JRC Scientific and Technical Reports

The State of the Electronic Identity Market:
Technologies, Infrastructure, Services and Policies

Authors: Toby Stevens, John Elliott, Anssi Hoikkanen, Ioannis Maghiros, Wainer Lusoli

EUR 24567 EN - 2010

JRC EUROPEAN COMMISSION

ipts Institute for Prospective Technological Studies

The mission of the IPTS is to provide customer-driven support to the EU policy-making process by researching science-based responses to policy challenges that have both a socio-economic and a scientific or technological dimension.

European Commission
Joint Research Centre
Institute for Prospective Technological Studies

Contact information
Address: Edificio Expo. c/ Inca Garcilaso, 3. E-41092 Seville (Spain)
E-mail: jrc-ipts-secretariat@ec.europa.eu
Tel.: +34 954488318
Fax: +34 954488300

http://ipts.jrc.ec.europa.eu
http://www.jrc.ec.europa.eu

JRC 60959
EUR 24567 EN
ISBN 978-92-79-17206-9
ISSN 1018-5593
doi:10.2791/4851

Luxembourg: Publications Office of the European Union

PREFACE

Identity is hardly a new issue – in fact, we have centuries of experience of face-to-face identity management. What is new in the Information Society is the digitalisation of identity management, both on the Internet and via offline databases. Authenticating onto systems, connecting to mobile networks and providing identity data to access services has become something we do several times a day. What is disruptive is that digital technologies fundamentally alter and upset the ways identity is managed, by people, companies and governments. One crucial question lies at the heart of digital identity management: how do I know you are who you say you are? A plethora of public and private services in the Digital Economy are trying to find a meaningful, convenient and reliable answer to the need for authentication.

There are also tools and systems to help people meet this need. Technological progress in cryptography, identity systems design, smart card design and mobile phone authentication has been remarkable. Today, a toolbox of useful technologies may give European users peace of mind in accessing services, both in person and remotely on the Internet (where the "who are you?" question is hardest to tackle). Yet, these advances have not enabled secure and convenient authentication to services across people's many spheres of activity: work, leisure, health, social activities. Least of all have they been used to enable cross-border service implementation in the Single Digital Market, or to ensure trust in cross border eCommerce.

It is true that recently the Commission and Members States have spearheaded several key initiatives in this area, both discretely and jointly – the European Large Scale Action on eID, the Future Internet Public-Private Partnership. But very seldom, if ever, the socio-economic impacts of these initiatives are clearly assessed, or the added value for Europe stated. We welcome this report as it joins up the dots, and provides significant exploratory evidence of the potential of eID for the Single Digital Market. A clear understanding of this market is crucial for policy action on identification and authentication, eSignature and interoperability.

The study offers an initial exploration of markets where people's identity data are converted into credentials for access to services. The picture portrayed is sobering. In principal, the report finds that the market for eID is immature. It claims that the potentially great added value of eID technologies in enabling the Digital Economy has not yet been fulfilled, and fresh efforts are needed to build identification and authentication systems that people can live with, trust and use. The study finds that usability, minimum disclosure and portability, essential features of future systems, are at the margin of the market and cross-country, cross-sector eID systems for business and public service are only in their infancy.

The good news is that the European Institutions and Members States hold the key to this potential, via procurement of strong eID in eGovernment services, enhancement of federation and interoperability as regulators, support of open governance and participation in standardization in international fora. Lastly, the report emphasises the need for future, further research on interoperable credentials, mobile phone and smart card authentication, which is where the value added may lie for European citizens, public services and business.

We are confident that this report makes a valuable contribution to this cause.

Detlef Eckert
Director, Lisbon Strategy and Policies for the Information Society - Directorate General Information Society and Media, European Commission

John Bensted-Smith
Director, Institute for Prospective Technological Studies, Joint Research Centre, European Commission

ACKNOWLEDGMENTS

The data collection and part of the analysis for this Report were conducted by Consult Hyperion for the IPTS. As well as acknowledging their role as co-authors, we are very grateful to Toby Stevens and John Elliott for their responsiveness in addressing our needs and requests, as more and more interesting insights emerged in the course of the study.

EXECUTIVE SUMMARY

Empowering citizens to be active and confident in the new digital society, which must deliver sustainable economic and social benefits, is of prime importance to Europe. EU Information Society Ministers are adamant in the Granada Declaration[1] that electronic identity (eID) will be a key driver of economic recovery in Europe. A crucial action in this respect will be the creation of an encompassing, interoperable, open-standards e-Authentication scheme for Europe; one that increases the capacity of the EU business and public sector to reduce the costs of and barriers to the provision and take up of services, cross-border and online; and one that empowers citizens to take and expect responsibility in the digital domain [action points 8-10, 13, 14, 18-21]. The European Digital Agenda[2] also sees eID as central to the EU27 economy, as it will help to unlock the added value of the Single Market. Key actions in this domain include intervention regarding e-Authentication and e-Identification, interoperability and open standards, consumer trust and confidence, and strengthening the eCommerce single market.

It is true that trusted and reliable online identity management and authentication are the gateway to the digital economy now in the making. They create enormous potential for advanced, high quality and efficient services. Though eID systems and processes have been developing over decades, they are still not particularly trusted or fit for the many activities that European citizens expect to conduct in their everyday digital lifestyles. Strong authentication based on cryptography is one of Europe's strength, but has not yet found fertile ground in business and government applications. Equally, secure tokens such as smart cards and digital credentials, are under-utilised and the growth of awareness and use among consumers and small businesses is sluggish. Additionally, the market for eID products and services is fragmented, far from efficient and lacks viable business models. Services based on mobile authentication and identity management have not yet realised their huge potential value. There are great engineering and legal differences between industry- and government-supported identity management systems across the EU27. As a result, the evolution of inter-country, interoperable, user-centric eID systems and processes is slow.

On the other hand, there is the realization that eID technologies and authentication services are essential for transactions on the Internet in both the private and public sectors (see footnote 2). Trusted, secure and interoperable eID is a key enabler of the Single Digital Market. The fulfilment of several objectives of the Digital Agenda and of the Granada Declaration rests on the possibility to convert personal identity data into usable, safe and trusted credentials for the implementation of cross-border, interoperable public and business services. The outcome of both agendas will depend on the capacity to understand, measure and monitor, with valid and reliable gauges, the consequences of this eID conversion in Europe.[3] Effective regulation of the personal identity space and its economic externalities requires a clear understanding of how the market for identity functions. But very little is

---

1 EU Telecoms Ministers. Granada Ministerial Declaration on the European Digital Agenda. Granada, 19 April 2010: Informal Meeting of Telecommunications and IS Ministers, 2010. Available from <http://www.eu2010.es/export/sites/presidencia/comun/descargas/Ministerios/en_declaracion_granada.pdf>.

2 European Commission. Communication from the Commission - A Digital Agenda for Europe. (COM(2010) 245). Brussels: European Commission 2010. Available from <http://ec.europa.eu/information_society/digital-agenda/links/index_en.htm>.

3 Point 28 and 29, and Heading 3, of the Digital Agenda and of the Granada declaration respectively.

known about emerging identity markets and the business models that support the use of personal identity data in transactions. Outcomes go well beyond issues regarding technical systems for identification and authentication. Identity has never been monetised to the extent that it is today: targeted profiling based on personal identity data is used for behavioural tracking; the lead business model for online free services is focused advertising; significant savings are achieved in the delivery of public services. Revenues in these fields are significant, taking the ideas of authentication for access to services to a different level.

