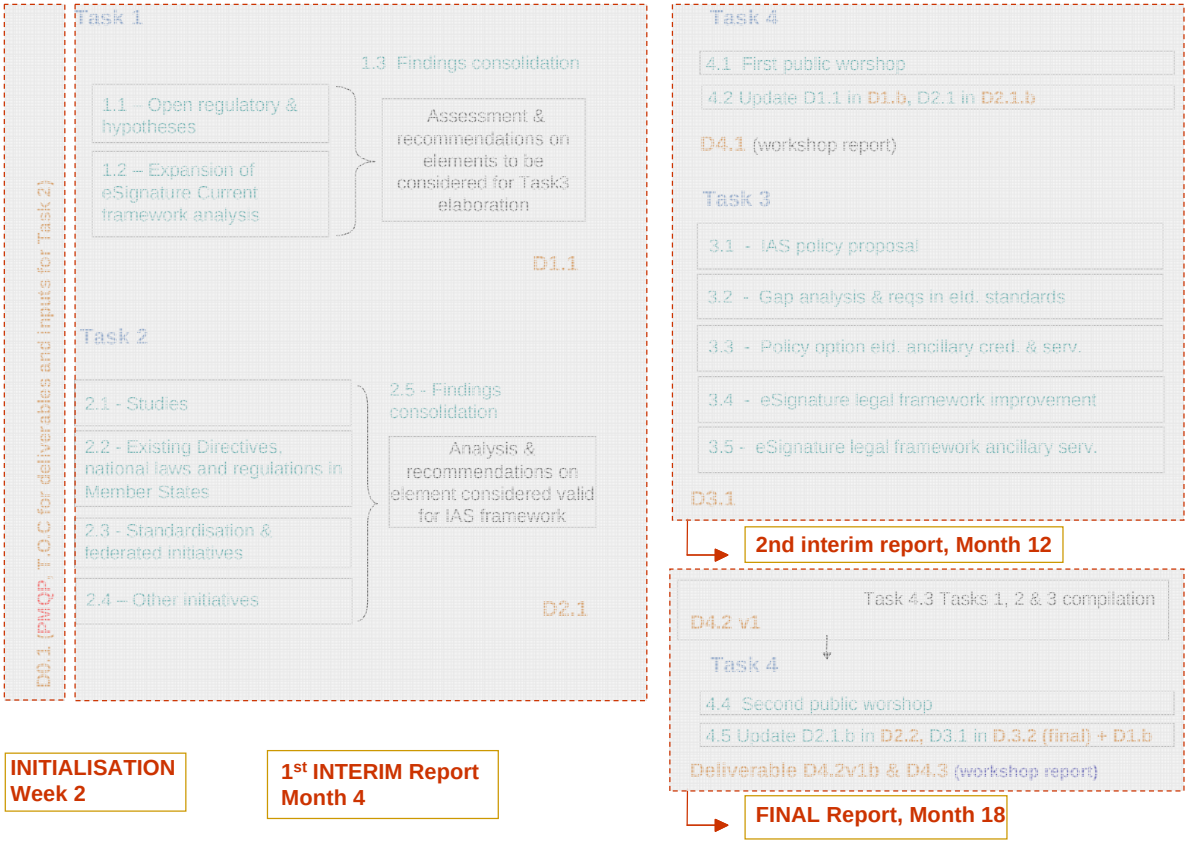
Our task structure adheres to the task structure of the RFP, preceded by an additional Task 0 to ensure efficient and effective execution in the subsequent tasks.

1.8.1 Tasks articulation

The next schema represents the four tasks of the project and all the deliverables *(red text)* that will be issued during the project, each with a bullet point list of the key elements to be tackled *(in green)*. The schema also shows how the deliverables are linked to each other, through black arrows highlighting elements that are feeding a subsequent deliverable.



Tasks planning for delivering interim and final reports:



1.8.2 Overview of deliverables

The deliverables will be gathered in inception, interim and final study reports according to the planning presented in the tender. The deliverables of the project will be progressively issued and fined-tuned as result of the different tasks to be performed, according to an ad-hoc working method presented in the next sections.

The following deliverables will be provided:

§ **Deliverable D0.1 (Inception report)** will be the first report delivered to the Commission. It will describe the project methodology, the project's objectives and an outline of the content of deliverables 1, 2 and 3.

In addition, D0.1 will present a roadmap of the project (based on the preliminary roadmap set out on page 53 of this offer), and will outline how the project will be managed.

§ **Deliverable D0.2 (Technical report)** will report on the work done, and will highlight any problems encountered during the day-to-day management of the project. In annex, it will contain the meeting minutes of all meetings with the Commission, as well as detailed timesheets and expenses.

§ **Deliverable D0.3 (draft webpage)** covers the content for the public website that will be set up by the Commission.

Although an initial version of the web content will be provided early in the project (at the latest one month after contract signature), the tenderer will regularly provide updates to the Com-

mission's IT services, in order to keep the website up-to-date with the latest developments of the project.

While the Commission will host the website and publish the content, the tenderer wants to point out that it has ample experience in setting up websites itself. This experience will foster strong cooperation with the Commission's webmaster. For example, if this would prove easier, it could also be envisaged to upload content directly to the Commission's services. Also, the tenderer would welcome the use of any "Web 2.0" tools (such as surveys, interactive comments, etc.) to accelerate the dissemination and feedback of the project results.

- **Deliverable D1** will contain the work, analysis and recommendations of Task 1 (IAS framework conceptual basis), and will be provided in two versions (draft version 1 and final version 1b).
- **Deliverable D2** will contain the work, analysis and recommendations of Task 2 (stock taking). It will be provided in four versions (1, 1b, 2 and final version 2b), through feedback received from the two workshops.
- **Deliverable D3** will set out the results of the work performed under Task 3 (defining building blocks). It will be provided in three versions (1, 2 and final version 2b).
- **Deliverable D4.1** will contain the report on the first workshop, and **Deliverable D4.2** will contain the report on the second workshop.
- **Deliverables D4.4** contain the draft minutes of specialised meetings, for which the Commission may request to draft minutes.

  Please note that, irrespective of the requirements of D4.4, the tenderer plans to always draft meeting minutes of any meeting with the Commission.
- The **first interim report** will cover both Task 1 and Task 2, and will consist of the first versions of Deliverable D1 and D2. The **second interim report** will be made of the first version of Deliverable D3.
- The **final study report (D4.2)** will consist of the second versions of D1, D2 and D3. The final study report will be provided in two versions (draft version and final version). It will also contain an executive summary and a glossary.

The next sections provide more details about the four Tasks and the specific topics that will be analysed in the study. The next sections also show how these elements will be compiled into the expected deliverables (providing a first flavour of what these deliverable will look like).

In section 1.10, we describe the resources allocated to analyse each issues and topics.

1.8.3 Task 0: initialisation

To the four tasks described in the tender, we also add a **Task 0**, which is an initialisation task that aims to ensure an efficient start of the project and a swift preparation of the deliverables.

In the context of this Task 0, we will provide the European Commission with the required deliverables D0.1. We suggest to split D0.1 into the following parts:

- **a Project Management and Quality Plan** (PMQP) that will specify the methodology, resources and objectives provided in the tender in accordance with the indications provided by the Commission during the inception meeting (based on the previous, current and next sections of the present offer if suitable for the European Commission). As such, the PMQP is the **first part of Deliverable D0.1** the "Inception report".

  The PQMP will also provide templates for the Technical reports D0.2., the ad-hoc report D.4.4. and the workshop reports (D.4.3.1. & 2).

- A specific document detailing the list of initiatives and legal instruments to be analysed during Task 2 (Stock Staking). A first draft of this document is set forth in Annex XIII to this offer. As such, this document is **the second part of Deliverable D0.1** (the "Inception report"). The proposed list aims to point out key elements that are already mastered by the team.

  Some of them being cornerstones for an IAS framework, we are convinced that the deep knowledge of these elements before starting the mission will provide an unmatched time-to-market to the European Commission.

- The tables of contents for Deliverables 1, 2 and 3. As such, this document is the **third and last part of Deliverable D0.1** the "Inception report".

- Task 0 will also be the occasion to prepare the first inputs for the web page presenting the project and its progress (D0.3).

