

**European Large Scale bridging Action
(ELSA):
Electronic Identity Management
Infrastructure for trust worthy services**

FULL TABLE OF CONTENTS

EXECUTIVE SUMMARY	5
1 NEEDS AND OBJECTIVES.....	6
1.1 SOCIETAL NEEDS & CHALLENGES	6
1.1.1 <i>Setting the scene – the role of eID in the Information Society</i>	6
1.1.2 <i>Limitations</i>	6
1.1.3 <i>Ubiquity of eID</i>	7
1.1.4 <i>Long-term eID vision</i>	7
1.1.5 <i>User-centric needs</i>	7
1.2 THE FIRST KEY MID-TERM TARGET	9
1.3 FOCUSED OBJECTIVES	9
1.3.1 <i>A review of the issues</i>	9
1.3.1.1 What is electronic identity and who it is for?	9
1.3.1.2 Who is involved in the management of identity?.....	9
1.3.1.3 Management of relationships: how do identities relate?	10
1.3.1.4 Reliability of identity: how can your identity be trusted?	10
1.3.1.5 Seamless identity: using identity in an application.....	10
1.3.1.6 Clear legal framework: regulating the use and management of identity	10
1.3.1.7 Private & secure identity: integrating users’ rights w/ the infrastructure.....	10
1.3.1.8 Decreasing the risk of crime through technology.....	10
1.3.1.9 Clear Business Model.....	10
1.3.1.10 Future-Proofing	11
1.3.1.11 An electronic single market	11
1.3.1.12 Interoperability with the rest of the world: A global view.....	11
1.3.1.13 Leveraging the results of efforts already underway	11
1.3.1.14 Electronic Documents (eDoc) and eSignature	11
1.3.1.15 Additional requirements.....	12
1.3.2 <i>Preliminary list of Objectives</i>	12
2 ROADMAP FOR ACHIEVING THE OBJECTIVES.....	13
2.1 LINES OF ACTION	13
2.2 MECHANISMS FOR IMPLEMENTATION	13
2.2.1 <i>Introduction</i>	13
2.2.2 <i>eID Observatory</i>	13
2.2.3 <i>Large scale pilots</i>	13
2.2.4 <i>Public-private Partnerships</i>	14
2.2.5 <i>Pre-commercial Procurement</i>	14
2.2.6 <i>Lead Market Initiative for eID</i>	14
2.2.7 <i>Study, Research & Development on a number of topics</i>	14
2.2.8 <i>Lessons learned from the past, on instruments</i>	16
2.3 SIGNPOSTS TO EIDM INFRASTRUCTURE	17
3 BARRIERS	18
4 OVERCOMING THE BARRIERS.....	20
4.1 STAKEHOLDER INVOLVEMENT	20
4.2 ARCHITECTURE AND MODEL	20
4.2.1 <i>The Requirements for European electronic identity infrastructure</i>	20
4.2.2 <i>A Meta-Model of Identity</i>	21
4.2.3 <i>Multiple Identity Service Providers (IdSP’s)</i>	22
4.3 A LONG TERM SUPPORTIVE PROCESS	25
4.3.1 <i>Maintaining the long term vision</i>	25
4.3.2 <i>Leveraging experience and knowledge from the private sector</i>	25
4.3.3 <i>Government officials in the forefront</i>	25

4.3.4	<i>Fostering/Supporting the eID community</i>	25
4.3.5	<i>Communications Policy</i>	25
4.4	EU-LEVEL LEADERSHIP AND GUIDANCE.....	25
4.4.1	<i>Standardisation</i>	26
4.4.2	<i>An ethics-monitoring body</i>	26
5	MEASURING THE IMPACT	27
5.1	GENERAL IMPACTS.....	27
5.1.1	<i>Leading by example</i>	27
5.1.2	<i>Industrial and Technological leadership</i>	27
5.1.3	<i>Growth of new markets and businesses</i>	27
5.1.4	<i>Attracting investment</i>	27
5.2	ENVIRONMENT	28
5.2.1	<i>The Internet of Things</i>	28
5.2.2	<i>Health and well-being</i>	28
5.2.3	<i>Energy Consumption</i>	28
5.3	EQUITABLE BUSINESS AND EMPLOYMENT OPPORTUNITIES	28
5.3.1	<i>Local, regional and territorial business competitiveness</i>	29
5.4	DEMOGRAPHY	29
5.5	ADEQUATE SERVICES AND INFRASTRUCTURE	29
5.6	CHANGES IN LIFESTYLE	30
5.7	MOBILITY	30
5.8	RETAIL MARKET IMPACTS.....	30
5.9	EMPLOYMENT AND INCOME.....	30
5.10	PUBLIC SERVICES.....	30
5.11	QUALITY OF LIFE	31
5.11.1	<i>Privacy</i>	31
5.11.2	<i>Ambient Intelligence</i>	31
6	MONITORING AND EVALUATION	33
6.1	PURPOSE	33
6.2	METRICS	33
6.3	MONITORING SYSTEM	33
6.4	MONITORING STUDIES/EVALUATIONS	33
6.5	CASE STUDIES	33
7	APPENDIX	34
7.1	TERMS AND ABBREVIATIONS	34
7.2	OVERVIEW OF WORK TO BE DONE.....	36
7.3	IMPACT ANALYSIS BY EU POLICY AREA.....	37
7.3.1	<i>Agriculture and Rural Development</i>	37
7.3.2	<i>Competition</i>	37
7.3.3	<i>Economic and Financial Affairs</i>	37
7.3.4	<i>Education and Culture</i>	37
7.3.5	<i>Employment, Social Affairs and Equal Opportunities</i>	37
7.3.6	<i>Enterprise and Industry</i>	37
7.3.7	<i>Environment</i>	37
7.3.8	<i>Fisheries and Maritime Affairs</i>	38
7.3.9	<i>Health and Consumer Protection</i>	38
7.3.10	<i>Internal Market and Services</i>	38
7.3.11	<i>Justice, Freedom and Security</i>	38
7.3.12	<i>Regional Policy</i>	38
7.3.13	<i>Research</i>	38
7.3.14	<i>Transport and Energy</i>	38
7.3.15	<i>Taxation and Customs</i>	39
7.3.16	<i>Information Society and Media</i>	39
7.4	SERVICE-ORIENTED ARCHITECTURAL MODEL FOR IDENTITY MANAGEMENT	40

ELSA Thematic Working Group on Electronic Identity Infrastructure

7.5	CEN TC224 : THE "EUROPEAN CITIZEN CARD" (ECC).....	41
7.6	REPORT FROM THE ELSA THEMATIC WORKING GROUP ON ELECTRONIC IDENTITY MANAGEMENT 26 MARCH 2009.....	43
7.7	LAST MEETING OF THE ELSA THEMATIC WORKING GROUP ON ELECTRONIC IDENTITY MANAGEMENT.....	54
7.8	STAKEHOLDER INPUTS	55-125

EXECUTIVE SUMMARY

The purpose of this document is to present the work of the Thematic Working Group on Electronic Identity Management Infrastructures, and to provide the necessary background for the European Large Scale bridging Action for eID.

The ubiquitous deployment of electronic identities as envisioned here will be an agent of societal transformation, and is the key to all the benefits to be enjoyed in the new landscape.

An ubiquitous eID infrastructure¹ for the information society, will offer a wide range of functionalities, including the provision of multiple identity instances, from government-approved to commercially accepted, and ranging from near- or quasi-anonymity to strong and unambiguous identification. Furthermore, the system will be user-controlled and privacy-protective, providing the basis for accountability and innovative applications in an open and competitive market.

It will be user centric, in that by design it is the user - and not some authority or private entity - that maintains control over how a user's identity attributes are created, and the degree to which the user's identity attributes can be revealed to service providers.

It will enable eID-enabled entities to interact in new ways, including with a trustworthy, intelligent environment, spawning new businesses, markets, business models, etc.

Transactions will be conducted in an environment of trust and security, which means that many more remote transactions of different types will be possible. Most current ones such as e-payments will be greatly simplified.

To achieve the ambitious targets, a common long-term vision must be developed, collectively. A process to establish and periodically update this vision and the supporting infrastructure with changing circumstances must be established. This will require the active involvement of an especially broad spectrum of stakeholders, including member states' public administrations, providers of IT services and products, industry, end-user fora, NGO's, and others.

The paper presents a specific first mid-term target: By 2015, all electronic identification processes offered in the EU either publicly or privately, locally or cross-border, and between administrations or businesses or citizens should be secure, and rely on authenticated identities, when either *needed* or *desired by one or both parties*, and respecting the privacy protection regulations, ensuring all legal customer safeguards and mutually recognized at the appropriate level by all MS in the EU.

Achieving this ambitious target requires the achievement of a number of focused objectives, including establishing a meta-model for electronic identity, extensive legal and policy changes to support the new model, communication and other activities aimed at businesses and the public to increase awareness and uptake, along with technological advances in essential eID-related technologies.

The road to this future as envisioned is however strewn with many barriers of various types: Technological, Societal, Economic, Legal, Political, Conceptual, and Organisational. Concerted action over several years will be needed to overcome these barriers, including establishment of a detailed roadmap followed by the extensive, planned coordination of the activities, deployment of supporting implementation mechanisms of various types (including Lead Market Initiative, Pre-Commercial Procurement, Research & Development activities, etc.), and the establishment of a proper monitoring regime. A governance framework must also be eventually put in place to cover the operation, maintenance, evolution, and monitoring of the resulting eID "ecosystem."

The impact on society and business is expected to be very broad, bringing all sorts of benefits to Administrations (improved trustworthiness of communications, streamlining of activities, etc.), Businesses (new customers, new business opportunities, etc.) and Citizens (simplifications, cost savings, improved quality of life, privacy/safety/trust enhancements, etc.), but along with some possible areas of concern where extra care and vigilance/further study may be warranted to correctly judge the full societal impact.

¹ A conceptual construct representing the set of different infrastructures that are required to support the provision of the eIDM-related services considered in the scope of the ELSA program; see annex, section 7.1 for full definition

1 Needs and objectives

1.1 Societal Needs & Challenges

1.1.1 Setting the scene – the role of eID in the Information Society

By 2020 we envision that some 450 million EU citizens will be regular users of eID's, in a world of unlimited bandwidth, pervasive connectivity, ambient intelligence and electronically enhanced social networking. eID's will be the key that 'opens doors' to most services for citizens and businesses. The ability to identify who you are, anytime and anywhere, and authorising or authenticating becomes so simple and safe that citizens & businesses will use their eID's as part and parcel of their lives.

Secure online identity management and reliable authentication will be the foundations of a networked economy of the future, creating enormous potential for high quality, efficient and effective services. Appropriate architectures and legal measures will ensure privacy protection, and no-one without authorisation will be able to access or otherwise use somebody else's personal data. Every citizen will be in control of his/her data. Society at large will benefit from new forms of social networking and interaction, made possible by the safety and trust afforded by the transparent use of secure eID's.

eID is a key enabler of and catalyst for these transformations, bringing welcome changes, benefits and improvements, many inconceivable under current circumstances. It won't eliminate anonymity or any other freedoms that citizens & businesses currently enjoy, but will optimize and enable automation of the familiar.

A growing majority of the 450 million Europeans of 2020, both adult decision makers and their teenage children, will be 'digital natives'. To them, the internet will be as familiar as the television is to us; the shopping mall will seamlessly extend into their homes, and a significant proportion of socialising will be conducted electronically as compared with today, with geographic location being of sharply reduced relevance. Computerised exchanges will be the norm, and paper traces of transactions will be the rare exception, if they occur at all.

Increased reliance on strong user identities and related attributes will be transformative, resulting in paradigm shifts that will render the landscape of interactions between citizens, businesses and administrations nearly unrecognizable in today's terms. Society come to depend on new forms of social networking and interaction, their potential being unleashed by the safety and trust afforded by transparent use of strong identities, as well as the ability of citizens and businesses to selectively reveal only certain information about themselves to others.

The development of "Ambient Intelligence" promises an information society where many objects in everyday use will act as intelligent agents, in order to automate / facilitate many common tasks, and where services can be embedded in "intelligent" objects pervasively populating the environment surrounding the citizenry, directly assisting them or otherwise supporting their daily activities.

1.1.2 Limitations

Today, most web resources (blogs, social networks, exchange platforms, games...) only offer their full set of features to authenticated users and it is expected that to deliver a unique experience they will increasingly adapt their interactions based on user characteristics. Whereas ever more user related information is accumulated, privacy is only protected by vague policies, the level of security is dubious and it is expected that this situation will worsen, due to the increasing amount of citizens on the Internet, the launch of new services and the lack of control.

The citizens for their part do not currently enjoy the possibility to benefit from knowing in many instances exactly who they are dealing with in remote transactions. A leading example of this is spam.

The typical email user is inundated with spam, and does not have the possibility of automatically rejecting email messages from users that do not meet identification criteria of their own choosing.

Similarly, many eGovernment initiatives have only recently been launched aiming for broad adoption, whereas privacy protection and the digital divide are today underestimated threats. From a functional standpoint, the multiplicity of the identification and authentication mechanisms and the lack of common paradigms slow down the adoption of those new approaches: citizens already know how to use cards in their wallet to purchase things, to show membership or to enable relationships; they are used to managing their personal data in one place and to grant access when needed; they are keen to prove some of their attributes without revealing unnecessary details. It is however not so easy to do so online and the electronic equivalent of their national ID or travel documents do not presently provide them with significant added value for eServices.

Furthermore, the civil, private, and business spheres are increasingly interconnected, which leads to problems due to limitations in the currently fragmented identity schemes. As an example, consider the case where a citizen wishes to access a discussion forum based on his age, using as proof his National ID. The challenge for him is to do so while also maintaining a personal profile where he is able to limit access to other personal data linked to his National ID.

1.1.3 Ubiquity of eID

The envisioned common European eIDM framework for the information society and a digital economy will encompass a vastly increased number of connected entities, of many types, animate and inanimate, used in all (or most) transactions, providing high trustworthiness, seamlessness and extreme ease of use.

This aspect of eID as a vastly expanded and omnipresent central component we term “ubiquitous deployment” (UDeID).

Achieving this degree of uptake is a significant challenge. The partners most likely to accelerate uptake of eID will be those experienced services providers who have over a period of years confronted the difficult stumbling blocks and found solutions sufficient to enable them to acquire critical masses of customer loyalty.

1.1.4 Long-term eID vision

Ubiquitous eID for the information society involves the EU-wide availability of a multi-faceted trustworthy electronic identity management infrastructure to all citizens, throughout all domains, providing multiple identity instances, from government-approved to commercially accepted, and ranging from near-anonymity to strong and unambiguous identification. This should start from a user-controlled and privacy-protective perspective and provide the basis for accountability and innovative applications in an open and competitive market.

Electronic identities encompasses far more than what is currently supported through national IDs or passports, or than the multiple and fragmented identities that we are using on the Internet, including through social networks. In the envisioned new approach, electronic identities take multiple forms and enable new ways to interact while following fundamental principles such as the so-called “laws of identity” designed to preserve the interests of all stakeholders involved.

Ubiquitous deployment of electronic identities will be built on a vast, painstakingly built web of trust and will tremendously facilitate the automation of most key business processes (B2B, B2C, A2C, C2C), in addition to serving as a crucial building block for the uptake of trustworthy electronic documents and forms. It would open the doors to a whole spectrum/plethora of new applications and uses by empowering citizens, businesses and administrations alike.

1.1.5 User-centric needs

User-centricity distinguishes itself from other models of identity management by emphasizing that the user (not some public authority or private entity) maintains control over how his identity attributes are created and how they are revealed. Citizen-centric eID puts in place the model and supporting

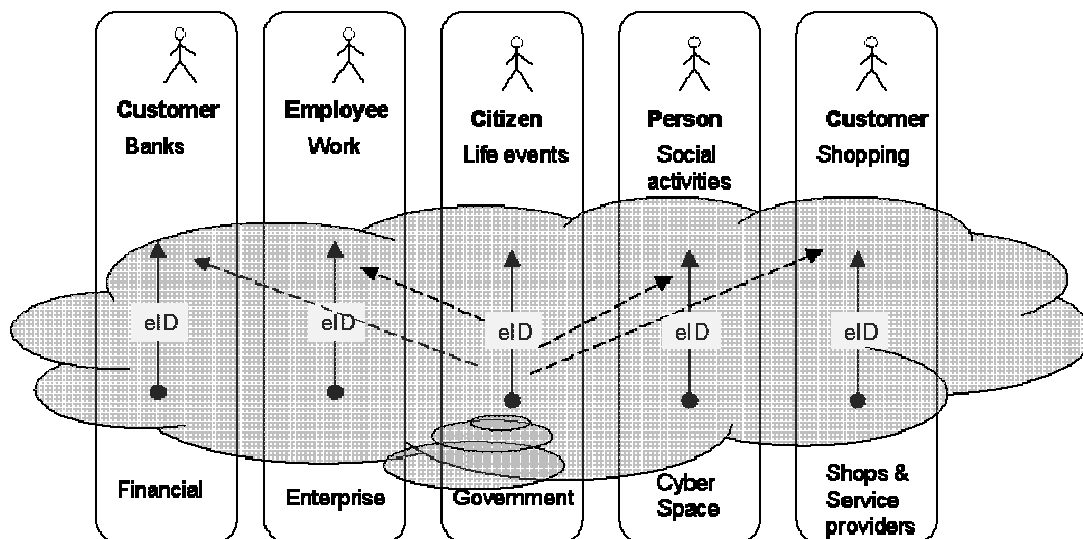
infrastructure that reflects users' needs, empowering them to effectively and efficiently manage and control the use of their electronic identity, particularly identity attributes disclosure. Users will have access to simple, understandable means of revealing only what they desire to, and no more.

There are many real-life examples where anonymous identity is relevant, e.g., where only a certain status (e.g. adult, resident of a country) or a relationship is relevant, such as mother-child, or car-owner. The envisioned eID approach must be able, under the relevant and appropriate circumstances, to merely provide needed attributes related to subjects without naming those subjects.

The use of eID allows for the service delivery tailored to the specific needs of a person. However, the information traces left behind when using the net makes it possible for malevolent persons and others with the expertise to build a detailed picture of a citizen's transactions, movements, and relationships. Two basic rules govern how people can better protect themselves online, according to PRIME². First, a *separation of contexts* so that observers cannot easily join data related to different activities. The second is data minimisation: only those attributes *necessary for a given transaction* are revealed.

Furthermore, it is a key for citizens to participate, be heard and accounted for in this new society. eID is a facilitating technology that allows for electronic interaction with banking systems, social websites, enterprise applications and government applications. In most case this interaction supposes the use electronic identification means specific for the application or the sector.

For remote transactions, private entities (e.g., banks, etc.) may require their users/customers use entity-issued eID's and associated access codes. This is generally done so that the entity in question can exercise risk management according to its own requirements, and so that they can clearly demarcate the responsibilities of their users/customers with respect to the entity-issued eID. Banks for example are quite comfortable after many decades of working with the issues related to identities issued to their users, including setting simple and clear rules ("report a lost or missing card within 24 hours") and the processes to deal with the eID lifecycle (issuing new cards, expiring old cards, replacing lost or stolen ones, etc.). In the workplace, access to IT systems is often local, employing logins based on username and password. Applications on the internet will also often ask users to register for a site-specific logon ID and password in order to obtain access.



User centrality also implies that users can choose an appropriate identity whenever possible. Today's citizens often already dispose of a set of "personal identities." Government-issued eID, enterprise IT system authentication, bank identification, and internet identity systems have evolved in parallel and in isolation. These systems are governed by diverse and in some cases divergent sets of rules and requirements. These separated Identity Management Islands have substantial interoperability issues outstanding. Consequently, unification of such systems into a coherent system raises questions of

² PRIME - Privacy and Identity Management for Europe

feasibility, as there may be mismatches of processes and assumptions to contend with. Users would nonetheless benefit greatly from their unification into a coherent system. We are in fact far from defining the different scenarios involved³, a prerequisite to allow for the evaluation of feasibility.

These identities are all complementary and overlapping to some degree, but as they are not interoperable and built according to different needs, they are normally not trusted across sectors or national borders.

While there are numerous examples of useful and natural cross-interaction between public and private service domains (e.g., the health sector), this is not generally possible. For example, internet oriented eID systems are in general not able to leverage government electronic ID cards/tokens, nor are government eID cards in the current format necessarily considered to be the right instrument to be used in all cases to access social networks or even simple web services.

A final area of particular concern for users will be the ease and safety of the revoke and renew processes (and other protection mechanisms) triggered in case of identity loss or theft, so that they do not have to unfairly contend with potentially catastrophic consequences.

1.2 The first key mid-term target

ELSA for electronic identity is a strategic program to achieve long-term objectives for eID in Europe. While the vision is long-term, these objectives need to be phased in over time. Furthermore, the program needs to take into account the different activities already underway, and their results. This entails the setting of some concrete shorter-term targets on the scale of 2015-2018.

By 2015, all electronic identity related processes offered in the EU either publicly or privately, locally or cross-border, and between administrations or businesses or citizens should be secure, and rely on authenticated identities *when either needed or desired by one or both parties*, and respecting the privacy protection regulations, ensuring all legal customer safeguards, and mutually recognized at the appropriate level by all MS in the EU.

1.3 Focused objectives

Achieving the ambitious goals laid out in the previous sections will require that we set a limited number of focused objectives that can be completed within the time frame under consideration. In order to set those objectives, it is necessary to first separate out and identify the different issues or questions that must be addressed.

1.3.1 A review of the issues

1.3.1.1 What is electronic identity and who it is for?

For the purposes of a European eIDM infrastructure, the scope and meaning of ‘identity’ needs to be clarified. Intuitively we tend to think of identity in terms of physical people. From an eGovernment and business perspective, legal entities are equally important, however. The exchange of electronic identity information is already complex, simply due to the lack of common semantics (e.g., even the fundamental notion of a “name” associated with a given electronic identity exposes cross-cultural differences sufficient enough to pose difficulties).

1.3.1.2 Who is involved in the management of identity?

Who creates eID’s, and how are these managed? It needs to be clear who registers and verifies attributes (if at all), and on what conditions these can be exchanged or re-used. Simply relying on market mechanisms to choose an economically optimal solution may not provide desirable results

³ A first step could be to define the set of mainstream application scenarios, which could include: public sector interactions, inter-enterprise interactions, web interactions, banks and credit-card interactions, insurance interactions, internet provider interactions, and health-sector interactions.

from data protection or other perspectives. Member States as well as other private entities in particular have invested considerable effort and cost into their respective national electronic ID solutions, and any final system would have to build on these (or at least be compatible with them), to ensure those investments were not lost.

1.3.1.3 Management of relationships: how do identities relate?

An identity model needs to be able to manage links between identities. Simple examples include linking parent A to child B, or linking manager C to company D. Mandate management and role management is the main example of this. Further study will be required before a workable model (on scope, relationships, mandates, delegation, etc.) can be established and practical tools made available to users of the system to verify and manage such links.

1.3.1.4 Reliability of identity: how can your identity be trusted?

The reliability of an identity, either in terms of being generally reputable (considered trustworthy) or in terms of real guarantees (accountability in case of problems) is an issue. From the end user's perspective, functionality (e.g., ease of use) can be more important than guarantees, as can be seen in the increasing importance of reputation based identification (e.g. in social networks). From the service provider's perspective, trustworthiness – especially in terms of accountability and liability – is much more important. The future eIDM infrastructure in Europe should be multi-level, i.e. permitting varying levels of security/reliability.

1.3.1.5 Seamless identity: using identity in an application

It is important to uncouple services (applications) from dependence on specific eID infrastructure. An 'invisible eID infrastructure' is key to creating an open eID model widely taken up in commercial and public sector applications. Application/Service independence of the eID infrastructure is critical.

1.3.1.6 Clear legal framework: regulating the use and management of identity

There are some relevant national legal barriers which impede certain approaches to the issuance and management of eID's; Guidance is necessary on what the consequences of European initiatives will be, and how to operate within the limits of applicable laws given the lack of direct European regulatory competence to harmonize eID regulations. The principle of minimum disclosure must be practiced and the amount of printed/stored data should be minimized. Questions of liability, and other obligations of parties involved in transactions where eID's are used must be clarified.

1.3.1.7 Private & secure identity: integrating users' rights w/ the infrastructure

Privacy and security are central concerns in the design and use of eID. These concerns should be addressed in a European eIDM infrastructure, early in the process; security and privacy protection cannot be tacked on as an afterthought. Partial identities are one of the key means by which users can actively protect their privacy, and they will play a key role in future electronic services as well as in public security. Respect for all applicable Data Protection regulations needs to be verifiably incorporated into any EU-wide eID infrastructure.

1.3.1.8 Decreasing the risk of crime through technology

The confidence of the public and of the business community in eID-based transactions must be earned, in tandem with comprehensive efforts at reducing the risk of fraud through technology. Fears about identity theft and other negative scenarios (including the appearance of new types of "cybercrimes") must be allayed through awareness raising, but also by the design of appropriate built-in security, and enforcement mechanisms and safeguards that are effective, durable, and transparent.

1.3.1.9 Clear Business Model

Who should pay for eID? What value does the eID model create that interests service providers and end users? There are two aspects to this: investments to participate, and transaction costs. Private

issuers often prefer their own solution which gives them full and exclusive control over the business model and their own tokens can act as an advertising medium (a “branding space”) in a way that generic eIDM would not be able to offer. For relying parties, the potential access to new customers must figure strongly in the calculation. A common idea is that they should pay the transaction costs.

1.3.1.10 Future-Proofing

Any measures taken at the European level need to be sufficiently flexible to take up newer approaches to identity management that might emerge or increase in popularity, e.g., new means of authentication, etc. This will require appropriate abstractions be considered in the model(s) eventually chosen for electronic identity.

1.3.1.11 An electronic single market

Financial transactions, including payment for goods and services will be drastically simplified and streamlined. Highly trusted transactions and their certification with eID’s will enable the appropriate linking of operations much more quickly and in total security: orders, invoices, credit, transfer of funds, etc. Interactions between citizens and legal entities with perfect remote identification and trusted transactions (together with archiving and conservation), will reduce operating costs substantially.

This could be envisioned as an extension or generalisation of the Single European Payments Area (SEPA) which is itself an extension of the trust chain combining a management mandate and collateral or underlying commercial transactions with the payment. Therefore, in commercial situations it would be unnecessary to have two systems of trusted digital identity, but only one, common to both financial and informational needs. Of course, this vision does not preclude other secure added-value networks which could provide services to guarantee the value of commercial and financial transactions for particular closed communities of interest.

1.3.1.12 Interoperability with the rest of the world: A global view

In order to fully leverage the advantages of this information society, European citizens and businesses will have relationships, both private and commercial not only locally, across Member States, but also globally. Therefore, interoperability criteria should take other initiatives around the world into account. Interoperability might be extended outside of the EU in cooperation with EU-external partners, including International standards bodies. The needs of non-EU citizens or visitors to a given Member State must also be taken into account.

1.3.1.13 Leveraging the results of efforts already underway

Some of these issues are already being addressed in STORK, PEPPOL and by private sector partners. There are also other activities (e.g., PRIME, PRIME-LIFE, research projects under FP6 & FP7, studies) which are relevant to eID, whose results should be taken into consideration by this ELSA. STORK has already developed a common specification for interoperable electronic identity for eGovernment services, which will be tested on number of pilots, including the SPOCS pilot for the Services Directive as well as the ePSOS pilot on patient records. These and other large scale pilots are driven by, and demonstrate the commitment of the Member States.

1.3.1.14 Electronic Documents (eDoc) and eSignature

The usage of electronic documents of various types is already widespread in current society, although their use in official contexts (e.g., eGovernment services) is still at a relatively early stage. Electronic signatures are already a reality, including legal support provided through an EU Directive. The relationship between eID and these 2 other closely linked initiatives is not fully appreciated or properly taken into account in the related respective efforts, which may result in a variety of difficulties, including conflicts (e.g., user-centricity vs. issuer-centricity perspectives), lack of interoperability or other incompatibilities, needless complexity, etc. A complete, conceptual-level

consensus regarding the relationship between these related initiatives is a prerequisite to the supporting eIDM infrastructure.

1.3.1.15 Additional requirements

It is likely that during the elaboration of the eID model some additional Domain and sector specific requirements and principles will be revealed. For example: government e-transactions, banking, e-commerce, digital consumption in the consumer sphere and intra/inter-company employee/agent aspects, including roles, responsibilities, and rights of parties may be sources of additional requirements. Universities could also be one of the most promising areas for pilot projects as the Bologna Process should support the mobility of students in the EU, which is currently not supported by an adequate identity management solution across the universities in the Member States.

1.3.2 Preliminary list of Objectives

Based on the discussion of the issues given in the preceding sections, the following (non-exhaustive) list of concrete objectives has been synthesized. Further reflection and refinement will be necessary.