At the moment, we know very little about eID as an enabler of the Digital Economy. Intelligence on market and innovation dynamics is needed to sustain market growth, improve service quality for citizens and offer a more cost-efficient and competitive identity framework for Member States. In this context, this report explores the trends, barriers and dynamic evolution of the European eID market, the roles of key public and private stakeholders within the eID marketplace and the processes which these use to create value. The report finds that:

1. eID infrastructure technologies, embedded in operational applications and services, will be critical to the development of broader eID applications, which are likely to emerge as a 'critical mass' of infrastructure becomes available. Whilst development of this infrastructure is a commercial issue, governments may be able to accelerate the process by providing incentives and framework conditions for standardisation, open development platforms and innovation.
2. Increasingly advanced eID services, that take the existing infrastructure and technologies as a starting point and build on them, so as to create novel added value services, are needed. These need to be accompanied and complemented by 'softer' services; for instance, consultation, training and risk or credit management. Moreover, a more flexible offer of products and services, which would allow customer companies to 'mix and match' the most relevant components according to their particular demands, would make the eID market more dynamic and better able to adapt to changing economic conditions. While most of the above are expected to be offered commercially, governments may be able to enhance the ability of companies to offer valuable eID solutions by motivating intercompany partnerships, where each company specialises in the activities they are most proficient in.
3. Interoperability and credential portability are key issues in eID market development. Currently, the eID market is relatively fragmented, with several standards and procedures across the EU27. Increased portability of credentials and use of federated identity schemes would result in higher take-up and more extensive use of eID solutions, thus contributing to market growth. Future online public services will rely on effective and interoperable credentials. For this to happen, appropriate Certificate Authorities, and permitted use of government root certificates and regulations to permit certificate use in mobile devices, would be needed.
4. Self-asserted credentials are gaining significant public trust and must be taken into account by eID interoperability initiatives. Self-assertion and volunteered personal information are shifting the balance of power in identity relationships away from traditional providers, initially national authorities and lately companies, towards data subjects. This may result in disintermediation for third parties that are no longer required, and lead to new business models for eID. However, governments have yet to make widespread use of self-asserted eID schemes; therefore a centrally-regulated, identity assurance framework for government use of commercial credentials, both within and between EU Member States, may be needed.

5. The availability of enhanced token devices that consolidate existing multiple tokens, and offers users additional functionality through local card readers (or embedded equivalents) would lead to greater adoption of certificate-based services, as would the incorporation of two-factor authentication into a wider range of identity processes.
6. Governments are in a key position to drive the development of the eID market, in many respects:
    a. As the largest customers of eID, governments have a significant influence on what solutions will be developed, what features and functionalities will be required, and what identification technologies will be used;
    b. As market regulators, governments may procure a common legal framework enforcing the trust new eID services need to flourish. Moreover, governments may encourage relevant industry standardisation bodies to work on the rollout of interoperable digital certificates;
    c. Innovation in the public sector, particularly in citizen-centric public services, will be a catalyst for eID market growth. More rigorous enforcement of existing regulatory frameworks to ensure a 'level playing field' may favour market growth.

Further development of affordable and interoperable infrastructure (i.e. smart-card readers), raising consensus on dispute resolution and liability management procedures, sharing through public-private partnerships of high cost/high risk activities (i.e. arising from large-scale eID enrolment schemes) and collecting and disseminating independent and authoritative data on eID markets, so as to support commercial and public decision-making processes, will also positively influence eID market growth.

To address these issues, the study proposes a number of policy options for the Commission to consider, which can be organised according to the layers of the eID value chain model that forms the basis for the analysis. These range from the technical layer to the legislative layers.

- ***Policy:*** develop shared standards and harmonised objectives for clusters of eID activities (with very different objectives), supported by public domain information about the eID market;
- ***Regulation:*** provide leadership and a standardised EU approach, delivered through improved interoperability of Member State eID schemes and a shared regulatory framework for eID activities, while not stifling natural innovation;
- ***Exploitation:*** promote innovation and cooperation between government and private organisations with a view to delivering open interfaces to eID systems and the use of federated eID schemes;
- ***Infrastructure:*** accelerate the process by incentivising standardisation and innovation and by undertaking the provision of costly components such as enrolling populations into eID schemes;
- ***Technology:*** encourage private sector organisations to develop enhanced user tokens, improved biometrics, and portable certificates for use across a range of devices.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION

1.1 Overview

Electronic identification and identities (eID) are indispensable to ensure access to public and private services – including health, education and security. Increasingly more of the personal sphere is recorded, stored and analysed to warrant access (e.g., nominal e-ticketing binds identity tags to transactions that were previously anonymous). These identity-based transactions take place via an increasing number and variety of identity systems. On the Internet, a heterogeneous system of identity assurance has built up over time, through a mix of open standardisation, engineering ingenuity and sheer monopolistic inertia. There is today a plethora of sector specific solutions (based on e.g. SSL encryption, PIN, tokens) and e-services (e.g. based on a PKI infrastructure with either strong or weak authentication).

Personal identity data are the keystone of these systems. People use personal identity data to authenticate themselves on systems, to access services on the internet such as email and social networking sites; their personal identity data are harvested and analyzed to provide contextual advertising and personalised services. In online transactions, personal identity data have never been used and monetised to the extent occurring today; they are becoming an important enabler of the digital economy. The number of identity-based transactions, both on and off the Internet, has grown significantly and will most likely continue to do so. This trend is linked to the increasing prevalence and multiplicity of eID systems that feed on such data, channelling personal identity data into identification, authentication and access to goods, services and resources.[4]

The interoperability eID across the public and private sectors generates significant economic externalities. While the economic significance of eID may be largely invisible today, emerging mobile, sensor-based and social networking applications facilitate the creation of novel services that, in addition to their other functions, enable users to perceive the economic importance of their electronic identities.

The European eID market is considered to be growing, but it is fragmented and often lacks viable business models. This raises the a challenge for policymakers of how to ensure that businesses abide by existing regulations, while at the same time supporting the economic development of electronic identities and services based on them. There is a well-known tension between the collection of personal identity data in business-to-consumer transactions and the respect for users' privacy preferences.

Effective regulation of the eID market requires a clear understanding of how it functions. Relatively little is known about new identity markets and what business models may support the exchange of identity data for services. Research on market and innovation dynamics will support the Commission's efforts to sustain the growth of the industry as to provide a more efficient and competition-supporting eID framework in Europe. It is thus necessary to study the current state of the identity markets, the roles and respective positioning of the various stakeholders and the dynamics of the value chain. This Report describes both the method and the substance of an exploratory study on the roles and strategies of the stakeholders in the eID market within Europe. It is meant to prepare the ground for a larger, more systematic assessment of the eID market in Europe, in the framework of theEurope2020.

[4] See M. Meints. Identity Management Systems - recent developments. (Deliverable D3.17). ICPP, Germany: FIDIS Network, 2009. Available from: <http://www.fidis.net/fileadmin/fidis/deliverables/new_deliverables/fidis-wp3-del3.17_Identity_Management_Systems-recent_developments.pdf>.

1.2 Research context and objectives

A significant number of companies operate in the eID market in Europe and worldwide. However, the industry is quite fragmented and in some cases lacks viable business models. Research on market and innovation dynamics is needed to support the growth of the industry, contributing to improved quality of life for its citizens and a more cost-efficient and competitive identity framework for the Member States.

eID is at a relatively early phase of market development, and consequently still face many challenges. It is thus an especially interesting object for study both in terms of market and innovation dynamics and in a prospective manner as an example of emerging digital applications. In this context, the study is exploratory of the development and dynamics typical of today's eID markets, the key trends taking place in the markets, and the differences of the various European identity markets (in terms of factors such as market size, relative development, and key drivers and obstacles).

This study gathers knowledge about the strategies, product portfolios, financial information, dynamics between players and about other relevant factors of eID market stakeholders in Europe. This knowledge contributes to the overall analysis of the eID market and to a better understanding of the economic factors affecting the eID markets national level, the drivers and barriers that affect the uptake of electronic identities, the business models likely to prevail and the other factors that contribute to generating innovation in the market. The focus of the study includes privacy, security, and new business models enabled by development in eID. It is expected to reveal:

- the nature, structure, developments and dynamics for today’s European eID markets;
- the key trends in the markets;
- who the key stakeholders in that market are;
- the key differences between the European eID markets in terms of size, relative development and key drivers and barriers.
- on what information companies base their eID-related business decisions;
- what external data sources they have at their disposal.

1.3 Methodology, data collection and analysis

The scope of work includes an accurate but not exhaustive analysis of the eID market, of the key stakeholders within that market, and the data sources that are available. A number of European countries were chosen in light of their eID infrastructure: Belgium, Finland, France, Germany, Spain and Turkey. The project methodology was light weight and exploratory but theoretically informed; it is sufficiently robust to provide the foundation for a possible larger future project.