1.8.4 Deliverable D1.1 "Assessment & Recommendations on elements to be considered for Task 3 elaboration"

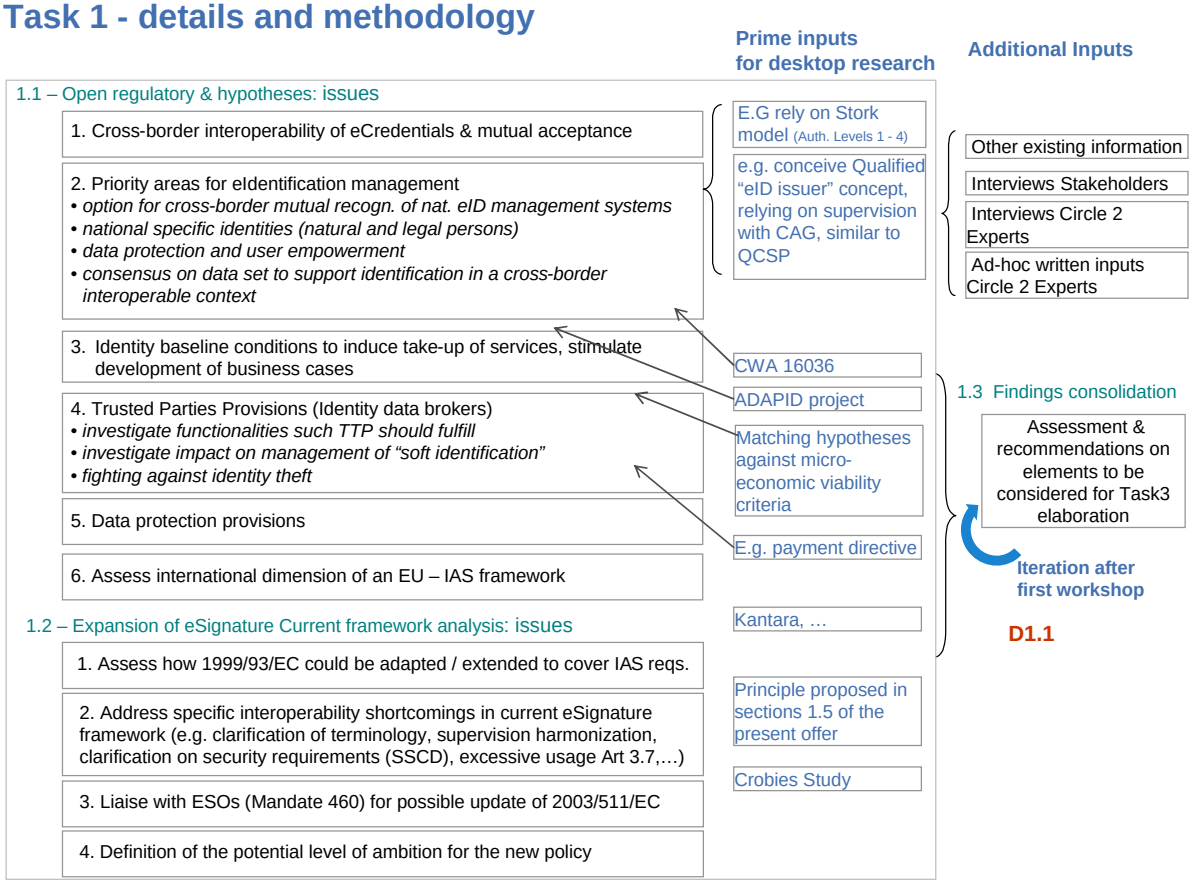
During Task 1 ("Defining the contextual basis for an IAS framework"), to be initiated in parallel with Task 2, we will draft the first version of Deliverable D1.1, on the basis of inputs already identified in the next schema (*prime inputs*).

The issue list and the inputs to study/solve these issues will be completed at the time the Inception report (D.0.1) is being prepared. In addition, we will take into account the interviews with the Field Experts Team and stakeholders (*additional inputs*).

D1.1 will serve as a basis for the first workshop. The first version of D1.1 will be presented during the first workshop and will be updated in D1.1.b. according to the feedback of the workshop.

The table of content of D1.1 will likely encompass the elements listed under points 1.1 and 1.2 in the next schema.

Task 1 - details and methodology



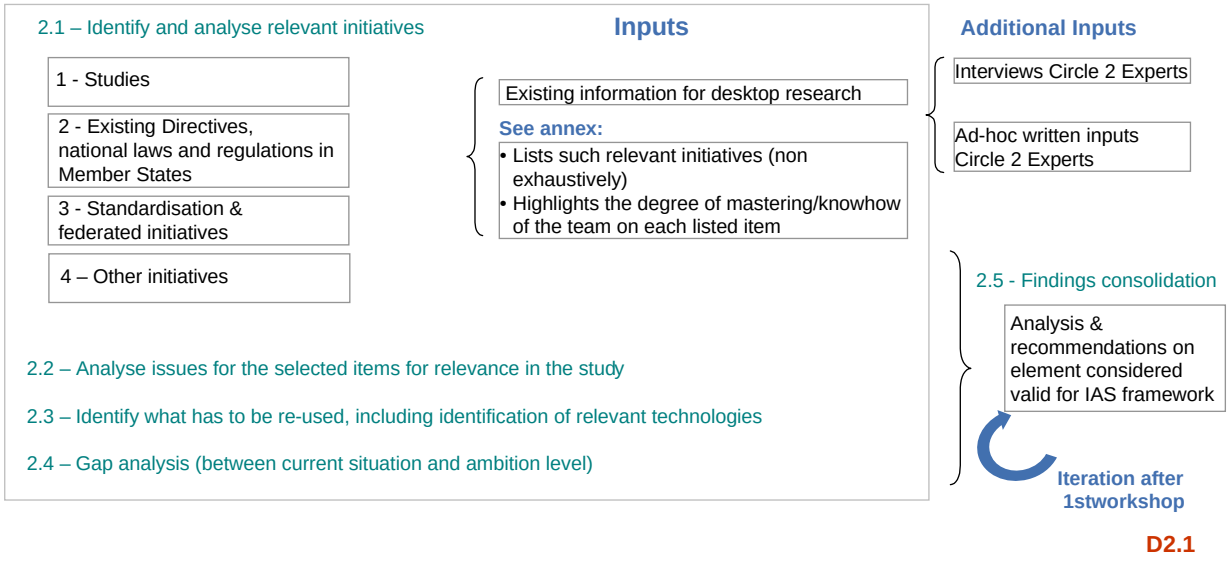
1.8.5 Deliverable D2.1 "Analysis and Recommendations on elements considered valid for the IAS framework"

During Task 2 (Stock Taking), to be initiated in parallel with Task 1, we will draft the first version of Deliverable D2.1, based on input we already identified in the next schema, as already set forth in Annex XIII to this offer. D2.1 will be completed when D.0.1 is prepared, and will take into account the input received from the interviews with the Fields Expert Team and stakeholders (*additional inputs*).

This first version of D2.1 will be presented during the first workshop and will be updated in D2.1.b according to the feedback of the workshop.

This deliverable will be updated after the second workshop, in order to consider a possible evolution of the landscape during the project (we are aware that current initiatives are numerous and arise frequently).

Task 2 - details and methodology



1.8.6 Deliverable D3 ("Defining the building blocks for IAS")

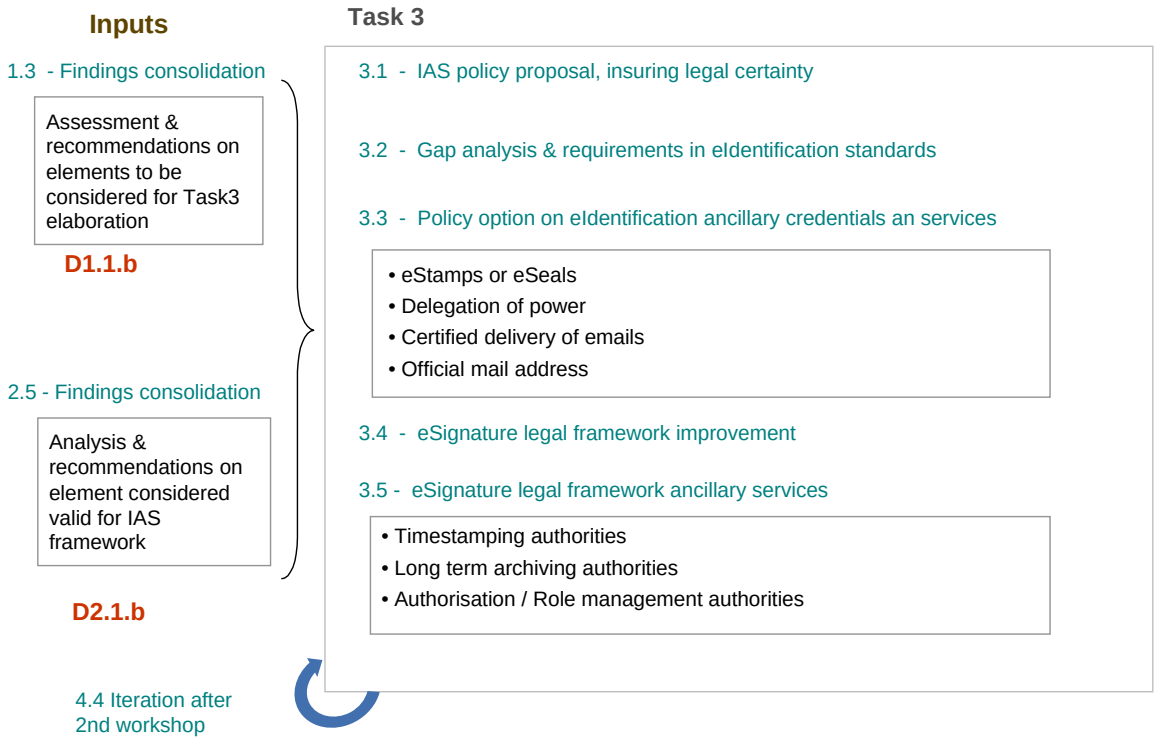
During Task 3, yet in parallel with Task 2, we will draft the first version of Deliverable D3.1, based on the deliverables D1.1.b and D2.1.b. Also for D3.1, we will take into account the input from the Field Experts Team and the stakeholders (*additional inputs*).

This first version of D3.1 will be presented during the second workshop and will be updated into D3.1.b. according to the feedback received during the workshop.

The table of content of D3.1 will likely encompass the elements listed under points 3.1 to 3.6 in the next schema.

Deliverable D3 is the culmination of the project, and we will devote great time and care to it. The project team is well aware that this deliverable will be an important milestone for the Commission to address Key Points 3 and 16 of its Digital Agenda.