1. The establishment of personal identity frameworks that allow citizens to be in control of their digital selves and their personal data, respecting data protection requirements, and that respects cultural differences.
2. Electronic identity should be usable, providing a consistent user experience, and available to all citizens
3. Citizen's national eID should work seamlessly across sectors and borders
4. Establish promotional actions to increase the understanding among the general public of eID benefits and risks
5. All legal persons and entities, including public administrations and public service providers (but also businesses) should be holders of electronic identities usable throughout the EU
6. The existence of a European architecture and model that covers the needs of citizens, business, administrations and nations, that encompasses different current approaches to eIDM, and that anticipates emerging approaches to eIDM to the greatest extent possible
7. An omnipresent eID infrastructure at European level offering interoperability at technical, semantic and organisational levels
8. European eID industry should hold a leading position on the global eID scene
9. Established world-class European knowledge and skills on the eID ecosystem (technology, business models, cost benefit analysis, etc.)
10. A proactive eID governance at Member State and European level based on cooperation, and the exchange of and promotion of best practice solutions at different levels of administration
11. A European regulatory/governance framework for the use of eID at European level, and facilitation of eIDM across public and private sectors, including data protection aspects
12. The needs of non-citizens resident inside the EU, as well as the needs of businesses and citizens who interact with extra-EU entities, must both be taken into consideration

2 Roadmap for achieving the objectives

2.1 Lines of Action

Achieving this main policy objective will require the stakeholders, including the commission, to conduct a number of initiatives (some aspects of these may be done in parallel, in other cases there are dependencies requiring specific sequencing) which can be seen to fall into the following main “lines of action”:

- Informing the public and the business community (awareness, benefits, empowerment) to achieve the required UPTAKE
- Implementing the necessary LEGISLATIVE SUPPORT to cope with the new paradigms across the EU
- Advancing the TECHNOLOGY, especially in the areas of bandwidth and conductivity
- Stakeholders making the necessary directed and coordinated PREPARATIONS, including establishing the common long-term vision & model, and implementing the supporting infrastructure

To a first approximation, the most visible achievements in each action line can be seen on the Signposts diagram which follows⁴.

2.2 Mechanisms for Implementation

2.2.1 Introduction

The following do not present an exhaustive list or analysis of all the implementation mechanisms to be used, but merely represent an indicative list of possible ones to be considered⁵. At the appropriate times, the most suitable ones, i.e., those best suited to achieve intended results, will be selected and incorporated into the roadmap. In addition, it is expected that other expert groups will consider this topic in much more detail, especially given that there are also other thematic areas to be addressed under the ELSA initiative. Possible mechanisms include:

2.2.2 eID Observatory

Collecting and disseminating overviews of the European state of the art and best practices in eIDM solutions is an important means of encouraging take-up of early adaptor solutions. It also serves to highlight significant standardization efforts (e.g., standardization of interfaces) taking place under the auspices of different initiatives. Identification and dissemination of best practices in European eIDM initiatives is already being explored through the European eID Observatory at ePractice.eu.

2.2.3 Large scale pilots

The ICT Policy Support Programme addresses technology and non technology innovation that has moved beyond the final research demonstration phase. ICT PSP is concentrating funding on a limited number of actions in predefined themes. The themes are supported by a limited number of high impact pilot projects as well as thematic networks addressing specific objectives.

⁴ A much more detailed breakdown and description of work to be done can be found in the annex, section 7.2, “Overview of work to be done”, page 35.

⁵ It must also be emphasised at this point that a large proportion of the effort and investments will necessarily be conducted under National auspices.

2.2.4 Public-private Partnerships

Public-private partnership (PPP) involves a contract between a public sector authority and a private party, in which the private party provides a public service or project and assumes substantial financial, technical and operational risk in the project.

In some types of PPP, the cost of using the service is borne exclusively by the users of the service and not by the taxpayer. In other types (notably the private finance initiative), capital investment is made by the private sector on the strength of a contract with government to provide agreed services and the cost of providing the service is borne wholly or in part by the government.

In practice, different elements of the infrastructure and related identity services may be provided and/or operated by the same or different organizations. The ID Management system is therefore a complex and integrated one, whose components may be provided and/or operated by different collaborating organizations that must agree on a common set of rules and policies according to regulatory constraints, in order to operate the system. The participating organisations will include both public and private sector entities.

2.2.5 Pre-commercial Procurement

This is an essential tool in the framework of the cycle of innovation in the EU, and an essential instrument in the policy “toolbag”.

It may be directed towards projects that are so wide, with a cost so high, and involving potentially leading-edge technologies, so that it is not commercially feasible to fit the costs of “normal” projects. It may “prime” the Marketplace through research and development of foundational elements and trialling and demonstration of feasibility, based on which traditional projects with traditional procurement cycles can then be launched.

2.2.6 Lead Market Initiative for eID

A lead market is the market of a product or service in a given geographical area, where the diffusion process of an internationally successful innovation (technological or non-technological) first took off and is sustained and expanded through a wide range of different services.

The Lead Market Initiative is an EU framework aimed at fostering emergence of markets with high economic and societal value. The estimations of the Societal and Economic impact of eID, especially as reflected in the (preliminary) long-term vision, demonstrates the enormous potential for bringing high added value to citizens and businesses. The market related to eID is highly innovative, is inextricably linked to users’ needs, has a strong technological and industrial base in Europe, and depends more than other markets on the creation of favourable conditions through public policy measures.

Establishing a Lead Market in eID would provide a pre-existing structure and approach for the appropriate EU and MS authorities (national, regional, and/or local) involved in eID-related activities to stimulate and sustain innovation in eIDM, push developments in the right direction through concerted deployment of finely honed instruments (Legislation, Public procurement, Standardization, labelling and certification, Complementary instruments, etc.), and to thereby expand diffusion and uptake of the technology in question.

2.2.7 Study, Research & Development on a number of topics

The long-term eID vision will encompass a number of unknowns. Focused inquiry into several issues will be necessary to enable achievement of the vision, in a number of different areas.

For example, the conceptual model behind the functionality that we are looking for is not clear: how can specific roles and responsibilities be defined and organized in a general eIDM framework, and how can the advanced technological options be integrated into this framework?

Another key locus of unknowns are the economics behind eIDM, which are not well understood: it is not entirely clear how the objectives that we have envisaged above can be implemented in a way that is attractive for end users and service providers alike.

Furthermore, some objectives clash with others, and different stakeholders have different interests. For example, many service providers with an extensive existing customer base and the required infrastructure want cheap access to as much information as they can use, while end users are more interested in convenience than in security, and some end users may not be willing to pay a premium for security. The implications of such diverging needs, including the proper tradeoffs to be struck will require still further study and investigation.

Areas requiring further study could be summarized as follows:

Area of Activity	Objectives
Extrapolation of technology trends and ongoing research	Validate the feasibility of a user-centric all-inclusive model for electronic identities delivered as a utility in an ambient intelligence perspective, achieve needed advancements in eID Technology (biometrics, RFID's, tokens, etc.) and networking/communications (bandwidth, connectivity, etc.)
Reaching interoperability objectives	Achieve technical, semantic and organisational interoperability
Develop a broader perspective encompassing the entire ICT ecosystem	Deliver a sustainable converged model covering the needs of the administrations, businesses and citizens and where risks are adequately mitigated
establishing a governance model for a converging eID infrastructure	Determine how the eID infrastructure will be operated (determine which identity is appropriate/permisible for any given context) , maintained (rollout of updates) and governed (evolution)
The societal perspective	Align the target model with societal expectations (use patterns, trust, privacy, user-centricity,...)
Privacy by design	Develop privacy-preserving technologies applicable in the context of the converged model of electronic identities. Develop technology and standards for implementation of necessary and justifiable use and minimal data disclosure.
Accountability and transparency of data processing	Tools for reporting and auditing to support accountability and transparency of data processing
Security	Devising the strategy and means of adequately protecting individuals, businesses and society with built-in mechanisms, processes, etc.
User requirements	Adequately capture user needs at the level of individual and societal ergonomics
Evolution of the legal context	Align the legal basis to the new challenges and societal expectations resulting from the converged model of electronic identities
Raising awareness	Improve the public's trust and confidence
Understanding the market	Validate that the target model is economically sustainable and brings tangible benefits to all stakeholders
The eGovernment perspective	Align eGovernment initiatives and the target converged model of electronic identities
Organising the convergence	Deploy the infrastructure supporting the target model and ensure adoption by PEGS (Pan European government services).

2.2.8 Lessons learned from the past, on instruments

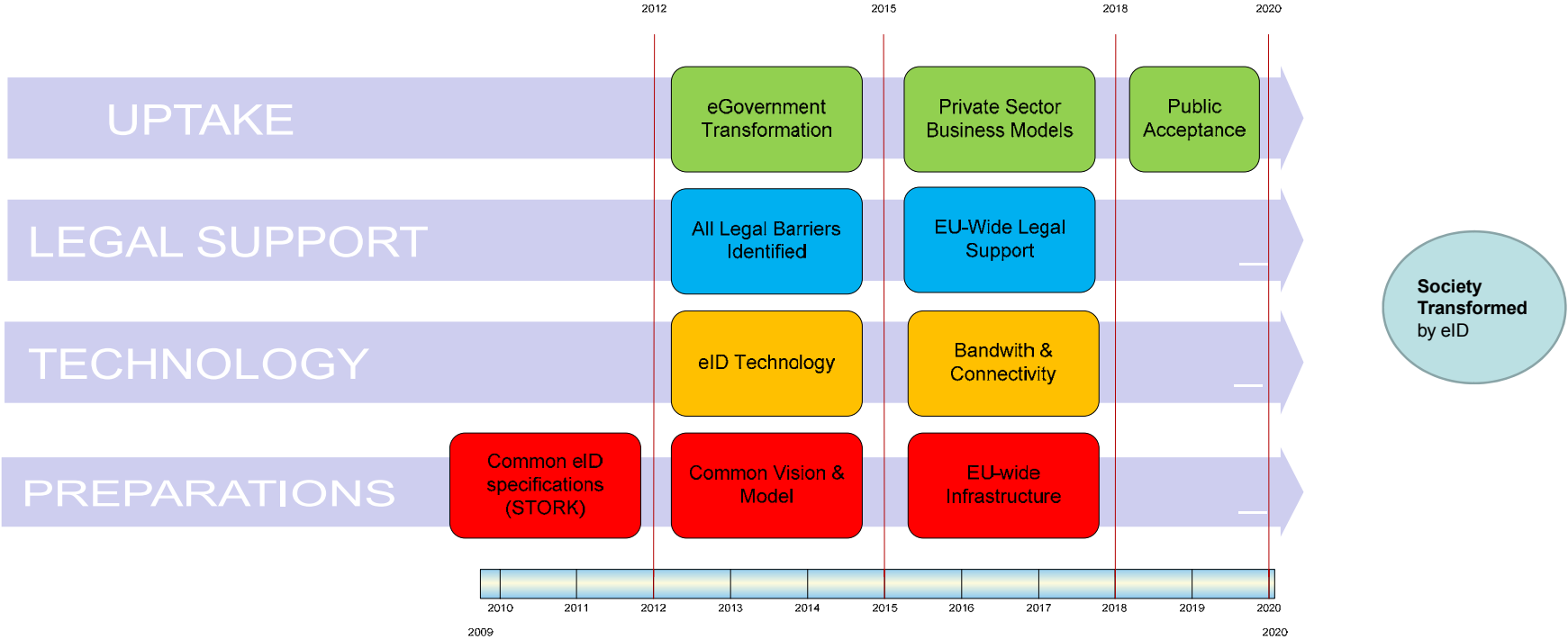
An initial analysis of each of the instruments reveals that none of them, at least in their present form, are sufficient to meet the objectives of the ELSA for eIDM.

An initial consideration shows that any new instrument or a variation/combination of some of the existing instruments, needs to have the following characteristics:

- Co-ordination at EU level
- Management and running at local level (possibly at MS or application based level)
- Requires EU funding possibly at 75% initially in particular for public authorities, but leading to a self sustaining situation in the medium term.
- Infrastructure other than internet should be paid for by the MS or service providers (for example telecom operators), through ERDF or other sources of funding (this merits much more consideration, as it can be complex)
- Considerable training and awareness will be required through piloting
- Defining and providing services should be decided at the local level, with loose co-ordination at central level
- It should not be a loose connection of a large number of separate, individual projects, which will not lead to the results/impact that the programme is intended to achieve. (thus actions like ETP, or a number of IP's, or thematic networks, etc., are alone not sufficient or appropriate)
- Pre-commercial procurement will have the strength in buying in new research solutions, but may not be suitable for large scale implementation

2.3 Signposts to eIDM Infrastructure

A large number of actions must be taken, on several fronts simultaneously. Measurable progress can be discerned via the passing of a series of high-level signposts representing specific capabilities, building blocks or other concrete achievements that will be needed on the way to realisation of the final/ultimate objective. Some of the most significant are depicted below with indications of timescale.



3 Barriers

In this section are outlined some of the most important groups of barriers to achieving the objectives (widespread uptake of eID). The list below is not exhaustive, nor is it intended to be so. The list is intended to be indicative and to serve as a starting point for the detailed investigations which must follow.

Technological Barriers	Lack of interoperability at the technical, semantic, organizational, and legal levels
	Complex and fragmented standards landscape
	New challenges related to scalability, connectivity and bandwidth
	Lack of bullet-proof reliability and redundancy
	Lack of framework to provide expected (and uniform) levels of security and privacy protection
	Manage the complexity of multiple electronic identities
	Lack of harmonized eID middleware implementations in existing operating systems distributed by major vendors
	Lack of services architecture and meta-model capable of accommodating different channels and eID types/sources, and covering public/private sector, etc.
Societal Barriers	Lack of citizen trust in areas of privacy: loss of anonymity, persistence of activity traces
	Lack of citizen capabilities to effectively use and protect their electronic identities
	Lack of ease of use of eID
	Lack of citizen awareness of benefits of the use of eID including a lack of understanding/appreciation of the <i>role</i> of eID, i.e. the value and place of anonymous/pseudonymous communications.
	Cultural Resistance to the use of eID in some regions and for some types of activities
Economic Barriers	Need for large up-front investments in leading edge technologies
	Need for significant investments to meet new legal obligations
	The cost for businesses to setup or migrate to use of eID in their standard business activities
	Potentially high (prohibitive) transaction costs in some cases
Legal Barriers	Lack of framework for assessing liability in cases of misuse (fraud, theft, etc.) of eID
	Lack of legal framework addressing the multitude of sources of eID (issuers, verifiers, etc.), how they are to be used, etc.
	Instability in transaction cost structure in the short- and medium-terms leading to uncertainty
	Limitations on re-use of nationally issued eID's in some MS/jurisdictions
	Lack of uniformity in MS Data Protection expectations and policies, perhaps even incompatibilities
	Lack of information on the differences between national laws on personal data protection, especially for users
	Lack of information on the proof requirements for electronic signing in a member state other than one's own

Political Barriers	Difficulties arising from the presence of certain administrative boundaries (esp. but not limited to the sacrosanct cases involving subsidiarity)
	Need for high levels of cooperation between various public administrations, and even private operators when things go wrong with eID (identity theft, infrastructure problems, etc.)
Conceptual Barriers	Lack of a common societal view on the concept of electronic identity, including ownership of attributes
	Lack of a common long-term vision on eID
	User interface issues: lack of a uniform and simple-enough interaction paradigm
	The “Not Invented Here” syndrome, wherein interesting and/or useful approaches, tools, practices, etc., are rejected, to the detriment of the overall objectives, due solely to their origin
Organisational Barriers	Lack of appropriate public/private collaboration structures involving all relevant stakeholders
	Digitally agnostic persons, citizens without access to PC’s
	Lack of complete, clear set of scenarios to be supported by the eID infrastructure
	Lack of an EU-wide eID infrastructure capable of supporting all of the above
	Lack of global governance on eID issues
	Rollout challenge due to scale

4 Overcoming the barriers

4.1 Stakeholder Involvement

Due to the exceptionally broad impact of ubiquitous deployment of eID on society, business and citizens lives, nearly everyone is a stakeholder. We can however list the key ones, all of which will play important roles, as follows:

- Public administrations
- Citizens
- Electronic Identity technology providers
- Manufacturing Industry Sector groups
- Academy/University researchers
- Businesses which can be electronically enabled, and which can offer their services remotely
- Businesses which supply technology and services to other businesses and administrations in setting up and/or using eID in their business activities
- Businesses which manufacture, distribute or provide support for any type of eID enabled devices or appliances
- Businesses which provide and maintain the supporting infrastructure elements underlying ubiquitous deployment of eID

The initial report from the launch of the ELSA Thematic Working Group on electronic identity management held on 26 March 2009, can be found in the section 7.6, “Report from the ELSA Thematic Working Group on electronic identity management 26 MARCH 2009”, page 43. The final meeting of the ELSA Thematic Working Group on electronic identity management was held on 22 October 2009; the list of participants can be found in the annex, section 7.7, “Last meeting of the ELSA Thematic Working Group on electronic identity management”, page 44. The contributions of some stakeholders submitted by some stakeholders as a result of the consultations can be found in the annex, beginning in section 7.8, “Stakeholder Inputs”, page 54.

4.2 Architecture and Model

4.2.1 The Requirements for European electronic identity infrastructure

We can begin with a summary of the conceptually ideal characteristics of a European electronic identity:

- It is a digital entity associated with⁶ one and only one natural person or legal entity (businesses) - one person or legal entity may own one or more of these digital identities;
- It is not necessarily embodied in a specific physical token, although such a token might be used to access the eID in question;
- It is provided through a trusted authority and is valid (at the least) within the specific jurisdiction or scope of applicability of the authority in question;

⁶ Eventually expanded to include objects/devices at some point in the future, however this is not in the scope of the current discussion.

- It is practically unforgeable⁷, meaning that it is strongly protected against the creation of undetectable false identities, or against the issuance to a person to whom it does not belong; The veracity of its assertions are therefore widely trusted;
- It is universal in that it is designed to be usable in any context where an electronic transaction requiring identification at the security level offered by the eID is possible;
- It is user-centric, in that it is the holder of the electronic identity in question who decides how it is used, how much information to reveal about himself; it is the user who decides in which additional contexts he wishes to use his eID; user assent is required by default to disclose any and all identity related information (justified law-enforcement requirements excepted of course);
- It is extensible, in that the functionality of electronic identity (in terms of its management as well as sector-specific use) can be extended by means of user-selected and user-managed tools;
- It is interoperable, not being limited to use only within the jurisdiction of the issuer, but is designed to be usable in the same way in all EU Member States, especially for access to eGovernment services;
- It can be linked to other eID's to indicate specific types of relevant relationships (e.g., "parent-child", "owner of", mandates, etc.);

4.2.2 A Meta-Model of Identity

There are different eIDM initiatives⁸ already competing in the marketplace, based on different sets of use-cases and other requirements. Some of these, including OpenID v2, Shibboleth, Liberty Alliance and SAML, ECP (SAML), Information Cards, etc., attempt to resolve the question of which Identity Provider should be used by providing the service provider (relying party) with means to determine the proper Identity Provider that should be used to authenticate the user. The characteristics of these identity systems vary greatly, posing difficulties to compare them; Each solution has its benefits and drawbacks.

It would be useful for standardization purposes, to agree on some criteria that may help to classify and compare the main services and functionalities that an ID Management service provides and their impact on the system architecture and governance. This should permit the stakeholders to assemble appropriate models/solutions from the available building blocks, including borrowing ideas, technologies or other elements from ongoing initiatives (including those mentioned above, or others), emerging technologies, etc.

It is nonetheless clear that various abstraction layers will be needed in any solution, to properly accommodate existing efforts and systems, plus possible future channels, paradigms, etc. A more detailed description of a Service Based architecture for eID can be found in the Annex, see section 7.4, "Service-Oriented architectural model for identity management", page 40.

In addition, any model must address multiple levels of reliability of presented credentials (with associated authentication levels), according to the appropriate context, as well as multiple levels of

⁷ This is only a *hypothesis*, which requires a fall-back measure in case of failure, which is also the case for several of the other characteristics listed here for eID

⁸ Technologies such as OpenID offer an open, decentralized, framework for user-centric digital identity and it is at one's option that one shares the personal information with a relying party. Similarly, solutions like the Austrian eID scheme allow to link together a set of identifiers related to several sectors while maintaining a clear segmentation. Solutions like Information Cards can be used at the identity provider to keep credentials from being stolen. Access to these credentials and their attributes is itself secured by means of strong authentication mechanisms. Furthermore, zero-knowledge and blind signature approaches are aimed to manage personal information, without disclosing any information to the server providing the service. Based on a "hide nothing" approach (including the source code access) they bring trust and really support the protection of personal data.

ease-of-use. For example, a sports club membership would be an example of an eID issued “on the spot”, with minimal or even no background checking involved; such an electronic identity⁹ would be nothing more than “the person that paid for a 3-month membership, starting 1st of October”.

One possible fundamental principle that could be chosen to underlie the eID system is a meta-model based on a claims-based paradigm for the identity interactions. A key component of such a system is the “claims broker” which is a “black box” that transforms assertions about attributes of an eID holder, into the form needed by the relying party.

The laws of identity¹⁰ are another useful point of departure for the discussion on the model to be adopted:

- User control and consent (digital identity systems must reveal information identifying a user only with the user’s consent),
- Limited disclosure for limited use (the solution that discloses the least identifying information and best limits its use is the most stable, long-term solution),
- The law of fewest parties (digital identity systems must limit disclosure of identifying information to parties having a necessary and justifiable place in a given identity relationship),
- Directed identity (a universal identity metasytem must support both “omni-directional” identifiers for use by public entities, and “unidirectional” identifiers for private entities, thus facilitating discovery while preventing release of correlation handles),
- Pluralism of operators and technologies (a universal identity metasytem must channel and enable the internetworking of multiple identity technologies run by multiple identity providers),
- Human integration (a unifying identity metasytem must define the human user as a component integrated through protected and unambiguous human-machine communications), and
- Consistent experience across contexts (a unifying identity metasytem must provide a simple consistent experience while enabling separation of contexts through multiple operators and technologies).

4.2.3 Multiple Identity Service Providers (IdSP’s)

Any possible future pan-European eID system and infrastructure will entail multiple identity issuers, each following its own rules and processes. In this scheme, national ID cards are only one element of the system. Electronic Identities, and physical “trusted containers” such as “smart cards”, could be issued by public bodies or by private entities with a specific government mandate.

Some of these providers could even become “highly trusted” “Identity Service Providers” (IdSP’s), following some supervision/accreditation scheme, and whose issued eID’s could therefore be accepted for some or all eGovernment services. The proposed “European Citizen Card” is one possible participant¹¹ in this scheme (see Annex, section 7.5, “CEN TC224 : The “European Citizen Card” (ECC)”, page 40).

⁹ Some applications could function by using a set of data that is more appropriately characterised as a profile (containing only the relevant characteristics of an individual without necessarily identifying him/her), rather than as an eID per se (which would require unique identification by definition). The example given here however does involve unique identification, as the hypothetical sports club’s interest is to ensure the integrity and proper use of sold subscriptions.

¹⁰ “*The Identity Metasytem*”, **Linux Journal**, September 2005

¹¹ The inclusion of this particular effort at standardization does not indicate a preference for the solution. The purpose is rather to point out that there are serious efforts underway that should be carefully considered, and this particular effort is included merely as an illustrative example of the degree of progress being made. Ideally, it should be explored how the different and separate efforts could cooperate or work towards convergence.

These IdSP's could offer eID's based on the citizen's National ID constituting part or all of the enrolment process. The process of generating a new credential from a National ID would be accomplished via a one-way algorithm (hashing) that would prevent backward tracing of the National ID from the new credential. In this way, the new credential would inherit the status of the original National ID without presenting any risk of compromise of the privacy of the original. IdSP's could be private sector entities, public sector entities or combined private/public partnerships, and could offer different levels of liability, opt-in/out capabilities, and 'affinity' credentials to personalise the identity.

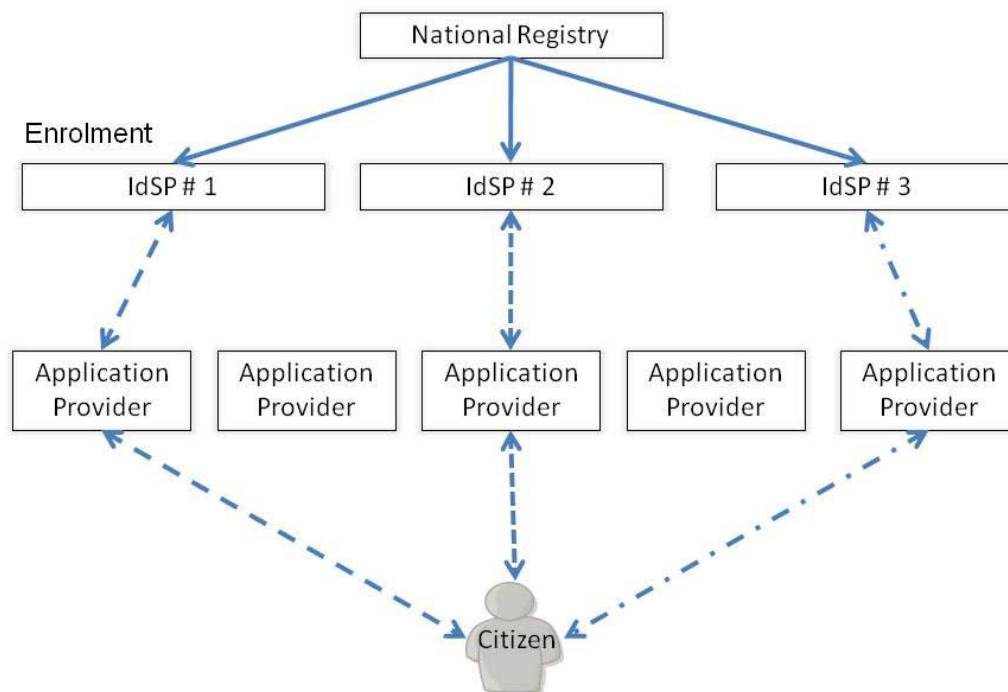
In fact, any entity that deals with identities and customers on a large scale (e.g., eBay) might be persuaded of the potential benefits of extending its own identity scheme to partners or others, and incorporate that into its' business model, thereby becoming an IdSP itself.

These IdSP's also have a role to play in the lifecycle of electronic document and transaction lifecycles. Different legal obligations will apply in different circumstances, as part of the legal arrangements put in place whereby such electronic documents and transaction traces have certain legal weight. Some organisations will be better placed to exercise this role than others, due to their relationships with other entities participating in different transactions involving electronic identities.

The documentary proof used by one IdSP would be interoperable with that of other IdSP's, and each could be members of different trans-national groups. The legal aspects of such arrangements could be managed according to the provisions of the contract between the IdSP and the eID holder, which could take the form of a standard terms agreement. This would have to be adapted to each jurisdiction's specific environment and security policy, whether national and/or community based. IdSP's would be able to benchmark against one another and accept with confidence the digital identities issued by their trusted counterparts.

A Citizen could choose his eID from any IdSP within his own Member State of citizenship or an IdSP of another Member State should its terms of operation be acceptable to both parties. Indeed, the citizen could choose to hold more than one eID, as is often the case currently. Each of the citizen's individual eID's could not be linked together to aggregate data inappropriately, but would however be traceable back to the citizen in question, in order to ensure consistency and non-repudiation.

An application provider could accept identity attributes from a range of IdSP's. This acceptance would be based upon using a commonly understood identity assurance framework to match the declared risk profile of the application against the level of trust in a credential. Some IdSP's may choose to support different identity credentials, each with a distinct level of trust, whereas others may specialise in credentials of a particular trust level.



This arrangement would require certification within each Member State and each certification would need to be assessed by a risk-based methodology comparative to that undertaken by DNV in Norway for BBS operations.

Applications that use the new credentials would be owned and operated by existing and new business providers, and would use IdSP's to provide the information relied upon by their clients, the relying parties.

Having established the concept of an IdSP role, and defined its necessary characteristics, it would then be a matter of market evolution to determine the particular configuration of this new industry within the EU.

This idea of an evolving marketplace in IdSP's poses policy questions regarding certification of the players and industry supervision that will require further study.

It is necessary to agree as to the certification of IdSP as providers of electronic documentary certification services, if only by a general or basic security policy, bringing together the largest number of candidates to establish an initial level of certification and interoperability between countries.

In any event, if the States do not do so, the strength of the demand of large companies and banks will see the adoption of industry-led solutions, such as the SWIFT cooperative has done for the interoperability of payments and the dematerialisation of the financial instruments e.g. CEDEL, EUROCLEAR, EURONEXT, CLEARSTREAM, etc.

The absence of a simple, clear, pragmatic, organisational and cheap "value proposition" by States will lead public companies towards the first certification and interoperability solution which they must have for the mandatory cover of their systematic risk.

4.3 A long term supportive process

4.3.1 Maintaining the long term vision

The long-term vision should be dynamic: it should evolve over time through a process of continuous improvement. The process has several steps, as follows:

1. Develop a set of objectives in the form of a Long-Term vision
2. Get an accurate snapshot of the current situation
3. Identify, assemble, exchange and disseminate information on what is being done; develop information exchange events between different groups.
4. Establish a roadmap for implementation of the vision
5. Repeat on a regular basis to renew the long-term vision, and update the roadmap

With a long term vision, the stakeholders can proceed with the essential foundation steps of developing the needed architectural and technical models, and the strategy and plans to implement these models. These are large and ambitious elements that will take considerable time and effort to develop, and the active involvement of many stakeholders.

4.3.2 Leveraging experience and knowledge from the private sector

Some of the most experienced actors in the field of eID are in the private sector, particularly “web actors”, working on projects of much smaller scope, but of great practical utility. In the financial sector, banks and other institutions have decades of experience in dealing with eID. Their knowledge and experience of legal liability, usage scenarios, and commercial deployment can provide critical perspectives in the areas of operation and management of complex infrastructures in a cross-border context, and will be invaluable in achieving practical goals, and must therefore be fully leveraged .