Specifically, it comprised:

- a review of past pan-European analyses in the public and private sectors;
- an analysis of findings in view of modelling the eID landscape; and
- an assessment of market and innovation dynamics.

In order to define a theoretical model, existing principles of value chains were drawn upon, modified appropriately so as to apply to the European eID market. This resulted in a fresh theoretical model, based upon a study of academic best practice, that brings together key issues of infrastructure and technology provision; value-add eID services; control and regulation; and the dependence upon existing paper-based ID services to create value for eID.

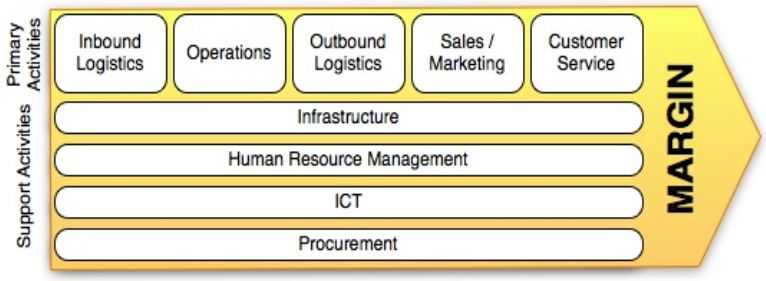


Figure 1: Theoretical example of value chain model
Source: Authors' elaboration from existing principles

In accordance with the theoretical model, the study collected detailed information about the eID market in Europe, so as to analyse the principal stakeholders in the field. Specifically a view of key issues influencing the global, European and national marketplaces, and characteristics of member states that may influence their eID strategies was built up. Largely subjective in nature, this work drew upon the researchers' expertise and experience rather than formal academic studies. Sources are credited as footnotes within the text.

A number of key stakeholders were interviewed. Telephone interviews based upon a set list of questions were used; and summaries of some of the organisations who have contributed have been provided, but individual interviewees or sources have not been identified.

Comprehensive information was gathered about industry stakeholders and their products, services, applications, needs and benefits. Data items were assigned one or more metadata ‘tags’ whici described, for example, the country, stakeholder type, value chain position or role. Tags were assigned on an *ad hoc* basis to ensure the broadest possible coverage of key issues. Data items were grouped by tags, to draw out the key themes from a range of perspectives. Where similar or synonymous tags were identified, these were aggregated under a single tag heading.

The groupings, and their inter-relationships, were examined in order to develop a value chain model for eID. The model describes the overall business, its structure and the relationships between the various actors, the functioning of the markets and the role/position of the various key stakeholders therein. The data items were mapped against the value chain model to define where they are within that model; this process was repeated to reveal different findings relating to market sectors, stakeholder types or nationalities.

2 MODELLING THE EUROPEAN EID LANDSCAPE

2.1 Applying value chains to eID

To understand the eID landscape it is necessary to examine the relation between different credential types, and hence their issuers; to consider their lifecycle, and hence how their value chains are structured; to analyse their maturity; and to look at their usage. Key to a successful model is the ability to understand the primary and supporting activities in the eID Value Chain. For this assessment, the primary activities have been classified into six layers as follow:

- ***Policy:*** Government policy and legislation that shapes and scopes the possible market for eID services;
- ***Regulation:*** Controls set in place by government and industry to control the eID market;
- ***Liability:*** Liability and accountability mechanisms used to build stakeholder trust in eID;
- ***Exploitation:*** Use of eID services and technologies by industry, public sector, individuals and non-commercial organisations;
- ***Infrastructure:*** Provision and operation of baseline eID infrastructure services;
- ***Technology:*** Underlying technologies used to build and operate eID systems.

These layers are derived from our experience of the current eID market, and they extend from the highest policy levels, through to the low-level technologies that are used to deliver eID systems. These are shown in the template Value Chain in ***Figure 2***.

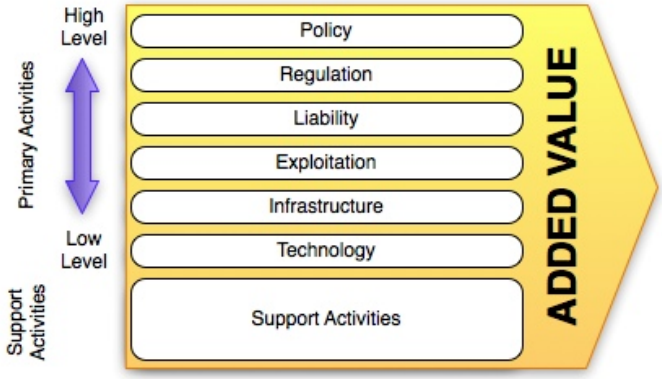


Figure 2: Value chain template

Additional supporting activities are those that do not specifically rest within these categories. For example, provision of paper-based credentials to authenticate an asserting party during the establishment of an eID relationship is considered to be a supporting activity in this context.

2.2 Considering eID qualities within the value chain

eID schemes may have different locations and qualities within the value chain. Issue and usage, applicability, lifecycle and maturity are all key issues within the value chain. These are shown on the value chain template in ***Figure 3***:

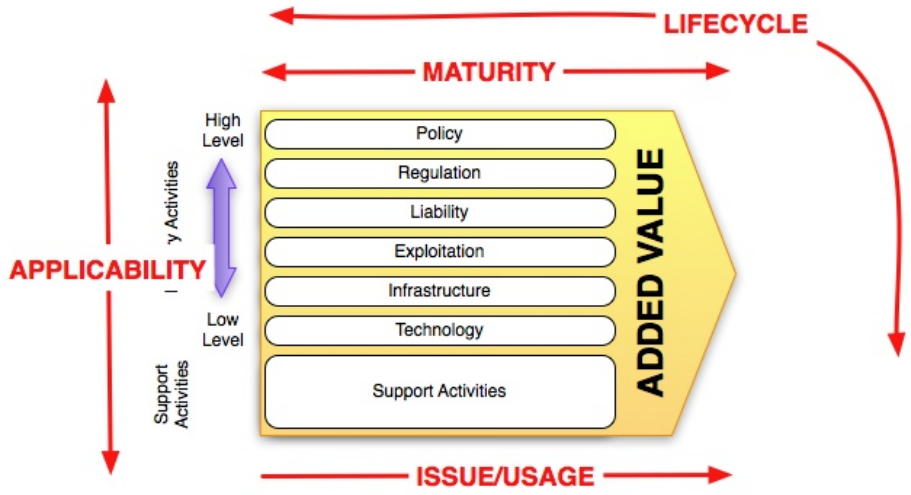


Figure 3: Applying credential types and usage to the value chain model

There are of course exceptions to this general approach, but it provides a useful framework for considering credentials where:

- ***Issue and usage:*** credentials may be issued or used across the length of the value chain; more commonly from start across to finish, since these represent more 'trusted' credentials (e.g. State-issued documents);
- ***Applicability:*** credentials (or components of credentials) may apply at different levels within the chain – for example a token may provide a credential but not be exploited;
- ***Lifecycle:*** the lifecycle (discussed in this section) covers all aspects of the credential from creation through to revocation;
- ***Maturity:*** defines the position of a credential or scheme within a maturity model.

These characteristics are explained in this section, which also describes the broader value chain model, considers the trends within the market and draws conclusions about likely long-term outcomes.

2.3 Credential issue and usage

The market for eID in Europe is characterised by three principal divisions, where these divisions are controlled by credential issuers:

1. ***State-issued credentials:*** these include national credentials such as passports, and regional/federal/departmental credentials such as local entitlement cards or residency passes. Credentials are issued in paper, electronic and 'hybrid' form (where a hybrid credential might be a plastic card with an embedded digital certificate).
2. ***Commercially-issued credentials:*** these include corporate credentials issued to employees for access to premises or IT services, banking credentials provided to individuals for online access to services, or telecommunication credentials (including mobile phone SIM cards). They are provided in paper, electronic and hybrid form.
3. ***Self-asserted / user credentials:*** these credentials are those generated, asserted or trusted by individuals or communities without necessarily having any reference to a trusted issuing authority. Dominated by 'low value' credentials such as those issued for access to online communities, these are predominantly electronic-only.