Task 3 - details and methodology



1.8.7 Task 4 as project support

Support

4.s. On-going Support to EC, including liaison with Member States, ESOs and other stakeholder, support in implementation of the Action Plan COM 2008 798, …

Task 4.s will be supported by:

- **Deliverables D0.2.*** (project reporting)
- **D4.4.*** (reports as needed, according to ad-hoc support, task 4 S)
- **D0.3.*** (webpage and support for dissemination of findings, debates, …)

Templates for D0.2* and D4.4.* are provided in the PMQP

Synthesis and Workshops

4.1 – Worshop #1 organisation, based on Tasks 1, 2 complilation
4.2 – Worshop #1 follow-up : report of workshop and deliverables 1 and 2 update
4.3 - Tasks 1, 2 & 3 complilation
4.4 – Worshop #2 organisation
4.5 - Worshop follow-up : report and all deliverables 2 and 3 up-date

Task 4.1 and 4.4 will be supported by:
- **PPT presentation of the Deliverables and physical presence of the 8 Circle 1 experts and the Project Manager**
- **Possibilities for the attendance to react or ask questions by mail after the presentation**
- **Presence of 5 representatives of civil society invited by the tendered**

1.9 Meetings

In accordance with the tender requirements, the tenderer will participate in several meetings with the Commission, and will organise public workshops to discuss the results of the project.

The tenderer wants to emphasize that, thanks to the fact that almost all members of the Core Team are based in Brussels, the tenderer can easily hold meetings with the Commission whenever the need would arise.

- The **inception meeting** will be held within two weeks after contract signature. During this meeting, the tenderer will present its Core Team, and will discuss the Commission's objectives and concerns for the project Together with the Commission, the tenderer will agree on a roadmap (based on the preliminary roadmap set out on page 53 of this offer).

- **Progress meetings** will be held every six months.

- Two **public workshops** will be organised for about hundred attendees, respectively within five and seventeen months after the contract signature. These workshops will provide the opportunity to present the draft findings and results of the study, and to invite comments from various stakeholders.

  The tenderer will organise both workshops (incl. sending invitations after approval), and will invite at its own cost least five representatives from civil society. The premises of the meetings (including catering) will be organised by the Commission.

  The tenderer will attend preparation and debriefing meetings for the workshops.

- About **eighteen specialised ad-hoc meetings** will be attended by the tenderer (average frequency of about one meeting each month). Most of these meetings will take place in Brussels, although about three two-day meetings outside Brussels are expected. In these meetings, the tenderer will accompany the Commission, in an adviser capacity, to meetings with stakeholders (e.g. meetings with standardisation bodies or technical committees).

  In addition, about **eighteen preparatory internal meetings** at the Commission will be attended by the tenderer (also with an average frequency of about one meeting each month, and generally organised in Brussels). These meetinsg will cover specific detailed issues regarding the subjects of this study. The tenderer wants to emphasize, again, that most members of its Core Team are based in Brussels, so that even meetings on short notice are generally possible.

1.10 Tasks breakdown

The following table presents the tasks breakdown for the members of the Core Team.

The numbers refer to the number of mandays. Project management is not included in the table.

		DLA Piper	Time.Lex	SNG	PwC	SEALED
Task 0	**Initialisation**					
0.1	PMQP (in preparation of the kick)off meeting)	(PJ)				
0.2	Inputs for Stock staking (list of initiatives)	0,5	0,5	0,5	0,5	0,5
0.3	Table of Content for deliverables 1, 2, 4	0,5	0,5	0,5	0,5	0,5
Total for Task 0		1	1	1	1	1
Task 1	**Defining the contextual basis for an IAS framework**					
1.1	**Open regulatory & hypotheses**					
a.	Cross-border interoperability of eCredentials & mutual acceptance	2	2	2	2	2
b.	Priority areas for eIdentification management					
-	option for cross-border mutual recognition of national eID management systems	2	2	1	2	1
-	national specific identities (natural and legal persons)	1	2	1	2	1
-	data protection and user empowerment	2	1	2	1	
-	consensus on data set to support identification in a cross-border interoperable context	2	2	1	2	2
c.	Identify baseline conditions to induce take-up of services, stimulate development of business cases (Matching hypotheses against micro-economic viability criteria)	1	1	1	2	1
d.	Trusted Parties Provisions (Identity data brokers)1					
-	investigate functionalities such TTP should provide	1	1	1	1	1
-	investigate impact on management of "soft identification"	1	1	1	2	2
-	fight against identity theft	0,5	0,5	0,5	2	2
e.	Data protection provisions	1	1	1		
f.	Assess international dimension of an EU – IAS framework	2	1	1	1	1
1.2	**Expansion of eSignature Current framework analysis**					
a.	Assess if/how the eSignatures Dir. could be adapted or extended to cover IAS requirements	1,5	1,5	1,5	1	1

	DLA Piper	Time.Lex	SNG	PwC	SEALED
b. Address specific interoperability shortcomings in current eSignatures framework	1	2	1	1	2
c. Liaise with ESOs (Mandate 460) – in part. for possible up-date of Directive 2003/511/EC			2		2
Total for Task 1	18	18	17	19	18
Task 2 Defining the contextual basis for an IAS framework					
2.1 Identify and analyse relevant initiatives	3	3	2	2	3
2.2 Analyse issues for the selected items for relevance	2	2	2	2	2
2.3 Identify what has to be re-used (directly or indirectly), including identification of relevant technologies	2	2	2	2	2
Total for Task 2	7	7	6	6	7
Task 3 Defining Building Blocks for IAS					
a. IAS policy proposal, insuring legal certainty	1	1	1	0,5	0,5
b. Gap analysis & requirements in eIdentification standards	1	1	2	3	3
c. Policy options on eIdentification ancillary credentials and services					
- eStamps or eSeals	1	1	1	1	1
- Delegation of power	1	1	1	1	1
- Certified delivery of emails	1	1	1	1	1
- Official mail address	1	1	1	1	1
d. eSignature legal framework improvement	2	2	2	0,5	0,5
e. eSignature legal framework ancillary services					
- Timestamping authorities	1	1	1	0,5	1
- Long term archiving authorities	1	1	2	1	1
- Authorisation / Role management authorities	1	1	1	1,5	1
Total for Task 3	11	11	13	11	11
Task 4 Support & synthesis workshops					
a. Support (profiles to be allocated according to EC needs)	7	7	7	7	7
b. Workshops	4	4	4	4	4
Total for Task 4	11	11	11	11	11
Total number of mandays	48	48	48	48	48

1.11 Achieving Quality of Service

In this section, we provide a description of the measures we will employ to ensure the quality of the services (QoS) we will provide to the Commission.

The QoS, both in terms of quality of deliverables (content and style) and in terms of due respect of the obligations (delivered in time, within budget), will rely on the articulation of the three essential pillars of our offer:

- **A limited core team of highly skilled experts in the Core Team**

  To provide the required flexibility and quality, our Core Team is voluntary limited in size, while gathering best in class expertise and competencies to successfully conduct the study. These eight consultants, each providing real unmatched competences, may rely on ad-hoc inputs provided by the members of the Field Experts Team, but will be the sole persons in charge of writing the deliverables. In addition to the quality review of any deliverable (see below), each member of the Core Team from will review all deliverables before submission to the Commission.

- **An ad-hoc methodology encompassing a quality assurance dimension**

  The purpose of Quality Assurance (QA) is to ensure that the deliverables are delivered in time, within the budget and according to the customer's requirements through regular checking. QA is an essential process that will be carried out throughout all stages of the project.

- **Professional project management**

  The Quality Assurance is performed by the Project QA manager (Maarten Truyens), who will on a regular basis verify if the project is executed conform to the methodology and the agreed project management and quality plan (PMQP). He will also organise the verification and validation of the deliverables. This person will monitor both the process control (verifying whether project tasks are completed in accordance with the methodology quality system) and the validation and verification of documents and deliverables.

1.12 Meetings and workshops – indicative roadmap

The roadmap below provides a proposed description of the study work plan, the methodology and the timetable to be followed.

We propose to use the following time-line as a first basis for further discussion and refinement. At the kick-off meeting with the European Commission during Week 1 of the project, we intend to include further details on timing of the interviews, internal meetings, etc.

We will make use of project management software (such as Microsoft Project) to build up and monitor the continuity of the project.