4.3.3 Government officials in the forefront

Government officials are uniquely positioned to lead by example. eGovernment initiatives involve the re-engineering of government-operated IT systems, including the introduction of eID as an integral part. By being the first trained, guaranteed users of these systems, government officials can play a key role in pilot projects, participating in efforts to resolve roll-out and other issues, demonstrate feasibility, build confidence, promote uptake and otherwise aid the eGovernment efforts in crucial ways.

4.3.4 Fostering/Supporting the eID community

The eID community (e.g., online communities like ePractices.eu, etc.) is broad and diverse. It is also very active, and is making progress at a rapid pace. It is important that synergies be developed, and that the possibilities for sharing & reuse of information and solutions take place, and that collaboration is supported, developed and enhanced. This is also important from the additional perspective of achieving high levels of buy-in from the public.

4.3.5 Communications Policy

Successful uptake by Citizens and Businesses depends on overcoming certain societal barriers related to attitudes and lack of information. The communications policy must therefore be put in place covering identification and dissemination of best practices in European eIDM initiatives and the state of the art in eIDM solutions, but also educating the public on the use and benefits of eID, including privacy-enhancing features. This education must also focus on developing skills in effective identity management, bringing all Europeans up to the same level of knowledge and know-how. School and University programs should be developed and adapted to future eID evolutions and requirements.

4.4 EU-level Leadership and Guidance

Overall there is a very important role to be played at the EU-level. In brief, coordination, guidance, support (€), and leadership (organization & coordination of stakeholders, driving debate in certain

directions, promoting achievement of certain milestones, in keeping with the roadmap) will be indispensable.

There must be a sustained and comprehensive effort to stimulate and sustain innovation in eIDM, push developments in the right direction through concerted deployment of finely honed instruments aimed at preparing the way, by disseminating technology and information to spur uptake.

An integrated, thematic approach to providing active, coordinated and sustained political support for the long-term vision, through both supply-side and demand-side public policy measures is needed. This includes in-depth analysis, intense consultations as well as extensive feed-back mechanisms. It encompasses the design of processes to better streamline legal and regulatory environments and accelerate the growth of demand.

EU institutions have a role to play in technological developments, including ensuring broad support for the eID system and its standards in off-the-shelf commercial software and hardware. Playing this role will entail a number of different collaborations with IT suppliers, and in monitoring best practices on a global basis.

Guidelines provided at EU level could be very useful for different public administrations' efforts at establishing the rules and regulations to issue/manage eID's, despite the lack of direct European regulatory competence to harmonize national eID regulations. An appropriate paradigm for an eIDM infrastructure must be established. In the absence of direct European regulation, this could also take the form of regulatory guidance, model arrangements and agreements (as is e.g. applied in the banking sector, albeit based on a contractual hierarchical model), and support for existing and new standardization initiatives. Collectively, this might allow the creation of a consistent and complete European normative framework.

4.4.1 Standardisation

EU institutions also have a role to play in collaborating and facilitating alignment between EU efforts and the work of various standards-setting bodies, as well as with other global eID-related initiatives.

Industry-led efforts tend to optimize their solutions for their specific market segments and perspectives. The public interest has to be represented effectively in standardisation efforts. To build up an EU of e-Services, standards must enable the integration of the existing ID Management technologies currently deployed, but also enable any EU citizen in any EU member state to perform public and possibly private remote procedures in each EU member state using his own ID credentials issued by its own Member State.

Those standards should be consistent (no contradictions), complementary (no overlaps), sufficient (no gaps, effective means to achieve interoperability) and realistic (costs for implementation compatible with business cases).

4.4.2 An ethics-monitoring body

In parallel with efforts to establish EU-level mechanisms dealing with personal data protection issues, establishment of an ethics-monitoring body responsible for supporting the application of ethics at relevant phases of eID-related efforts affords a unique opportunity to incorporate a solid ethical underpinning in all aspects of eID. Each service provider, component and process could include an ethical check to ensure that the highest standards are incorporated from the outset – not as an afterthought. These would need to be continually monitored by an independent body. This high ethical standard would assure citizens of the ultimate 'fairness' respected in eID-involved dealings, required for entrusting service providers with storing and releasing personal data and attributes.

5 Measuring the Impact¹²

eID is a growth area and eID is an international market. The ELSA on eID could greatly contribute to Europe becoming a global leader in the field. The introduction of eID as envisioned herein involves seizing new opportunities & reinforcing current strengths.

5.1 General Impacts

5.1.1 Leading by example

There are new opportunities for leadership associated with this eID initiative. Success breeds emulation elsewhere, a well-known pattern. The EU possesses the potential for these UNIQUE achievements:

- establish ***THE*** model for implementing a secure, robust, manageable, and evolving electronic economy on a large scale, in which privacy is fully protected
- establish a workable model of public/private partnership that demonstrates how governments can ensure that public policy objectives are met in the course of large, complex, long-term initiatives involving mostly private industry expenditures

5.1.2 Industrial and Technological leadership

The introduction of eID as envisioned herein would help to establish Europe's industrial and technological leadership, through the development and rollout on a continent-wide, international scale of an infrastructure based on existing and new technologies at the core of the eID infrastructure (biometrics, security, privacy, service brokering); Implementing the EU's ambitious goals in this area will result in reality-tested infrastructure at the core of the next electronic economy, and will provide a model that many countries and regions around the world will want to emulate.

5.1.3 Growth of new markets and businesses

The introduction of eID as envisioned herein would facilitate the emergence & growth of new markets and businesses; deployment of eID is transformational. It will create an environment rich in possibilities (many inconceivable at the present time) for new young companies with innovative business models selling new types of products and services; this is because eID extends the scope of trust and thereby enables remote/electronic interactions into new scenarios and types of transactions. This means new opportunities for business activity where it was before limited or non-existent.

5.1.4 Attracting investment

The introduction of eID as envisioned would increase Europe's attractiveness to investments and skills. Building the new infrastructure will require large investments and therefore present opportunities to suppliers of all the needed types of products and services to build it.

The new electronic market will be a unique one in the developed world, and as it will be stable, trusted, secure, and privacy enabled environment thanks to eID, it will be very attractive for businesses from everywhere in the world to invest in, participate in the establishment, search for customers, etc.

Europe is well-positioned as it is the only region on earth where such ambitious undertakings is underway; furthermore, it faces unique problems that are at the core of the efforts (multilingualism, socio-cultural diversity, semantic interoperability) that will result in solutions reusable in other parts of the world. Europe will gain know-how that is only available (at least in the short term) in Europe.

¹² An overview of impacts by EU policy area can be found in the annex, section 7.3, "Impact analysis by EU Policy area", page 36.

5.2 Environment

5.2.1 The Internet of Things

The internet becomes not just a place where individuals meet but also the place where “everything is.” It becomes a place that is populated by both individuals and devices of all types.

This paradigm shift in combination with specific types of sensory devices will enable humanity to obtain a much more accurate, comprehensive, detailed and up-to-date view of the state of the earth, including various environmental measures.

5.2.2 Health and well-being

While the subject of health care is deserving of individual treatment in a separate study, we here can summarise some of the key expected impacts: Improvements in the infrastructure and efficiency of the health care system, and at the many points in the “health care chain” are expected to have significant and positive impacts, over the long run on Individual and population health.

On the other hand, the more objects are interconnected and the more they communicate with each other, the more infrastructure that will be required to support the communications, the more communication bandwidth that will need to be used and made available, and (potentially) the more unwanted background radiation that might be produced (especially for wireless communications). There may be lingering questions as to the long-term implications for health and well-being of citizens.

The degree of increase in background electromagnetic emissions is not precisely known, and could therefore have a potentially significant negative impact. The ubiquitous nature of UDeID would imply a significant increase in these emissions. The health and well-being implications are not clear, but there are many ongoing inquiries into the subject (see <http://www.emrpolicy.org/science/forum/index.htm> , etc.). It must be noted however, that baseline conditions are already significant, and have been for decades in most of the developed world.

The impact on Community and cultural group cohesion is less clear; including the impact on Family cohesion and Cultural maintenance. Overall expectations of a neutral impact is the first estimate.

5.2.3 Energy Consumption

With more objects disposing of electronic identity, and therefore engaging in a variety of electronic transactions of all types, net energy consumption will probably rise. While precise figures are not available, some initial estimates could be made, based on raw numbers of interacting devices, persons and transaction volumes. The results are expected to indicate modest to significant increases in energy consumption, at least in the short term. The development of new low-energy technologies could however mitigate or even reverse the trend.

5.3 Equitable business and employment opportunities

This is often the first step in conducting a traditional Business Impact Assessment: identifying which categories of companies could actually be confronted with the proposed changes, followed by some quantitative analysis on the number of companies in those categories, etc.

While eID brings many new business opportunities, they are not all spread evenly. Due to its intrinsically technological nature, companies where technology already plays an important role in the core business processes.

We can immediately identify a number of types of businesses that will experience clear and swift benefits:

- Businesses which benefit from targeted advertising
- Businesses which can be electronically enabled, and which can do business remotely

- Businesses which supply technology and services to other businesses and administrations in setting up and/or using eID in their business activities
- Businesses which manufacture, distribute or provide support for any type of eID enabled devices or appliances¹³
- Businesses which provide and maintain the supporting infrastructure elements underlying UDeID

This list is however non-exhaustive.

Businesses which could experience a negative impact (or a neutral impact), at least in the shorter term, are all those that continue quite happily with paper-based business processes, as well as those in which dealings with their customers are sometimes preferably conducted on an anonymous basis (e.g., charitable contributions), and desire to remain so.

5.3.1 Local, regional and territorial business competitiveness

This initiative is expected to result in a great expansion of Employment opportunities for local, regional and territorial residents, as new markets are created.

Initially there may be some new associated requirements of Training and career development for local, regional, territorial residents. In Europe, there may be a complex dynamic between increased population mobility and increased business competitiveness at Local, regional and territorial levels.

Over the last several decades during which IT arose to play a central role in western societies, there was a general avoidance of boom and bust cycles (e.g. via economic diversification). This trend could be expected to continue and be amplified by the initiative's effects herein.

5.4 Demography

By means of improvements to public services related to migration of citizens within the EU, as well as the potential solutions to the language barriers inherent to migration within Europe, eID is likely to have dramatic impact on inwards and outwards migration.

We can expect to see broad Changes in social and cultural makeup of affected communities, as the mobility of European workforce increases significantly, resulting in more broadly based European multicultural communities across Europe.

5.5 Adequate services and infrastructure

Dramatic improvements, simplifications, streamlining of provision of social services such as health care, education, and justice will likely at least in the short term, result in increase pressure on these service providers as they struggle to cope with sharply increased demand

Corresponding, we can expect to see concomitant impacts on Traffic and road safety as well as other pressures on physical infrastructure

¹³ One example is home furnishings, as the diffusion of the idea of the “internet of things” changes residents’ expectations of functionality of their homes, working spaces and other buildings. This will affect both new and existing buildings: The advantages of integrating the internet of things concept into new house and building construction from the design phase will become apparent. Evolution in the concepts of essential services such as smart utilities and connections (gas, electricity, water), garbage pickup, home security, etc., will lead to new standards and paradigms for construction. Refurbishing and modernization of existing homes with new capabilities will be a growth business, as spill over from the perceived conveniences afforded by the features seen in newly houses and buildings. Such pressures will likely be only temporary (over a period of perhaps 10-20 years) even possibly contributing to a new housing bubble, as the supply of upgrades and new houses struggles to meet sharp increases in demand. Issues of affordability, availability, and appropriateness may even come into play.

5.6 Changes in lifestyle

eID will have the likely impact of increasing the overall amount of wealth in the community, through economic growth that it spurs.

We can expect to see more efficient uses of wealth in the community as a result of highly personalized advertising and services. This will have the effect of increasing the efficiency of electronic marketing in general, with the knock-on effect of having an effective multiplying effect on disposable income.

There are additional positive knock-on effects, including reduction in Local and regional costs of living.

The distribution of costs/benefits among affected people, i.e., the impact equity, is likely to be on balance, positive.

Furthermore, new forms of “e-working” will appear or become more prevalent, as new ways of working and being paid arise in the eID-enriched society. Work and pay being central parts of people’s lives, this change will undoubtedly have positive impact on society as citizens enjoy more choices and opportunities.

Public Services benefits to citizens are expected to be completely equitable, with the exception of digitally agnostic persons.

There are few expected adverse lifestyle changes (such as increased gambling, crime, substance abuse); in fact the opposite is expected, as eID will at least in the general case of gambling and crime, facilitate the efforts of law enforcement officials in combating illegal gambling, and many other types of crime (copy text from eID vision paper).

5.7 Mobility

eID will facilitate citizen and business mobility to an unprecedented degree, now linking mobility to a virtual but trustworthy concept of electronic presence rather than to geographic location. This will have far-reaching effects on demographics, leading to improvements in the functioning of the internal market, lower unemployment, etc. As a result, new business opportunities and markets for businesses, and new products and services for consumers will appear.

New, improved and more useful mobile applications are expected to become available, which could involve remuneration based on usage or downloading.

5.8 Retail market impacts

Enormous impact expected, as the utility and convenience of eID enabled devices becomes clear. Any consumer or business product that could experience such benefits will see the introduction of new product lines to take advantage of the new possibilities. This includes all many of household appliances and furnishings, consumer entertainment devices, both fixed and mobile, etc.

5.9 Employment and income

It is expected to have a high impact on jobs and growth, as we are talking about highly innovative activities that will on the one hand require significant R&D as well as commercial investments, and on the other hand will bring huge new business opportunities as new classes and generations of products and markets will appear as a direct result of implementing this vision.

5.10 Public services

The eventual yet gradual incorporation of interoperable e-signatures and e-identification into the ambient environment of ABC will dramatically simplify and therefore facilitate access of enterprises and citizens to cross-border electronic public services.

5.11 Quality of life

5.11.1 Privacy

The impact on privacy is likely to be one of the most sensitive and complex to cope with as citizens and businesses struggle to comprehend and accept the new world of possibilities and constraints imposed by UDeID, such as sharply reduced opportunities to engage in a wide variety of interactions with other entities in an entirely anonymous fashion (also for national security and other security reasons).

The scope of impact is essentially that a great many transactions become no longer anonymous, with the added risk of traces and aggregations of such activities becoming track-able and storable; there are clear benefits to both businesses and administrations of having such new possibilities, but the threat to citizens is that they will lose control over their personal data, that information about them will be kept and used in ways they are unaware of or don't agree to.

Among the potential privacy issues and risks associated with widespread (i.e., sharply increased over current levels), are several well-known issues; the occurrence of inappropriate aggregation of private data (the big brother scenario), identity theft and its impact on the victimized individual, as well as the greatly increased risks of catastrophic events in the event of such identity theft by malicious persons. The key stakeholders are of course the citizens and businesses that will have to adopt eID, the others are people who have to accept liability for parasitic cases/scenarios. Another concern arising from ubiquitous deployment aspects are related to Ambient Intelligence (see below), where the very environment in which you exist can “spy” on you, by providing traceability of mundane data, such as ones location at any time of the day, and going further, ones actions.

Privacy is a highly sensitive issue in all jurisdictions of interest, although there are significant differences in culture and legislation, even within the EU, especially with regard to data protection. Some jurisdictions have quite stringent regulations in these areas, which highlights a key risk for cross-border transactions.

One of the key challenges of eID is therefore to make progress towards a common understanding of privacy needs and protections. As there are different degrees of privacy required in different contexts, a common effort to define privacy levels, and associated protections (analogous to efforts currently underway to define a common scheme for authentication levels), is one possible approach.

5.11.2 Ambient Intelligence

This is one of the most important transformative trends, in which the very environment that individuals and businesses exist within becomes radically different, unleashing many possibilities.

The central idea is that objects become relying parties that can offer “services” to eID holders¹⁴. These services could be either pre-programmed behaviours or tailored behaviours that are designed to cater to the specific needs of individuals.

One of the key ways in which a world with ubiquitous eID can be significantly different is that the general environment is enriched with intelligence so as to significantly enhance the everyday life and experience of individuals. The progressive diffusion of such intelligence into the environment, which recognizes individuals and consequently provides appropriately customized service offerings accordingly creates what at some point could be termed “ambient intelligence” (AmI).


Typical (abstract) scenarios involving AmI:

- AmI could carry out routine actions on behalf of the individual requiring a minimum of his involvement (such as arranging for payment of purchases, etc.) – just signalling assent.
- AmI can provide warnings to the individual

¹⁴ The concept wherein objects present in or embedded in the environment can themselves be holders of electronic identities is not within the scope of the current effort, but is mentioned as part of the reflection on the impact of long-term goals on shorter-term perspectives, and for the sake of completeness of the concept of AmI.

- AmI could provide targeted and customized commercial information, according to stated or implied preferences

Of course, the advent of AmI raises a host of privacy concerns which must be duly recognised and managed, and it is clear that concurrent with its introduction there need to be associated mechanisms for privacy and data protection, simple opt-out, and other controls that would allow the individual to adjust the level of his interaction with the ambient intelligence embedded in the environment according to his own preferences and/or comfort level.



6 Monitoring and evaluation

6.1 Purpose

Program monitoring involves the ongoing collection of data on implementation of the ELSA eID program to determine if programs are operating according to plan. The collected data will permit comparison of achievements with stated and desired objectives. It will provide valuable information for all stakeholders involved in the program, e.g. funders and overseers of the program, interested outsiders, and program staff and administrators.

Basic monitoring data serves a preventive maintenance function, by tracking indicators of critical elements that, if they deviate too much from the expected norm, signal a program problem. For example, if some metrics pass a warning threshold, immediate action may be required to stabilize the program.

6.2 Metrics

The set of metrics to be used are closely dependent on the details of the “plan”; more precisely the definition of metrics used for monitoring and evaluation will depend on the set of measures and instruments that have been decided to be deployed to implement the program has been more developed.

There have been some preliminary reflections on this issue. The following could serve as a starting point for discussions on selection of appropriate metrics, aligned with/linked to the overall program:

- Numbers of Users of eID (as counted/reported by issuers)
- Financial turnover of applications which make use of cross-border electronic authentication
- Savings made compared to the costs incurred by applications without eID

These will be difficult to measure, and more progress will be needed on the preliminary stages of defining a vision (with progress in the areas of architecture model and infrastructure characteristics) to proceed further.

6.3 Monitoring system

Due to the size and scope of the ELSA initiatives it is advised to establish an especially comprehensive and systematic monitoring regime to provide continuous feedback to those responsible for steering the program, as well as to stakeholders more generally.

6.4 Monitoring studies/evaluations

Monitoring studies should be initiated at predefined milestones in the programme, but may also be initiated on an ad hoc basis.

6.5 Case studies

Case studies should be used to develop best practice knowledge and understanding of what would have happened without the program.

7 Appendix

7.1 Terms and abbreviations

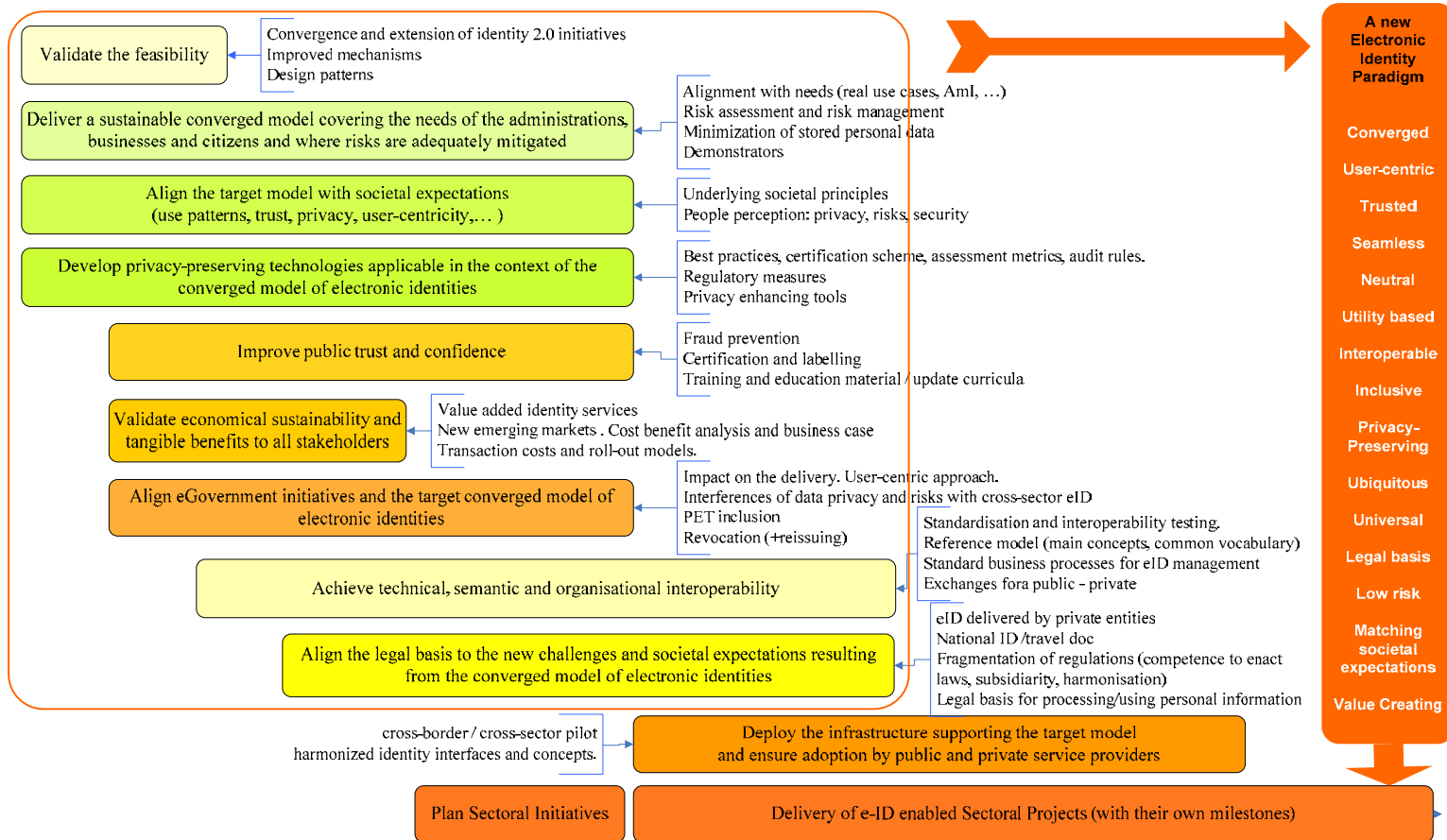
This table of terms and abbreviations is not meant to be exhaustive, or to serve as a dictionary on the subject. For any terms used in this document but not defined in this table, the commonly-used standard definition should be applied

Term	Definition	Source
Assertion	The identity information provided by an Identity Provider to a Service Provider	
assurance level	a quantitative expression of Assurance agreed between a Relying Party and an Identity Provider.	ITU-T Y.IdMsec
authentication	The provision of assurance of the claimed identity of an entity.	
Authorization	the granting of rights, which includes the granting of access based on access rights.	
Authorization policy	Assuming that an identity is authenticated, there is some formal or informal policy that permits or prohibits activity.	
Claim	An assertion made by a Claimant of the value or values of one or more Identity Attributes of a Digital Subject.	
Credential	Data that is transferred to establish the claimed identity of an entity.	ITU-T X.800 & ISO 7498-2
federated identity	a collective term describing agreements standards and technologies that make identity and entitlements portable across autonomous domains	
Entity	An entity is anyone (natural or legal person) or anything that shall be characterized through the measurement of its attributes. This definition is open to any type of person, including legal persons, but also to any other type of entity, such as objects (e.g., computers or other forms of machinery), digital resources or processes.	MODINIS
UDeID	Ubiquitous Deployment of Electronic Identities	
eID Infrastructure	A conceptual construct representing the set of different infrastructures that are required to support the provision of the eIDM-related services considered in the scope of the ELSA program; Functionally, it encompasses all the different elements that need to be in place to support the use of eID's as envisioned, including physical elements (terminals, tokens, telecoms, etc.), organisational elements (cooperation/collaboration structures, cross-border business processes, etc.), technical/design elements (interoperability, common/harmonized models, etc.), legal elements (appropriate agreements and other legal supports), etc.	
Relying Party	The party to an authentication transaction who is requesting the authentication of the user party as a condition to granting access to the service it provides	
IdSP	Identity Service Provider	
CSP	Certification Service Provider	

WSDL	Web Services Definition Language	
-------------	----------------------------------	--

7.2 Overview of work to be done

It can be useful to visualize the complete set of actions to be taken, over the long-term, and how they relate to one another, in diagrammatic form. The following diagram lays out different sets of activities and their relationships, on the way to achieving the final objectives for eID.



7.3 Impact analysis by EU Policy area

The following is an alternate approach to assessing the impact of eID. By considering the impact from the point of view of policy areas, we can analyze how policies can be created or adapted to both maximize and facilitate positive impacts and mitigate or prevent negative impacts through deployment of the different instruments available in each of the given policy areas.

7.3.1 Agriculture and Rural Development

The general requirement to equalize access to the benefits of UDeID could serve as a motivation / excuse for infrastructure upgrades in rural areas.

The internet of things and its impact on the agricultural sector is limited, but not non-existent.

7.3.2 Competition

UDeID will have a huge impact on competition; the transformational effects provide a great opportunity to level the playing field significantly, but this depends to a large measure on how the key technology is made available. If a sufficiently open approach to architecture, standards and technology is mandated, a much more perfect market for the knock-on products and services can be engendered. This suggests certain specific policy measures to mandate the desired level of openness.

7.3.3 Economic and Financial Affairs

Financial Services across the globe are already to a large extent automated and electronic, making full use of the possibilities afforded by electronic identities of various types. However, they still stand to benefit considerably from harmonization and convergence, as well as the increased trust and convenience afforded by true standardized and interoperable UDeID.

7.3.4 Education and Culture

Societal change of this scale will inevitably be reflected in fundamental changes in education. The computer revolution had the dual effect of expanding the IT-related curricula of high schools and universities as well as transforming education itself as the computer became an essential tool of classroom instruction in general, regardless of subject. The internet revolution had similar effects in education and UDeID will continue this dual-pronged trend, to a greater or lesser degree.

University

7.3.5 Employment, Social Affairs and Equal Opportunities

Expected to have a large net positive impact on unemployment, but the benefits may not be equally spread out, without concerted government action.

7.3.6 Enterprise and Industry

This has already been discussed heavily throughout this document, but heavy industry, such as manufacturing could experience some benefits to their assembly lines, distribution lines, and interactions with their suppliers.

7.3.7 Environment

The total, eventual impact is somewhat unclear. The long term effects of the ubiquity of electronic and wireless transactions at high bandwidth are a key consideration, and a partial unknown. Most believe current levels of saturation of populations by microwave radiation are still safe, but more research may be needed. The effects of an increase of several orders of magnitude in intensity as well as geographical pervasiveness (increasing the percentage of time that individuals remain exposed for significant periods of time) remain unknown, probably not good, but does merit much more in depth/intensive study.

In addition, the energy dimension must also be measured and weighed. A vastly expanded communications infrastructure will place significantly increased load on the transnational energy grid, which could lead to problems in meeting carbon emissions targets (Kyoto).

7.3.8 Fisheries and Maritime Affairs

The internet of things may have a positive impact on regulation of the fishing industry, by facilitating tracking of some aspects of commercial fishing-related activities.

In the area of maritime safety, the possible effects are quite similar, and range from the tracking of ships and persons, to the tracking of shipping containers and their contents.

7.3.9 Health and Consumer Protection

Both are expected to improve dramatically. With regard to consumer protections, the deployment UDeID in into (national and even transnational) food production cycles should

On the more mundane level of general health care for citizens, eID will facilitate health records access & use, accuracy, organization of efforts related to provision of any and all health care services.

7.3.10 Internal Market and Services

As already made clear by efforts such as STORK and various implementation efforts surrounding the services directive, UDeID will greatly facilitate perfection of the internal market as regards services.

7.3.11 Justice, Freedom and Security

UDeID should facilitate law enforcement efforts at all levels, for many types of crimes, as well as significantly aiding the fight against terrorism, both of which are enabled by the revolution in forensics brought about by and facilitated by eID. However this requires considerable research and a society-wide dialogue to arrive at a consensus and a 'balanced approach' to achieving the objectives while ensuring that citizens' privacy is well protected. net positive impact

7.3.12 Regional Policy

There may be regions that will be especially disadvantaged by the eID initiative. The existing mandates, mechanisms and regulations covering regional policy should be adapted to take into account this new dimension of assessing disadvantaged regions (including inputs on the uptake of eID, the mixture of active businesses in the given region and their relations).

7.3.13 Research

Obviously, due to the large number of unanswered questions on the details of widespread eID rollout, the initiative will be an enormous source of increased research topics & opportunities. EU policy should aim at identifying and prioritizing the different research topics in the area, encouraging the work, and channeling funds into the most urgent projects, assessing the results, etc.

7.3.14 Transport and Energy

UDeID will have a revolutionary impact on travel, especially international travel.

Logistics transport will also be greatly affected, due to increased and even real-time traceability of shipments, with little extra effort. Integration with other technologies such as GPS and GSM is also likely to occur and have further dramatic impacts.

The situation with regard to energy consumption is not completely clear. There will be of course a net increase in energy needs due to ubiquitous deployment, but these may be offset by efficiency or other gains elsewhere; further study required (see similar comments above).