In general, State-issued credentials are considered to be the 'most trusted,' whilst self-asserted are the 'least trusted,' although increasingly there are exceptions to this rule. The challenge for self-asserted

credentials is that of becoming acceptable for use in regulated environments, and in particular in the financial sector, where 'know your customer' (anti-money laundering) rules demand that institutions obtain copies of recognised credentials prior to opening accounts. This gives rise to a value chain as shown in ***Figure 4***. In this system, the self-asserted credentials are both supporting the State-issued and commercially-issued credentials, and deriving their own value from them: operating in a 'hybrid' mode, where they are often enhanced after their initial use by a check on other credentials, and thus move from the 'supporting' row to the end of the chain on the right hand side of the diagram. For example, an individual may open a PayPal account without providing any form of credential check, but if they wish to transfer larger or more frequent sums of money, or to obtain a more trusted 'verified' status, they must submit other credentials for verification.

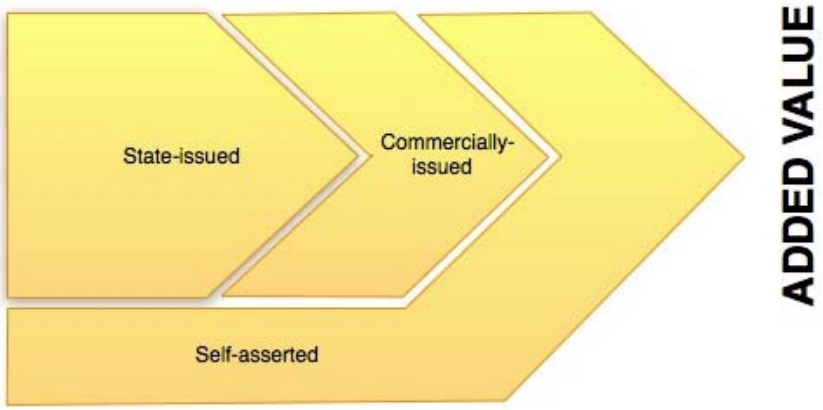


Figure 4: Credential value chain

2.4 Applicability of credentials

Credentials are not exclusively confined to a single division, but may in fact cross through them. This most commonly happens where there is a need for greater trust which draws upon a more trusted credential than is available to an application, for example:

- use of a passport as a supporting credential when verifying an individual's identity during the opening of a bank account;
- driving license used as proof of age;
- utility bills used as proof of address when requesting local government services;
- 'photo ID' used in support of payment cards.

This crossover/repurposing of a credential generally occurs where there is a need for a trusted credential at a new point in the value chain, which has to be filled by a more trusted authority in the absence of any other source.

2.4.1 Problems

Few, if any credentials are issued with no regard to where or why they might be used; in other words, they are designed and issued with a particular context in mind, even if that context is a very 'inclusive' one. However, in many parts of the world, social security numbers and driving license numbers have been repurposed as universal indices to track and identify individuals across public and private sectors. This may have repercussions for issuing authorities when problems arise; for example, most European states offer little or no liability for fraud arising from errors in national identity or passport documents. Such frauds themselves give rise to a complex 'illegal' value chain where false credentials are generated from an original fraudulent breeder document such as a passport, and propagate through the identity ecosystem.

The problem is amplified when the context spans national or sectoral boundaries, since credentials are then being used outside of the regulatory and legal environments in which they were issued.

2.4.2 Opportunities

Crossover/repurposing of credentials also presents a market opportunity, since it indicates a need for a new or enhanced credential type. It is this repurposing that will form a focus of the value chain modelling within our method, since it joins together the steps in the chain.

2.5 The credential lifecycle

It is also worth noting that credentials are generally subject to a number of different usage models over their lifecycle. Lifecycles themselves vary greatly, but can generally be mapped against a trust model as shown in ***Figure 5***.

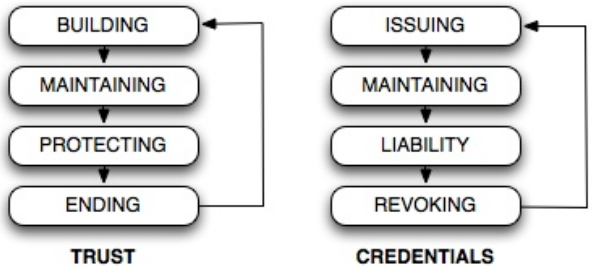


Figure 5: Credential lifecycle / trust model

In this model, the lifecycle comprises four stages:

- ***Building/Issuing:*** The strength of the trust relationship depends upon the integrity of how it is established; if rigorous checks are made to ensure that a credential is issued to the correct individual, then trust is created.
- ***Maintaining:*** Throughout its usage, trust – and the credential – must be maintained. This includes monitoring and updating the credential where necessary.
- ***Protecting/Liability:*** Trust must be protected: the strength of a relationship is judged by what each party will do to protect it when there is a problem. This applies to credentials, where all parties – but particularly the issuer – must take steps to protect them against fraud or failure. Where problems occur, the liability model becomes important, and defines the role of each party in repair and restitution.
- ***Ending/Revoking:*** For a trust relationship to maintain its integrity, it must be ended in a controlled manner that is satisfactory to all parties, otherwise it will quickly lose its reputation. This applies equally to credentials, which must be revoked in accordance with the expectations of all stakeholders.

This lifecycle model, whilst not directly part of our analysis, provides a useful framework to assess the effectiveness of a credential scheme.

2.6 Maturity and adoption

Whilst in many cases crossover/repurposing represents the use of a more ‘mature’ credential to establish greater authority, that is by no means a rule. The level of maturity is less important in establishing trust in a credential scheme than the trust in the issuing authority for a credential. Traditionally, a government-issued credential would be more trusted than one issued by, for example, a supermarket. There are examples of less mature schemes that have become very trusted: an eBay

vendor account with a very high reputational score may be considered highly trustworthy in a retail relationship without the need for further supporting credentials.

There is also the question of how, against a background of innovation, some technologies gain adoption, and achieve acceptance and maturity, much faster than others. For example, EDI messaging was slow to grow and never achieved consumer adoption; and SMS messaging was largely ignored by consumers (despite being available from the earliest days of GSM mobile telecommunications) until the late 1990s.

This adoption rate is most likely driven by a broad range of factors including:

- the underlying need, and readiness of the adoption community;
- the motivation to adopt the technology, which may include cost-savings or profits for users, mandatory/compliance issues, and intervention by government or commercial providers to incentivise adoption;
- removal of barriers to adoption, which may include initial cost, ease of use, cultural acceptability or consumer understanding of the need.

Of course, bringing together all these factors does not provide assurance of adoption: HD-DVD, DAB radio, PGP encryption are all examples of technologies that should by rights have succeeded, but have failed to meet their potential. Conversely, there are cases where technologies have succeeded despite there being no apparent need, or little motivation to adopt: Apple's iPod has become a byword for portable music players, despite early critics failing to understand why people might want the technology.

2.6.1 Achieving maturity

In considering maturity, it is worth bearing in mind the generic maturity levels in a capability maturity model[5] that describe the state of a system:

- ***Initial:*** ad-hoc or poorly defined;
- ***Repeatable:*** process dependent upon individuals;
- ***Defined:*** process defined and institutionalised;
- ***Managed:*** measured process;
- ***Optimising:*** improvement fed back in to process.

2.7 Scope and scale

Key to assessing the success of a particular eID scheme is the scale of adoption of that scheme. There are a number of qualities that characterise successful eID schemes; whilst not common to all successes, they are certainly present in many:

- ***Compulsion:*** where credentials are mandatory (e.g. National ID Card schemes) or a necessity for normal life (e.g. passports), they achieve widespread adoption. This is normally only achievable for State-operated eID schemes;
- ***Convenience/Transparency:*** the SIM cards in mobile phones provide a trusted eID infrastructure conveniently and transparently to the user;
- ***Pervasiveness/Practicality:*** where an eID scheme has achieved market dominance – e.g. payment cards – people will accept it as a *de facto* standard.