Date	Task	Code	Responsible
		First Month	
Day 1	Signature of the contract	C.1.1	Joint
Within 2 weeks after C.1.1	Inception meeting with the Commission	C.1.2	Joint
After 1.2 and before C.1.4	Kick-off meeting of the Core Team	C.1.3	Tenderer
5 days after C.1.2	Submission of Inception Report	C.1.4	Tenderer
Within 4 weeks after C.1.1	Submit roadmap	C.1.5	Tenderer
Within 1 month after C.1.1	Draft Webpage of the study	C.1.6	Tenderer
Within 1 week after C.1.6	Comments on roadmap	C.1.7	Commission
Within 1 week after C.1.7	Submit final roadmap	C.1.8	Tenderer
		Months 2-6	
After C.1.8 and within 4 months after C.1.1	Start drafting the Interim Study Report	C.2.1	Tenderer
	Deliver 1st interim study report to the Commission	C.2.2	
	Assessment and recommendations	C.2.3	
	Result analysis and recommendations on external elements	C.2.4	
10 days before C.2.7	Contact Commission to manage practical details of the Joint Workshop	C.2.5	Joint
After C.2.5, before C.2.7	Send summary and presentation to Commission	C.2.6	Tenderer
Within 5 months after C.1.1	Hold 1st Public Workshop	C.2.7	Joint
5 days after C.2.7	1st Workshop Report	C.2.8	Tenderer
After C.2.8	Update 1st Interim Study Report	C.2.9	Tenderer

Within 6 months after C.1.1	Technical reports	C.2.10	Tenderer
	Assessment and Recommendations v1b	C.2.11	
	Analysis and Recommendations v1b	C.2.12	Joint
	Progress meeting	C.2.13	
Five days after C.2.13	Deliver detailed meeting notes	C.2.14	Tenderer
		Months 7-12	
Within 12 months after C.1.1	2nd Interim Study Report	C.3.1	Tenderer
	Technical reports	C.3.2	
		Months 13-18	
Within 16 months after C.1.1	Draft final study report D4.2 v1	C.4.1	Tenderer
	Update analysis and recommendations on external elements v2	C.4.2	
	Update 2nd Interim Study report v2	C.4.3	
10 days before C.4.6	Contact Commission to manage practical details of the Joint Workshop	C.4.4	Joint
After 3.4, before C.4.6	Send summary and presentation to Commission	C.4.5	Tenderer
Within 17 months after C.1.1	2nd Public Workshop	C.4.6	Joint
Five days after C.4.6	2nd Workshop Report	C.4.7	Tenderer
Within 18 months after C.1.1	Update 2nd Interim Study report v2b	C.4.8	
	Update Final study report D4.2 v1b	C.4.9	
	Update analysis and recommendations on external elements v2b	C.4.10	
	Technical reports	C.4.11	

2. FINANCIAL SECTION

We foresee two areas of costs: professional fees (for the members of the Core Team and the Field Experts Team), and travel expenses (for the Core Team, Field Experts Team and Stakeholders). As the participation of the Stakeholders is on a voluntary basis, we do not foresee any costs in this area.

The tenderer accepts that the total amount stated below is fixed, and will not be subject to revision.

Costs	Cost Area	Total
Professional fees	Core team	270,000 EUR
	Field Experts Team	40,000 EUR
Travel and subsistence expenses	Core Team	11,000 EUR
	Field Experts Team and workshops	10,000 EUR
Other expenses	N/A	0
	Total amount	**331,000 EUR**

2.1 Professional fees for the Core Team

The table below shows the contribution of each member of the Core Team to the Study, which includes all study activities, time for travelling, meetings with the Commission (also covering the specialised ad hoc meetings) and internal meetings with the other members of the Core Team.

The members of the Core Team will be **dedicated** to the project, and will themselves undertake the final editing and consolidation of the deliverables, and present and attend the workshops. No task will be delegated to any other person.

The fees for the project management (assigned to Maarten Truyens) include the costs of organising the workshop (sending invitations, correspondence with attendees, etc.).

All administrative costs (telecom, printing, etc.) are included in the daily rate of each member of the Core Expert team.

Member	Task	Per day	Days	Total
Patrick Van Eecke	Legal expert	1,000 EUR	48	48,000 EUR
Riccardo Genghini	Legal expert	1,000 EUR	48	48,000 EUR
Jos Dumortier	Legal expert	1,000 EUR	24	24,000 EUR
Hans Graux	Legal expert	1,000 EUR	24	24,000 EUR
Olivier Delos	Technical expert	1,000 EUR	24	24,000 EUR
Sylvie Lacroix	Technical expert	1,000 EUR	24	24,000 EUR
Marc Sel	Technical expert	1,000 EUR	24	24,000 EUR

Frederic Van Hoorebeke	Economic expert	1,000 EUR	24	24,000 EUR
Maarten Truyens	Project management	1,000 EUR	30	30,000 EUR
Total amount				**270,000 EUR**

2.2 Professional fees for the Field Experts Team

We foresee an **average of four working days** for each member of the Field Experts Team. The actual amount of working days for each member may, however, differ (between three and eight days), depending on each member's field of expertise, the deliverables assigned, and the issues he / she raises during the review of the deliverables prepared by the Core Team.

Member	Task	Per day	Days	Total
John Bullard	eID as a business service	1,000 EUR	4	4,000 EUR
Claudia Diaz	Technical expert privacy & anonymisation	1,000 EUR	4	4,000 EUR
Marit Hansen	Technical aspects of security and privacy	1,000 EUR	4	4,000 EUR
Stephen Kent	Technical expert authentication technologies and systems	1,000 EUR	4	4,000 EUR
Chris Reed	Legal expert electronic signatures	1,000 EUR	4	4,000 EUR
Teemu Rissanen	Technical implementation of eID/eSignatures, Porvoo Group	1,000 EUR	4	4,000 EUR
Stefan Santesson	Expert electronic signatures	1,000 EUR	4	4,000 EUR
Marc Stern	Expert eID / STORK	1,000 EUR	4	4,000 EUR
Eric Verheul	Technical expert security (eGovernment, National Accreditation schemes)	1,000 EUR	4	4,000 EUR
Jane Winn	US legal expert. Federated IDM, international aspects (US, EU, China), LA/Kantara initiative	1,000 EUR	4	4,000 EUR
Total amount				**40,000 EUR**

2.3 Travel expenses

a. Core Team

For the **inception meeting** and the two **public workshops**, we foresee travel expenses for only one member of the Core Team (Riccardo Genghini). For all the other members of the Core Team, no travel expenses apply for the inception meeting, progress meeting or public workshops, as they are all based near Brussels.

As regards the **specialised ad-hoc meetings**, the tenderer budgets three two-day meetings to cities outside Brussels, and two one-day meetings outside Brussels.

b. Field Experts Team

The Core Team expects to communicate with the members of the Field Experts Team through modern communication technologies. Some members of the Field Experts Team may also be met in person, for example when these members are based in Brussels or travel to Belgium.

Therefore, no travel expenses are budgeted for the members of the Field Experts Team.

c. Stakeholders

In the day-to-day management of the project, communication with the stakeholders will take place through modern communication technologies, which avoids travel costs.

The tenderer does budget costs for the five stakeholders (an average of 1,000 EUR) it will invite to the two public workshops.

d. Overview

The following table presents out travel budget.

Please note that, due to the fact that in most cases it is unknown who will travel and from which location, we use an average expected cost per day of (1,000 EUR). In some cases, this budget will not be used (e.g., a person travelling from the Netherlands), and in some other cases this budget may be exceeded (e.g., a person travelling from Finland).

Member	Per day	Days	Total
Riccardo Genghini: attending inception meeting and two public workshops	1,000 EUR	3	3,000 EUR
Member of the Core Team: attending three two-day ad-hoc meetings outside Brussels, and two one-day meetings outside Brussels	1,000 EUR	8	8,000 EUR
Stakeholders (5 x 2)	1,000 EUR	10	10,000 EUR
		Total amount	**21,000 EUR**

3. ADMINISTRATIVE SECTION

I. Administrative identification forms

II. Legal entities forms

III. Financial identification form

IV. Declarations of honour

V. Statutes of DLA Piper UK LLP

VI. Notice of appointment

VII. Letter of intent from each subcontractor

VIII. Enrolment in a professional register

IX. Evidence of financial and economic capacity

X. CVs for the Core Team members

XI. Detailed expertise of the members of the Core Team

XII. Example input for D0.1 (Inception Report)

Annex I.

Administrative identification forms

(based on Annex 1 of the tender specifications)

Identification of the tenderer and its subcontractors

This tender is submitted as Option 3, *i.e.* submission by one tenderer with subcontractors (as defined under section 2.2 of the tender specifications).

Tenderer: **DLA Piper UK LLP**, Avenue Louise 106, 1050 Brussels, Belgium

Subcontractors: **SEALED** sprl, Rue de la Paix 12, 7500 Tournai, Belgium

Studio Notarile Genghini, Via Turati 29, 20121 Milan, Italy

Time.Lex BV cvba, Congresstraat 35, 1000 Brussels, Belgium

PricewaterhouseCoopers Enterprise Advisory cvba, Woluwedal 18, 1932 Sint-Stevens-Woluwe, Belgium

In addition, ten individual **external experts** will be involved (as described in section 1.3). In accordance with page 26 of the tender specifications, these external experts are not part of the tenderer's staff, but are also considered subcontractors of DLA Piper UK LLP.

Brussels,

14 July 2010,

Kristof De Vulder

Partner DLA Piper UK LLP (Brussels)

Annex II.

Legal entities forms

(based on Annex 2 of the tender specifications)

Annex III.

Financial identification form

(based on Annex 3 of the tender specifications)

Annex IV.

Declarations of honour
with respect to the exclusion criteria and the absence of conflict of interest

(based on Annex 4 of the tender specifications)

Annex V.

Statutes of DLA Piper UK LLP

Annex VI.

Notice of appointment

Annex VII.

Letter of intent
from each subcontractor

(based on Annex 6a of the tender specifications)

Annex VIII.

Enrolment in a professional register

Annex IX.

Evidence of financial and economic capacity of DLA Piper

Turnover from contracts in the field of the study in the last three years

DLA Piper UK LLP (Brussels) has undertaken, or is currently undertaking, the following projects for the European Commission in the field of analysing science, research and innovation / IT policies and legislation in the last three financial years. The aggregate total value of these contracts amounts to approximately **2.35 million EUR**.

Several other (smaller) contracts have also been undertaken by DLA Piper UK LLP for various Belgian and international governmental authorities in the field of IT law and analysis of policies. The aggregate value of these contracts in the last three years approximates 500,000 EUR.