7.3.15 Taxation and Customs

eID will have a revolutionary impact on Taxation and Customs systems as it is already a highly automated sector. Also, eID should be a strong impetus towards and facilitator of achieving single window environments, which has been a key strategic long-term objective in this sector of long-standing.

7.3.16 Information Society and Media

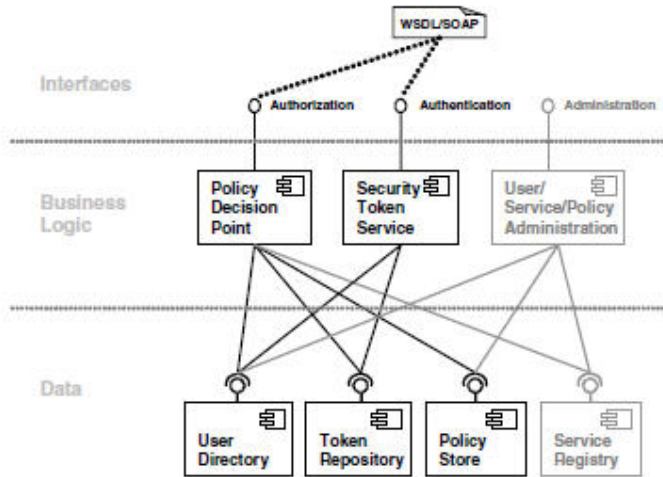
The impact is broad in a number of areas.

- The world of eID is a much more secure one. Security methods, tools and technologies will necessarily undergo great advancement
- Regulation for electronic communications – as there will be an enormous amount of traffic related to authentication flowing around when there is UDeID, there is an urgent need for updated regulation properly adapted to the new situation, addressing all the relevant issues, some of which are competing / conflicting.
- Audiovisual policy has been a key sticking point with AV policy in the internet age, as piracy has exploded due to the power of technology to violate intellectual property rights. Digital rights management regimes are not yet completely effective nor are they completely synchronised with societal expectations or supported with underlying legislation in all cases. eID for its part, is a facilitator of better, more efficient and more thorough DRM regimes, which will greatly benefit content producers, while bringing clarity to the situation.
- Major undertakings are expected in various relevant areas of ICT-related study & research, including new biometric technologies, how to integrate ICT into all or most processes, how to broaden access to ICT (“for all”)
- Public service reform – it has a huge impact here, as eID is a key enabler in the provision of pan-european public services; in many cases extensive re-engineering in the back-office is necessary to provide certain PEGS, and according to the EIF, eID is one of the first and most important Building Blocks (of type “Base Registries”) used to construct PEGS.

7.4 Service-Oriented architectural model for identity management

A leading contender for a globally-applicable architectural model for identity management is one which is service-oriented; this architectural model type conceives of electronic identity management as a set of identity-related services to be provided to providers of electronic services and their users.

The bare bones of this model can be depicted as follows:



The service architecture for electronic identity depicted above consists of three categories of services, whose implementation is separated into three logical layers. The top layer consists of these three well-defined and stable service interfaces to be used by other identity-user services:

- The authentication interface provides operations to authenticate a subject and issues a temporary security token to be used for further access control, thereby enabling single sign-on (SSO).
- An access control decision can be delegated to the authorization verification service.
- Management of users, groups as well as access control policies is done through the administration interface.

Behind the interfaces are depicted abstract representations of the necessary building blocks which implement these service interfaces, divided into Business Logic and Data layers, respectively. These abstractions explicitly allow for different types of implementations, possibly simultaneously.

In the business logic layer, a secure token service component performs the authentication of subjects and a policy decision point (PDP) component encapsulates access control decisions logic.

7.5 CEN TC224 : The “European Citizen Card” (ECC)

The European Citizen Card standard intends to provide some balanced solutions where both the legitimate concerns of the citizens for the freedom of use of his/her card and the control by the Government on the ID credentialing process are taken into consideration.

The consideration by the CEN TC224 WG15 standards (The “European Citizen Card”, ECC) of the ID Management issues as presented in the above sections is multiple. The ECC is defined as a smart card storing an ID Credential, issued under the authority of a Public Administration which may be used by the cardholder for secure access to e-Government services. Since the beginning of WG15 a concern was to make the ECC visible to the ID Management system in charge to verify ECC-stored ID credentials. The communication between the card and the e-Service Provider is achieved by establishing a connection between an Application resident in the Card and the so-called Client Application which is an agent of the e-Service. This interconnection of applications takes place through a standard middleware which is an extension of ISO/IEC 24727 tailored to the requirements of EU Public Administrations. One of the main principles for WG15 activity is to influence and converge with ISO standards.

This middleware is accessed through an API (Application Interface) of services. Through this API, the ID management system may retrieve an ID credential and also call for authentication procedures to be executed by the card. That way, the ID management, identifier the user, thanks to the data provided by the card through successive API calls. Thus the middleware and the card jointly constitute a true authentication system. This system is accessible through the API , which constitutes the logical interface between ID Management System and the Authentication System, meaning that this separation between systems is effective.

CEN TC224 WG15 has also provided a substantial effort so that implementations of the ECC standard be fully compliant with European Directives (Data Protection, Electronic Signature).

By its own nature, the ECC stores Personal Identifiable Information (PIA) and must comply with EU Regulation on the Protection of Personal Data . A liaison has been set with ENISA in order for WG15 experts to be fully aware of the technical implications in terms of ECC functionalities derived from the applicable regulation. In particular an objective for the ECC is to support cryptographic security mechanisms supporting those functionalities required to face the privacy threats identified by ENISA.

In relation with the European Directive, the ECC implements the IAS (Identification, Authentication and Signature) paradigm. The ECC authentication and signature mechanisms comply with EN 14890, and therefore complies also with the European Directive terms. This functionality is useful when the e-Service requires a formal proof of consent by the user with legal value

Because of the ECC issuance context, the e-Services to be accessed will in principle be in close relationship with the Public Administration Card Issuer. That means that at first sight the ECC is Issuer-centric. However when looking at the full set of mechanisms provided by the standard, this assertion is only partially true:

- The fact that the ECC only provides IAS services upon the cardholder authentication and therefore disclosure of Personal Identifiable Information is under control by the cardholder
- The ECC protects the privacy of the cardholder, due to the card capability to authenticate an external entity and then to create an encrypted communication channel
- The ECC cryptographic mechanisms enable direct authentication of a Service Provider provided that (1) this Service Provider is able to transmit a Card Verifiable Certificate format and (2) the ECC is aware of the Certification Authority that issued the Certificate to the Service Provider. This functionality may be useful when agreements are signed between the Issuer Government and Private Service Providers. On that edge, as an example ID Management Systems operated by Banks may accept e-ID Credentials issued by their Governments to

To summarize, the ECC standard accepts that all the requirements for an User-Centric pure approach (Section 1, §12) cannot be achieved when his/her ID credential is issued by Governments but tries to position anyway the citizen in the center of the system;

On that edge it is worth to mention that the new part of the ECC standard, ECC part 0, provides insight into a Federated Model for the ECC, which provides a solution when cross-border interoperability is required. Different system configurations ECC-compliant supportive of different business models may be considered there.

Finally notice that the same model has been proposed for the CWA e-EHIC (electronic European Health Insurance Card) for access to e-Health services. Common Infrastructures for ID Management may therefore identify users accessing either e-Government or e-Health services.

7.6 Report from the ELSA Thematic Working Group on electronic identity management 26 MARCH 2009

“TOWARDS AN ELECTRONIC IDENTITY MANAGEMENT INFRASTRUCTURE FOR TRUSTWORTHY SERVICES IN E-GOVERNMENT AND E-COMMERCE”

**Report from the ELSA Thematic Working Group
on electronic identity management
26 MARCH 2009**

Preface – European eIDM ambitions in the post-i2010 perspective

The present Working Group meeting was organized against the background of a new Communication being adopted by the Commission on 13 March 2009 on "A Strategy for ICT R&D and Innovation in Europe: Raising the Game"¹. A number of potential initiatives are being considered as focus points within this Communication, including the creation of a European electronic identity management infrastructure for trustworthy services in e-government and e-commerce.

A lot of work has been done in recent years in the field of electronic identity management, including through a series of research programmes and pilot projects, including the ICT-PSP large scale pilot STORK with a significant role. While each of these projects contributes new elements to the field of electronic identity management, it is also clear that the results will need to be developed further, refined and integrated.

In preparation for this meeting, a discussion document was disseminated on the need for a “multi-faceted electronic identification (eID) system for all citizens”, as a key enabler for trustworthy interactions between public authorities, businesses, citizens, and within the large spectrum of social networks and communities. This concept, which is also referred to as an ubiquitous eID infrastructure for digital life, is envisaged to offer a wide range of functionalities, including the provision of multiple identity instances, from government-accredited to commercially accepted, and ranging from near-anonymity to strong and unambiguous identification. Furthermore, the system should be user-controlled and privacy-protective, providing the basis for accountability and innovative applications in an open and competitive market.

European eIDM ambitions are thus high, and it is not yet fully clear how existing initiatives and projects can be integrated into a common vision, or what framework would be needed from a technical, infrastructural, organisational and legal perspective. There is a need for discussions and consultations to determine exactly what can be expected from a European eIDM infrastructure, what the approach and goals should be, and which steps need to be taken next to realise this vision. As a first step in addressing these questions, the Commission decided to organise the present Working Group meeting, bringing together a number of experts in the field of electronic identity management.

¹ See http://ec.europa.eu/information_society/newsroom/cf/document.cfm?action=display&doc_id=597

Introduction – Context and goals of the Working Group meeting

As a general introduction to the Workshop, the Commission first provided a short summary of its expectations and of the role of the present debates in ongoing European eIDM initiatives, against the backdrop of European innovative ICT policy. It was emphasised that these debates and the desire for a European eIDM infrastructure should be seen as a logical extension of ongoing projects such as STORK or PRIME, and should aim to build on the outcomes of these efforts. At the same time, the current discussions are also indicative of a change in policy that will require strategic thinking to move beyond traditional research to actual uptake of innovative ICT solutions.

M. Khalil Rouhana (Head of Unit DG INFSO) illustrated how eIDM fit into the broader European ICT ambitions in this regard. As noted above, a Communication was adopted by the Commission to establish a new R&D strategy for European ICT, as a follow-up to the Lisbon agenda (i.e. a post-i2010 strategy). This Communication addresses the Commission's main R&D objectives for the next period of financial perspectives (2014-2020).

Briefly summarized, this Communication stresses the need for Europe to increase its performance when it comes to the use of innovative ICT solutions, especially in the public sector. In a European context this emphasis on appropriate public policy is justified, due to the public sector's larger stake in GDP than in other regions of the world. To increase the use of innovative ICT solutions, three interlinked lines of action are proposed in the Communication:

- Raising investment in research and innovation, including through public procurements (especially in areas where Europe underperforms relative to the rest of the world);
- Improving the quality and coherence of our investment efforts, as there is currently too much fragmentation which dilutes the efficiency of our investments;
- Stimulating the demand for R&D, by opening up new markets for R&D to respond to real needs and challenges.

A set of measures for the public sector to achieve these goals will be proposed, including large scale actions that go from research to actual procurement and deployment, to ensure that R&D investments have a real impact in practice. This can build on existing building blocks that have already been used in Europe, such as Large Scale Pilots, Public-Private Partnerships and pre-commercial procurement of R&D – a concept endorsed by the European Parliament in 2008. One of these areas in which this approach will be applied is the deployment of innovative European eID solutions.

As regards timing and actual approach, the basic elements proposed in the Communication are scheduled to be in place by November. This will include a clearer description of the goals and steps forward, including planning for research, testing, and deployment. Realizations should materialize by 2014, and the Commission proposes to commit significant budgets (300-400 million EUR) to achieving these goals, in collaboration with the Member States and including via partnerships with the private sector.

Of course, the Commission is aware that input from key stakeholders and experts needs to be sought, to ensure that the general goals and plans espoused in the Communication are ambitious, realistic and in line with the state of the art. Part of this meeting is therefore dedicated to defining our eID horizon for the future: how far can we look ahead, and what is it that we hope to achieve?

Needs and objectives

After these introductory remarks and considerations, the meeting was chaired by prof. Reinhard Posch, who opened the discussions on the needs and objectives of a European eIDM system: what is it that we expect of something termed a “ubiquitous eIDM system for digital life”? What will the expected/desired impact be, and how far do we want to go?

As a preface to these discussions, the chair commented on the current general trends in information society services. After the development of basic internet services, service paradigms have moved on to web 2.0 services and are now shifting towards a cloud computing model. In this model, eID is often seen as one element of web services that needs to be able to integrate smoothly with other services. If this is to work in practice, a great deal of flexibility will be expected of the underlying eID infrastructure.

One of the first elements of debate in the group was the basic question of what constitutes an eID. This seems to be a very basic question, and a lot of research has been done on this point, but different perspectives can be taken, which will have a very significant impact on how a European eIDM infrastructure should be created. Key questions and goals discussed during the meeting – although not always ending in full consensus between the participants – included the following:

- The scope and meaning of ‘identity’ (at least for the purposes of a European eIDM infrastructure) needs to be made clear. Intuitively we tend to think of identity in terms of physical people. From an e-government and business perspective, legal entities are equally important however; and it is even possible to consider the broader notion of an identity of things/objects. The scope and definition of eID changes when we try to outline what we want to identify, and this is particularly important when examining semantics. Currently, exchanging electronic identity information is very complicated simply due to the lack of common semantics (e.g. even the simple notion of a name is interpreted differently from country to country).
- Related to this is the question of management of identities: who creates eIDs, and how are these managed? In reality, end users rely on a multitude of “partial identities” to represent or authenticate themselves in specific contexts, and it is unclear how this can be supported in a European eIDM infrastructure, or to what extent it should be. In order to address this question, it needs to be clear who registers and verifies attributes (if at all), and on what conditions these can be exchanged or re-used, or simply confirmed. Relying on market mechanisms to choose an economically optimal solution may not provide desirable results from a data protection perspective.
- Thirdly, an advanced identity management system needs to be able to manage links between entities. Simple examples include linking parent A to child B, or linking manager C to company D. Mandate management and role management is the main example of this. There is a lot of work still left to be done on this point: tools need to be created that allow users of a European model system to verify and manage such links.
- A fourth crucial element is the reliability of identity information, either in terms of being generally reputable (considered trustworthy) or in terms of real guarantees

(accountability in case of problems). The role of the public and private sector was discussed in this regard as an interesting example: ‘official identities’ or ‘formal identities’ are often issued or managed by the public sector, but this doesn’t necessarily mean that identification services provided by the private sector are less trustworthy or less usable in practice. From the end user’s perspective, functionality is more important driver than clear guarantees in relation to the trustworthiness of identity information, as can be seen in the increasing importance of reputation based identification (e.g. in social networks, which are largely based on establishing trustworthiness via peer-to-peer appreciation). From the service provider’s perspective, trustworthiness – especially in terms of accountability and liability – is much more important, and reputation as such may not hold sufficient appeal from this perspective. It has already been made clear in the past that future eIDM infrastructure in Europe should be multi-level, i.e. permitting varying levels of security/reliability. This is one of the key gaps that still needs to be filled.

- Functionally, it would be important to uncouple the provision of electronic identification or authentication services from specific applications. An ‘invisible eID infrastructure’ is key to creating an open eID model that could be taken up in commercial and public sector applications. In that respect European governance has the benefit of being conceptually based on a roughly “federated” model. A web of services is a model that plugs into this same concept of thinking: application independence (service-independence) of the eID infrastructure is important.
- There is also the question on whether a European legal framework, or at least European guidelines for regulations, is needed. This issue was raised in relation to a number of points, including the multi-level reliability issue addressed above: some participants felt that governments needed to set up the rules and regulations to issue/manage tokens/eIDs, preferably based on European guidelines. Currently, national legal barriers impede some approaches that are being explored at the European level; examples include the German ban against the intervention of intermediaries in the relationship with the public sector (including e-government services), which impedes the use of proxy based identification models; and the ban on using permanent unique identifiers for generic purposes in Germany and Hungary, which means that any European approach cannot require the prior existence of such identifiers. Guidance is necessary on what the consequences of European initiatives will be, and how we can operate within the limits of applicable laws, given the lack of direct European regulatory competence to harmonize eID regulations.
- Finally, the privacy and security aspect should take a central role. The point was made and discussed that private industry (on-line service providers, financial services, mobile communications, ...) does not have much of a problem in getting the identity information that they want and as reliable as they need it to be. But there is a significant problem from the opposite perspective: how do you empower users to enforce their rights and manage their data? This should be addressed in a European eIDM infrastructure as well, and this should be done soon; security and privacy protection cannot be taken up as an afterthought. Innovative systems exist in current research, but the infrastructure must be set up to implement this.

Collectively, the considerations above contain a good summary of what can be expected or should at least be considered as the needs of a European eIDM infrastructure (in no particular order):

- Clear definition of scope: what is the concept of identity that we want to address at a European level?
- Management of identity: which entities need to be involved in managing an identity, and what is their function?
- Management of relationships: how do entities whose identities are managed relate?
- Trustworthiness of identity: how can you trust the identity, especially in terms of accountability and liability?
- Identity provisioning in applications and services: how do you use identity in an application?
- Clear legal framework: how to regulate the use and management of identity?
- Privacy protection and secure identity management: how do you integrate users' rights into the infrastructure?

Of course, these issues will need to be iteratively refined in discussions over the coming months in preparation of the next Communication.

Possibilities for implementing the objectives

Having discussed the needs in relation to a European eIDM infrastructure, the meeting next examined how an infrastructure meeting these requirements could be implemented, taking into account the diverging and demanding needs in relation to such issues as identity re-use, tiered reliability and trust, private sector support, privacy-by-design and enforcement of applicable rules.

The first aspect extensively discussed in this regard was the strong role that innovative technologies could play in developing this infrastructure. Regardless of the preferred technology, any electronic identity management system is inherently dependent on the use of a secret in some form over another. There are already advanced identity management models in place that allow you to spread a secret robustly over many locations, and that allow you to limit the disclosure of identity information (such as e.g. IBM's Idemix or Microsoft's U-Prove). This allows you to increase security and reliability and improve data protection enforcement. Such PETs need to be developed and deployed further, and it needs to be examined in particular how take-up of such advanced models can be encouraged. The development of a business case around such models is crucial in this regard, as will be further discussed below. Finally, any approach taken at the European level needs to be sufficiently flexible to take up newer approaches to identity management that might emerge or increase in popularity, including e.g. identification based on biometric encryption (through local verification of biometric information) or mobile identification.

As a complement to the technological tools deployed, the architecture as a whole also needs to be designed to meet the objectives above. The role of validation services and proxy services was mentioned in this respect, as solutions that were currently being tested in STORK and PEPPOL, and that were also being examined by private sector partners. These approaches are appealing, as the main issue to be resolved here is to determine reliability/authentication levels at the European level; other issues could then be handled by

federating (i.e. managing them at the national level). However, other participants in the meeting rightly indicated that such solutions would need to implement strict safeguards to address privacy and security issues: it should be ensured that such solutions cannot become a single point of failure, and that they do not retain information on identity use; otherwise, they constitute a significant privacy threat. Other approaches should therefore also be considered.

Both with regard to technology and infrastructure, the importance of working with industry partners was generally recognized to be crucial. Public-private partnerships and systematic coordination with industry was seen as a key way of ensuring that any model adopted at the European level would also see substantial take-up in reality. It is necessary however to consider the different stakeholders, and particularly the different interests between eIDM users and eIDM vendors. Without a proper link to industry however, European initiatives risk remaining at the theoretical or pilot level, or seeing limited practical use. The integration of harmonized eID middleware implementations in existing operating systems distributed by major vendors was given as an example to be looked at. By harmonizing protocols, the integration and use of existing and new eID solutions could be facilitated to a significant extent.

However, measures to achieve the desired outcomes should not be focused exclusively on the technological and infrastructural aspects, but also on legal issues. There was some doubt whether European regulation was a useful (or even possible) route forward, given the fact that identity management is generally regarded as a national competence, but it was considered that guidance and support could be provided at the European level once an appropriate paradigm for an eIDM infrastructure was established. In the absence of direct European regulation, this could also take the form of regulatory guidance, model arrangements and agreements (as is e.g. applied in the banking sector, albeit based on a contractual hierarchical model), and support for existing and new standardization initiatives. Collectively, this might allow the creation of a consistent and complete European normative framework.

In addition to the technical, infrastructural and legal challenges, perhaps one of the most challenging issues is creating a model that has sufficient appeal to end users and service providers, i.e. ensuring that the European eIDM platform has real business appeal. To do so, we need to make sure that our own goals and expectations as described above match those of the stakeholders. For instance, while data protection issues and user control are societal needs that must be protected to safeguard our European values, end users' perceptions seem to be driven more by short term convenience. There may be a need to reflect on future needs and values in the discussion between experts and end users in this respect.

Naturally, we need to make sure that there is a real business model that makes sense to stakeholders. The example of banks was discussed on this point: even banks that could use a generic eID token (like a government issued eID card) are generally reluctant to do so, even if it would be more secure than their own existing solutions. At least part of the reason is that having their own solutions gives them full and exclusive control over the business model, and that their own tokens act as an advertising medium in a way that generic eIDM tokens would likely not be able to offer. Can this be addressed appropriately? This concern however would be completely different for small innovative service companies.

Globally, while there was a strong consensus on the importance of each of the aforementioned issues (technology, infrastructure, legal framework, business case), it was also felt that some additional research would be required to offer satisfactory answers that would allow the creation of a coherent and suitable European eIDM framework. The question was raised on whether an ‘eIDM research roadmap’ was needed, and if so, what it would look like. This is a complicated issue, due to the need to continuously take into account the changing eID landscape in each of the countries involved and in the eID industry. A flexible approach would thus be needed, with a strong emphasis on maintaining open communications with industry representatives.

Despite this complexity, if we want to go from research to implementation as envisaged by the planned Communication, we need to make sure that our knowledge of the eIDM landscape is complete, and research on a number of key issues still seems needed. Principally, the conceptual model behind the functionality that we are looking for is not clear: how can specific roles and responsibilities be defined and organized in a general eIDM framework, and how can the advanced technological options commented above be integrated into this framework? Secondly, the economics behind eIDM are not well understood, or more accurately: it is unclear how the objectives that we have envisaged above can be implemented in a way that is attractive for end users and service providers alike. Broadly painted, many service providers with an extensive customer base and the required infrastructure want cheap access to as much info as they can use, and end users are more interested in convenience than in security; at any rate, it seems unlikely that end users would be willing to pay a premium for security. It would be interesting to see if there are cases currently available that are supported by the market (as opposed to government mandate or subsidies), or what encouragement measures are being applied effectively to improve the economic appeal of electronic identities.

Apart from the concepts and economics, the issue of accountability was presented as an area of discussion. Electronic identity management is needed to support accountability, by giving the service provider a way to reliably link certain actions to certain users. Currently, this operates mostly within closed contexts: service providers can rely on electronic identities either because they issue or manage them themselves, or because they have a clear contractual relationship with the issuer of the credentials. Open eID infrastructures that are not limited to a closed group of service providers see much less uptake, and the issue of accountability plays an important impeding role here. This becomes even more clear when discussing whether private sector issued eIDs should be usable in a public sector context. While there is no objection to this in principle, there is still a substantial lack of trust and a real need for sufficient accountability guarantees.

In addition, as was also noted above, even if accountability from the end user is sufficiently guaranteed to the service provider, the inverse relationship (accountability of the service provider to the end user) is not yet guaranteed in practice; this is an aspect where further research or possibly regulatory guidance might be needed, including in terms of implementing real privacy-by-design solutions, to ensure that our envisaged European eIDM approach is sufficiently focused on the end users’ interests as well. In the same respect, the questions of usability and accessibility were raised: solutions need to be inclusive to all users. While a lot of research has already been done in this domain, there is a clear need to link this research to real results.

Globally, there was a consensus that new research would be needed to coordinate existing knowledge and know-how (which is already available to a significant extent in Europe) into a coherent vision. A comprehensive approach would be needed to form a coherent picture of how existing solutions and newer innovative approaches could be integrated into an eIDM infrastructure that supports the needs and objectives defined above. The issues of accountability, economics and inclusiveness were identified as key problems to be addressed in this research. Further efforts could then focus on creating the necessary components in a second stage.

Measures to consider

It is thus clear that future research will be instrumental in shaping the approach taken towards creating the envisaged ubiquitous European eIDM infrastructure. Specific tools are available at the European level to steer this research or to bring it to fruition, including through pilot implementations or actual deployment. Some possibilities to do so were already presented in the discussion paper disseminated before the meeting, and include public-private partnerships, pre-commercial procurements and Lead Market initiatives. The Commission confirmed its openness to suggestions for the most effective approaches.

However, there was a certain sentiment in the working group that defining the most suitable tools would be difficult as long as no clear concept or model for a European eIDM infrastructure was available yet. A number of interesting possibilities for moving forward were none the less discussed, including:

- Identification and dissemination of best practices in European eIDM initiatives, as is currently already being explored (e.g. through the eID Observatory);
- Collecting and disseminating clear overviews of the European acquis/state of the art in eIDM solutions, as a way of encouraging take-up of advanced solutions by currently less advanced market players and as a way of permitting frontrunners to explore innovative solutions more easily;
- Focusing on standardization efforts (e.g. standardization of interfaces) to reduce the complexity of the problems we are facing;
- Identifying and exploring innovative eIDM approaches, to determine which approaches are already being tested/implemented that could meet some of the requirements above.

These approaches are appealing, as they would allow progress to be made irrespective of the final outcome to be chosen. However, it is clear that a coherent model for a European eIDM infrastructure would need to be determined before the outcomes from these approaches can be leveraged fully, and that the full societal context needs to be considered, including the need for inbuilt privacy protection and security.

Anticipating the socio-economic impact

One of the main goals of the meeting was also to discuss the socio-economic impact of creating a European eIDM infrastructure, including in terms of financial gains and general benefits to all stakeholders.

From a macro-economic perspective, one of the first interesting aspects of this debate focused on export possibilities. The European approach to identity is rather particular, and reflects our cultural attitudes towards identity, data protection and privacy. The discussions above (including on technical, infrastructural and legal needs) reflected this: there is a desire to ensure that our eIDM infrastructure matches our cultural perceptions on these issues. While this European approach may not be universally welcome, it does open interesting avenues for exploitation. Some regions (including e.g. in Asia) have shown some interest in European personal data paradigms, and we should thus not overlook the possibility that the eIDM solutions developed in Europe could prove to be valued exports. Thus, from a macro-economic perspective, there appears to be a real potential for validation.

However, the micro-economic perspective must also be considered, and it was clear that on this point the socio-economic impact depends on whose interests you're considering (service providers, end users, or solution vendors). The return on investment therefore also depends on whose perspective you take, and one of the key complexities to be overcome is the need to make sure that there is a fair distribution of benefit; otherwise, the solution will not be taken up. This is linked to the business model question raised earlier: who is profiting from the infrastructure, and who is paying for it? These two aspects need to be sufficiently linked.

The meeting discussed billing of the relying party in an authentication process as an example of a business model. Such a model is not necessarily a best practice (or legally permissible in countries that require CSPs to offer free verification services), but it does illustrate the point: without a real business model that matches cost with benefit, uptake will suffer. The Norwegian and Swedish public sector examples were also discussed: in these cases, the public sector acknowledged that they wanted end users to take up eIDM, and that taking up part of the bill as a government was an acceptable cost of public policy. In contrast, in the UK initiatives relying on the users' willingness to pay for authentication certificates failed. This was acknowledged to be a key question: how do you model pricing and benefits to optimize uptake?

In that respect, it is clear that underlying costs that affect the price tag must also be acknowledged and accounted for. Liability is a key component of cost: during the discussions, Nordic approaches emphasizing trust were contrasted with other European approaches emphasizing accountability. While both approaches can function within their respective markets, interconnecting them will be quite complicated, due to the need to bridge this difference in perception of accountability requirements. Similarly, there is often a price to be paid for simplicity and accessibility: username/password systems may be easy and seem cheap, but when support costs for forgotten passwords are factored in, the picture may change. These elements also play a role if you want to accurately gauge costs and benefits.

Conclusions and wrap-up

After these fruitful discussions, it seems that there was a good consensus on the objectives for a European eIDM approached as commented in the first section above, and on the need for additional research on a number of issues, including on accountability, economics and inclusiveness. These should permit the creation of a coherent concept for a ubiquitous European eIDM infrastructure, suitable for adoption by public and private sector service

providers, and adjusted to the needs and expectations of the end users. The creation of an appealing business model that links costs to benefits will be crucial to ensure real take-up, keeping into account that both costs and benefits will have clearly visible and less apparent implicit components.

These issues will not be solved in the short term, and further reflection and refining of the positions above will still be needed to arrive to a clearer picture of Europe's post-i2010 objectives and strategies in the field of electronic identity management. The Commission acknowledged the importance of today's debates as a first step in this reflection process, and expressed its desire to organise further reflection group meetings, including through the i2010 Conference in Gotland. The Commission hopes to put forward certain key ideas at this time, building on the inputs provided in the discussion meeting today.

In conclusion, the Chair thanked participants for their inputs and discussions, and thanked the Commission's openness in organizing this debate.

Drafted by Hans Graux, acting as rapporteur to the European Commission

2 April 2009

7.7 Last meeting of the ELSA Thematic Working Group on electronic identity management

Following is the list of participants at last meeting of the ELSA Thematic Working Group on electronic identity management, held on 22 October 2009.