Compulsion and pervasiveness may of course be highly undesirable characteristics, as has been evidenced by protests against mandatory national ID schemes in the UK, or 'hidden' RFID tracking in supermarkets.[6]

[5] http://www.ogc.gov.uk/documents/PRINCE2_Maturity_Model_Version_1.pdf

2.8 Summary

The general Value Chain model can be applied to eID implementations by considering issues of policy, regulation, liability, exploitation, infrastructure and technology. These aspects will change according to the issue and usage of a credential, its maturity, position within the lifecycle, and applicability through the chain. The degree of trust afforded to a credential, and consequently its usage, will depend upon its position within the value chain, with State-issued credentials generally trusted more than commercial equivalents. In considering the adoption and use of a particular credential or scheme, it is important to consider its maturity and position within a trust lifecycle; and aspects of compulsion, convenience and pervasiveness in the credential infrastructure.

[6] http://www.spychips.com/metro/protest.html

3 PUBLIC SECTOR STAKEHOLDERS

3.1 Country profiles

In order to better understand the European eID landscape, it is necessary to consider how individual countries' eID markets have developed. This section describes the eID market in a selection of European nations.

3.1.1 Country analysis: Belgium

3.1.1.1 Policy

Belgium has a population of approx 10m individuals, most of whom are expected to hold an eID chip-card for national identification. The eID card is compulsory from the age of 12, but prior to that, the equivalent 'Kids-ID' is a voluntary credential. The eID card must be carried from the age of 15, unless one is within 200 metres of home.

Belgian citizens living overseas can also obtain ID credentials.[7] In June 2009 the Consulate General in Lille began issuing e-ID cards to Belgian citizens, in a service to be extended to all other Belgian embassies and consulates. The intention is to facilitate travel in or out of Belgium, and to simplify administrative procedures when the citizen temporarily or permanently returns to the country.

3.1.1.2 Regulation and liability

The state exercises a monopoly over the granting of eID cards, but not of the identities or, in general, the attributes of physical persons. The state may, for instance, retain an exclusive right to 'bestow' a particular attribute on an individual (for instance, the attributes associated with an office of public administration, a title, etc.) but this does not preclude, say, professional bodies retaining the exclusive right to bestow other attributes.

The laws on identity distinguish between physical and moral persons; there is no eID card for moral persons (i.e. corporate entities, companies etc), though the state retains the exclusive right to issue an identifier to moral persons (e.g. company registration number).[8] The individual's Numéro de Registre National (NRN) is considered to be a public value (in fact, it is visible in every eID cardholder's certificate), but (as in Norway) third parties are not supposed to use it without explicit prior approval from the administrative committee of the National Register.[9] There is, however, no apparent technical protection to prevent such use – the control is legislative only.

3.1.1.3 Exploitation

There is a wide range of public sector, community and commercial service providers exploiting the eID card, with applications including diary management for Prime Minister's Chancery; access to regional GIS databases; education (all tiers); healthcare, electronic patient records and database access, clinical data; transport and ticketing (e.g. de Lijn); generic access control – i.e. third party developers implement eID-based authentication for service providers; digital signing by card-holder; electronic tax returns and other e-administrative tasks, forms etc.; real estate transactions.

---

7 http://www.diplomatie.be/en/press/homedetails.asp?TEXTID=97135
8 http://eid.belgium.be/fr/binaries/FAQ_FR_tcm146-22451.pdf
9 http://eid.belgium.be/fr/binaries/FAQ_FR_tcm146-22451.pdf

3.1.1.4 Infrastructure

The Belgian eID card has been used as the basis for a broader eID infrastructure in which private sector organisations can participate. This has been achieved by developing a middleware interface where the government has published (but retains control of) the source code. The client (card reader) software is based on a Debian Linux open source library.

3.1.1.5 Technologies

The Belgian eID scheme[10] is built upon Sun Microsystems' Java Card technology, with Gemalto providing the cards, in a project that was managed by CSC.[11] Cardholders are able to purchase readers as well to simplify online use of the card for authentication and signing (the government has in fact 'primed' the market for readers by encouraging vendors to integrate them into all new PCs). Furthermore, interfaces have been provided into Adobe and Microsoft software to simplify and encourage adoption.

3.1.2 Country analysis: Finland

3.1.2.1 Policy

Finland's population of 5.3m individuals are subject to a voluntary ID card scheme, although all are obliged to register in the National Population Register.[12] Finnish eID cards were the first ever to be issued, and have been issued since 1999, at which time the National Population Register also began to issue digital certificates.[13]

3.1.2.2 Regulation and liability

Finland's data protection environment is regulated by the Data Protection Ombudsman, appointed by the Council of State.[14] National identity and eID issues are overseen by the Population Register Centre. Finnish citizens have the option to forbid disclosure of their National Population Register data for several purposes, including direct advertising, genealogical research and public directories.

The Finnish Communications Regulatory Authority (FICORA) supervises Certification Authorities (CAs). The Population Register Centre is the Government's own CA. Certain Finnish telecommunication operators are authorised by the government to issue electronic certificates for use in mobile applications. Certificates may be embedded in the eID card, a chip embedded Visa Electron card issued by the OP Bank Group, or the SIM card of a mobile telephone.[15]

3.1.2.3 Exploitation

Finnish eID cards are issued by local police in normal, minor and temporary forms.[16] From 2004 Finnish citizens were allowed to include their health insurance data in their ID card, thus removing the need to have a separate card for each. From 2008 KELA (the social insurance institution) stopped issuing new photo-cards – though photo-less ones continue to be issued.

---

10 http://www.cosic.esat.kuleuven.be/publications/article-769.pdf

11 http://www.csc.com/be/case_studies/9579-electronic_id_card_belgium_implements_affordable_digital_id_cards

12 http://www.ips.gov.uk/cps/files/ips/live/assets/documents/2005-02-07_URN_13_FOICR394_Final_Reply.pdf

13 http://www.e.finland.fi/netcomm/news/showarticle.asp?intNWSAID=15229

14 http://www.tietosuoja.fi/1560.htm

15 http://www.epractice.eu/en/document/288228

16 http://www.poliisi.fi/poliisi/home.nsf/pages/F082D8AB29097DB5C2256C29002BA66C

A national strategy for IT in health and social care was issued in 1996, and by 1998 there were pilot projects for the integration of previously fragmented county-level (regional) Electronic Patient Record (EPR) systems. In the early 2000s a 'reference directory' was established to provide an integrated source of information about the location of EPRs in local and regional systems. By 2011 clinicians will be required to use this directory.[17]

3.1.2.4 Infrastructure

Finland's eID approach demonstrates a high degree of integration between card- and mobile-based authentication services, probably largely because of the extremely high penetration of mobile networks and the distributed, low-density population pattern.

As of March 2007 a US OpenID provider (TrustBearer) announced[18] support for the Finnish eID card – meaning that the card could be used to gain access to sites requiring an OpenID authentication. In November 2008, Valimo (mobile identification service provider) and Elisa (mobile network operator) agreed[19] to implement mobile electronic identification, digital signature and PIN-based Single Sign-On to web services for Elisa's 2.5m mobile subscribers. In Finland this requires a linkage between the individual's registered ID and the SIM card. Valimo's services are also in use in Estonia (Elisa) and Turkey (Türkcell). Finland has issued biometric passports since 2006, citing EU security goals as the justification.[20]

3.1.2.5 Technologies

The cards are based on Gemalto technology, manufactured in Finland and using Java Cards.

3.1.3 Country analysis: France

3.1.3.1 Policy

France's national identity card (CNI) has been voluntary since 1955 for the 62m population. Unfortunately, it has for many years been undermined by mistrust, for example retailers would ask to see another form of ID as well as the card, when accepting cheques because of the simplicity of forging a card. In 1988 the card was 'rebranded' as a secure national identity card (CNIS) when additional security features were added (but without eID features). Machine-readable cards were introduced in 1995.

In 2005 the then Prime Minister, Dominique de Villepin, endorsed proposals for a new national identity card along lines very similar to the UK: biometrics on the chip, a centralised register of biometric and biographical details, and a fee for issuing the card. The French card was to be compulsory. As the National Commission on IT and Liberties (CNIL) observes,[21] this was the first time an identity document had been introduced in France with the sole aim of identifying the bearer, as opposed to establishing their entitlement to exercise some right. The proposals spurred massive debate, and as a result, the project was effectively halted pending a Senate commission review. A subsequent e-Passports project continues, and as of June 2008 the CNIL was expressing its reservations about this, the first ever centralised database of French citizens' biometric details.[22] Its view was the Government's case for the database failed to show that it was proportionate to the expected outcomes.