- **Ongoing – Comparative law database on unfair commercial practices** – The aim of this study (value: approximately **500,000 EUR**), commissioned by the European Commission (DG Health and Consumer), is to create a database of various elements related to the Unfair Commercial Practices Directive and its implementation in the Member States. The project, which is being led by Patrick Van Eecke, involves gathering the input from lawyers from the 27 European Member States, and is centrally coordinated from the DLA Piper Brussels office.

- **(2008-2009) – Study on the legal analysis of a single market for an information society** – The aim of this study (value: approximately **300,000 EUR**), commissioned by the European Commission (DG Infosoc), is to review the "acquis communautaire" on online services and markets, in order to identify its benefits, gaps, lack of future proofing and implementation hurdles. It covers a broad range of topics, including e-commerce practices, services, data protection, consumer protection, applicable law and jurisdiction, e-payments, illegal and harmful content, protection of minors, security, taxation and e-procurements. This project's website is available at www.euinternetlaw.eu.

- **(2006-2007) EU Study on the specific policy needs for ICT standardisation.** Patrick was leading a multidisciplinary, international team of researchers advising the European Commission on ICT standardisation policy issues. The study (value: approximately **370,000 EUR**) analysed the current European ICT standardisation policy and the prospective evolution in ICT services, products and applications for the coming 10 years. The study subsequently identified the evolving needs of a European ICT standardisation policy that is required to serve the needs of industry, societal requirements and public authority expectations. The study also put forward a set of recommendations for establishing a new European ICT standardisation policy. See also *www.ictstandardisation.eu*

- **(2006 - 2009) – EU study on technology transfer** – In this study (value: **1,181,000 EUR**) Patrick Van Eecke leads of team of 30 lawyers (EU, US, Japan) analysing how to improve the regulatory environment for R&D in Europe. The main objective of this study, commissioned by the European Commission (DG Research), is to foster the development and use of European intellectual property systems in a research policy perspective. Two different categories of issues are being addressed: legal topics on the one hand, and issues relating to training and awareness on the other hand. This project's website is available at www.eutechnologytransfer.eu.

Annex X.

CVs for the Core Team members

Annex XI.

Detailed expertise of the members of the Core Team

This Annex XII provides an overview of relevant expertise of each member of the Core Team: speeches delivered at conferences, security certifications, publications, reports, participation in standardisation committees and participation in consensus building undertakings.

Patrick van Eecke (DLA Piper)

Speeches

- Legal aspects to consider when using eID in business applications, ADM, Brussels, 21 March 2009
- eID and the law, KU Leuven, 3 April 2008, EEMA
- eID congres, Leuven, LSec, 28 February 2008
- The European rules on ICT Standardisation, Brussels, 12 February 2008
- Automation and the Law / Standardisation as a regulatory measure. Aula Magna at Stockholm University, 18 November 2008
- eID: legal issues, Leuven, LSec, 7 November 2007
- Legal aspects of information security, COSIC, 11 July 2007
- EU directives on E-signatures and analysis of relevant laws of EU member states. Cairo, Egypt, 11 July 2006, US-Egyptian conference on eCommerce
- Comparative Overview of Int. Legal Framework and Electronic Contracting. Gulf Hotel (Manama, Bahrain), 11-12 September 2006, Conference on E-commerce Fundamentals and Regional Perspective
- US Data Privacy & Security Legislation: "Should the EU be a model?", Mc Enery Convention Center in San Jose- California). 13 February 2006, RSA Conference
- The European Data Protection Directive, a good example for the United States? Washington, 2 May 2006, 16th annual Conference on Computers, Freedom and Privacy
- Legal aspects of electronic signatures – Vienna, 19 October 2005, RSA
- The legal value of e-Mail. Madrid, 23 October 2004, AIJA
- Legal aspects of eID Brussel. 2 December 2004, TMAB
- Electronic signatures: Overview of European legal initiatives. Berlin, 27 September 2004, ISSE

Books

- P. VAN EECKE, Wetboek ICT, 2010
- P. VAN EECKE, *De handtekening in het recht*, Larcier, Gent, 2004, 622 p.
- RIENHOFF, O., P. VAN EECKE, LASKE , C., WENZLAFF, P. & PICCOLO, U., *A Legal Framework for Security in European Health Care Telematics*, Volume 74 Studies in Health Technology and Informatics, 2000, 202 pp.
- DUMORTIER, J. & P. VAN EECKE, *The Legal aspects of digital signatures*, Mys & Breesch, Gent, 1999, 566 pp.
- P. VAN EECKE, *Bewijsrecht op de informatiesnelweg – Bewaar- en bewijsproblematiek bij gebruik van elektronische communicatiemiddelen*, Ced. Samsom, Diegem, 1998, 73 pp.

- P. VAN EECKE, '*Criminaliteit in Cyberspace, Misdrijven, hun opsporing en vervolging op de informatiesnelweg*'. Mys en Breesch, Gent, 1997, 131 pp.
- P. VAN EECKE, Uitdagingen van de Informatiemaatschappij en opdrachten voor het justitiebeleid, *Deel I: Criminaliteitsbestrijding op de informatiesnelweg,* Ministerie van Justitie, September 1996.

Publications

- P. VAN EECKE, "Klokkenluiden in het bedrijfsleven: privacyaspecten", DAOR: internationaal tijdschrift voor ondernemingsrecht, 2010, p. 21-39.
- P. VAN EECKE & M. TRUYENS, "Privacy en sociale netwerken: gedwongen huwelijk legt wettelijke tekortkomingen bloot", Computerrecht, March 2010
- P. VAN EECKE, "De elektronische handtekening in het recht", Tijdschrift voor Belgisch handelsrecht, 2009, p. 283-315.
- P. VAN EECKE & M. TRUYENS, "Standardisation in the European ICT sector: official procedures at the verge of being overhauled", *Shidler Journal of Law, Commerce & Technology*, juli 2009.
- P. VAN EECKE & M. TRUYENS, "Legal issues in technology transfer - findings from an EU-level study", EARMA (the European Association of Research Managers & Administrators) Link, October 2009
- P. VAN EECKE & A. MITRAKAS, "The European Directive on Electronic Signatures", in A. Büllesbach, Y. Poullet, C. Prins (ed.), Concise Commentary on European IT Law, Kluwer Law International, Alphen aan den Rijn, 2006, p. 349-405.
- P. VAN EECKE, "European laws and electronic signatures" (Japanese), in IBUSUKI M., *Cyberspace law* 2000, Tokyo, p. 205-209 (Japanese).
- P. VAN EECKE, G. GRAVESEN & J. DUMORTIER, "Die europaïsche Signaturrichtlinie – Regulative Funktion und Bedeutung der Rechtswirkung', *Multimedia und Recht, Zeitschrift für Intormations-, Telekommunikations- und Medienrecht*, oktober 1999, p. 577-585, Verlag C.H. Beck München.
- J. DUMORTIER & P. VAN EECKE, "De Europese ontwerprichtlijn over de digitale handtekening: waarom is het misgelopen? *Computerrecht*, 1999; 1:3-10.
- P. VAN EECKE & J. DUMORTIER, "Electronic Signatures. The European Draft Directive on a common framework for electronic signatures", *Computer Law & Security Report*. 1999; 15(2): 106-112.
- P. VAN EECKE & J. DUMORTIER, "Een juridisch kader voor Trusted Third Parties in België", *Computerrecht*, 1998, 5, 228-233.
- P. VAN EECKE, "Burgerlijke rechtspleging: Inrichting van de rechtbanken en procedure", *Milieu- en Veiligheidsmanagement*, 1997.
- P. VAN EECKE & J. DUMORTIER, "Naar een juridische regeling van de digitale handtekening in België", *Computerrecht*, 1997, 4, 154.

Consensus building

- **EU Study on the specific policy needs for ICT standardisation.** Patrick was leading a multidisciplinary, international team of researchers advising the European Commission on

ICT standardisation policy issues. The study analysed the current European ICT standardisation policy and the prospective evolution in ICT services, products and applications for the coming 10 years. The study subsequently identified the evolving needs of a European ICT standardisation policy that is required to serve the needs of industry, societal requirements and public authority expectations. The study also put forward a set of recommendations for establishing a new European ICT standardisation policy. See also *www.ictstandardisation.eu*

Maarten Truyens (DLA Piper)

Speeches

- LSec "Virtualization Security and Cloud Computing Issues 2009 Revisited", 26 January 2010, "Legal Challenges in Cloud Computing"
- "Legal developments in open source in the US and the EU", iTechLaw conference for IT Lawyers, 6 November 2009
- "How Liable Are You with Identity Theft?", RSA Security Conference 2007
- "Legal aspects of risk management and security" (Telindus / Belgacom, June 2007)
- "Internet Crime" (Tiscali, November 2006)

Publications

- P. VAN EECKE & M. TRUYENS, "Privacy en sociale netwerken: gedwongen huwelijk legt wettelijke tekortkomingen bloot", Computerrecht, March 2010
- P. VAN EECKE & M. TRUYENS, "Standardisation in the European ICT sector: official procedures at the verge of being overhauled", *Shidler Journal of Law, Commerce & Technology*, juli 2009.
- Contributions to "Handboek internetrecht" (on marketing and Web 2.0), forthcoming, 2010
- "Monitoring and analysis of technology transfer and intellectual property regimes and their use", together with P. VAN EECKE, J. KELLY and P. BOLGER (2009)
- P. VAN EECKE & M. TRUYENS, "Legal issues in technology transfer - findings from an EU-level study", EARMA (the European Association of Research Managers & Administrators) Link, October 2009
- P. VAN EECKE & M. TRUYENS, "Long awaited opinion on the use of search engines", BNA International World Data Protection Report, April 2008
- P. VAN EECKE & M. TRUYENS, "Standardisation in the European ICT sector: official procedures at the threshold of being overhauled", ICT Standaardisatie, SBJ April 2008
- K. DE VULDER & M. TRUYENS, "Wat zegt de wet over security?" (Data News ICT Guide, 2007)