First name	Surname	Organisation
Miguel	Alvarez Rodrigues	Ministry of Public Administration, Spain
Bruno	Benteo	Eurosmart
Andre	Braunmandl	BSI
Guus	BRONKHORST	Ministry of the Interior and Kingdom Relations
Nils Inge	Brurberg	Nils Inge Brurberg: nib@bsk.no
John	Bullard	IdTrust
Danny	De Cock	COSIC, K.U.Leuven,
Bernhard	ESCHERICH	DIGITALEUROPE (SAP)
Alicia	GARCIA	ATOS
Lorenzo	GASTON	European Citizen Card - representing CEN
Hans	GRAUX	Partner - time.lex - information & technology law
Detlef	Houdeau	Eurosmart
Michael	KULBICKAS	TRASYS (Rapporteur)
Reinhard	POSCH	CIO, Federal Chancellory, Austria
Jim	PURVES	eDT - Transformational Government (CIT) - Department of Work and Pensions
Kai	RANNENBERG	T-Mobile Chair for Mobile Business and Multilateral Security at Goethe University Frankfurt
Stefan	Santesson	AAA-sec.com
Amardeo	Sarma	NEC
Jon	Shamah	representing EEMA
Max	Snijder	European Biometric forum
Marc	STERN	FEDICT
Thomas	WALLOSCHKE	Fujitsu

7.8 Stakeholder Inputs

The following sections of the appendix contain inputs submitted by the following stakeholder organisations:

- eID Vision Paper in association with EEMA
- EUROSMART
- DIGITAL EUROPE
- Standardisation Bodies
- STORK

INFORMATION SOCIETY TECHNOLOGIES (IST)



Vision Paper

European Electronic Identity

A new Pan-European Currency of Personal Identity

An introductory white paper written in response to {SEC(2009)289}: “A Strategy for ICT R&D and Innovation in Europe: Raising the Game”

This paper is a vision paper submitted to the European Commission (DG INGFO, ICT for Government and Public Services) for consideration, in the follow up of the proposed electronic identity management infrastructure of the European Large Scale Action.

AUTHORS:

**JON SHAMAH
GEOFF LLEWELLYN**

REFERENCE GROUP:

**ERIC BLOT LE-FEVRE NILS INGE BRURBERG
JOHN BULLARD ROGER DEAN
ALVIS ERGLIS DAVID GOODMAN
HANS GRAUX ARKADIY KRAMER
LORRAINE SPECTOR TOBY STEVENS
KEITH VALANCE**

IN ASSOCIATION WITH EEMA

KEYWORDS:

IDENTITY, DIGITAL SIGNATURES, NATIONAL ID, ID CARD, INTEROPERABILITY.

GLOSSARY:

CONSISTENT WITH STORK DELIVERABLE V6.0

REPORT NUMBER:

01 OF 01

REPORT CLASSIFICATION:

UNRESTRICTED

REVISION:

VERSION 1.01B

Abstract

A model describing eIDs infrastructure system as critical fully integrated components of society is described together with some of the building blocks needed in the short, medium and longer terms

TABLE OF CONTENTS

- 1. INTRODUCTION..... 4**
- 2. EXECUTIVE SUMMARY 5**
- 3. FUTURE VISION FOR EID..... 6**
 - 3.2. KEY ASSUMPTIONS FOR THIS VISION 7
 - 3.3. DAY TO DAY LIFE FOR THE CITIZEN..... 8
 - 3.4. THE DAY TO DAY CORPORATE ENVIRONMENT..... 9
 - 3.5. THE CORPORATE’S INTERACTIONS WITH MEMBER STATE GOVERNMENTS..... 9
 - 3.6. THE CORPORATE INTERACTIONS WITH OTHER CORPORATES 9
 - 3.7. THE INTERNET OF ‘THINGS’ 10
 - 3.8. GEOGRAPHY AND POLITICAL LIMITATIONS 10
 - 3.9. FUNDAMENTAL BARRIERS TO ADOPTION..... 10
- 4. NEEDS AND OBJECTIVES 13**
 - 4.1. SOCIETAL ASPECTS..... 13
 - 4.2. TECHNICAL & ARCHITECTURAL SOLUTIONS..... 17
 - 4.3. ECONOMIC ASPECTS 22
 - 4.4. POLITICAL ASPECTS..... 26
- 5. ROADMAP FOR ADDRESSING OBJECTIVES AND OVERCOMING BARRIERS..... 28**
 - 5.1. PHASE # 0: IMMEDIATE NEXT STEPS 28
 - 5.2. PHASE #1: SCOPING 29
 - 5.3. PHASE #2: ACCEPTANCE..... 29
 - 5.4. PHASE #3: PLANNING 29
 - 5.5. PHASE #4: DEVELOPMENT 30
 - 5.6. PHASE #5: FIRST ADOPTER PILOT TESTING..... 30
 - 5.7. PHASE #6: GRADUAL ADOPTION..... 31
- 6. TIMETABLE..... 32**
- 7. MEASURING THE IMPACT, MONITORING AND EVALUATION 33**
- 8. CONCLUSION..... 34**
 - 8.1. AUTHORS’ CONCLUSIONS..... 34
 - 8.2. AUTHORS’ SIGNATURES: 35
 - 8.3. REFERENCE GROUP..... 35
- 9. APPENDIX 1 - DETAILED BARRIERS & THEMES..... 36**
 - 9.1. SOCIETAL..... 36
 - 9.2. TECHNOLOGY 36
 - 9.3. ECONOMIC..... 37
 - 9.4. POLITICAL 37
- 10. APPENDIX II - THE INFLUENCE OF ORGANISATIONS ON OVERCOMING BARRIERS..... 39**
- 11. APPENDIX III – EXISTING INITIATIVES 40**
 - 11.1. EEMA 40
 - 11.2. STORK 40
 - 11.3. BBS GLOBAL VALIDATION SERVICE 40
 - 11.4. BANKID 41
 - 11.5. AUSTRIAN EID 41
 - 11.6. IDENTRUST..... 41
 - 11.7. TIME-LEX..... 41
 - 11.8. ENISA 41

11.9.	PRIMELIFE.....	41
12.	REFERENCE GROUP BIOGRAPHIES.....	43
12.1.	ERIC BLOT LE-FEVRE	43
12.2.	NILS INGE BRURBERG.....	44
12.3.	JOHN BULLARD	45
12.4.	ROGER DEAN	46
12.5.	ALVIS ERGLIS.....	47
12.6.	DAVID GOODMAN.....	48
12.7.	HANS GRAUX	49
12.8.	ARKADIY KRAMER	50
12.9.	LORRAINE SPECTOR	51
12.10.	TOBY STEVENS.....	52
12.11.	KEITH VALLANCE	53
13.	REFERENCE GROUP MEMBER POLICY STATEMENTS	54
13.1.	ERIC BLOT LE-FEVRE	54
13.2.	LORRAINE SPECTOR	55
13.3.	HANS GRAUX	56
13.1.	NILS INGE BRURBERG.....	57
14.	APPENDIX IV - BIOGRAPHIES OF AUTHORS	58
14.1.	JON SHAMAH	58
14.2.	GEOFF LLEWELLYN.....	59

1. INTRODUCTION

The deployment of electronic identity (eID) credentials, across Member States is inevitable – the logic of so doing is as strong as that for a common currency because it provides a shared framework of identity attribution and identity assertion, which is as important as money. Indeed, since most money in circulation today is actually credit, which is intimately associated with the creditworthiness and identity of the individual, the issue of identity is of increasing significance to the working of the economic system. Just how that will be seen by the average individual and how the individual's life will be shaped by this is difficult to predict. Different historical and cultural backgrounds of the Member States give a very different context for “ID Cards” – with the UK and Belgium probably marking the extremes of acceptance of the concept. However by envisaging potential outcomes of the process, an understanding of what steps need to be taken, socially, technically, economically and politically can be achieved.

To avoid any doubt, it should be noted that the use of eID is for the moment intended to be optional and left to the initiative of each citizen, and that eID should not be considered synonymous with electronic national identity cards which are subject to the respective legislation of the Member States.

2. EXECUTIVE SUMMARY

This document outlines a possible scenario wherein eIDs are a critical fully integrated component of society and describes what is needed to achieve that in the short, medium and longer terms. It assumes that the use of Government issued National IDs, electronic or otherwise, to provide a trusted projection of the individual into the private electronic environment is generally considered to be unlikely to be universally adopted by Member States.

That notwithstanding, an eID that is recognised as valid and trusted by each Member State is an essential measure for the interoperability of transactions between people using different service providers who may be located in different countries. This ensures security and legal value of any transaction or action. In banking, a digital identity depends on a single, relatively closed security system, taking the form of a personal contribution of money, which is enough to establish trust. But in an open, multi-interest world, with the fight against money laundering, and where 80% of payments are computerised, the absolute recognition (both legally and evidentially) of a digital identity should be agreed by all parties to the transaction.

This document looks at the steps needed to be taken, and the practical barriers needed to be overcome to adopt privately operated and self-funded eIDs that are truly interoperable across all of the European Union and use National Registries only to establish a fraud-free enrolment and a framework of trust.

Public trust in eIDs is encouraged by formally incorporating ethics and privacy considerations throughout every phase. This is re-enforced by a strategic educational program in each Member State.

Similar privately operated eIDs schemes, such as BankID in Norway, are already in their initial stages of use and can be used as models on which to base this much broader vision. It is suggested that operating consortia will include participants from banks, insurers, credit agencies, and telecommunication providers, who would also assume liability for failures.

This document draws on the views of a broad-based reference group comprising individuals who are subject matter experts in the various subjects identified in this paper as being major factors for success.

Immediate next steps, a potential timetable and thematic packages with outcomes are described, leading to full adoption in Member States by the year 2030.

3. FUTURE VISION FOR eID

Despite popular belief, ours is not yet the 'New Internet Society'. The first decade of the 21st Century is one of transition from a society being populated by a majority of adults who were born in the early stages of the 'Computer Revolution', to one where the entire population have never experienced a world without near instantaneous communications and messaging.

To this new generation, the so-called 'digital natives', who will be the 450 million adult decision makers of 2040, the internet will be as familiar as television is to us; the high-street will seamlessly extend into their homes, and socialising will be conducted largely electronically, with geographic location being of little relevance.

The new generation will be the first to have computerised exchanges with no paper records of the transactions or conversations. But trust and legal proof cannot be established and guaranteed systematically by trusted third parties until eIDs are universally accepted and trusted themselves. What is important in this new environment, is knowing that each citizen shall have, as in the banking network, an eID service provider (IdSP) which guarantees its digital identity and the certification of the trust (according to a scale of probative value) for all transactions with counterparts. That trust must be underpinned by a liability framework in which every provider and user of the service understands the contractual obligations to underwrite the service in the event of fraud or failure.

Hundreds of thousands of companies and their activities will also reflect this extension of society to the virtual world. Electronic communications are already replacing traditional postal methods for delivering orders, invoices and notification of payment.

These communications are quickly becoming legally enforceable and trusted transactions, representing a growing value and their use is also spreading to small and medium sized businesses of all kinds.

In the financial world, Single European Payments Area (SEPA) is an extension of the trust chain combining a management mandate and collateral or underlying commercial transactions with the payment. Therefore in certain commercial situations it may be unnecessary to have two systems of trusted digital identity, but only one, common to both financial and informational needs.

This vision does not preclude other secure added-value networks which will provide services to guarantee the value of commercial and financial transactions for particular closed communities of interest.

Trusted transactions and their certification with eIDs will enable us to link operations much more quickly and in total security: for example, orders, invoices, credit, transfer of funds, etc. It is expected that interactions between citizens and legal entities with perfect remote identification and trusted transactions (together with archiving and conservation), will make it possible to reduce operating costs by operational risks substantially¹.

- 3.1.1. As this 'Internet Society' grows and establishes itself as the norm, driven by a generation who communicate with Facebook and SMS, and who appear willing to determine trustworthiness on the basis of peer-to-peer communication and reputation, how can society ensure that traditional certainties of identity and authorisations be maintained so that commerce and interactions are not blighted by a super pandemic of identity fraud and impersonation?

With those same individuals growing up into a borderless European Union with a single market, should they not expect that their individuality, as expressed via the prevalent communications technologies, be inviolate and secure?

It is the obligation and duty of the European Union to guard against factors that will retard and degrade our hard earned unity. An interoperable Identity Standard is one of the tools that must be used. Whether it is owned and operated by the Public or Private sectors remains to be determined but will be a critical element of infrastructure.

Common agreed standards for eID are a prerequisite for transactions to be trusted either legally or financially, at least in a professional or business context. All citizens and legal entities seeking to protect themselves against errors and fraud, require a secure guaranteed service suitable for all their transactions. The accreditation of the legal trusted value of digital identities, digital documents, documentary and financial correspondence and the electronic archiving of their proof, shall save the administrative costs of management, support, disputes, transport, postal fees, etc., for both individuals and legal entities.

3.2. Key assumptions for this vision

- 3.2.1. Whilst detailed technologies will undoubtedly change and evolve, there will be no fundamental disruptive innovations at a very high level.
- 3.2.2. Within the next 10 years, it is unlikely that there will be harmonisation of National eID credentials between all member states. As the EU enlarges this situation will become entrenched as even more national credential schemes are forced to show return on existing investment and there is no framework for a 'Top-Down' initiative similar to HSPD12² in the United States.

¹ "e-Invoicing and e-Archiving - taking the next step" - PricewaterhouseCoopers 2005

² See <http://hspd12.org>

- 3.2.3. Member States will generally be reluctant to accept any liability for transaction errors arising from authentication or authorisation which utilise a National ID registry at any point in that transaction. This has proven to be one of the key inhibitors to the adoption of government-issued eIDs, whereas schemes such as Visa have seen global uptake because they are built around a robust and trusted liability model.
- 3.2.4. Member States will generally be reluctant to share chip-space or credential visible ‘real-estate’ with the private sector on their National eID cards, thus leaving a gap in the market for alternatives.
- 3.2.5. Deployments of National eID credentials or the construction of National Identity Registers will become accepted throughout all the Member States (whilst acknowledging that the nature of those Registers may vary to comply with national constitutions and local cultural tolerances).
- 3.2.6. In the current technological environment, an interoperable eID will need, in the majority of cases, to be implemented through a ‘chip card’ as well as other forms to aid portability of the credential and associated information. This is reiterated by regulations such as those laid down by the International Civil Aviation Organisation (ICAO) for card standards³.

3.3. Day to day life for the Citizen

The case for implementing eID is compelling for the citizen. As geographic boundaries become increasingly administrative rather than national or cultural, services will be supplied and consumed without geographic consideration. The citizen will interact with any government or private service from any Member State, from any location, transparently with language options defaulting to the language of citizenship. The need for this is already being realised as people often may live in one country and commute to another for work.

Examples:

- 3.3.1. A Belgian Citizen using a Belgium eID as a breeder enrolment document as part of ‘Know Your Customer’ procedures (i.e. anti money laundering controls) to open a Polish Bank account while on holiday in Spain.
- 3.3.2. A Latvian holidaymaker using their eID in Italy, to verify their age in order to enter a nightclub.
- 3.3.3. An English citizen obtaining an eID card from an Austrian Identity Service Provider, and using the UK Government Gateway as the Identity Breeder.

³ “Machine Reading options for td1 size Machine Readable Official Travel Documents”
Published by authority of the Secretary General; ICAO/NTWG Sub-Working Group For
New Specifications Td1 Card

- 3.3.4. A first aider in Hungary using a Dutch accident victim's eID to obtain the medical information at the scene of an accident in Germany. Also the first aider would be confirming qualifications to the German Authorities.
- 3.3.5. A teaching permit in France being issued to a UK citizen after a police criminal record check against the UK National registry or an eID.
- 3.3.6. An employee of a French company purchases hardware over the internet from an English computer hardware company which is installed by a Portuguese service company with its subsidiary in Lisbon, remembering that the hardware is leased through an Irish company.
- 3.3.7. An EU citizen who has lost their credentials whilst travelling and using an eID to recover them.

3.4. The Day to Day Corporate Environment

- 3.4.1. A first-time visitor to a customer's office presents an eID which is 'linked' via an identity application (contracting to the IdSP) to the visitor's employer with role attributes. The customer's Physical Access System and ID badge system matches the visitor to a booked visit and issues the badge with appropriate privileges in the secure knowledge that the visitor's ID, status and employer were all accredited with the application provider.
- 3.4.2. A corporate employee in the treasury department can access the e-channels provided by each of the banks with which the company holds accounts, using a single eID to authenticate and sign transactions on behalf of the business.

3.5. The Corporate's Interactions with Member State Governments

As a further assertion of the "Single Market" and Service Directives, – Corporate registrations being recognised across the EU enabling cross-border activities to be fully transparent.

- 3.5.1. A Corporate HQ engages a workflow with touch points to government agencies in multiple Member States using a single corporate eID issued by a certified chamber of commerce.
- 3.5.2. European companies also have subsidiaries in all countries of the Union. Companies like VW, British Airways, or Accord, have more than a thousand subsidiaries in the Euro zone. The reality of the European Union is that cross-border trade and financial flows continue to grow.

3.6. The Corporate Interactions with other Corporates

- 3.6.1. eSignatures on contracts using contractual frameworks aside from Digital Signature laws at Member State level to engage in e-procurement.

- 3.6.2. There is an important historic role of Contract Law which is applicable in any transaction, electronic or otherwise and which relies on privacy, authenticity, integrity and non-repudiation regardless of geography and is particularly relevant cross-border. Closed communities have already been formed, such as Exostar for the defence and aerospace industries, where trusted environments have been formed for the exchange of documents and project collaboration.

3.7. The Internet of ‘Things’

- 3.7.1. The use of eIDs need not be restricted to citizens or corporates. The identification, authentication and attributes of animals, devices, products and other objects can also be incorporated into the vision. IdSPs may grow up which specialise in this form of identity, as well applications and appropriate regulatory environments. Individuals may wish to delegate aspects of their credentials to devices or avatars; for example to authorise a computer to automatically order groceries when needed.

3.8. Geography and Political limitations

- 3.8.1. This is not a just a Pan European issue. In reality in order to survive and prosper, the citizens and businesses located in Member States will have relationships, both private and commercial not only locally, across Member States, but also globally and therefore interoperability criteria should take other initiatives around the world into account. International standards bodies, such as the ITU should be consulted to determine how interoperability might be extended outside of the EU

3.9. Fundamental Barriers to Adoption

More detailing of barriers to adoption can be found in Appendix I.

- 3.9.1. Privacy: Who owns an identity? – The Concept of Choice.

The concept of identity ownership has to date, not been investigated sufficiently at the practical level. To the average citizen in any democratic country, the attributes and details of one’s life are deemed to be personal and owned by the individual, yet this is not clearly stated in European law. This can lead to resentment when Government or Industry use this information without the permission of the citizen. There is a misunderstanding regarding which attributes are owned by the consumers of those attributes and which are owned by the associated individual, due in part to the vague distinctions and frequent conflicts between concepts such as data ownership, data subject rights, privacy and confidentiality obligations, and intellectual property rights

Given the emergence of electronic transactions with real value, financial or otherwise, the responsibilities and roles of service providers on which the trust, certified value and interoperability are based needs to be carefully defined.

The concept of the ownership of credentials requires trust in the service provider who guarantees the protection of the personal identity attributes. It also requires sealing authority and management mandates to compose, send and archive attributes and person data on the citizen's behalf.

Banking secrecy prevents banking operators from revealing the identity and attributes of their customers, outside of the strict framework of monetary operations. Similar secrecy for transactions or civil and commercial correspondence should prevent service providers from revealing the identity and attributes of their customers, outside of the strict framework of their operations. For a more effective choice, service providers may specialise in providing services in specific sectors such as health, education, business, etc., where they may believe that their branding will provide additional levels of confidence for the citizen.

For interoperable eID to succeed, participating nations will require coherent constitutional (or equivalent) protections over how credentials and registry information are used and protected.

3.9.2. Identity as a Threat

The spectre of 'Big Brother' looms over all attempts to bring eIDs to the Citizen⁴. A fear of the centralisation of data and utilisation of that data in a way that is to the detriment of the Citizen is both rational and understandable to us now.

However in the New Internet Society, that fear will be unknown. Already children are apparently carefree with their personal information in a way that adults are rarely seen to be, publishing personal data on websites regardless of security protocols. This lack of concern – at least in the way that adults understand it - needs to be better understood by policymakers to avoid a slide into an explosion of freely available personal data which could be exploited by both future unscrupulous governments and criminals. This would have an effect of retarding growth and reversing the gains already made.

Part of the interoperable infrastructure must comprise of safeguards that are constructed as an integral part of the technology to prevent losses of privacy, and also to provide security against theft.

Insofar as specifications for service providers will be produced as cautiously as for banking operators, and by their accepting to specialise, risks may be minimised. In addition, a critical and well informed user population is needed, as they will increasingly need to be able to distinguish reliable from unreliable data sources. While technological progress can support and facilitate decision making in this respect, it can never fully replace it.

⁴ Martin Aaron K., van Brakel Rosamunde E. and Bernhard Daniel J. (2009) "Understanding resistance to digital surveillance Towards a multi-disciplinary, multi-actor framework, Surveillance and Society" 6(3), 213-232

Currently trusted market sectors such as Financial Institutions could play a strong role in assisting the citizen in acceptance of eIDs as has been seen in Norway and Sweden⁵. Additionally the financial institutions in both countries already have a strong measure of regulatory control.

Legislation and good practice is not enough. It can be changed or ignored. Privacy and security must be built-in technologically so that it is as integral and essential as any other component and cannot be circumvented by failures in the legal process.

3.9.3. Utilisation of National eIDs for non-Government Business

Many governments, such as UK and Norway are choosing to restrict their National eID credential to ICAO functionality only and attempting to avoid liability for any losses to 3rd parties by specifically declaring that the credential should not be used outside of state-related activities. Nonetheless in the absence of alternatives these credentials will be utilised elsewhere as forms of trusted identification. This is evidenced in the UK where the UK Passport is the most trusted identification credential in use, despite being based on the ICAO standard.

From the private sector's viewpoint, the physical 'real-estate' and regulatory formats on the visually readable surfaces of credentials limits the branding opportunities available, provided that governments would even be willing to allow this. The third party application operator becomes just another anonymous use of the National Identity Credential.

It therefore may not be in a Government's or business's interests to utilise the National Identity Credential as an eID for third party use for all applications. However this document does not preclude a government agency becoming an Identity Service Provider (IdSP) itself, as one among many IdSPs. This will ultimately become a citizen choice as which IdSP to use, and a Government's choice as to whether it should seek involvement in non-eGovernment interactions.

⁵ Sources: BankID Sweden (www.bankid.com) , BankID Norway (www.bankid.no)

4. NEEDS AND OBJECTIVES

The needs and objectives of this vision can be classified into four thematic areas that might form a basis of future work. The lists below, together with the points in Appendix I present a non-exhaustive list of issues that must be addressed. These thematic titles are meant to assist in the consideration of the much larger number of issues that will emerge as the vision becomes reality.

4.1. Societal Aspects

4.1.1. Ethics

In any voluntary transaction regardless of context and value, the citizen needs to be assured that his interests are served and are of importance to the service provider. Even in a straight forward purchase, the citizen must trust that the provider is obligated, either through regulation or code of conduct to honour the transaction and associated processes. When that trust fails, citizens will usually not transact. This is one major aspect of brand management and can be clearly demonstrated by the growth in use of organisations such as Visa, where their intermediation between the retailer and consumer means that purchases are made with confidence, knowing that liability to the consumer is with Visa, not the retailer. This has enabled retail internet transactions to grow substantially.

In a large complex project such as the eID, the measurement of trust for the citizen is difficult and the issues may be too complex. Yet the transactions can be of vital importance to the citizen. Re-assurance is required and knowing that the citizen's interests are pro-actively considered from the earliest stages of design will provide some assurance.

There is a unique opportunity to incorporate a solid ethical underpinning in all aspects of the eID. Possibly for the very first time in a major societal infrastructure program, each service provider, component and process could incorporate an ethical check to ensure the highest standards are established from the outset – not as an afterthought. These would need to be continually monitored by an independent body.

This high ethical stand would assure citizens of ultimate 'fairness' in dealing, required for entrusting service providers with storing and releasing personal data and attributes. It is important to note that this stand may also necessitate the exclusion of certain National ID schemes or commercial services where they are deemed to fail to meet necessary standards of liberty, privacy and trust. These will be difficult decisions and will require considerable investment in the establishment of the ethics body.

This common ethical standard would provide a fresh yet pervasive cultural and legal bond between European states. Additionally this ethical stand would be a signal to other societies globally that Europe intends to lead in aspiring to the highest standards of public service.

4.1.2. Universality

eIDs will need to be accepted wherever they are presented within the European Union and eventually beyond. This has implications on both the electronic design and appearance. Because they are to be used in a variety of circumstances and locations, the principle of minimum disclosure⁶ must be practised and printed/stored data should be limited.

However balanced against this is the ability to use the credentials in off-line, near-off-line and non-powered environments. Informed public debate should be commenced to establish an acceptable balance between privacy and usability as is already emerging in the case of ePassports.

The IdSP should assume its obligations in the same way as a bank in this field.

There needs to be an agreement between citizen and service providing agreed security and compensation measures. Each IdSP may will be able to connect to one or more applications services specialised in a professional or economic activity and generally capable of performing operations for exchanges, correspondence and transactions.

The higher the level of security established at each counterparty's eID service provider, the easier the dematerialisation of correspondence and archiving.

Credentials may take the most appropriate form depending on their use and personal preferences: for example, a chip and PIN card, certificate embedded in a mobile phone, laptop or computer. Each citizen may hold their credential in many different form factors.

4.1.3. Inclusivity

eIDs must address the needs of all groups and subgroups in society, even the most marginalised. The availability of these must be funded by government to ensure that all sections of the population within their jurisdiction are provided with credentials.

Efforts should be made to address 'hard-to-reach' communities who may be fearful of government issued credentials. These are often the people who are not 'citizens' and have no trusted breeder documents to gain an eID. Inclusivity MUST mean no barrier to entry – anyone can enrol without providing documents, entitlements can be awarded later when they

⁶ "Privacy Features of European eID Card Specifications", ENISA Position Paper, Ingo Naumann, Giles Hogben, Date: 27/01/2009

have been reliably established. Consideration should therefore be given to the method of distribution of eIDs and their marketing to various groups.

Any aspect is the empowerment of non-EU citizens that may be residents or visiting a Member State. Even though eIDs will not be compulsory, accommodation of this community must be considered.

4.1.4. Individuality

Independently of governmental authorities which may establish very strong National Identities or not, with a card including a photograph, biometrics and a personal signature, certain communities may wish to organise themselves by organising their own enrolment, their own conditions of registration appropriate to the social context. Assurance that all operations in this community will be secure, trusted and interoperable might be through strong certification by an independent inspection and accreditation body.

An example of these communities could be the populations that annually migrate between Finland and Norway.

Alternatively, and significantly easier, they may wish to use an affiliate mechanism, where the external branding of the credential may convey a specific message.

4.1.5. Accessibility

It is assumed that the reach of the internet to the citizen will be near total within the next three decades, but the small minority that will not have access to the internet will need to have access to public services that will develop exclusively as web applications. For those that require public service internet terminals, security and confidence will need to be assured in order to overcome the possibility of the theft of identity details and attributes. This is an area where banks, with their network of ATMs may be able to be extended and utilised. A complementary option would be public terminals or kiosks under some kind of acceptable supervision. Early discussions with financial institutions and local government bodies will therefore be essential.

Roaming use of the Internet is increasing rapidly with the widespread coverage of wireless broadband and the increasing use of the mobile phone to interact online and conduct business. The ubiquity of the mobile phone indicates that the mobile operators and equipment suppliers will have a strong role to play in providing both access to services and dictating form factors for credentials.

4.1.6. Resilience/Availability

Because of the need to operate in environments where communications and readers may not be present, basic authentication is needed on the credential. Presently the standard card with a photograph is the only form

factor that can meet this requirement, but others may be developed over time. Minimum guidelines for information availability and operation in diverse circumstances will need to be established. These could include contingencies such as local failures of Critical National Infrastructure and should take into account not only application services but also enrolment processes.

4.1.7. Acceptance & Education

Key to the success of any eID program will be the general population accepting and embracing eID credentials as an integral part of day to day life, and this in turn will require investment in education and awareness. One aspect is the wealth of applications taking advantage of eIDs available early on in the deployment. This is discussed elsewhere in this document.

Privacy and security are the cornerstones of any eID, however there will be an increasing exposure of the population to on-line activities. Education focussing on the responsible management of personal information and the divulging of that information (either directly in an ad-hoc fashion or using eID applications) should be encouraged in all Member States. It is proposed that educational programs in each Member State should be funded and recommended to be included in respective national curriculums to prepare for the eID environment. The content of these programs need to be developed in a consistent and complimentary fashion, although localised to accommodate cultural differences.

An integral part of the educational process should be to encourage high standards of integrity and honesty in all the service providers and to publicize their processes of accreditation, ethical auditing, legislation and regulation.

4.1.8. Marketing and Public Perception

Successful campaigns in Belgium and Estonia show the way forward as to how long term marketing can be used to promote acceptance. Similar long term campaigns could be used to prepare Member State populations. The content of these campaigns need to be developed in a consistent and complimentary fashion, although localised to accommodate cultural differences.