---

17 http://www.ehealtheurope.net/features/Finland/

18 http://www.trustbearer.com/news_fineid.html

19 http://www.arcticstartup.com/2008/11/03/valimo-signs-elisa-to-offer-mobile-identification-in-finland-and-estonia/

20 http://www.poliisi.fi/poliisi/home.nsf/pages/578F1B567FAFF824C22571CE00530098?opendocument

21 http://www.cnil.fr/dossiers/identite-numerique/fiches-pratiques/article/287/que-contient-la-carte-nationale-didentite-aujourdhui/

22 http://www.edri.org/edrigram/number3.13/IDFrance

3.1.3.2 Regulation and liability

In the 1970s a proposal to create a single, centralised index linking all citizens' departmental (state) IDs via a single 'national identity number' provoked such opposition that the CNIL was created specifically to guard against the erosion of citizens' liberties through technology.

It is not unusual for police to ask for proof of ID in France: the law says the citizen may prove their identity 'by any means': it is up to the law enforcement officer to decide whether the means offered is valid.[23] Citizens may present a driving license or a passport, even an expired one, or call witnesses.[24] France has a well-developed Certification Authority infrastructure, with 11 authorised CAs.[25] France is currently testing digital signatures at a local government level.

3.1.3.3 Exploitation

Two government portals (service.public and mon-service.public) offer public service information and citizen-centric functions respectively. For example, service.public has life-event themed information about commonly-used public services; as of Jan 2008, two-thirds of public services had been put online via the portal. The complementary mon-service.public portal provides a virtual vault where users can store the authoritative version of their personal information (such as address) and electronic copies of documents relating to their interaction with public bodies (such as birth certificates and tax returns).

3.1.3.4 Infrastructure

An additional eID healthcare card has been issued in France:[26] the SESAM-Vitale card is provided by a group of health insurance funds and used for healthcare access only. It does not have a bearer photo on it. As of 2004 it was reported that there were 10m more SESAM-Vitale cards in circulation than eligible citizens. As a consequence, SESAM-Vitale 2,[27] a technology refresh with better security, started in 2007. In the new architecture, the card does include a bearer photo, and must be used along with the healthcare professional's card (CPS) to unlock access to the central EPR system. SESAM-Vitale-2 is a joint project of SAGEM, France Telecom and Atos Origin.

3.1.3.5 Technologies

France has an exceptionally well-developed eID industry, which includes industry-leading technology in fingerprint recognition (SAGEM), and smart-card/SIM and related capabilities (Oberthur, Gemalto – with its heritage of Bull, Schlumberger, Gemplus and Axalto).

3.1.4 Country analysis: Germany

3.1.4.1 Policy

It is compulsory for Germany's 82m citizens to register for national ID cards from age 16, although there is no obligation to carry the card.

3.1.4.2 Regulation and liability

The German constitution prevents centralisation of personal information by the State (although this does not apply to visa applicants or people registered by the police for investigation into criminal activity). The German ID Card Act 1987, prohibits the use of unique ID numbers and storage of data

[23] http://en.wikipedia.org/wiki/Identity_document#France
[24] http://www.edri.org/edrigram/number3.8/ID
[25] http://www.net-entreprises.fr/Html/certificat.htm
[26] http://www.ehealtheurope.net/Features/item.cfm?docId=195
[27] http://www.sesam-vitale.fr/programme/programme_eng.asp

on a central register. The population are generally supportive of ID cards, but wary of biometric ID technologies. An example of this nervousness about some technologies is the high-profile opposition to the Metro Group's experiments with RFID item level tagging and contactless loyalty cards.

A Federal Information Commissioner and State Information Commissioners oversee the use of personal information, and have a reputation for punitive intervention where data protection rules are breached, e.g. Citibank/German Railways,[28] SWIFT.[29] Digital signature laws provide stringent technical definitions for the use of e-signatures.

Germany has a well-established ecosystem of Certificate Authority (CA) service providers, including issuers of certificates and digital-signature-capable smart cards, including TeleSec, D-Trust, Deutsche Post, TC Trust Center, DGN Deutsches Gesundheitsnetz Service, Medisign and Deutscher Sparkassen Verlag. The government accredits CAs, and government-issued ID underpins most identity services. Germany generally suffers lower levels of identity-related fraud compared with other developed nations.

3.1.4.3 Exploitation

The new German eID card is intended for government and commercial use. Commercial functions include allowing users to generate one-way pseudonyms for privacy protection. German railways also operate a contactless ticketing system in which customers can purchase a ticket using a mobile phone. Because of the legacy system, the ticket is sent as a bar code via MMS, which can then be machine-read from the phone's display. German citizens also use an Electronic Health Card for access to health services.

3.1.4.4 Infrastructure

German public services rely heavily on the national ID card. The cards are produced by the (Federal) Bundesdruckerei, but managed regionally. From Nov 2010, an eID card will replace the current scheme, and is envisaged as having three principal uses: a biometrically-secured travel document; a physical vehicle for an electronic ID credential, allowing the user to make trustworthy assertions to third parties online; a means for the citizen to generate qualified electronic signatures, for e-Gov and e-Business applications. The user has control over eID functions in online use. Service providers need a Federal certificate which specifies the card fields they may access, and that access is user authorised with a PIN.

3.1.4.5 Technologies

Germany has a well-established eID marketplace, with Giesecke+Devrient (G+D) the leading provider of smart card technology, and Deutsche Telekom (T-Mobile) and Siemens wielding a great deal of influence.

3.1.5 Country analysis: Spain

3.1.5.1 Policy

Spain's population of 40m are subject to a compulsory national ID card (Documento Nacional de Identidad – DNI) for all citizens over the age of 14. The bearer must present it if demanded by a police officer, but this may take the form of asking the police officer to the place where the card is kept. The DNI is used as proof of identity for a very wide range of transactional functions, including loan/bank account applications, contract signature, police fines etc. It is one the valid forms of identification which may be used to prove identity for voting (though driving license, passport and some other official documents are also valid).

[28] http://www.privacyinternational.org/survey/phr2003/countries/germany.htm
[29] http://www.privacyinternational.org/article.shtml?cmd%5B347%5D=x-347-542162

An eID version of the DNI was introduced in 2006, and includes digital signature capabilities. Roll-out of the electronic card reached 420,000 citizens by March 2007, and some 9 million by March 2009. Also since 2006, Spain has been issuing EU-compliant ePassports with biometric data on the chip.

3.1.5.2 Regulation and liability

The Spanish Data Protection Authority is the Agencia Española de Protección de Datos.[30] Spain has very specific regulations for the management of personal information; for example, the exact nature of security measures to protect personal information is specified in law. Spain has 14 commercial Certificate Authorities as well as several non-commercial providers.[31]

3.1.5.3 Exploitation

Spain has long-established commercial CA services: ACE (Agencia de Certification Electronica) was set up in 1997 as a joint venture between Telefonica, Sermepa (IT and payment services provider) and others, with Verisign CA technology and Visa/Mastercard licenses. ACE did pioneering work on qualified certificates and signatures in the early 2000s.[32] The PKI/CA infrastructure in Spain is relatively mature. There is a public CA (CERES) and a multi-PKI validation service (@firma), the latter set up explicitly to encourage the use of eID and eSignature capabilities in the delivery of G2C applications and services. Spanish regional and commercial PKI capabilities are also quite well-established. In the early 2000s, the Spanish were already demonstrating digital signature-based applications for multi-party real-estate transactions (i.e. including transfer of title, mortgage approval and so on), e-voting (first municipal e-voting elections held using a mobile e-polling station[33]), and in 2004 remote e-voting systems were piloted in several regions.

3.1.5.4 Infrastructure

Spain has a highly federated government structure, with 17 autonomous regions; these and 16 central government ministries are all linked by a governmental intranet, conceived in 2000 and implemented in 2002. There is also a network (SARA) which connects central government agencies, all the autonomous communities and 1,600 local municipalities. SARA provides public sector bodies with common access to the following functions: checking a person's identity and residence data; @firma , the multiPKI validation platform for eID and eSignature services; notification of a change of address; certified electronic notification; payment gateway; single electronic registry; catalogues of the procedures of the Public Administrations; videoconference; Voice over Internet Protocol (VoIP); collaborative working environments.