Riccardo Genghini (SNG)

Speeches

- 2009, ISSE2009, Den Haag, October 6th, *"Virtual Signing Room"*.
- 2009, Eurochambers Conference, Stockholm, June 26, *"ETSI Interoperability Tools"*
- 2007, Keynote speech at Cyprus Standards Organisation, in Nicosia (Cyprus), July 6, *"Application of PKI "Technology in e-Government in Europe"*.
- 2005 Keynote speech at ASIA PKI-Forum, in Beijing, November 5, *"Application of PKI "Technology in e-Government in Europe"*.
- 2005 Conclusive speech at ASIA PKI-Forum, in Taipei, September 13, *"IT Security Policy Recommendation for Network Society — The Vision and Experience from Europe"*.
- 2005 Keynote speech at the establishment of AFRICA PKI-Forum in Tunis, *"PKI Deployment in Europe"*.
- 2001 Keynote Speech at the establishment of ASIA PKI-Forum in Tokyo, June 12, *"The Electronic Signature Infrastructure in Europe"*.
- 2001, Keynote Speech of ISSE 2001 London, September 26: *"Freedom Law and Digital Self-regulation"*.
- 2000, Herbsttagung of the Europäische Akademie in Bad Neuenahr, September 21: *"Steintafeln… Papyren… Bits"*.

Publications

- GENGHINI, R., "L'atto notarile digitale" (appendix to GENGHINI, L., La forma degli atti notarili, 2009)
- GENGHINI, R. "Tavole di pietra… papiri… bit", ICT Security 2002, 5, 23

Consensus building

- Riccardo Genghini, had decisive role in finding the compromise in the security criteria of Secure Signature Creation Devices (SSCD) in 1999, in chairing (as a substitute to the absent chairman) the Cen-ISSS E-Sign meeting in Brussels, where the decision was taken to adopt two different security profiles for SSCDs, leaving to the marketplace to decide which to adopt. He participated as chairman in the Experts group who was drafting the two technical specifications (CWA 14168 and CWA 14169).
- Subsequently Riccardo Genghini has been Chairman of CEN-ISSS E-Sign, from 2001 until ist disbandment (2004). Under his tenure, further important technical specifications have been approved. Under his tenure the practice of co-located meetings with ETSI-ESI was established, introducing a four years time of close cooperation between CEN and ETSI in the field of electronic signatures.
- Starting from 2004 Riccardo Genghini is the Chairman of ETSI-ESI. Under his tenure all relevant electronic signatures technical standards have been maintained, improved and completed. Several new companies and organisations have since joined ETSI, in order to participate to the works of ESI.

Jos Dumortier (Time.lex)

Speeches

Relevant recent speeches in the last months include:

- EEMA Event on *Corporate PKI Certificate Provisioning - Certificate policy and practice plus certificate trust levels,* London, UK, 18 May 2010
- Presentation to the eProcurement Expert Group meeting on the evaluation of the Action Plan for the implementation of the legal framework for electronic public procurement, including eSignature interoperability issues, Brussels, Belgium, 22 June 2010
- Panellist in discussion *"Electronic signature, interoperability and general electronic services. Are we finally witnessing the beginning of a breakthrough on the European scale?"*, European Forum on eSignature, Miedzyzdroje, Poland, 9th of June 2010

A full list of speeches can be found at the following URL:
www.law.kuleuven.be/icri/presentations.php?action=byAuthor&staffid=1&where.

Publications

Relevant recent publication include:

- C. GEUENS and J. DUMORTIER, "Mandatory implementation for in-vehicle eCall: Privacy compatible?", Comput. Law and Secur. Rev. (2010), doi:10.1016/j.clsr.2010.03.009
- B. VAN ALSENOY, D. DE COCK, K. SIMOENS, J. DUMORTIER, and B. PRENEEL, "Delegation and digital mandates: Legal requirements and security objectives", CLSR 2009, vol. 25, pp. 415-431.
- J. DUMORTIER, editor Cyberlaw, International Encyclopaedia of Laws, Daniel VAN DER MERWE, "Cyber law South Africa", 181 pag., BLANPAIN R. general editor, Kluwer International, The Hague, July 2009.
- J. DUMORTIER, and F. ROBBEN, "Gebruikers- en toegangsbeheer bij het bestuurlijke elektronische gegevensverkeer in België, Identity-management verzoenen met privacybescherming: hoe doen de Belgen dat?", *Computerrecht, Tijdschrift voor informatica, telecommunicatie en recht, 2009*, nr 2, p. 52-60
- J. DUMORTIER, and G. SOMERS, "Introduction to the technical concepts of Digital Signature and Authentication", p. 75-84 in Best Practice for applications using the electronic Identity Card (eID), 2008, 98p editor SEALED, DIS authors, ISBN 978-2-9600761-0-3

In addition to the reports mentioned above, a full list of publications can be found at www.law.kuleuven.be/icri/all_pubs.php?action=pubs_staff&staffid=1&where.

Reports

Author and co-author of the study deliverables mentioned above, in particular the next studies published on various European Commission websites:

- 2004 Study on the Legal and Market Aspects of Electronic Signatures
- 2007 and 2009 Preliminary studies on mutual recognition of eSignatures for eGovernment applications
- 2007 and 2009 eID Interoperability for PEGS studies

A more comprehensive list of reports can be found at the following URL: www.law.kuleuven.be/icri/projects.php?projectid=202&where=

Consensus building

- Jos has assisted the Commission in its discussions with Member States throughout various studies, including the aforementioned studies with respect to eSignatures, eID and ePro-curement. In each case, consensus had to be built on existing issues and on suitable ave-nues for the Commission to move forward.
- Jos is the Director of the Interdisciplinary Centre for Law and ICT at the K.U.Leuven, a re-search group comprising 29 lawyers (professors, researchers and affiliate researchers), and has frequently lead studies that required liaising with stakeholders in 32 European countries.

Hans Graux (Time.lex)

Speeches (latest)

Relevant recent speeches in the last months include:

- EEMA Event on *Corporate PKI Certificate Provisioning - Certificate policy and practice plus certificate trust levels,* London, UK, 18 May 2010
- Presentation to the eProcurement Expert Group meeting on the evaluation of the Action Plan for the implementation of the legal framework for electronic public procurement, including eSignature interoperability issues, Brussels, Belgium, 22 June 2010
- Panellist in discussion *"Electronic signature, interoperability and general electronic services. Are we finally witnessing the beginning of a breakthrough on the European scale?"*, European Forum on eSignature, Miedzyzdroje, Poland, 9th of June 2010

Publications (latest)

Almost all reports mentioned in the section below have been published on European Commission websites. In addition, Hans is the author of several Belgian legal publications, especially focusing on data protection and e-commerce.

Reports (latest)

Author and co-author of the study deliverables mentioned above, in particular the next studies published on various European Commission websites:

- 2009-2010 – Study on Cross-border Interoperability of eSignature (Crobies)
- 2009 – European Federated Validation Service (EFVS) study
- 2007 and 2009 – Preliminary studies on mutual recognition of eSignatures for eGovernment applications
- 2007 and 2009 – eID Interoperability for PEGS studies
- 2008 – report for ENISA on the state of pan-European eIDM initiatives
- 2009 – Study on electronic documents and electronic delivery for the purpose of the implementation of Art. 8 of the Services Directive
- 2008 – Preliminary Study on the electronic provision of certificates and attestations usually required in public procurement procedures

Consensus building

- Hans co-drafted of Commission Decision 2009/767/EC of 16 October 2009. This clearly shows his ability to build consensus, as it required the **agreement of the 27 Member States**.
- Hans has assisted the Commission in its discussions with Member States throughout various studies, including the aforementioned studies with respect to eSignatures, eID and eProcurement. In each case, consensus had to be built on existing issues and on suitable avenues for the Commission to move forward.
- Hans is the managing partner of time.lex, a law firm comprising 14 lawyers, and has frequently lead studies that required liaising with stakeholders in 32 European countries.

Olivier Delos (SEALED)

Speeches (latest)

- Panellist in discussion *"Electronic signature, interoperability and general electronic services. Are we finally witnessing the beginning of a breakthrough on the European scale?"*, European Forum on eSignature, Miedzyzdroje, Poland, 9th of June 2010
- *"Cross-border interoperability of e-Signatures (CROBIES)"*, ISSE 2009 the 6th of October 2009
- *"Cross-border interoperability of e-Signatures: challenges and key success factors"*, the 2009 EU-CHINA Information Society Summit (ECISS'09) 18th of April 2009, Chengdu, P.R. China
- A series of Workshops on eSignatures has been given to the European Civil Servants in the framework of IT trainings provided by DG DIGIT (2008-2009)
- *"Cross-border eContracting: using e-Signatures in an interoperable and cross-border way"*, eSignature Common Technology Training organised by the China Center of Information Industry Development (CCID) and the EU-CHINA Information Society Project, 15th of April 2009
- *"Standardisation aspects of e-Signatures: rationalized framework"*, eSignature Common Technology Training organised by the China Center of Information Industry Development (CCID) and the EU-CHINA Information Society Project, 16th of April 2009
- Several interventions in the Signature Common Technology Training organised by the China Center of Information Industry Development (CCID) and the EU-CHINA Information Society Project, March 2009
- *"Practical and legal aspects of electronic signatures"*, conference held together with BSSLAW and LuxTrust s.a, at the Luxembourg Chamber of Commerce, 27th of November 2008
- L-SEC eID Congress: *"Gaining the benefit of eID from correctly implemented applications"*, 28 February 2008, Leuven, Belgium.
- See www.sealed.be/events.htm for older presentations and speeches.