4.1.9. Co-ordination

Because it is to be expected that take-up of eID will occur over an extended period of time, there will be a need to plan a consistent long term and pan-European message. As with the current techniques of addressing re-cycling and environmental issues, inducements can be offered to Member States to co-ordinate their activities. The long term planning and ongoing co-ordination function should continue to be the responsibility of the European Commission, structured in a way to maintain continuity.

4.2. Technical & Architectural Solutions

In order to address the barriers to adoption, there needs to be a fundamental review of the role of Governments in any proposed new identity process. This review should take into account the issues raised in section 3.9 of this document.

The solution of a security and trust infrastructure should be relatively inexpensive, highly flexible, open-ended and available to all.

Already there has been considerable action at the periphery of the European Union. Both Norway and Sweden have decided that while they have National Registries uniquely identifying the citizen, the costs to fully deploy a single credential to act as a combined National ID credential and eID would be prohibitive.

As a result, the private sector has already issued eID credentials utilising a National Register of citizens as an identity authority “breeder”. These credentials have become the defacto identity credentials in the respective countries. The predominant scheme is called “BankID” and is sponsored and financed by a consortium of all the major banks in the region. Through private operators jointly owned by the banks, over 5 million credentials have already been issued to their customers. (These operating companies: BBS in Norway and BGS in Sweden may provide a model for wider adoption)

There are also alternative providers in addition to the above that also issue eID credentials. In Norway “BuyPass” is operated by the Norwegian National Lottery.

In Norway, while a number of applications have been developed to utilise BankID and BuyPass, the large scale use of the eIDs remains financially orientated. The success of BankID and BuyPass for public sector applications has in turn diminished the need for the deployment of a National ID Credential in Norway. This credential is only now being considered for issuance and eventually may only serve as a “light” version of the ePassport, with only an ICAO applet for travel within the European Union and Nordic nations.

This model of utilising national identity registers by organisations in the private sector as an ultimate reference identity to generate new eIDs for use by citizens may be considered to be a strong argument in favour of the study of the problems raised above.

4.2.1. Delivering Identity as a Choice

The situation in Norway whereby a citizen has a choice between two suppliers of credential derived from (or “bred by” the National ID), points to a possible model for wider adoption because:

- 4.2.1.1. *The citizen retains a choice of Identity Service Provider and is not obliged to use a State-issued credential, nor unnecessarily to share information with the State.*
- 4.2.1.2. *The citizen determines which attributes are disclosed through the chosen supplier.*
- 4.2.1.3. *The citizen retains the ability to alter the range of attributes and to opt in or out of uses according to their own preferences.*

Under this model, there could be a number of operators – which could each be termed as an “Identity Service Provider” (IdSP) - that would be offering eIDs based on the citizen’s National ID being part or all of the enrolment process. The process of “breeding” a new credential from a National ID would be through a one-way algorithm which would prevent backward tracing of the National ID from the new credential. In this way the new credential would inherit the status of the original National ID without presenting any risk of compromise of the privacy of the original.⁷ Each IdSP could be either a private company, from the public sector or a private/public partnership and could offer levels of liability, opt-in/out capabilities and ‘affinity’ credentials to personalise the identity, in a similar fashion to the current EMV (Europay, Mastercard, Visa) market offers.

This corresponds approximately to the position of the IdSPs, insofar as their functions enable them to establish the link between their affiliates and the document management or transactional operators to provide services with probative value for documents or transactions carried out and their interoperability.

Any other trust model is likely to be ineffective in overcoming all problems and in protecting the freedom and flexibility which all those involved require.

These organisations could charge citizens for the eID and also generate transactional income from the suppliers of applications who offer retail and business applications to the final network. Some examples of such an organisation: a consortium of joint ventures made up of banks, telecommunication operators and credit rating agencies.

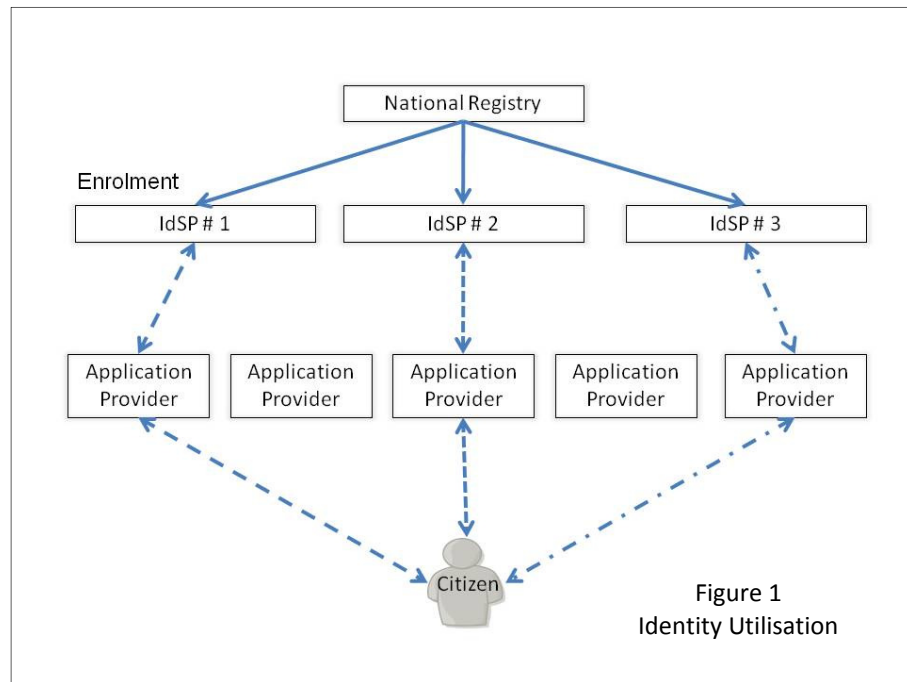
The documentary proof would be interoperable with those of other IdSP and each IdSP could potentially belong to a trans-national group. The legal aspects of such a cross border arrangement could be managed according to the provisions of the contract between the IdSP and the individual and could be perceived as a standard terms agreement. This would be adapted to each country and security policy, whether national and/or community based. Service providers would be able to compare each other and accept

⁷ IDABC Case Study: “eID Austria”: <http://ec.europa.eu/idabc/en/document/4486/5584>

the digital identities and operations of their counterparts carried out on their behalf with confidence.

A Citizen could choose his eID from any IdSP within his own Member State of citizenship or an IdSP of another Member State should its terms of operation be acceptable to both parties (Figure 1). Indeed, the citizen could by choice have more than one eID, and as occurs within the BankID scheme, each of the citizen's individual eIDs would be linked to ensure a consistency of ultimate non-repudiation.

An application provider could accept identity attributes from a range of IdSPs. This acceptance would be based upon using a commonly understood identity assurance framework to match the declared risk-profile of the application against the level of trust in a credential. It is expected that some IdSPs will support different identity credentials each with a distinct level of trust, whereas others may specialise in credentials of one specific trust level.



This arrangement would require certification within each Member State and each certification would need to be assessed by a risk-based methodology comparative to that undertaken by DNV in Norway for BBS operations.

Applications that utilise the new credentials would be owned and operated by existing and new business providers and would use IdSPs to provide the information relied upon by their clients, the relying parties.

Having established the concept of an IdSP role, and defined its necessary characteristics, it would then be a matter of market evolution to determine the particular configuration of this new industry within the EU.

This idea of an evolving marketplace in IdSPs poses policy questions regarding certification of the players and industry supervision which will need further exploration.

It is necessary to agree as to the certification of IdSP as providers of electronic documentary certification services, if only by a general or basic security policy, bringing together the largest number of candidates to establish an initial level of certification and interoperability between countries.

In any event, if the States do not do so, the strength of the demand of large companies and banks will see the adoption of industry-led solutions, such as the SWIFT cooperative has done for the interoperability of payments and the dematerialisation of the financial instruments e.g. CEDEL, EUROCLEAR, EURONEXT, CLEARSTREAM, etc.

The absence of a simple, clear, pragmatic, organisational and cheap "value proposition" by States will lead public companies towards the first certification and interoperability solution which they must have for the mandatory cover of their systematic risk.

4.2.1.4. Example Scenario

An example scenario could be the transactions involved in purchasing a car using credit. The car vendor (Relying Party) contracts to a finance provider (Application Provider) who identifies the credit applicant using the eID. The eID is authenticated against the credit applicant's IdSP of choice who is able to check the revocation status of the eID from the National Registry and also checks the credit worthiness of the applicant with a third party credit agency. The IdSP may also inform the Driver Licensing Authority as part of national legislation. The applicant has previously made a choice of IdSP to represent his credentials and credit status. The applicant may choose another IdSP for maintaining other attributes such as age status or affinity memberships. As this is a high value financial transaction, on this occasion, the applicant is not given the choice to discard transaction details and they would remain available for audit at a later date.

4.2.2. Key Features – The IdSP “Rulebook”:

We must clearly distinguish the role and functions of IdSP from the role and functions of the Applications Providers.

4.2.2.1. IdSPs would be licensed and regulated in each Member State of operation to act as providers of eID credentials and attributes.

4.2.2.2. IdSPs would be licensed to communicate, on behalf of the citizen with government agencies in order to provide information to 3rd parties / cross border, at the request of the citizen.

4.2.2.3. IdSPs would underwrite the transactions (in conjunction with

financial institutions and (as per an agreed schedule) the operations of the affiliates who's on line identification they are responsible for.

4.2.2.4. *There would be a choice of IdSP per country and individuals would be able to distribute permissions to a number of IdSPs.*

4.2.2.5. *Application providers could be under different ownership or be separated from the IdSPs by strong governance and transparency.*

4.2.2.6. *The individual could exercise opt-in for the sharing of particular attributes to any particular application provider.*

4.2.2.7. *The individual could have the choice to retain or discard transaction details for certain transactions, such as age verification, so enhancing personal privacy.*

4.2.3. The Gap between current State-of-the-Art technologies and actual ICT requirements

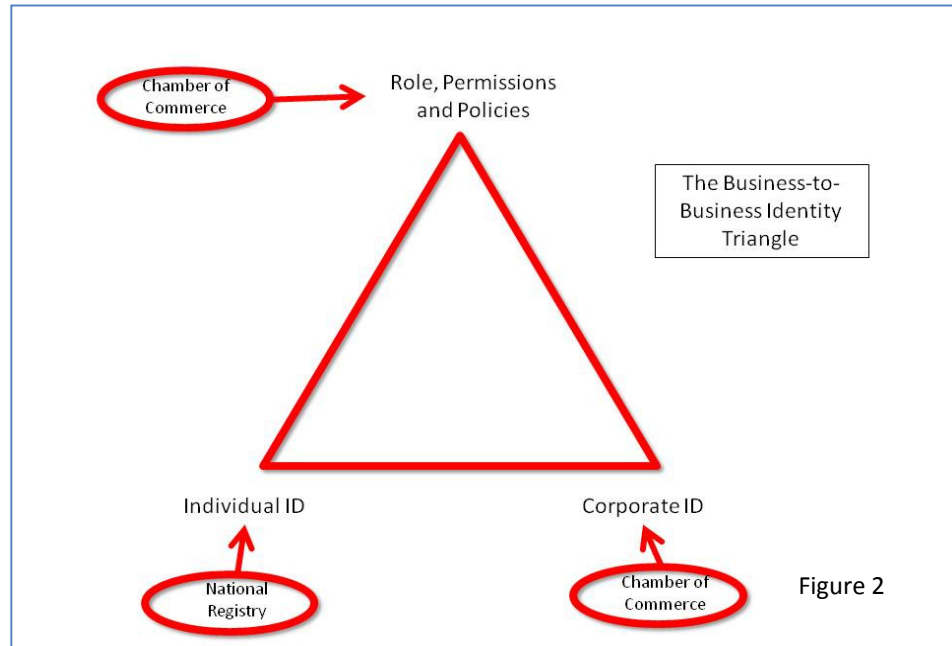
There are already many individual initiatives, in both the private and public sector that can contribute to the overall success of the scheme outlined above: These are listed in Appendix III.

4.2.4. The Business Identity

Businesses have additional requirements when asserting the employee's business identity when dealing with individuals or government. These attributes relate to the employee's specific role within the company and various permissions. (Figure 2)

Corporates may wish to delegate aspects of their credentials to individual employees, eg to allow them to procure goods or sign contracts. There is also a compelling need for corporates to identify themselves to governments when dealing with company registrations, tax returns etc.

The application provider itself may be able to apply tests to authenticate the employee and company. However if the application is no more than an introductory hub, the IdSP or Validation Authority may be required for authentication and policy verification.



Corporate Identity is usually maintained by a Chamber of Commerce and this could be extended to certain externally facing roles and authorisations of employees. This could either be via an external database held at the Chamber of Commerce, or via published lists by larger corporates. Alternate authorities are possible: organisations such as Dun & Bradstreet.

Such service providers who may be eligible for this type of function must be subject to the security and trust chain for all processes which ensure the security and legal value of the correspondence or on-line transaction. Their role shall be an integral component of the security and trust infrastructure. The current analysis of the market lacks a coherent model providing such a clear vision, and a precise structure of a certified multilateral transaction network.

4.2.5. Interoperability

Technology is seldom an inhibitor. A common set of mature Open Standards backed up by contractual agreements will guarantee interoperability. A mechanism to introduce new standards as they are developed and mature will be required to ensure that interoperability remains intact between IdSPs in all Member States.

4.3. Economic Aspects

4.3.1. Revenue flows

Underpinning any model for identity provision must be solid recognisable revenue flows (Figure 3). A full financial business model needs to be constructed to ensure that all tiers are financially viable.

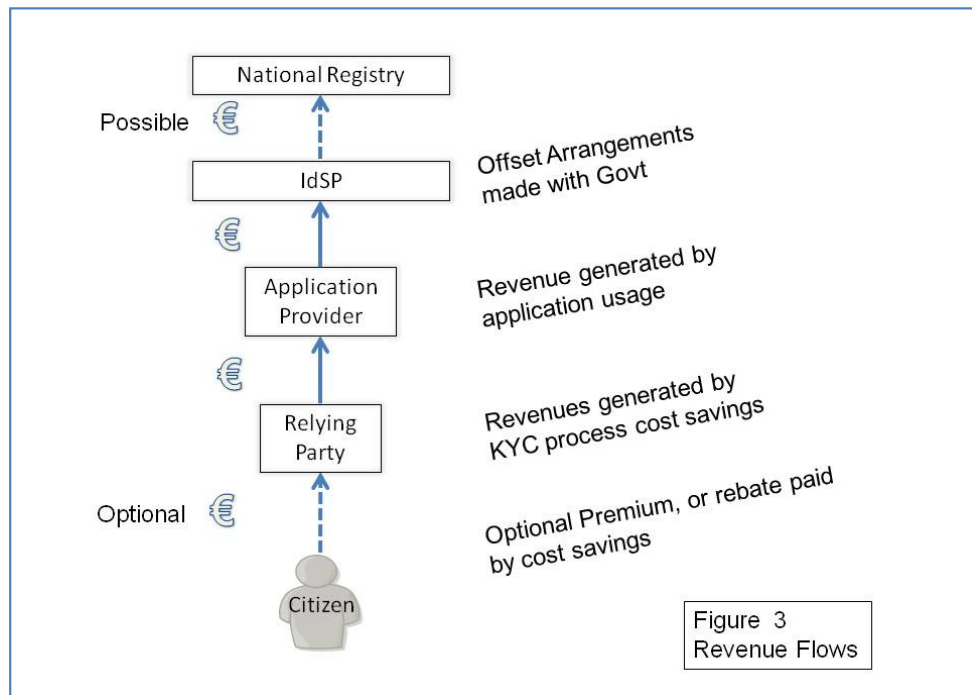


Figure 3
Revenue Flows

4.3.2. Liability

In order to be of value to relying parties, IdSPs will need to provide guarantees for the data that they provide. This liability is fundamental to the use of identities and attributes by applications and throughout the entire chain of value liability must be considered.

In many countries the government provides a limited liability for transactions that rely on the National eID card. This value is typically between €1,000 and €10,000 (2009 values) per transaction. For example for the Belgium eID, the government’s liability limit is set to €2,500 per transaction for signing using that credential, although for authentication, general liability applies.⁸

In reality the anecdotal evidence is that the number of occasions where liability has been tested is very low.

In a commercial context, this can cause significant problems, since it means that there is a ‘void’ at the root of the contractual liability chain. Until sufficient statistics are available to quantify the financial risk, one option is for governments to incentivise commercial adoption by underwriting commercial insurance of the identity value chain, so that protection is given against fraud where an error in the government’s registry is the cause.

Historically, similar liabilities, such as ‘Cardholder-not-Present’ have been actuarially determined and underwritten. An IdSP could likewise

⁸ Article 9.2 of the Belgium eID CPS.

underwrite the risk of each transaction with an insuring institution. Statistically, the accuracy of information, and level of fraud within the National Registry will be calculated and so risk can be minimised.

Rather than capping the risk at a lower value, a variable tariff might be applied to applications depending on the value of the transaction. It is for this reason that it is recommended that an insurance institution is included within an IdSP management company.

4.3.3. Role for Banks and Financial institutions

Banks and other financial institution have always been trusted to act as trusted third parties not only for high value commercial transactions but also for the billions of small transactions in the Business-to-Consumer environment.

Already banks in Norway and Sweden have chosen not to wait for government issued credentials to become available, preferring to utilise their own extensive experience in financial credential issuance and authentication, together with agreements with national authorities, to distribute identity credentials to their customers. In these countries the concept of the IdSP has already become an accepted and mature ingredient of everyday life.

It is recommended that the BankID concept be examined as to how it might be used as part of any European Identity model or potentially re-used as an architecture test-bed.

4.3.4. Justifying eID in a Fiscal Environment

While technical visionaries have already expressed a view of what could be possible to achieve, the working through of these ideas in terms of practical implications to Gross National Product at Member State and European Union level has not been done.

One of the most difficult issues to address for any nationally operated eID is to identify and describe solid business cases in the Citizen-to-Business or Citizen-to-Government environment. Most examples currently described can, on a national level, be achieved using non-eID methods. The Return on Investment for converting processes to include eID is hard to identify especially in the transition period between the use of 'dumb' credentials and eIDs. Additional complications arise as funds for modifying existing applications are drawn from local departmental budgets whereas saving often are seen as aggregates at Member State level.

It is therefore essential to build and continue to maintain a strong knowledge-base of possible eID applications and to provide sufficient data for the ongoing aggregation of potential savings for the European Union as a whole as well as for member-states. This data will need to be detailed and quantifiable.

4.3.5. Funding the Transition

It is recognised that the effectiveness and acceptance of any eID is proportional to the penetration into the target population. In countries where National eIDs have already been deployed, the private sector has waited until it has become cost effective to rewrite existing systems to incorporate the new credentials. Typically this threshold has been found to be between 70% and 80%. Until this threshold penetration has been reached (Figure 4) and applications appear, the enthusiasm of the citizen for the new credential has been tempered, especially if its use has not been mandated.

This will make it difficult for capital investments to be justified in the early phases of any eID program. Rapid deployment of eIDs and applications funded initially by the state is therefore essential as well as the encouraging of applications to be written before the threshold is reached.

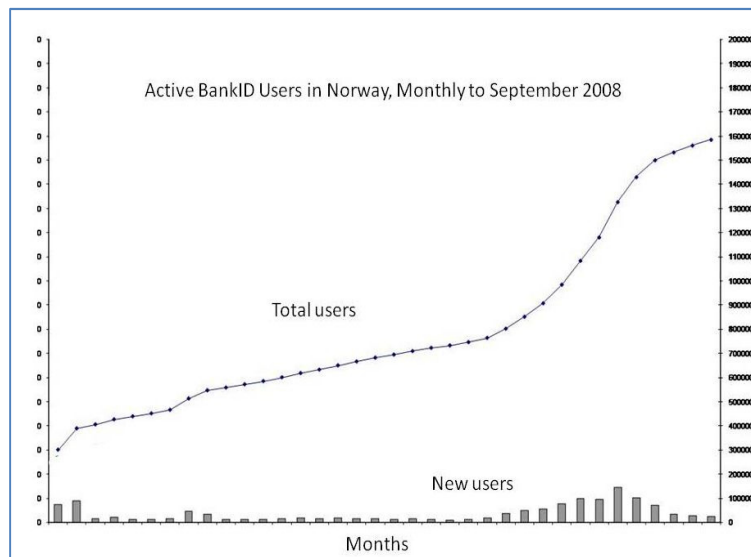


Figure 4

It is within the ability of the European Union to assist in the rapid adoption of third party eIDs by providing financial inducements to develop appropriate applications before the critical threshold is reached. As mentioned already, one way to fund this adoption might be to underwrite (i.e. act as the 'insurer of last resort') fraud in the eID value chain.

The mechanisms needed to provide financial and other inducements to accelerate this process need to be investigated in detail.

4.4. Political Aspects

4.4.1. Legality

One of the most important initial objectives to be achieved to ensure that the vision of an eID becomes reality is to ensure that there is a legal framework to ensure that IdSPs are responsible for any guarantees that they offer in relation to their data, irrespective of where it comes from. In some cases IdSPs may get their data from the public sector. Member State legislation may be needed to permit the use of a National ID to provide “breeder” source data.

4.4.2. Quality

Accreditation bodies will need to be established across the European Union to regulate IdSPs and components which will form part of the Critical National Infrastructure of each Member State.

These bodies will need to regulate assured quality of policies, processes and equipment and it is likely that they will comprise organisations already performing certifications in conjunction with the interests of Privacy groups and the security services.

4.4.3. National Security

There will need to be legislation to address issues surrounding the protection of personal privacy and establishing “rules of engagement” with security services and government agencies who may desire to utilise the transactional data that will be flowing through each IdSP.

Consideration will be needed towards the storage of this data and options for removing transactional information both at the instigation of the citizen and the IdSP. A number of transactions will need to be retained under any circumstances.

It is important that eID is treated in a similar fashion as any other personal data has been treated in the past. The comparison to the interception of telephone communications, with the legal requirement for a court order, can be made.

Within the education process citizens need to be reassured concerning their rights and obligations regarding the use of eIDs and their relationships to IdSPs.

4.4.4. International Aspects & Vision

There will need to be maintained a consistent co-ordination of activities at EU level to ensure that such a long term plan is driven forward and does not lose momentum. How this is achieved is to be determined.

Early in the program, investigation will be needed as to whether there is a need to extend existing digital signature directives to embrace the envisaged eID model.

Additional framing of EU legislation and policies may be required to permit and foster the establishment of cross-border IdSPs or IdSP consortia offering services in all sectors (Business-to-Business, Business-to-Citizen, Business-to-Government, Citizen-to-Citizen, and Citizen-to-Government).

Inducements to speed up the adoption of eIDs through an early spread of useable applications. (Possibly financial or concessionary) will need to be investigated and incorporated.

5. ROADMAP FOR ADDRESSING OBJECTIVES AND OVERCOMING BARRIERS

Whilst this document does not attempt to address or resolve all the objectives and barriers for this vision, a process can be established that can enable measurable progress to be made towards this goal.

This can be realised in a number of overlapping phases: Scoping; Acceptance; Planning; Pilot Development; Testing; Gradual Adoption.

Each phase will be broken down into Work Packages (and potentially sub-packages) across the themes of; Societal, Technology, Economic and Political.

Because of the size and complexity of the vision, it is envisaged that during the course of realising this goal, a number of independent but parallel projects could be initiated, with scopes and outcomes that would in part, contribute to the final outcome. Identifying and initiating these projects and others that are relevant but initiated elsewhere will commence from Phase #1 onwards.

5.1. Phase # 0: Immediate Next Steps

5.1.1. Description

Reference groups responsible for the four themes of the program: Societal, Technological, Economic and Political should be established to secure core skills and enable oversight of the program going forward.

The most appropriate form of program management and short term budgets will need to be considered to ensure success of the phases #1, and #2

Limited budget to ensure cohesion and momentum of the program

5.1.2. Timeline

3-6 months

5.1.3. Outcome

A coherent formal program with a wide ranging respected set of participants able to contribute to the further early phases.

5.2. Phase #1: Scoping

5.2.1. Description

This phase further defines and expands on the objectives and barriers raised in this document in order to provide a comprehensive and fully detailed vision of eID. Initial contact with ‘interested’ private sector organisations will commence. Monitoring across the range of projects outside of European Large Scale Action (ELSA) will be conducted for establishing synergies.

5.2.2. Timeline

12-24 months

5.2.3. Outcome

A completed series of projects and documents providing sufficient information being used by the European Commission to obtain the acceptance of a significant number of Member States in Phase #2 and to obtain funding for the ongoing delivery of the eID vision.

5.3. Phase #2: Acceptance

5.3.1. Description

This will be predominantly a political and economic phase and will consist of lobbying the various stakeholders in order to win support for the vision. Source data and collateral will be the outcome of Phase #1.

5.3.2. Timeline

12 months

5.3.3. Outcome

The acceptance and support of the vision by a significant number of Member States and importantly the allocation of sufficient budget to fund Phase #3 and Phase #4. Additionally a process will be set in place that ensures that projects initiated in any relevant fields have as part of their formal goals, contributory components to the overall vision.

5.4. Phase #3: Planning

5.4.1. Description

This is the detailed implementation plan across all aspects of the vision; Societal, Technology, Economic, Political, and will involve both private and public sector organisations. Programs for education will be developed early in the phase, together with engagement with privacy lobbies.

The commencement of surveying of stakeholder perception will commence in order to determine if any additional concerns have not been identified and also as a datum by which to measure the success of the societal aspects of the program.

5.4.2. Timeline

24 months

5.4.3. Outcome

All objectives and barriers will be addressed and technical development and legislative activities will be commencing. Educational programs will be beginning to be used in Member States.

5.5. Phase #4: Development

5.5.1. Description

The technical development, together with economic and political aspects will be undertaken. Education programs in Member States will commence. IdSPs will be established in the Member States agreeing to the introduction of Large Scalable eID Pilots. A number of applications will also be developed for practical use in the testing phase. These should include a number of applications in each of the areas: business-to-government, business-to-business, citizen-to-business and citizen-to-government.

Continued surveying of stakeholder perceptions will be undertaken in order to determine if any additional concerns have not been identified and also as a measure of the success of the educational aspects of the program. Continuing educational and political efforts will be undertaken.

5.5.2. Timeline

24 months

5.5.3. Outcome

Large Scalable eID Pilots, ready to commence operations with local IdSPs, together with the appropriate infrastructure.

5.6. Phase #5: First Adopter Pilot Testing

5.6.1. Description

First Adopter testing and fine tuning of the Large Scalable eID Pilots and adaption for full deployment. Testing of Interoperability and the introduction of applications.

Measures of usage are critical, broken down by sector and demographics so as to spot the “early adopters” trends

Continued surveying of stakeholder perceptions will be undertaken in order to determine if any additional concerns have not been identified and also as a measure of the success of the educational aspects of the program. Continuing educational and political efforts will be undertaken.

5.6.2. Timeline

24 months

5.6.3. Outcome

All the necessary information and technology that is required for the gradual production deployment to have been developed and tested and adoption will commence.

5.7. Phase #6: Gradual Adoption

5.7.1. Description

Gradual adoption of the eID vision across all Member States.

Continued surveying of stakeholder perceptions will be undertaken in order to determine if any additional concerns have not been identified and also as a measure of the success of the educational aspects of the program. Continuing educational efforts will be undertaken. These efforts will be handed across to the respective IdSPs as appropriate.

5.7.2. Timeline

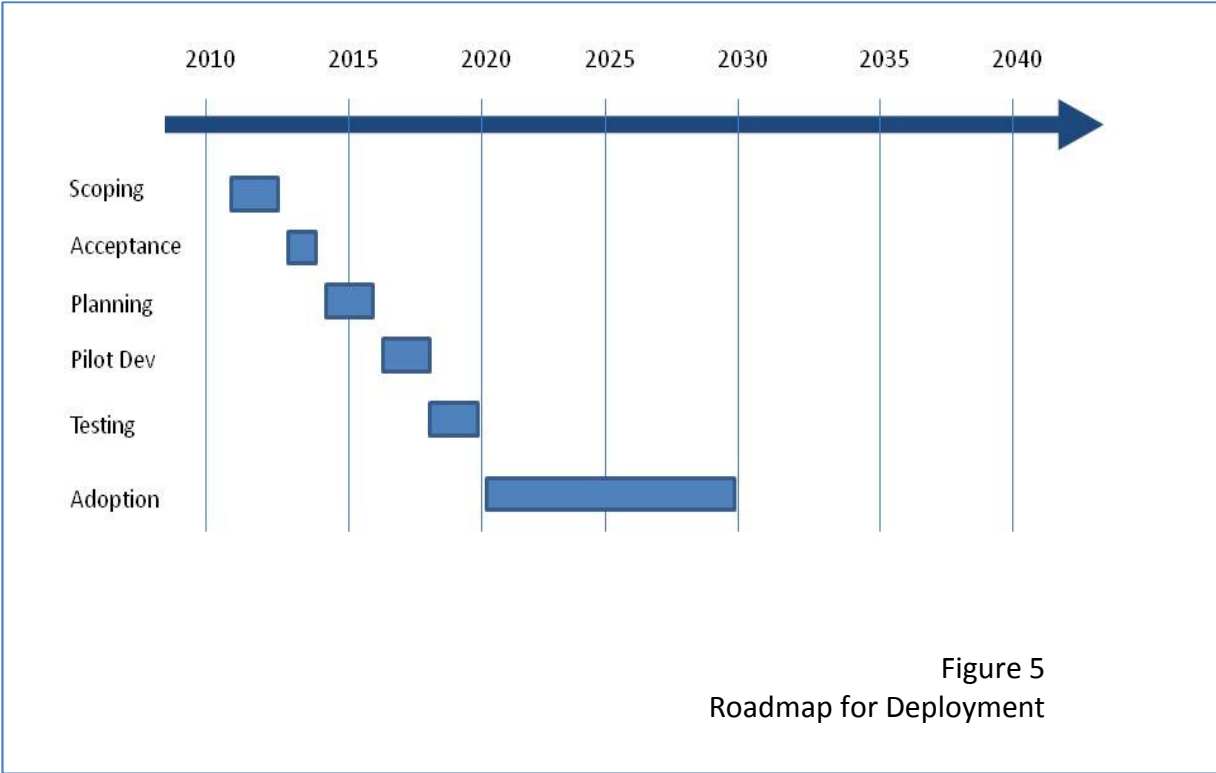
10 years.