Citizen e-government delivery is achieved through a 3-part system called ‘Red 060’ (‘Network 060’).[34] The portal was launched in 2006, and as of March 2009 linked to some 1,225 public service providers at local, regional and national level. There is also a programme to reduce the effort required for local/municipal bodies to implement and deliver common e-government and e-administration services. The Avanza[35] project is run by FEMP – the Spanish Federation of Municipalities and Provinces. It makes available a standard application suite and set of IT platforms so that authorities can integrate citizen-facing services with back-end functions such as accounting and geographic information systems (GIS).

30 https://www.agpd.es/portalweb/index-ides-idphp.php
31 http://www11.mityc.es/prestadores/busquedaPrestadores.jsp
32 http://www.enisa.europa.eu/doc/pdf/publications/enisa_quarterly_10_08.pdf
33 http://www.tiresias.org/research/guidelines/evoting_projects.htm#spain
34 http://www.060.es
35 http://www.planavanza.es/AvanzaLocal/Estrategia/ContextoPlanAvanzayEELL/AvanzaLocalSolu/

3.1.5.5 Technologies

Spanish ID Cards (DNIe) are provided by the Royal Spanish Mint (FNMT-RCM), using embedded chips provided by ST Microelectronics.[36]

3.1.6 Country analysis: Turkey

3.1.6.1 Policy

Plans for a biometric eID card for Turkey's 70m citizens were announced in July 2007. The card will be used solely for identity verification purposes, and will store static identity-related information but no dynamic information such as address, healthcare data etc. It will include a fingerprint biometric, but this is to be stored only on the card, with no centralised copy. The July 2007 announcement also detailed a 3-stage pilot implementation project with initial stages in healthcare and social services use of the eID card. Phase 2 is reported to have concluded in Jan 2009 and Phase 3 started in May 2009.

3.1.6.2 Regulation and liability

Turkey's strategy for eID is overseen by the 'eTransformation Turkey Project[37]' which includes representation from ministries, central public agencies, NGOs and universities. The government has enacted e-signature laws that are EU Member States compatible and has three commercial Certification Authorities.

3.1.6.3 Exploitation

The Turkish mobile sector is relatively mature and sophisticated, with operators such as Turkcell delivering innovative mobile-based services including digital signature (since March 2008). The banking sector is similarly mature, with 12 banks already capable of using mobile signatures by 2007, and five of those signed up to the Turkcell mobile signature programme.[38] Consumers use the signature services for loan applications, authentication, mobile banking, cardless ATM usage and transaction confirmation services. The e-Government portal (e-Devlet Kapısı),[39] developed and operated by Turksat (satellite network and IT services company), combines about 19 agencies and over 50 services. The portal was launched in December 2008.

3.1.6.4 Infrastructure

Since January 2003, the MERNIS central population register has maintained a single ID number for some 120m Turkish citizens (living and deceased), including computerised birth certificates. Public agencies with appropriate security authorisation are able to access MERNIS through KPS – the Identity Information Sharing System. For tax, online theft reporting, job search and library services a relatively mature, a semi-transactional online service is available. For most other e-government functions the service is information-only and/or geographically patchy in implementation (e.g. Ankara-only).

3.1.6.5 Technologies

The Turkish government is now piloting the new eID scheme in the town of Bolu. It has developed a smartcard reader terminal for commercial and home use.

---

36 http://www.st.com/stonline/stappl/cms/press/news/year2006/t2079.htm

37 http://ec.europa.eu/idabc/servlets/Doc?id=29099

38 http://goliath.ecnext.com/coms2/gi_0199-7518968/TURKCELL-LAUNCHES-MOBILE-SIGNATURE-SERVICE.html

39 https://www.turkiye.gov.tr/portal/dt?channel=icerik&icerik.kat=Vatanda%C5%9F

3.1.7 Summary

A selective analysis of six EU nations reveals developmental differences in their adoption of eID technologies. Whilst the sample is not sufficiently large to draw 'definitive' conclusions, it would appear reasonable to conclude that the provision by the State of a trusted eID mechanism, in which businesses are prepared to invest trust, is key to promoting adoption of eID technologies. To make this work, a government eID scheme requires supporting infrastructure that includes:

- open access to the eID scheme by industry, including the ability to utilise system interfaces without licensing fees, and publication of clear standards for interface purposes;
- availability of Certification Authorities who can issue certificates for specific applications, sectors or territories;
- portability of certificates so that they are not embedded solely in a smartcard (or the ability to make copies for use elsewhere);
- provision of a smart card infrastructure so that individuals can reasonably expect to have access to card readers at home, work and in public places.

3.2 Comparison of national identity schemes

The Country Profiles in ***Section 4.1*** suggest that government provision of a population-scale eID infrastructure, coupled with open access, availability of Certification Authorities, portability of certificates and provision of smart card readers, are all factors in the success of an eID scheme. This section explores these aspects of national eID schemes for a broader range of European countries.

3.2.1 Evaluation criteria

Based upon the criteria suggested by Section 4.1, a number of factors have been selected to compare eID implementations by key headings:

- ***Policy:*** whether there is an obligation to enrol in a scheme, carry an eID card, or the ability to use it as a travel document (for this we assume travel to be within the Schengen zone[40]);
- ***Implementation:*** details of the issuer, and approximately how many individuals have been enrolled;
- ***Exploitation:*** availability of independent national Certification Authorities (CAs), and availability of 'portable' certificates (i.e. those which can be used outside of the issued credential, such as embedded in a mobile phone);
- ***Infrastructure:*** availability of smartcard readers for end-users to interface with the scheme.

3.2.2 Comparison of National Identity Schemes

The comparison of National Identity Schemes is shown in ***Table 1***, with key notes as follows:

- Compulsory enrolment: where individuals are legally obliged to enrol in the scheme, and the minimum age is known, this has been indicated;
- 3rd-Party CAs: every country under scrutiny operates independent Certification Authorities (CAs), but where the number of CAs is known, this has been indicated;
- Portable Certificates: indicates whether the certificates can be copied/issued to devices other than the ID card;
    - ***End-User Card Readers:*** indicates whether the scheme supports card readers for end users (as opposed to solely for government use).

[40] http://europa.eu/abc/travel/doc/index_en.htm

Feature	Population (m)[41]	Scheme	Policy[42]			Implementation		Exploitation		Infrastructure	
Country			**Compulsory Enrolment**	**Compulsory Carry**	**Travel Document**	**Issuer**	**Rollout Status**	**3rd-Party CAs**	**Portable Certificates**	**Open Interface**	**End-User Card Readers**
Austria	8.1	Bürgerkarte	N	N	Y	Ministry of Finance	8m	Y	Y	Y[43]	Y
Belgium	10.4	eID	From 15	Y	Y	FEDICT	8m	2	Y	Y	Y
Estonia	1.3	ID-Card/ Mobiil-ID	Y	N	Y	Ministry of Economic Affairs and Communications	1m	Y	Y	Y	Y
Finland	5.2	FINEID	From 16	Y	Y	Population Register Centre	265,000	Y	Y	Y	Y
France	60.0	INES	N	N	Y	Interior Ministry	N/K	11	Y	Y	Y
Germany	82.6	Digital IDCard	Y	Y	Y	Interior Ministry	Pending	Y	N	N	Y
Italy	57.8	CIE	N	N	Y	Local Administrations	40m	19	N/K	N/K	N/K
Netherlands	16.3	DigiD / eNIK	From 14	Y	Y	Interior Ministry	N/K	4	N/K	N/K	N/K
Spain	42.5	DNIe	From 14	Y	Y	National Police	18m[44]	14	N/K	N/K	N/K
Sweden	9.0	Nationellt Identitetskort	N	N	Y	Tax Office / Police / Transport Board	3m[45]	Y	Y	Y	Y
Turkey	71.3	eID Card	From birth	Y	N	General Directorate on Population and Citizenship Affairs	Pilot area	3	N	N	Y
United Kingdom	61	NIS	With passport	N	Y	Home Office	Pilot area	4	N	N/K	N

Table 1: Comparison of eID Schemes

41 http://www.nationsonline.org/oneworld/europe.htm
42 http://en.wikipedia.org/wiki/List_of_identity_card_policies_by_country
43 http://www.a-sit.at/pdfs/rp_eid_in_austria.pdf
44 http://blog.negonation.com/en/smart-cards-in-europe-eid-avalanche/
45 Data as of 2006: http://www.epractice.eu/en/document/288382

3.2.3 Summary

The analysis does not provide conclusive information about interoperability or adoption of eID in the nations surveyed, since there are such great variations in the nature, age and delivery of national eID programmes. Clearly a compulsion to enrol and carry an ID card will ensure a greater level of adoption. However, it is clear that certain schemes have been more successful than others: Belgium and Estonia in particular have achieved widespread adoption and delivery of eID services.