Publications (latest)

Author and co-author of numerous Certificate Policies and Certification Practices Statements for numerous administrations or corporate clients

[DIS08] O. Delos *et al* (DIS Group). Best Practice for Applications using the electronic Identity Card (eID). SEALED (Editor), February 2008.

[LD05] S. Lacroix and O. Delos. How to dematerialize tendering to RFPs and tenders opening Processes? In S. Paulus, N. Pohlmann, H. Reimer (Editors): Securing Electronic Business Processes, Vieweg (2005), 242-25

Reports (latest)

Author and co-author of the here above mentioned studies deliverables, in particular the next studies published on the European Commission websites:

- European Commission Study on Standardisation Aspects of electronic Signatures

- Cross-border Interoperability of eSignature (Crobies)
- European Commission Study on User identification and authentication methods in e-payments

Consensus building

- As a partner of SEALED, Olivier was a key person in the building of the technical specifications and annex of Commission Decision 2009/767/EC of 16 October 2009. This clearly shows his ability to build consensus, as it required the agreement of the 27 Member States.
- By the nature of his Director of E-Trust function within Certipost, Olivier acquired and proved his strong capacity in building consensus.
- Olivier took part to specific standardisation works related to the information and cyber-security topics.
- Active participation in various standardisation bodies dedicated to e-security, e-signature standardisation in particular (EESSI, ETSI, DAVIC).
- Participation in the ETSI ESI meetings in order to liaise with the CROBIES study.

Sylvie Lacroix (SEALED)

Speeches (latest)

- *"Towards a more comprehensive framework for eSignatures and ancillary certification services"*, European Forum on eSignature, Miedzyzdroje, Poland, 10th of June 2010
- The CROBIES Study: *"Towards a more comprehensive framework for eSignatures and ancillary certification services"*, The European eID interoperability conference (EEMA), 16th of March 2010,
- A series of Workshops on eSignatures has been given to the European Civil Servants in the framework of IT trainings provided by DG DIGIT (2008-2009)
- Pannelist in session titled "Long Term Validation of Electronic Signatures in the European Legal Context", RSA Europe Conference, 21st of October 2009
- "The European eID Cards: trends and lessons learned", eSignature Application Training organised by the China Center of Information Industry Development (CCID) and the EU-CHINA Information Society Project, 16th of April 2009
- Pannelist in session titled "The legal challenges of cross border personal privacy & data protection" at the EEMA European eID Interoperability Conference, 17th of March 2009
- "Practical and legal aspects of electronic signatures", conference held together with BSSLAW and LuxTrust s.a, at the Luxembourg Chamber of Commerce, 27th of November 2008
- See www.sealed.be/events.htm for older presentations and speeches.

Publications (latest)

- Author and co-author of numerous Certificate Policies and Certification Practices Statements for numerous administrations or corporate clients
- [DIS08] S. Lacroix *et al* (DIS Group). Best Practice for Applications using the electronic Identity Card (eID). SEALED (Editor), February 2008.
- [LD05] S. Lacroix and O. Delos. How to dematerialize tendering to RFPs and tenders opening Processes? In S. Paulus, N. Pohlmann, H. Reimer (Editors): Securing Electronic Business Processes, Vieweg (2005), 242-25

Reports (latest)

Author and co-author of the here above mentioned studies deliverables, in particular the next studies published on the European Commission websites:

- European Commission Study on Standardisation Aspects of electronic Signatures
- Cross-border Interoperability of eSignature (CROBIES)
- European Commission Study on User identification and authentication methods in e-payments

Consensus building

- By the nature of her Project Manager, and then Manager of a Project Managers Team, functions, Sylvie acquired and proved her strong capacity in building consensus.

- Sylvie took part to specific standardisation works related to the information and cyber-security topics.
- Active participation in various standardisation bodies dedicated to e-security, e-signature standardisation in particular (EESSI, ETSI, DAVIC).
- Participation in the ETSI ESI meetings in order to liaise with the CROBIES study.

Marc Sel (PricewaterhouseCoopers)

Speeches

- *"Oracle Database - Security, Audit & Control Features"*, jointly with Sanjay Vaid, ISACA Belgian Chapter Round Table hosted by Oracle Belgium (June 15, 2010)
- *"NeIDs and STORK"*, European Identity Conference 2010 in Munich, Germany (May 4-7, 2010)
- *"Security architectures and design"* – jointly with Erika Vranckx, lecturer in the Solvay Business School's program for Executive Program in ICT Audit and Security (May 10, 2010, Brussels, Belgium)
- *"eHealth Round Table"*, Round Table chairman at PwC - Aprico Consulting - Bholdcompany joint event (March 10, 2010, Brussels)
- *"Next Generation Privacy Enhancing Technologies (PETs)"*, Brighttalk webcast (April 9, 2010, CET 14:00)
- *"Dataloss prevention and implementation"*, Brighttalk webcast (February 11, 2010, GMT 9:00am)
- *"Demistifying SAP security"*, EEMA/ISSE 2009 (October 6..8, 2009, The Hague, The Netherlands), here's the agenda, and you can watch me, on YouTube
- *"The multi application transit/financial payments card"*, at Cards Middle East (May 17-20, 2009, Dubai)
- *"Identity as a Service: identity services als een fundament voor de toekomstige generatie van applicaties."* – jointly with Stefaan Seys - SAI (May 12, 2009, Brussels, Belgium)
- *"Security architectures and design"* – jointly with Erika Vranckx, lecturer in the Solvay Business School's program for Executive Program in ICT Audit and Security (May 11, 2009, Brussels, Belgium)
- *"Security architecture - case studies and a generic model"*, at aEA's Belgian Chapter Architecture Café (March 26, 2009, Gent), organised by Loqutus
- *"Future challenges"* at the European eID card conference and the second STORK industry workgroup (March 17-18, 2009, Brussels)
- *"ICT authorisaties voor de Ziekenhuissector"*, Round Table chairman at PwC-Bholdcompany joint event (March 9, 2009, Antwerp)
- *"The evolution of Global Security Solutions"*, at the joint Fall Meeting of the ASIS Benelux Chapter & ISACA NL (November 21, 2008, Oud-Turnhout, Belgium)
- *"Security of Mass Transport Systems"*, jointly with Stefaan Seys - EEMA/ISSE 2008 (October 7..9, 2008, Madrid, Spain), agenda
- *"Integrated Controls - a case study of a Financial Services organisation"*, as main speech for the round table executive dinner on Risk Management organised by Colt Telecom in Hotel 't Sant (September 25, 2008, Antwerp, Belgium)
- *"IAM - Lessons learnt from various case studies"* - EEMA European e-Identity Conference (June 11, 2008, Den Haag, the Netherlands)
- *"Security architectures and models"* - lecturer in the Solvay Business School's program for Executive Master in ICT Audit and Security (April 29, 2008, Brussels, Belgium)

- *"Identity as a Service: identity services als een fundament voor de toekomstige generatie van applicaties"* – SAI CIO-summit (April 22-23, 2008, Lanaken, Belgium)
- *"Implementing and reviewing PKI"* - UAMS - Master in Computer Auditing (April 25, 2008, Antwerp, Belgium)
- *"Identity as a Service: identity services als een fundament voor de toekomstige generatie van applicaties."* - K.U.-Leuven/SAI avondsymposium (January 31, 2008, Brussels, Belgium)

Publications

- 2009 - Demistifying SAP security- for the ISSE2009 conference (published in the conference proceedings, ISBN 978-3-8348-0958-2)
- 2009 - De groeiende erkenning van IT security tools en processen published by Datanews in their 'IT storage & security guide' of March 13, 2009
- 2008 - The growing accreditation of IT security tools and processes (co-author with Vincent Villers, published by Business Review in Luxembourg)
- 2008 - Security of Mass Transport Systems- for the ISSE2008 conference (published in the conference proceedings, ISBN 978-3-8348-0660-4)
- 2007 - The business perspective on roles - for the ISSE2007 conference (published in the conference proceedings, ISBN 978-3-8348-0346-7)
- 2006 - Identity and Compliance - case study for PwC/Eurekify Webinar of 2006-11-07 on a European 25.000 employees company (unification and control libraries)
- 2006 - Identity and Access control - demonstrating compliance - for the ISSE2006 conference (published in the conference proceedings, ISBN-13 978-3-8348-0213-2)
- 2004 - Invited article on Corporate Governance for ISACA (published in the ISACA Journal)
- 2003 - Secure Financial Reporting through XBRL and Electronic Signatures - for the ISSE2003 conference (published in the conference proceedings, ISBN-3-528-05887-0)
- 2003 - Identity Management - published in CxO Magazine, december/january 2003
- 2003 - On Identity Management for the KU-Leuven ESAT-COSIC Summerschool
- 2003 - On BELPIC (the Belgian Electronic ID card)
- 2003 - BELPIC presentation at the Heizel government event (available on the CD of the Ministry of Interior Affairs)
- 2003 - The Belgian Electronic ID card (published in CXO magazine)
- 2002 - My thesis on 'Generic Security Architecture' for RHUL that won the David Lindsay award for best security thesis of the year
- 2002 - A presentation on the above thesis
- 2001 - Electronic Signatures - Position Paper
- 2001 - Electronic Signatures - Short Summary (published in the CCE Journal)
- 2001 - IT Governance article (co-author with Eddy Schuermans, Eric Guldentops et al, published by ISACA)

- 2001 - 'ChemResult en beTRUSTed: een veilige on-line markt voor chemische producten' (met Ingvar Van Droogenbroeck) - published in eBusiness Magazine, februari 2001 (today CXO magazine)
- 1999 - Java & Cryptography (published in the CCE Journal, Issue 2)

Reports

- Contributions to 'Baseline Controls - Microcomputers attached to a network' (ISF, 1990)
- Contributions to 'Baseline Controls - Local Area Network' (ISF, 1994)

Frederic Van Hoorebeke (PricewaterhouseCoopers)

Consensus building

- A new future for waste in Flanders – Frederic advised the province of Flemish Brabant on the new organisational model for the waste sector in Flanders. An important part of this project was to reach consensus between more than 35 stakeholders before implementing.
- PVCYCLE – Frederic assisted the management of PVCYCLE on a guarantee system for its members, reaching consensus between the literally dozens of producers all over Europe.