5.7.3. Outcome

Full implementation of the eID vision.

6. TIMETABLE

The timetable in Figure 5 represents a nominal timeline to achieve full adoption of the vision represented in this paper by 2030.



7. MEASURING THE IMPACT, MONITORING AND EVALUATION

There will be an ongoing monitoring of private and business perceptions of eID and how they are affected by the various educational initiatives.

These will be an integral component of each phase and be used as input to modify any terms of reference or specifications as needed. It is suggested that a review team monitor these surveys as a performance measure at frequent intervals in order to detect any divergence from the strategic plan especially in the non-technical aspects of the program

The appointment of a Program Manager for every phase, equally responsible for Societal, Technical, Economic and Political objectives is recommended.

8. CONCLUSION

8.1. Authors' Conclusions

This paper represents an initial vision of a viable European eID intended to overcome many of the cultural, historical and regulatory issues which are hampering a Common European Identity and with ethics, privacy and choice at its very core.

It has been shown that the vision is realistic and achievable within the next 20 years and has the potential to be one of the single most unifying and valuable initiatives to be undertaken by the European Union.

8.2. Authors' signatures:

Jon Shamah:

Date:

Geoff Llewellyn:

Date:

8.3. Reference Group

<u>Member</u>	<u>Affiliation</u>	<u>Specialisation</u>	<u>Country</u>
Eric Blot Le-Fevre	Trustmission	e-Commerce, Trust	France
Nils Inge Brurberg	BankID	Banking Based eID	Norway
John Bullard	Identrust	Banking Trust	UK
Roger Dean	EEMA	Program Coordination	Multi-national
David Goodman	Nokia Siemens Networks	eID & Communications	UK
Hans Graux	Time.lex	Legal / Policy	Belgium
Alvis Erglis	Lattelecom Technology	eSignatures / MobileID	Latvia
Arkadiy Kramer	RANS	International Standards	Russian Federation
Lorraine Spector	Independent Consultant	Business Ethics	UK
Toby Stevens	Enterprise Privacy Group	Personal Privacy	UK
Keith Vallance	SWIFT	Payments	Belgium

9. APPENDIX 1 - DETAILED BARRIERS & THEMES

9.1. Societal

- 9.1.1. Establishing Identity Protection awareness as part of basic schooling for all segments of society. It is vital that initially teachers are trained to be knowledgeable about the ethics as well as the technical processes of eID. They, in turn, need to have the materials to effectively communicate this information to students.
- 9.1.2. Communicating the philosophy of the eID initiative – fundamentals of roles regulations principles
- 9.1.3. Communicating, to both public and potential developers, potential use cases so as to enhance familiarity with the concept and practicalities of the kind of system envisaged
- 9.1.4. Addressing the cultural resistance to the concept of eID cards in those Member States which have not historically held cards of any kind. This complex mix of cultural, historical and constitutional issues needs to be addressed. The UK ID card debate gives one perspective on the barriers which have been negotiated with mixed success over the past 6 years
- 9.1.5. Addressing the legitimate concerns of the privacy lobby which has become more prominent in all member states over the past decade as data losses have become more frequent and alarming. The central issues are being able to strike an acceptable balance between privacy and usability and the concern about “ownership” of personal data and also the safeguards relating to the ethics of personal information distribution.
- 9.1.6. Ensuring inclusivity for hard-to-reach social sub-groups

9.2. Technology

- 9.2.1. Credential security – both physical and electronic
- 9.2.2. Credential authentication – discussion of appropriate methods including the options of biometrics, personally held secrets or other methods
- 9.2.3. Standardisation of non-repudiable time-stamping across national boundaries as initially addressed by the “BalticTime” project
- 9.2.4. Standard universal middleware integration into operating systems for interoperability and management of connectivity of credentials both nationally and internationally
- 9.2.5. Extension of STORK into non-government eID programs (such as BankID in Norway) and private sector utilisation.

- 9.2.6. Exploring various form factors in which the eID can be carried and used (for example NFC enabled mobile phones or USB tokens)
- 9.2.7. The non-repudiation, auditing and storage of transactions as appropriate
- 9.2.8. Ensuring Offline capability allowing the token to be usable in power-down or power off circumstances
- 9.2.9. Designing and securing the ability of businesses to interact in the eID environment (i.e. establishing protocols, roles and permissions for the different players in the business/state interface)
- 9.2.10. Designing processes and protocols for fast and easy revocation of credentials across all domains of use
- 9.2.11. Ensuring operational availability and resilience

9.3. Economic

- 9.3.1. Creating understanding of the economic benefits (GDP, growth and agility) of the availability of a convenient and secure method for the electronic “projection” of the individual identity, in all kinds of transaction.
- 9.3.2. Essential demonstration of a plausible model of both the build-up and the steady state environment in which such eIDs are a critical component of the infrastructure of economic cooperation. Reviewing current deployments such as BankID and Belgium National eID.
- 9.3.3. Addressing the fundamental issue of liability that will be present when increasing numbers of transactions are completed using eIDs

9.4. Political

- 9.4.1. National level legislation to ensure that the use of national ID registers to provide “breeder” source data is permitted
- 9.4.2. Addressing issues surrounding the protection of personal privacy and establishing “rules of engagement” with security services and governments
- 9.4.3. Extending existing digital signature directives to embrace the envisaged eID model
- 9.4.4. Framing of EU legislation and policies to permit and foster the establishment of cross-border IdSPs or IdSP consortia offering services in all sectors (B2B, B2C, B2G, C2C, C2G)
- 9.4.5. Certification bodies to be established to regulate IdSPs and components of the infrastructure

- 9.4.6. Inducements to speed up the adoption of eIDs through an early spread of useable applications. (Possibly financial or concessionary)
- 9.4.7. Co-ordination of Activities at EU level and program management.

10. APPENDIX II - THE INFLUENCE OF ORGANISATIONS ON OVERCOMING BARRIERS

In the table Figure 5 below, are presented the obstacles previously listed with an indication of those organisations which may have a role to play in addressing those issues. It will be seen that these organisations frequently have an impact on more than one of the issues

Figure 5 Impact on Organisations																											
Organisation	Societal					Technology										Economic		Political									
	9.1.1	9.1.2	9.1.3	9.1.4	9.1.5	9.1.6	9.2.1	9.2.2	9.2.3	9.2.4	9.2.5	9.2.6	9.2.7	9.2.8	9.2.9	9.2.10	9.2.11	9.3.1	9.3.2	9.3.3	9.4.1	9.4.2	9.4.3	9.4.4	9.4.5	9.4.6	9.4.7
European Commission	X	X		X	X		X	X	X	X	X			X	X	X			X		X	X	X	X	X	X	X
National Government	X	X	X	X	X	X		X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Local Government	X	X	X																			X					
Voluntary bodies	X	X	X		X	X																					
Health authorities						X						X															
Education authorities	X	X		X	X	X																					
Banks and other financial institutions		X					X	X	X		X			X	X		X	X	X	X					X	X	
Legal Institutions				X	X	X													X						X		
Economic Institutions		X																X	X	X					X		
Chambers of Commerce		X		X										X	X			X	X						X		
Trade bodies		X												X	X			X									
Security Services							X					X										X					
Police and Emergency Services							X							X	X		X										
Privacy advocacy group	X	X		X	X	X	X	X											X	X	X				X		
IT industry	X	X	X	X	X		X	X	X	X	X	X	X	X	X	X	X	X	X	X						X	X

11. APPENDIX III – EXISTING INITIATIVES

There are already many individual initiatives, in both the private and public sector that can contribute to the overall success of the scheme outlined above: These include:

11.1. EEMA

Since 1987, EEMA has been Europe's leading independent, trade association for e-Business, working to further e-Business technology and legislation with its European members, governmental bodies, standards organisations and e-Business initiatives.

EMMA was an acronym for 'European Electronic Messaging Association', but as the focus of both the association and our members changed, the full title was dropped, and the brand name has gained recognition for its work throughout Europe.

It brings together over 135 member organisations (and over 1,500 employees of member organisations) in a neutral environment for education and networking purposes.

- Enabling members of the association to compare common and contrasting views and experiences on specific areas of e-business by holding subject-specific workshops and regular teleconferences and face-to-face meetings, seminars and conferences.
- Facilitating the setting-up of working groups to produce useful work in the form of reports and white papers, of interest to the member participants and to the rest of the membership.

11.2. STORK

Funded by the European Commission to demonstrate interoperability between differing National eID credentials especially with consideration to the cross border protection of government owned data across multiple boundaries. STORK will provide the foundation for the requirements of data transformation middleware and linguistics and should be extended to include private sector IdSPs. The STORK program is expected to go-live in 2011.

11.3. BBS Global Validation Service

Originally formulated by DNV, this service is operational and provides a mediator between differing corporate/government policies and certificate authorities and delivers 'fit-for-purpose' advice for relying parties. The service relies on a Risk-Based assessment of credential quality similar to

those currently envisaged by EU studies and is currently in use by the Norwegian government HANDEL procurement portal.

11.4. BankID

A large scale bank consortium based eID delivering identity services to over 4 million users in the Nordics. Over 1 billion transactions are managed by the service per year, the majority being linked to identifying users for financial transactions. Other uses include eGovernment access and a small number of Business-to-Consumer applications. Authentication is via card, one-time-passwords, Mobile PKI or name/password depending on application.

11.5. Austrian eID

This government led eID has pioneered advanced cryptography methods allowing the use of multi-tier one-way identities similar to those required in this architecture. Different credential carriers are permitted including mobile phones and secure USB tokens.

11.6. Identrust

IdenTrust provides a unique legally and technologically interoperable environment for authenticating and using identities worldwide. The IdenTrust Trust Infrastructure is based on a proprietary framework that combines policies, legal framework, trusted operations and technology to create a comprehensive environment for issuing trusted identities.

11.7. Time-Lex

Time-Lex has undertaken a number of studies regarding digital signatures and cross border validation solutions. Both these themes play a crucial role in this paper's identity model.

11.8. ENISA

ENISA has recently undertaken a survey of existing status of National eIDs and concentrated on the EU service directives which call on single point of access for eGovernment services. Whilst this report comprehensively covers government related interactions, experience from the Nordics show that the vast majority of transactions are private sector.

11.9. Primelife

Primelife is a research project funded by the European Commission's 7th Framework Programme.

Individuals in the Information Society want to protect their autonomy and retain control over personal information, irrespective of their activities. Information technologies hardly consider those requirements, thereby putting the privacy of the citizen at risk. Today, the increasingly collaborative character of the Internet enables anyone to compose service and contribute and distribute information. Individuals will contribute throughout their life leaving a life-long trail of personal data.

This raises substantial new privacy challenges: A first technical challenge is how to protect privacy in emerging Internet applications such as collaborative scenarios and virtual communities. A second challenge is how to maintain life-long privacy.

PrimeLife will ensure that the community at large adopts privacy technologies. To this effect PrimeLife will work with the relevant Open Source communities and standardisation bodies, and partner projects. It will further organise workshops with interested parties such as partner projects to transfer technologies and concepts. This will also validate the project's results on a large scale. European industry will be strengthened by providing building blocks for trustworthy treatment of customer's data.

13. REFERENCE GROUP MEMBER POLICY STATEMENTS

13.1. Eric Blot Le-Fevre

13.1.1. Digital identity has a practical interest only when considered as part of the functioning of correspondence networks and on-line commercial and financial transactions, with all safety and interoperability measures required in the relevant countries or agreed between the parties.

13.1.2. For that reason, the major issues and best initiatives that must, in my view, be highlighted in order to make headway and educate the persons most knowledgeable in the digital economy (who are our first-level contact persons and intermediaries) are summarized in the 8 items below:

- Assessment of the management of the eIDs in the Countries,
- Role of the eID in the policy for legal, IT and professional safety,
- Role of the eID in the interoperability policy between suppliers of electronic certification services, IdSPs, suppliers of applications, users and countries (cross-border exchanges, export/import),
- Role of the eID in the policy for the certification of the legal evidentiary value of digital exchanges,
- eID practices supporting the convergence of security, interoperability and evidentiary value policies related to exchanges in Europe,
- Digital identity rating scale in terms of registration and authentication; this scale contributes to the measurement of the certain evidentiary value of correspondence, transactions and digital archives,
- White paper concerning the eID and the evidentiary value of personal on-line transactions: correspondence and financial and commercial transactions,
- 8. Creation of a “Corporate Reference Group” involving enterprises, banks and telecom operators, promoting the progress of methods and solutions.

13.2. Lorraine Spector

13.2.1. It is vital that at the core of this project an ethical framework be integrated in each process that includes principles, practical guidelines and a self assessment system.

eID must reassure citizens that the standards and processes are beyond reproach and engender trust that their identity will be protected at each stage.

Each process must be transparent and citizens must have access to their records and have choice in whether they decide to have an eID and what service providers they choose.

13.2.2. Ethical Guidelines

There are many aspects in which ethical guidelines need to be integrated including:

- Conflict Resolution
- Exception Management
- Conflicts of Interest
- Reputation Repair eg. those whose identity has been compromised

13.2.3. Ethical Audits

An Ethical Audit should have an enforcement process to monitor ethical behaviour by all involved agencies.

The Ethical Audit would:

- Ensure credibility
- Give vital feedback
- Be practical to implement
- Allow performance to be measured
- Promote the good practice of the provider to users
- Promote a global standard

13.3. Hans Graux

- 13.3.1. From a legal/policy perspective, it is clear that there is a need for an unambiguous governance framework to enable the trustworthy re-use of electronic identities across multiple contexts and across borders. If this framework is to be effective in the future, it will need to be open to public-private collaborations, as private sector stakeholders are crucial to create credible business cases and to ensure uptake by the end users.
- 13.3.2. Such a framework needs to acknowledge that different levels of trust are required in different contexts. As the example of social networking shows, even largely unreliable claims-based electronic identities are perceived as valuable and useful by end users, and the re-use of such profiles across multiple contexts and/or applications is a common practice for digital natives. While the legal value of such identities will likely always remain limited, it is none the less important to consider the lessons learned from these initiatives, given their enthusiastic reception with a large user base.
- 13.3.3. To accommodate these multiple levels of trust, a certain degree of supervision will be needed towards the key infrastructure providers in this identity model, including specifically towards identity providers. This supervision should ensure that identity providers comply with appropriate obligations linked to the claimed reliability of the identity they provide, and that they accept liability in proportion to their assurances.
- 13.3.4. It will need to be evaluated to which extent public sector intervention is needed in such a model. Conceptually, governance could be established entirely without public sector intervention, based on a voluntary/contractual model. However, this may not be the most desirable outcome from a public policy perspective, given that the governance framework in a purely private model may not take into account the public interest (including e.g. data protection concerns), and that interoperability may not be easily achieved at a European level without policy guidance.
- 13.3.5. In this respect, a mixed model could be adopted in which private sector stakeholders (including private identity providers) offer key identity services to citizens and businesses in accordance with minimal basic rules established at the European level, in particular to define common reliability tiers and to ensure semantic interoperability. Compliance with these rules may be assessed at the national level via appropriate supervision schemes, thus creating a scalable trust infrastructure, driven by market needs and keeping into account the interests of all stakeholders.

13.1. **Nils Inge Brurberg**

13.1.1. To be able for the future to use develop eServices we need eID's to support strong authentication and eSigning. To have success for the future the citizens have to be able to use the eID they have and is used to use. It is imperative that public and private must work together.

13.1.2. We support the concept outlined in this report



Toward an electronic identity management (e-ID)
infrastructure
ELSA – Beyond STORK

EUROSMART' Proposal Paper

1. Purpose of the Paper

Digital identity became a reality with electronic passports based on the international ICAO standard, electronic health cards, electronic national ID cards and electronic driving licences. All these digital identities are managed by public authorities. But citizens also have private identities as an employee in a company (badge card for building access or logical access) or as the holder of an email account (username). With more than 1 billion internet users, there are several billion digital identities in the virtual world.

Digital identities become more and more important in terms of immigration. Certainly foreigners have digital identities as well. Security and privacy are the big challenges for identity management systems.

This paper raises considerable challenges in terms of electronic identity management e-ID infrastructure and displays a first statement on the upcoming EU program, called ELSA (**E**uropean **L**arge **S**cale **A**ction). This document reflects an analysis of EUROSMART experts from the e-ID working group.

2. Status & Trends

The Web was still very much in its infancy fifteen years ago. Today we are living in a high-mobility, image-centered, digitalized world without boundaries in Europe. The Internet has turned this state of affairs into a daily reality. That explains why our current European society is moving. This move is based on four pillars:

- Society trends
- Economical trends
- Industry trends

- Government trends

The **society trends** could be resumed by the following aspects: People become more individual but are more virtually connected to others. The mobile telephony is a concrete example and was adopted around the world by all with several usages not always connected with telephony.

The **economical trends** are more connected with the citizens' moves motivated not only by holidays but also by work. Workers follow the move of the industry motivated by cheaper man-power or for a proximity delivery of services or products. Both moves are influencing our local national and European economy. The digital economy is born.

The **industry trends** are initiated with the first steps on e-commerce. These steps are being to be generalized. More and more businesses are now available on the web. We talk about on-line business with the opportunity for consumers to buy or sell 7/7 days and 24/24 hours.

The last pillar concerns the **government trends**. Governments are moving into the digital world with several objectives as cost reduction in administration, high quality and more convenience for the citizen.

3. Challenges

These four pillars impact all 27 European Members States and all 500 Million European citizens. The junction between these four pillars is the electronic identification which has a key role to play in this new world. It is already realized with the e-Passport which is based on a worldwide standard. And it is already sure that several added e-Services using e-Passport will be added in the future (e.g. automatic e-border controls). But this electronic identification also comes along with new features or new requirements such as authentication, digital signature, privacy, biometry, etc. Connected electronic applications to these features offer new opportunities with derived identification processes. An example could be the age verification for buying alcohol or tobacco.

So, this new digital world implies a profound rework on our fundamental concepts for a better usage of all these new technologies.

A good example is the legal aspects which must be improved, adapted and adopted. Another example is the interoperability of systems which is one of the most important aims in the new socio-economic world order that is emerging in the early part of the twenty-first century. It is no surprise to see ICTs and digital exchanges come to the aid of such a project. This is the first-rate opportunity for e-Government and related e-Services.

All these evolutions are challenging and must be managed in parallel. It is necessary to draw a complete picture of the global European context with national specificities and to develop compatible and interoperable solutions adapted to each one.

e-ID is becoming one of the key elements where the corresponding e-ID management infrastructure will integrate security and legal issues connected to interoperability and privacy requirements. Several connected topics should be probably deeply investigated in order to guaranty complex but useful systems.

4. Eurosmart proposals

EUROSMART members are deeply involved in the government eID programs in all European states, for citizens and for foreigners. All relevant key components, like eID-token, like application-SW, card – and identity management systems, like key management systems, like national PKI, like card-readers are developed, qualified and produced by members of EUROSMART.

EUROSMART members are also proactive in international standardization works, like ISO/IEC 24727 and CEN TC 224 and in national specification NPO-works like GIXEL in France, INTELLECT in UK and DIF in Germany.

EUROSMART eID WG could be the advisor for DG INFSO according to the upcoming eIDM 2020 program. EUROSMART eID WG could capture parts of the relevant aspects, like secure token, secure SW for eID application, secure channel for communication, include technology, standardization, interoperability, privacy and security. EUROSMART proposes that DG INFSO uses as second advisor the umbrella group on ICT in Europe, to fulfil the end-to-end approach for eIDM in Europe.

A first step down view of EUROSMART would be: Deployment of future scenarios for eIDM in Europe for 2010, 2015 and 2020 with the following aspects

- (1) application mainstreams on eID, eIDM in 2015 – 2020
 - along public sector
 - along enterprise sector
 - along banks and credit card service provider
 - along insurance organization
 - along internet provider
 - along health and social sector

- (2) collect a complete tool box concept for
 - all relevant technical components (HW/SW)
(e.g. token, application-SW, client-MW, server-MW, secure channel etc.)
 - interoperability in technology and security crossborder
 - uniform security in the same application class crossborder
 - semantic aspects in the same application class

- (3) deploy various business cases
 - with public service portals
 - with PPP models
 - with outsourcing of public service models
 - with enterprise service models
 - with banks service models

- with credit card service models
- with insurance service models
- with internet provider service models
- with health and/or social service models

EUROSMART eID WG members are not expert in legal aspects on eID and eIDM. Thus, EUROSMART could not capture any recommendations for legal works.

EUROSMART eID WG should deploy a roadmap for the advisory work, in case the ELSA program achieves a clear picture.

5. Annexes

ELSA should answer to the current European Commission questions on e-ID management infrastructure. There exist already some partial answers to these key questions. They are briefly resumed here and should be used for initiating an overall brainstorming on the fundamentals connected with the e-ID management infrastructure.

Long Term Vision

For some fifteen years now, profound changes have transformed the relationship between the individual and the collective. As economic deregulation and globalization continue to erode many of the guiding principles of the past, a considerable desire has developed for a new set of principles for the post-industrial era. There is a desire to qualify what we can consider as authoritative and trustworthy in the new digital age and to identify the keys to modern social cohesion and sustainable social harmony.

This emerging desire is the motivation for an e-ID management infrastructure. The adoption of the citizen-centric approach could be a response to a profound need to rebuilt a system of values in the face of the uncertainties of globalization and the overriding imperative to compete – a need to establish a framework that the majority of citizens can use to understand the modern world, to provide citizens with guidance, instil in them a sense of responsibility and involve them to the greatest possible extend in order to counter the growing risk of distrust and resignation.

This world could offer a permanent access to e-services with semantically and languages seamless interaction from private or public sectors. The coming information society should be a controlled secured labyrinth between users, administrations, companies and e-services. This means that data should be well managed without threats or risks regarding security and privacy; data should be used in a complete transparency regarding the reached e-service but also for the used e-services executed by others.

e-ID model, technology, mobility

e-ID is clearly a large revolution in the concept of life. This means that many things must be adapted or developed. It will be probably an error to focus on only one direction in terms of electronic identity. We must talk about several identities, each one connected to

a specific domain. Some of these electronic identities are official, others are already a subset which is less official and more “pseudo” oriented.

It is the reason why it could be dangerous to follow only one paradigm (usage scenario, trust model, architecture) but rather to develop different strategies for different cases and adapt each one during its own evolution. The trusted model will be probably well adapted for secure transaction when usage scenario will improve the e-ID key role into social website life.

Public/Private Partnership

The success of the e-ID depends on how frequently the connected services will be used by all concerned entities: European citizens but also public and private professional structures. Systems which will lead such e-ID deployments will offer real benefits, enduring quality of e-Services, and ease to access in return for financial outlay. Although e-ID is the key to build a modern social contact, it nonetheless remains subject to the fundamental need to win public acceptance.

The partners most likely to accelerate the widespread uptake of e-Services are those who have for many years found them confronted with the same stumbling block, due to difficulties in equipping customers, and who have managed to build a critical mass of customer’s loyalties.

Banks and telecoms operators should be probably the most obvious potential partners. Bank, because they remain the standard-setters in terms of secure payment authorization are the most credible provider of such services from citizen’s point of view. Telecoms operators are also candidates for PPP-programs, because they have similar credibility in the field of transmitting digital data in a secure and reliable way.

In such public/private partnership, the governmental authorities should preserve the electronic identity control when private operators can assume the security of the used infrastructure for the dedicated e-Service.

Regulation

Many risks are associated with migration towards a highly integrated and interdependent world, necessitating fundamental changes in legal frameworks relating to security matters. This represents an enormous set of problems at national and international level. An harmonization of legal aspects in Europe will facilitate such difficulty and offer the opportunity to simplify the global context. That means such compromise between existing national legislation must be found with a double objective: reduce legal distortion and minimize the cost for legal interference between Member States.

E.C. role

The coordination at European level could be done by the European Commission event if the E.C. has no mandate for interfering into national programs connected with identities. Regarding the European mobility and the coming challenges to solve, the E.C. could play a role of leader through fostering national actions & decisions. This could be done by managing the key strategic items as: legacy, technical convergence, interoperability, and communication/trainings towards all European citizens.



Eurosmart is an international non-profit association located in Brussels and representing the Smart Security Industry for multi-sector applications. Founded in 1995, the association is committed to expanding the world's Smart Secure Devices market, promoting Smart Security standards and continuously improving quality security applications and services.

Eurosmart members are suppliers and manufacturers of smart cards, semiconductors, terminals, equipment and technology for Smart Secure Devices, system integrators, application developers, issuers, associations, laboratories and independent experts. They work into dedicated working groups (communication, marketing, security, electronic identity, new form factors, and prospect emerging markets).

Eurosmart is acknowledged as representing "the Voice of the Smart Security Industry" and is largely involved in political and technical initiatives as well as research and development projects at the European and international levels.

For more information, please visit www.eurosmart.com

08 October 2009

DIGITALEUROPE COMMENTS ON THE EUROPEAN COMMISSION'S BACKGROUND PAPER ON EID INFRASTRUCTURE¹

1- INTRODUCTION

All social and economic interactions among human beings in modern civilization require the exchange of personal data. In everyday situations, we decide intuitively which data to make available, for instance whether to state our name when shaking hands. In the online world, each individual has to handle numerous accounts and data sets. These so-called partial identities will increasingly play a key role in future electronic services as well as in public security.

A basis for the provision of trustworthy services in eGovernment and e-commerce will be crucial for the competitiveness of the EU.

2- BARRIERS

Enterprises today face the challenge of finding a balance between protecting their online resources and meeting regulatory compliance requirements on the one hand — requiring enterprises to collect more information about the users accessing these resources — and accommodating rising privacy demands from consumers and legislators on the other hand, forcing enterprises to collect as little information as possible, and to adequately protect the information they do collect.

At the same time EU Member States lack a governmental infrastructure for authentication in the digital world, as authentication has been established with ID cards and driving licenses in the physical world for many years. Therefore even easy transactions like car rental are currently not supported in the digital world by a widely recognized authentication infrastructure.

This situation has led to efforts on all levels of public sector authorities and also enterprises (e.g. postal companies) in the Member States, which are currently not based on common accepted standards but are instead very diversified.

In combination with the fast pace of technology evolution in recent years this has caused risks in terms of fragmentation, lack of interoperability, closed solutions, privacy breaches, and lack of user control, transparency and accountability. To enable further adoption of eID technologies, industry and governments need to partner to create a scalable, future-proof, socially acceptable

¹ European Commission's Expanded Background paper "Towards a European electronic identity management (eID) infrastructure for a trustworthy Information Society", October 2009.

solution that embraces both the need for strong personal identification and the need for protecting personal privacy. Moreover for the implementation of the European eServices Directive pan-European standards would be beneficial.

3- OVERCOMING THE BARRIERS

DIGITALEUROPE believes that the most important step in addressing the eID challenges in a holistic way is establishing an effective public-private dialogue between the key stakeholders, including the EU and Member States governments, the local industry as well as key global solution vendors and integrators, data protection representatives as well as academia. The objective should be a clear definition of requirements for the pan-European eID solutions, including:

- A framework for interoperable identity systems which respects cultural differences and individual autonomy. That framework should be based on a classification of which services – especially government services – require which level of authentication (low risk vs. high risk).
- Requirements for establishing an end-to-end trust in the infrastructure based upon the concept of federated identities to support partial electronic identities
- Authority requirements
- Service provider requirements
- End-user requirements
- Requirement for pan-European harmonization and standardization of eIDs.
- Domain and sector specific requirements and principles: For instance government e-transactions, banking, e-commerce, digital consumption in the consumer sphere and intra/inter-company employee/agent aspects, including roles, responsibilities, and rights of parties. Universities could be one of the most promising areas for pilot projects as the Bologna Process should support the mobility of students in the EU, which is currently not supported by an adequate identity management solution across the universities in the Member States.
- Applying the principle of minimum disclosure in claims-based identity transactions.
- Ensuring broad support in off-the-shelf commercial software and hardware.
 - Best practice monitoring on a global basis
 - Easing the path for proven solutions to be used in the EU
- Policy principles that will facilitate and accelerate adoption.
- Respect for fundamental rights including adoption of privacy and transparency technology tools Collaboration and alignment with global eID initiatives (e.g. the OpenID standard).

DIGITALEUROPE would welcome a set of focused projects of significant scale and duration that cut across the innovation cycle to develop modern pan-European Information and Communication infrastructures in the area of eIDM.