Annex XII.

Example input for D0.1 (Inception Report)

Non exhaustive inputs on findings, recommendations, major third parties initiatives, and available legislations to use as input material for an IAS for Deliverable D0.1

Overview: why we already want to provide example input

The Inception report (D0.1) should be provided two weeks after the start of the project, yet should include the detailed list of initiatives and legislations to be analysed during Task 2. We have therefore already performed a first high-level screening of valuable findings and recommendations to use as input material for an IAS framework. These findings and recommendations were found in past and on-going undertakings supported by the European Commission, in major third parties initiatives, as well as in legislation.

In addition, we will consider any supplementary input information provided by the Commission, and will liaise with the eID Compass initiative in order to further sustain evidence made policy making, based on scientific experiences.

The list proposed below aims to point key elements that are **already mastered by the team**.

Some of them being cornerstones for an IAS framework, we are convinced that the deep knowledge of these elements before starting the mission will provide an **unmatched time-to-market to the European Commission**.

Studies

Reference	Degree of mastering
Study on the standardisation aspects of eSignatures (DG INFSO)	Study performed by SEALED and DLA Piper
Study of use identification methods in card payments, mobile payments and e-payments (DG MARKT)	Co-authored by SEALED
Study on the set-up of an Electronic Signature Service Infrastructure for the European Commission (DIGIT)	Study performed by SEALED
Cross-border interoperability of eSignature: Study and concrete outputs on Trusted List (lead the Member States test bed and major contribution the technical specifications and annex of Commission Decision 2009/767/EC of 16 October 2009 setting out measures facilitating the use of procedures by electronic means through the 'points of single contact') (see also below).	Study performed by SEALED and Time.lex
The European Framework for signature Validation Services (EFVS).	Study performed by Time.lex and SEALED
Study on eID Interoperability for pan-European government services	Study performed by Time.lex
EU Study on the specific policy needs for ICT standardisation	Study performed by DLA Piper

Directives, national laws and regulations in Member States (incl. preparatory initiatives)

Reference	Degree of mastering
Directive 1999/93/EC of the European Parliament and the Council of 13.12.1999 on a *Community framework for electronic*	Very well-known by all team members

signatures and Commission Decision 2003/511/EC of 14.7.2003 *on the publication of reference numbers of generally recognised standards for electronic signature products*	
Commission Decision 2009/767/CE of 16.12.09 setting out measures facilitating the use of procedures by electronic means through the 'points of single contact' under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market. (cc Directive 2006/123/EC of the European Parliament and Council of 12.12.06 on services in the internal market, OJ L376 of 27.12.06)	Significant contributions from SEALED and Time.lex
Belgian bill on trusted third parties (pending)	Prepared by DLA Piper
e-Seals § **AT**: E-Government Act, Article 19 (exact reference to be added) § **EE**: Concept of Company Digital Stamps associated with a signed Company Stamping Policy. The digital stamp is in the law on digital signatures (para 2) https://www.riigiteataja.ee/ert/act.jsp?id=13116484 (in EE OJ) and see the EN translation (of 2008) at http://www.legaltext.ee/et/andmebaas/tekst.asp?loc=text&dok=X30081K5&keel=en&pg=1&ptyyp=RT&tyyp=X&query=digitaalallkirja § **ES, IT, LV**: Existing § **PL**: Legal value of printouts from Pledge Register and Companies Register	Most of these laws were analysed in the context of IDABC studies conducted by Core Team members
Time-stamping / time-Marking: § **BE**: in preparation (bill on trusted third parties; the current Act on TTP also includes timestamping, but is defunct) § **CZ**: Section 2 of the National Act on Electronic Signatures (*http://www.mvcr.cz/micr/scripts/detail.php_id_1542.html*). § **FR:** http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005630796&dateTexte=vig § **DE**: www.bundesnetzagentur.de/cae/servlet/contentblob/11754/publicationFile/6307/FrameworkforElectronicSignaId1850pdf.pdf § **EL:** Project in progress**HU**: Act on Electronic Signatures No 35 of 2001	Most of these laws were analysed in the context of IDABC studies conducted by Core Team members

http://www.nhh.hu/dokumentum.php?cid=11962&letolt § **IT, LV, LT, PT, RO, SK, SI, ES**: Existing § **EE**: The Digital Signature Act provides the necessary conditions for using digital signatures and the procedure for exercising supervision over the provision of certification services and time-stamping services. § **PL**: Article 7 from the national law on e-signatures (http://isap.sejm.gov.pl/DetailsServlet?id=WDU20011301450). Legal effect for time marks when provided by "Qualified Service provider" and concept of "no later than" effect.	
e-Archiving: § **AT, EE, FI, FR, DE, IT, SK**: Existing § **BE**: in preparation § **HU**: Act on Electronic Signatures No 35 of 2001 and Ministerial Decree of the Minister of Economy and Transport No 117 of 2007 for archiving service providers	Most of these laws were analysed in the context of IDABC studies conducted by Core Team members
e-Registered Mail / e-Delivery: § **BE**: in preparation (no official reference yet) § **EE, IT, SK:** Existing	Most of these laws were analysed in the context of IDABC studies conducted by Core Team members
e-Identity (eID in national law exists either 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. Only Austria and Finland have specific laws on the subject): § **AT:** Existing § **FI**: Existing Through e-identification and as part of other laws : § BE: Identity is governed by Law on National Register and numerous royal decrees http://eid.belgium.be/fr/Informations_legales_et_techniques/Textes_de_loi/index.jsp § **EE**: The Identity Document Act and the Digital Signature Act are governing eIdentification § **ES, DE, IT, LV, NL, PT, RO**: Existing	Most of these laws were analysed in the context of IDABC studies conducted by Core Team members

The "new approach" 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).	Very well-known by all legal team members

Standardisation and federated initiatives that may demonstrate that some legal provisions can indeed be implemented

Reference	Degree of mastering
European Citizen Cards: § CWA 15264 (eAuthentication) § CWA 14890 (eSign) § CEN/TS 15480 suite (European Citizen Card)	Well-known by SEALED (used in customer projects)
ICAO international specifications for Passports and Travel Documents	100%, SEALED (used in customer projects)
EMV initiative (promoted by Visa and MasterCard)	Well-known by SEALED (used in customer projects)
Standard referred to in Commission Decision 2003/511/EC of 14.7.2003 *on the publication of reference numbers of generally recognised standards for electronic signature products*	100%, SEALED and other Core Team Members
All **ETSI ESI standards** and **CEN standards** on eSignature and ancillary services and the rationalisation framework induced by the European Commission Mandate M460 of 22.12.2009, *Standardisation mandate to the European standardisation organisations CEN, CENELEC and ETSI in the field of information and communication technologies applied to electronic signatures* (http://ec.europa.eu/information_society/policy/esignature/eu_legislation/standardisation	Well-known by SEALED and other Core Team Members

Other initiatives

Reference	Degree of mastering
STORK	Well mastered by PwC (Core Team) and Marc Stern (Field Experts Team)
PEPPOL	Many WPs well mastered by SEALED (liaison PEPPOL – CROBIES)
SPOCS	Liaison started during former studies by Core Team Members.

PORVOO reports, in particular Thomas Myhr analysis endorsed by the Porvoo Group : *"Regulating a European eID: A preliminary study on regulatory framework for entity authentication and a pan European Electronic ID, for the Porvoo e-ID Group"*, Thomas Myhr, 31.1.2005, available at porvoo9.gov.si/Thomas_Myhr_report.pdf	Well mastered by Field Expert Team member (Teemu Rissanen)
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 28.11.2008	Well-known by SEALED and other Core Team Members
Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions *A Digital Agenda for Europe – A policy for growth and innovation in the digital society*, COM(2010)245of 19.5.2010.	Well-known by Core Team Members
"Electronic signature in Law", Stephen Manson, Tottel publishing, 2007 for an exhaustive analysis of the meanings of a signature.	Well-known by legal Core Team Members
Liberty Alliance	Well-known by PWC and other Core Team Members
Kantara initiative	Well-known by PWC, SEALED and other Core Team Members
Primelife	Well-known by Timelex
Research and Innovation for Security, Privacy and Trustworthiness in the Information Society	Well-known by DLA Piper and other Core Team Members
White Paper "*Modernising ICT Standardisation in the EU - The Way Forward*" of 3.7.2009, COM(2009)324	Well-known by DLA Piper and other Core Team Members