ABOUT DIGITALEUROPE

DIGITALEUROPE, the organisation formerly known as EICTA, is the voice of the European digital technology industry, which includes large and small companies in the Information and Communications Technology and Consumer Electronics Industry sectors. It is composed of 62 major multinational companies and 48 national associations from 28 European countries. In all, DIGITALEUROPE represents more than 10,000 companies all over Europe with more than 2 million employees and over EUR 1,000 billion in revenues.

The membership of DIGITALEUROPE

Company Members:

Adobe, Agilent, Alcatel-Lucent, AMD, Apple, Bang & Olufsen, Bose, Brother, Buffalo, Canon, Cisco, Corning, Dell, EADS, Elcoteq, Epson, Ericsson, Fujitsu, Hitachi, HP, IBM, Infineon, Ingram Micro, Intel, JVC, Kenwood, Kodak, Konica Minolta, Lexmark, LG, Loewe, Micronas, Microsoft, Mitsubishi, Motorola, NEC, Nokia, Nokia Siemens Networks, Nortel, NXP, Océ, Oki, Oracle, Panasonic, Philips, Pioneer, Qualcomm, Research In Motion, Samsung, Sanyo, SAP, Sharp, Siemens, Sony, Sony Ericsson, STMicroelectronics, Sun Microsystems, Texas Instruments, Thales, Thomson, Toshiba, Xerox.

National Trade Associations:

Austria: FEEI; **Belarus:** INFOPARK; **Belgium:** AGORIA; **Bulgaria:** BAIT; **Cyprus:** CITEA; **Czech Republic:** ASE, SPIS; **Denmark:** DI ITEK, IT-BRANCHEN; **Estonia:** ITL; **Finland:** FFTI; **France:** ALLIANCE TICS, SIMAVELEC; **Germany:** BITKOM, ZVEI; **Greece:** SEPE; **Hungary:** IVSZ; **Ireland:** ICT IRELAND; **Italy:** ANITEC, ASSINFORM; **Lithuania:** INFOBALT, **Netherlands:** ICT OFFICE, FIAR; **Norway:** ABELIA, IKT NORGE; **Poland:** KIGEIT, PIIT; **Portugal:** AGEFE, APDC; **Romania:** APDETIC; **Slovakia:** ITAS; **Slovenia:** GZS; **Spain:** AETIC, ASIMELEC; **Sweden:** ALMEGA; **Switzerland:** SWICO; **Turkey:** ECID, TESID, TÜBISAD; **Ukraine:** IT UKRAINE; **United Kingdom:** INTELLECT.

How standards may help to deploy ID Management systems for e-Services

Introduction

In the context of the Single Market, EU citizens are free to travel and work within the EU Member states and carry out business across the EU. Legal Framework for the EU is intended to promote cross-border competition, meaning that citizens and corporations have to interact increasingly with any EU Public Administration using electronic means. E-Government seeks to improve the accessibility of public services and first of all to facilitate transactions so that pan-European e-Services becomes a reality.

In a highly distributed public network and services infrastructure with large numbers of mobile users and providers, Identity Management necessarily involves large numbers of queries and responses among diverse relying parties, alliances of relying parties, identity providers, and federations within which they may operate.

Standards target the global interoperability for ID management systems among service providers, network providers, government/regulatory agencies, countries/regional bodies and the citizens (end users/subscribers).

This Document has been developed by a team of experts involved in standardization activities on ID Management to capture the business requirements for ID Systems and the approach taken by the different standards bodies to specify architectures and frameworks.

Section 1 introduces ID Management system concepts as well as challenges that implementations have to face in a context of multiplicity of proposed solutions. Section 2 describes the rationale for standardization justified by the fact that harmonization of EU ID Management systems is required in view of providing cross-border access to services to mobile users. Section 3 describes some relevant aspects of the on-going ISO standardization effort followed in Section 4 by an explanation for the rationale for CEN and ETSI standardization initiatives. A short section for conclusion provides with some recommendations that summarize the different points discussed in this document.

1. The case for harmonization of ID Management systems

This section presents the different issues that an ID Management System is expected to solve with regards the usability and interoperability of e-Services, ideally cross-border, made at the disposal of authorized citizens, by the different EU administrations. This material is intended to introduce the approaches of the different Standards Bodies, ISO, CEN at ETSI involved in setting standards for ID Management.

- 1. In the following sections, it is assumed that authorization to access a service is achieved through the Identification of the user. Meaning that:**

- An authorized user is an user that has been successfully identified.
 - e-Services are therefore accessed through a four-stage process which starts with the Connection of an user to a distant Server to access a service, his/her Authentication, followed by an Authorization stage leading to the real Access to the required e-Service.
 - These core functions are to be available to all the actors involved in the provision of e-Services.
2. Authentication of an individual's identity appears as a fundamental component of logical access control processes meaning that an accurate determination of identity is needed to make the right access control decisions, either acceptance or rejection. Even if Authentication is another system entirely, system performs identification and authentication at the same time. However from a formal point of view, knowing who somebody is (identification) is different from the way somebody proofs who is he (authentication) and what he is allowed to do (privileges leading to authorization). This approach is accepted by on-going standards, recognizing the fact that from the system's security point of views this differentiation is fully justified.
 3. The ID Management System is a system with the ability to assert something about an individual pre-registered in the system. The problem to solve then is to ascertain as to whether an user claiming to be this pre-registered individual, is actually the same person that was pre-registered under a given identity. This given identity is made up of a series of attributes and is often associated with a unique Identifier. This Identifier may be submitted by an user as a claim of Identity. This pre-registered identity is associated with authentication information. If in addition of the claim, the user proofs knowledge of this authentication information associated with the identity, the claimer is assigned that identity, and he/her is said to have been identified. The process itself is the Identification. Identification is the fundamental service provided by any ID Management system.
 4. For the Identification Process to take place in the above terms, pre-registered users of the system must be issued an electronic ID credential, stored in some physical device under his/her control and compatible with the device used to Access the System. It is also clear that the reliability of the Identification process depends on the nature of the authentication information that the user has to provide to be successfully identified by the ID Management System. Before, or as the first step of the Authentication process, the validity of the ID credential to be presented by the user is to be verified.
 5. ID Management Systems, are made up of a series of logical and physical components implementing the set of processes needed for the creation, maintenance, utilization and verification of Identity Credentials. Components include access devices, personal or public, authentication personal devices, authentication and authorization servers and middleware. The system may be implemented using proprietary or standard technologies, that together constitute an Infrastructure for the provision of Services. Standards bodies initiatives make therefore consider that the adoption of future standard relies on their ability to provide an effective migration path, in both technical and economical terms, to existing proprietary ID Management solutions towards new harmonized ones.

6. Infrastructure and Services may be provided and /or operated by the same or different organizations. The ID Management system is therefore a complex and integrated one, whose components may be provided and/or operated by different collaborating organizations, that must agree on a common set of rules and policies according to regulatory constraints, in order to operate the system. Examples of these organizations include Identity Providers, Authentication Providers, Certification Authorities, Authorization Providers and Telecom Network operators, that other than providing ID – related data transport services may play other roles within the ID Management system..
7. In that context, Identity Providers role is central meaning that the number of Identity Providers is growing, and the choice of one of them could become complicated for a user. The Identity Provider issues the user with a form of Identity credential, that may be authenticated by a Service Provider and be adapted to the device that will be used to grant access to the service. The value of the ID Credential for the user depends on the number of ID Management systems that are able to process it. The importance of agreed standards is fundamental with regards to at least:
 - a. To enable the cooperation between different players as mentioned in point 5, through well defined and common logical interfaces
 - b. To maximize the acceptance of ID credentials by ID Management Systems
8. The objective of the ID credential is therefore to facilitate the authentication of the user in view to grant authorization by a Service Provider to access the offered on-line Services. Therefore the easy of deployment of Infrastructures for user Authenticate and authorization and the ability to handle ID credentials issued by different ID providers constitute key issues. An e-Services user , of course, does not care much how hard it is for the Service Provider to have the ID management system operating.
9. Ideally from the Identity Provider and Service Provider prospective, this Identity credential should accommodate to different access devices and transport networks to maximize usability and therefore the number of transactions thus generated. The success of a given on-line Service also relies on an harmonized set of procedures that make this access convenient and friendly regardless the specific device used for access and authentication. For the user, usability is what matters.
10. There are different IdM perspectives based on different sets of use-cases and requirements. As a result, there is no common global framework and infrastructure for ID Management .Several initiatives, including OpenID v2, Shibboleth, Liberty Alliance and SAML, ECP (SAML), CardSpace, try to resolve the choice of the Identity Provider by providing the service provider a way to determine the Identity Provider that can authenticate the user. The nature of these identity systems varies greatly, making hard to compare the proposed architectures. Each solution has its benefits and drawbacks. The rigorous benchmark of these solutions is out of the scope of the present document.
11. Due to the diversity of marketed solutions it is useful for standardization purposes, to agree on some criteria that may help to classify and compare the main services and functionalities that an ID Management service provides and their impact on the system

architecture and governance. Lack of a more general consensus, it is commonly accepted that ID Management Systems may be classified as:

- User Centric
- Service Provider Centric
- Identity Credential Issuer Centric

Yet these topologies are not a “black-and-white” ones and, in practice, real systems could be classified in a large range of “greys” dependent on the key use-case/s.

12. **User-centric** describes a model of ID Management developed primarily from the perspective of end-users and optimized for the interest of those end-users. User-centricity distinguishes itself from other models of identity management by emphasizing that the user - and not some authority - maintains control over how a user’s identity attributes are created, and the way the user’s identity attributes are released. The user’s control of identity attributes disclosure relates to the user’s willingness for privacy. Clearly all these features are difficult to achieve in a context of e-Services provided by a Public Administration, where the ID credentials are expected to be issued, then managed by the Government. The European Citizen Card standard intends to provide some balanced solutions where both the legitimate concerns of the citizens for the freedom of use of his/her card and the control by the Government on the ID credentialing process are taken into consideration. More details on this approach are provided hereafter
13. The above considerations mean that there is a strong case for standardization, in order to provide some degree of harmonization between proprietary solutions, that guarantees that the three basic functions, Access, Authentication and Authorization are interoperable and therefore doesn’t constitute a barrier for the deployment of new e-Services. Standards for ID management are expected to provide with a common set of protocols, semantics and processing rules that allows the various components of an identity management solution to interoperate.
14. Ideally standardized solutions should also be scalable, both in terms of the resources required for implementation and the diversity of Identity Credentials that might be authenticated. Because of legacy, migration considerations should be considered by standards bodies.
15. Barriers for adoption of an universal model for ID Management differ in their nature, including economical reasons (lack of killer business case, definition of priorities in the context of the crises), political (Governments expecting for Community Authorities to drive, lack of mutual recognition of electronic Identity Credentials), legacy (proprietary ID Management solutions that may go on as long as no cross-border e-Services are offered) and possibly legal (necessary harmonization of laws first at EU level, then at International) . It must also be kept into account that many ID Management operational systems are local, and do not attempt to become industry-wide standards.

2. Standardization context for ID Management

2.1 Barriers to the deployment of ID Management system

- **Multiplicity of existing proprietary solutions.**

A large number of industry groups and standards organizations are working on standardizing aspects of Identity Management (e.g., ITU-T, Eclipse (Higgins Project), Liberty Alliance, OASIS, OpenID, Shibboleth, W3C, ETSI, 3GPP, ATIS, and IETF are among the dozens of groups). ID Management models, frameworks and protocols have been defined by some of these organizations and compliant systems deployed. The result of today's highly distributed and autonomous ID environment has resulted in Identity Management islands with substantial interoperability issues.

- **Lack of sound Pan-European e-Service**

The lack of sound cross-border e-Services means that EU Public Administrations are deploying e-Services exclusively for their domestic market and native citizens using proprietary systems. This situation is likely to create in future barriers making it difficult further harmonization and EU-wide accessible new e-Services.

- **Insufficient recognition of the respective ID Credentialing Systems**

It's the consequence of the above. Recently there has been a significant ongoing coordination among EU governments on credential authentication platforms (ePassports and other Traveling Documents) and practices to identify persons within their jurisdiction. However for the ID domain this mutual recognition takes place through bilateral or multilateral arrangements which have to be motivated not only for political reasons but for the existence of common business models.

- **Existence of hard legal and regulatory requirements , including the protection of personally identifiable information**

There is clearly insufficient information on the difference between laws in EU.

When interacting electronically with an administration other than their own, it is often unclear for a foreign user to clearly capture all the legal consequences to provide for instance a proof of consent by signing electronically. This situation may create barriers for the development of cross-border e-procurement applications.

- **Role of the Citizen in the management of personal information**

Privacy laws impose controls on the interchange of personal information and specially identity attributes which should remain under control of its owner. Some of the proposed models for e-Government initiatives don't consider the citizen as an active player within

the system, but as the subject about whom different Public Administration exchange its personal information with no control from its own. That situation generates resistances from organizations that may campaign against the ID Management harmonization initiatives felt as favoring anti-privacy practices. Technologies that empowers the citizen on the control of his personal information (disclosure, confidentiality) go on the right direction.

2.2 Overcoming barriers: The case for standardization

At present different industry-led efforts tend to optimize their solutions for their specific market segments and perspectives (e.g., user-centric perspective, application-centric [web services and mobile/ electronic commerce] perspectives, and network/issuer centric perspective) with which they are associated. Since these standards may not meet the needs of certain industry segments or assume specific architectures and infrastructures, new standards efforts are inevitable.

In the context of building up an EU of e-Services, the technical objective for standards is to enable the integration of the existing ID Management technologies currently deployed. The case there is the creation and adoption of standards that specify platforms enabling any EU citizen in any EU member state to perform public and possibly private tele-procedures (including e-signatures) in each EU member state using its own ID credentials issued by its own Member State that will be processed according the EU law on privacy.

The concern for the e-Government vendors are that those standards be consistent (no contradictions), complementary (no overlaps), sufficient (no gaps, effective means to achieve interoperability) and realistic (costs for implementation compatible with business cases).

In that context the NWIP ISO/IEC 24760 assigned to ISO JTC1 SC27 WG5 constitutes in our opinion an attempt to provide some cross-industry bridges for near future. This project is explained in next section. CEN TC224 standards provides with more bricks targeting practical implementations and system integrators technical concerns.

3. The ISO SC27 WG5 Standardization Approach

ISO SC27 WG5 is currently involved in the definition of an ID Management Framework in a new standard ISO/IEC 24760. This valuable effort, however constitutes a first step towards the international harmonization of ID Management systems. As a good point, IUT-T experts are also involved in this ISO work, some government representatives are active as well. Notice that in our opinion for real interoperability to be achieved additional New Work Item proposals are needed to give rise to new parts of the standard to complement this initial work . These NWIP cannot anyway be submitted as long as the draft standard for ISO/IEC 24760 is not consolidated. The objective is to elaborate on the Framework and provide with more precise requirements for concrete interoperable implementations. For smart-card based solutions, that approach has been adopted by CEN TC224 WG15, refer to next section for further details.

ISO JTC1 SC27 WG5 differentiates between Identification, Authentication and Authorization systems even if it is recognized that these concepts are closely related. This approach enables the design of a system for access to on-line services as a layered implementation. Conceptually as explained in section 1, this separation of functions makes full sense. Work progress is inevitably slow because of the very own nature of the convergence process in an area where agreements at the most basic level (eg, vocabulary) are difficult to achieve.

At present a first Committee Draft Ballot for ISO/IEC 24760, has been launched, meaning that ISO JTC1 SC27 members are invited to submit comments to the text proposed by WG5. Probably at least two rounds of comments and the subsequent resolution of comments will be required in order to progress towards a first Final Committee Draft, meaning that the fundamental conflictual issues have been fixed.

4. European Standards for ID Management

CEN & ETSI have been collaborating in the past in common standardization efforts. An example is the publication of Common Work Agreements standard documents to specify the technical infrastructures, devices and logical interfaces to implement the European Directive on Electronic Signatures (1999/93).

For ID Management, the orientation of CEN & ETSI standards is to translate into the more general issue of the Web/ Telco convergence. From the citizen perspective this means the transparent processing of the different user identity credentials and implies the issuance of e-ID Credentials independent from access, transport network and type of terminal used.

CEN TC224 focuses rather on ID management from the Government perspective, whereas

4.1 CEN TC224

The consideration by the CEN TC224 WG15 standards (The “European Citizen Card”, ECC) of the ID Management issues as presented in the above sections is multiple. The ECC is defined as a smart card storing an ID Credential, issued under the authority of a Public Administration which may be used by the cardholder for secure access to e-Government services. Since the beginning of WG15 a concern was to make the ECC visible to the ID Management system in charge to verify ECC-stored ID credentials. The communication between the card and the e-Service Provider is achieved by establishing a connection between an Application resident in the Card and the so-called Client Application which is an agent of the e-Service. This interconnection of applications takes place through a standard middleware which is an extension of ISO/IEC 24727 tailored to the requirements of EU Public Administrations. One of the main principles for WG15 activity is to influence and converge with ISO standards.

This middleware is accessed through an API (Application Interface) of services. Through this API, the ID management system may retrieve an ID credential and also call for authentication

procedures to be executed by the card. That way, the ID management, identifier the user, thanks to the data provided by the card through successive API calls. Thus the middleware and the card jointly constitute a true authentication system. This system is accessible through the API , which constitutes the logical interface between ID Management System and the Authentication System, meaning that this separation between systems is effective.

CEN TC224 WG15 has also provided a substantial effort so that implementations of the ECC standard be fully compliant with European Directives (Data Protection, Electronic Signature).

1. By its own nature, the ECC stores Personal Identifiable Information (PIA) and must comply with EU Regulation on the Protection of Personal Data . A liaison has been set with ENISA in order for WG15 experts to be fully aware of the technical implications in terms of ECC functionalities derived from the applicable regulation. In particular an objective for the ECC is to support cryptographic security mechanisms supporting those functionalities required to face the privacy threats identified by ENISA.
2. In relation with the European Directive, the ECC implements the IAS (Identification, Authentication and Signature) paradigm. The ECC authentication and signature mechanisms comply with EN 14890, and therefore complies also with the European Directive terms. This functionality is useful when the e-Service requires a formal proof of consent by the user with legal value.

Because of the ECC issuance context, the e-Services to be accessed will in principle be in close relationship with the Public Administration Card Issuer. That means that at first sight the ECC is Issuer-centric. However when looking at the full set of mechanisms provided by the standard, this assertion is only partially true:

- The fact that the ECC only provides IAS services upon the cardholder authentication and therefore disclosure of Personal Identifiable Information is under control by the cardholder
- The ECC protects the privacy of the cardholder, due to the card capability to authenticate an external entity and then to create an encrypted communication channel
- The ECC cryptographic mechanisms enable direct authentication of a Service Provider provided that (1) this Service Provider is able to transmit a Card Verifiable Certificate format and (2) the ECC is aware of the Certification Authority that issued the Certificate to the Service Provider. This functionality may be useful when agreements are signed between the Issuer Government and Private Service Providers. On that edge, as an example ID Management Systems operated by Banks may accept e-ID Credentials issued by their Governments to

To summarize, the ECC standard accepts that all the requirements for an User-Centric pure approach (Section 1, §12) cannot be achieved when his/her ID credential is issued by Governments but tries to position anyway the citizen in the center of the system; On that edge it is worth to mention that the new part of the ECC standard, ECC part 0, provides insight into a Federated Model for the ECC, which provides a solution when cross-border

interoperability is required. Different system configurations ECC-compliant supportive of different business models may be considered there.

Finally notice that the same model has been proposed for the CWA e-EHIC (electronic European Health Insurance Card) for access to e-Health services. Common Infrastructures for ID Management may therefore identify users accessing either e-Government or e-Health services.

4.2 Mobile Telecom Standards for ID Management

4.2.1 ITU-T

The case for ID Management for Mobile Telecom operators is directly related to the deployment of new high-risk services, including mobile commerce and mobile payments. Network Operators and Service Providers appear highly dependent on ID Management to prevent and minimize fraud in the use their networks resources and services.

Different mobile financial services have different risk profiles. Cross-border money transfer may pose a higher risk, like for banks, but banks may often rely on a outstanding risk management system . The receiving party (the payee) may not be personally known of the Mobile Payment Service Provider. Indeed, Mobile Network Interoperability involves the availability and use of provider's network resources by other resources frequently worldwide. The compensation for this availability and use among Mobile Network Operators, and Mobile Service Providers requires for this industry in particular, standardized ID Management based accounting and billing regime.

Aware of these specific issues, ITU-T early launched efforts to agree on a set of basic requirements for Global Interoperable Identity Management as part of the ID Management -GSI (Identity Management Global Standards Initiative).The establishment of JCA-ID Management (Joint Coordination Activity for Identity Management) was approved in December 2007. At its first meeting of the 2009-2012 study period (Geneva, 28-30 April 2009), ITU-T agreed to the continuation of the JCA-IdM with updated terms of reference, and in particular the continuation of the ID Management –GSI work. The membership of the JCA-ID Management is composed of representatives from the ITU study groups and invited representatives from recognized ID Management external standards committees, consortia and forums. Thus a liaison has been established with ISO JTC1 SC27 WG5 to coordinate standards on-progress (ISO/IEC 24760 see section 3).

4.2.2 ETSI

ETSI has recently announced the creation of a new Industry Specification Group to develop a common industry view on Identity Management protocols and architectures, relating mainly to networks and services for the Internet of the future.

In the vision of the “Future Internet”, the notion of the network will move towards the 'Internet of Things' – an extremely complex world of numerous interconnected devices and services with a huge number of transactions to manage and bill, and therefore requiring effective and reliable identification of users. The triad (user, access device, service) is going to become increasingly complex to manage, specially considering that users assume different roles and identities at

different times and that they require access to different groups of services according to their current role.

ETSI assumption is that standardization of Identity Management has focused mainly on the web and application domains, with some activity also addressing Next Generation Networks. However, little has been done to address architectures and protocols that are the key to new networks and services and thus to business opportunities. ETSI has therefore identified the need to develop new common specifications to drive business out of Identity and Access management, for Mobile Network operators and Mobile Services Providers. The ETSI Industry Specification Group is expected to elaborate on the results of ID Management research and development (R&D) activity derived from European Union 7th Framework Project (FP7) on Identity Management.

The Kick-Off meeting took place last month and a basic consensus was agreed to develop specifications for:

- mechanisms, interfaces and protocols allowing service providers to perform authentication and retrieval of identity attributes through the network operator
- requirements on the use and application of distributed policy management such that, for example, authentication of the user by the communications network can enable their authentication for the various services they wish to access
- distributed user profile management where the network operator acts as an identity broker (taking responsibility for managing the user's identity)
- mechanisms, protocols and procedures allowing user access to their selected services based on “dynamic service level agreement (SLA)” negotiations.

Publication of these specifications is foreseen for March and October 2010. Notice however that many of these issues have already been addressed by ISO and CEN and Industry-led consortium. Because harmonized practices always favors adoption, to specify how large-deployed protocols for ID management may be supported by the card (SIM, UICC) would represent a significant and useful contribution from ETSI.

5. Conclusions

The Standardization effort must provide solution for some but not all the above mentioned barriers. In our opinion at present and at short-term the stress may be put in the following areas:

- The technical interoperability of ID Management systems taking into account legacy and migration aspects
- The openness of the different industry-specific initiatives to provide flexibility for later convergence when use cases justify for cross-recognition of ID Credentials between sectors
- To stick to the existing legal frameworks



COMPETITIVENESS AND INNOVATION FRAMEWORK PROGRAMME ICT Policy Support Programme (ICT PSP)

Towards pan-European recognition of electronic IDs (eIDs)

ICT PSP call identifier: ICT-PSP/2007/1

ICT PSP Theme/objective identifier: 1.2

Project acronym: STORK

Project full title: Secure Identity Across Borders Linked

Grant agreement no.: 224993

Challenges on eID beyond STORK Abstract document for ELSA eIDM

Actual submission date : October 09, 2009

Partner(s) contributing : Miguel Alvarez Rodriguez, Herbert Leitold, Marc Stern,
Yasmin Mazhari

Abstract: This document addresses challenges and issues that – from a STORK perspective – reach beyond 2011. These should be addressed in order to proceed to a sustainable European eID infrastructure.

Project co-funded by the European Community under the ICT Policy Support Programme

© Copyright by the STORK-eID Consortium

STORK is a European Project which brings together several EU Member and Associated States with the aim of elaborating a set of common specifications for the cross-border interoperability of governmental eIDs. The final goal of the project is to provide secure solutions for the electronic identification of citizens at eGovernment portals.

In the context of the project we have carried out work that could be classified as exploratory actions, aimed at identifying the main barriers for the interoperability of eIDs across eGOV services in Europe.

Basically, we have found legal, technical and organisational impediments. We are not convinced that we will be able to resolve all of the issues within the timeframe of the project; and we therefore see a need for a post-STORK action that will pick up from where we have left off, so as to address these questions.

The barriers for the interoperability of eIDs could be summarised as follows:

1. Obstacles linked to legal and organisational matters:

- **There is no common European regulatory framework on eID across Europe.** Diverging legislation and regulations on ID among the EU Member States is a serious barrier for the interoperability of eID solutions across Europe and even at national levels. There are many sectoral solutions on eID that are not compatible with each other from a technical and/or legal point of view. Furthermore, conflicting legislation on eID between MS adds extra complexity to interoperability. All of this makes the extension of eID solutions outside of the owner boundaries hard to achieve.
- **Trust and liability considerations** for the extension of eID that are used outside the owner's boundaries are a serious concern. This is true specially when there is no legal basis for the mutual recognition of eIDs issued, for instance, in another MS. In fact, one important topic to address for a future European interoperable scenario on eID, is the supervision schemes to be in place for the application of a common European Quality Authentication Assurance framework. There is a need to establish a common strategy that defines control-strategies to check whether the framework is applied according to its principles. **Security accreditation** of production systems and infrastructures that deal with eIDs is also an important matter to be discussed at European level.
- **Auditing.** The success of a European interoperable eID scenario depends on proper supervision and auditing procedure. The implementation of a cross-border framework for eID services must allow auditing procedures to promote adherence to the framework. For example, the current framework description defined by STORK allows for new eID solutions (of new member states) to be evaluated and assigned a proper level. This process, however, should be carefully monitored by some entities that are responsible for the overall quality and integrity of a European framework. Likely, these entities should have sufficient authority to solve sensitive liability issues that may occur between member states. In order to reach the desired interoperability, member states should perhaps use some kind of legal instruments. These legal instruments must specify the quality of service that member states can expect from each other.
- **Representation, mandates, and roles:** STORK addresses identification of natural persons as an important first step. Legal and operational differences in mandates, representation, and expressing roles add a further level of complexity. These aspects are however important to address A2A, A2B, B2C or B2B scenarios.

- Finally, **two legislative issues** have been identified that affect eID interoperability between EU member states: a) certain member states do not allow the use of persistent identifiers, and b) several national identifiers may not be used outside the specific member state.

2. Obstacles related to technical matters:

- **The great variety of standards and technical norms**, especially for smart-cards, makes the integration of eID solutions extremely challenging.
- In addition to this, it seems likely that **Contactless technology and near field communication or RFID, biometrics, Terrestrial Digital Television and mobile eID technologies** will play a key role in the field of eID in coming years. Furthermore, technologies based on **Trust Federation and Identity Frameworks** and **Credential based** approaches are emerging as very promising options. While the actual eID technology used does not directly affect the STORK model since it operates at a higher abstraction level in the cross-border federation, it does affect the client implementation landscape and needs to be kept in mind. Industry will have to work closely with governments so that these technologies can finally be expanded and suit eGOV needs.
- **User-centric identity frameworks** provide technical solutions to help users easily register with and sign on to web-based services. However, these frameworks alone cannot solve the human problem of establishing and maintaining trust. Convergence between user-centric and established federation standards and the incorporation of merged functionality into products are needed to bring user-centric identity management functionality to the mainstream. Combined, they would finally help to promote adherence to a European eID interoperable framework.

3. Other challenges not addressed in STORK:

- **Other ways of identification/ authentication** besides solely citizens and personal identification: Identification of public administration entities and workers, legal persons and delegation and representation/ empowerment of legal and non-legal entities.
- **Convergence of public and private sector solutions on eID**: Many governments are heavily investing in eIDs as one of the building blocks for providing secure eGOV services, encouraging the creation of a local industry for eID solutions. These public investments are also pushing the private sector in the same direction although at a moderate pace. Although there is great demand for the recognition of governmental eIDs in commercial applications, the lack of proper and simple routines that can cover many different solutions, are reasons why few Service Providers from the private sector support cross border activities. Although public eIDs meet many of the private sector needs, business models and propriety solutions still complicate, or even prevent, development and common deployment.
- **The private sector in some cases lacks the organisational and technological frameworks** for eID services. Instead, it is willing to use the solutions accepted and supported by the public sector, and also wants the public sector to handle an infrastructure that meets its need for flexibility. Public Sector Quality Authentication Assurance models could play an important role, as long as the Service Provider can rely on the mapping carried out by each national organisation.
- **Open or closed eID systems** are an important issue to the private sector, not from a security point of view but because of practical routines. As long as there are practical routines in place, the private sector could accept the same eID services as the Public

Sector, but there is need for a simple and stable routine to access eID services. eID services need to include entity authentication as well as digital signatures like signing data by natural persons and legal persons, or representatives of legal persons.

- **Public–Private sector synergies:** STORK focuses on eGOV applications, mainly using government issued eID. For long term sustainability, broad take up, all scenarios – A2A, A2C, A2B, B2C, B2B and C2C need to be considered.
- Business models are very important to the private sector and should be subject to further studies. It is important to provide flexible solutions in this regard.