> Where national eID schemes have been successful, it is likely that the availability of third-party certificates; portability of those certificates; and provision of end-user card reader devices have promoted adoption.

3.3 Public sector initiatives

In this section we describe a selection of the key public-sector eID stakeholders in Europe. These cover research projects and government agencies.

3.3.1 Projects

There are a number of key projects – primarily funded by the European Commission – that are exploring and establishing pan-European standards in eID.

3.3.1.1 FIDIS

The Future of Identity in the Information Society (FIDIS)[46] is a large EU FP6 Network of Excellence targeting various aspects of digital identity and privacy. The partners of the project are universities and companies working in areas related to digital identity. FIDIS areas of interest include new forms of ID cards, usage of identifiers in information systems, technologies used for citizen's identification and profiling. The activities cover:

- 'identity of identity' (definitions of key terms in the domain);
- profiling;
- interoperability of IDs and ID management systems;
- forensic implications;
- privacy and the legal-social content of identity;
- high-tech ID;
- mobility and Identity.

FIDIS has provided a number of publications on the changing nature of 'natural' to 'digital' identity, and predictive publications on possible scenarios for the future of ID. This includes substantial work on the nature of 'partial identities' or personae. FIDIS started in 2004, and whilst it has technically finished, the project continues to provide deliverables.

[46] http://www.fidis.net

3.3.1.2 STORK

3.3.1.2.1 Overview

STORK[47] is a large-scale pilot operated by a consortium of European Public Administrations and private partners and 50% co-funded by the EU. It aims to implement an EU-wide interoperable system for recognition of eID and authentication that will enable businesses, citizens and government employees to use their national electronic identities in any Member State. It will also pilot cross-border eGovernment identity services and learn from practice on how to roll out such services, and to experience what benefits and challenges an EU-wide interoperability system for recognition of eID will bring.

3.3.1.2.2 Objectives

The STORK interoperable solution for eID is based on a distributed architecture that will pave the way towards full integration of EU e-services while taking into account specifications and infrastructures currently existing in EU Member States. The goal is to simplify administrative formalities by providing secure online access to public services across EU borders. The solution provided is intended to be robust, transparent, safe to use and scalable, and should be implemented in such a way that it is sustainable beyond the life of the pilot.

3.3.1.2.3 Actions

The project will:

- develop common rules and specifications to assist mutual recognition of eIDs across national borders;
- test, in real life environments, secure and easy-to-use eID solutions for citizens and businesses;
- interact with other EU initiatives to maximize the usefulness of eID services.

3.3.1.2.4 Outcomes

STORK takes diverse implementations and reduces them to a simple set of architectural options, which simplifies interoperability of the member states' ID systems. Pilots including private sector Identity Service Providers are expected to go live in 2011.

3.3.1.2.5 Stakeholders

The project's key stakeholders include:

a) Private sector companies working on eID who collaborate through the STORK Industry Group;
b) other European Public Administrations (Member State Reference Group);
c) other EC funded Large Scale Pilots on eID; and
d) European Commission A2A services such as ECAS.

STORK does not have competitors as such, since it is a public sector driven initiate. Nevertheless, commercial solutions in the field of eID could somehow overshadow public administrations' efforts if alignment is not successfully achieved.

[47] http://www.eid-stork.eu/

3.3.1.2.6 eID value chain

STORK is intended to become a reference model that can be made extensively available to both the private and public sectors Europe-wide, given the large number of countries and administrations involved in the consortium and the extraordinary effort put to develop an infrastructure that covers most of the stakeholders' needs.

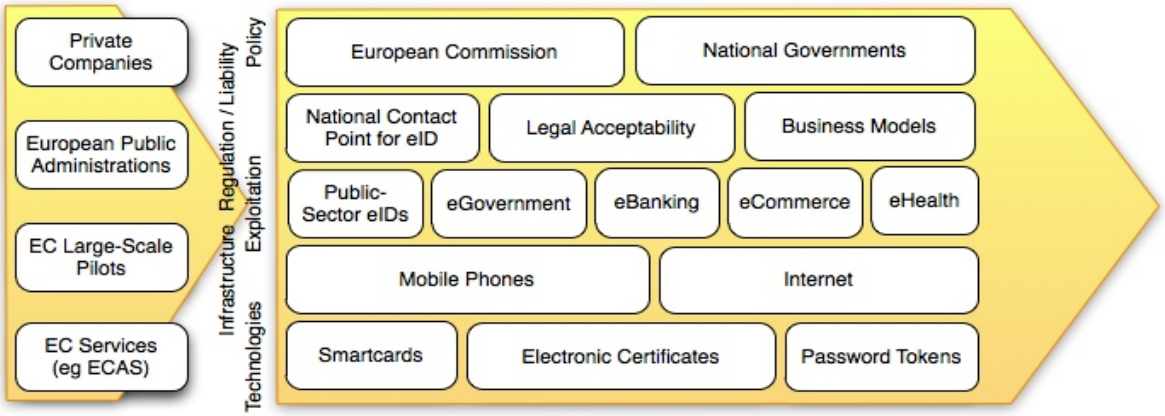


Figure 6: STORK Value Chain

3.3.1.3 PRIME

PRIME,[48] an EU FP6 project, concluded in June 2008. PRIME aimed to develop a working prototype of a privacy-enhancing Identity Management System, and included formative work on PETs (Privacy Enhancing Technologies) and their potential contribution to a trusted information society. To foster market adoption, novel solutions for managing identities had been demonstrated in challenging real-world scenarios, e.g., from Internet Communication, Airline Passenger Processes, Location-Based Services and Collaborative e-Learning. PRIME was primarily a research project. The work on prototype development was a means to validate its new scientific and research results. PRIME's work is now continued by PrimeLife, PRIME's follow-up project.

3.3.1.4 PRIMELife

The successor to PRIME, PRIMElife[49] is an FP7-funded project researching core privacy and trust issues. The programme's objective is to facilitate anonymity in life-long personal data trails without compromising on system functionality. To achieve this, PRIMELife will focus on areas of human computer interfaces, configurable policy languages, web service federations, infrastructures and privacy-enhancing cryptography. Open Source communities and standardisation bodies will be encouraged to adopt privacy technologies. The project started in 2009 and is still in its early stages, but highly relevant to eID interoperability.

3.3.2 Academic federation/inter-federation

3.3.2.1 Kantara

The Kantara[50] initiative was established in 2008 to create a robust focal point for collaboration within the identity community. The programme aims to bring together work on key issues including interoperability and compliance testing, identity assurance, policy, privacy and software development.

[48] https://www.prime-project.eu/
[49] http://www.primelife.eu/
[50] http://kantarainitiative.org/

Members of the initiative (who contribute towards its funding) include the DataPortability Project,[51] the Concordia Project,[52] Liberty Alliance,[53] the Internet Society (ISOC),[54] the Information Card Foundation (ICF),[55] OpenLiberty.org and XDI.org. Kantara is unique as the first time that so many other initiatives have collaborated on a common goal of improving adoption of interoperability within identity.

3.3.2.2 TERENA (EU)

Terena[56] provides a forum to collaborate, innovate and share knowledge in order to foster the development of Internet technology, infrastructure and services to be used by the research and education community. In the context of eID, Terena looks at interoperability between existing federations. Established US federation programmes with Terena liaison include Internet/2[57] and InCommon.[58] Terena is engaged in ground-breaking work in attribute-level authentication, and technical and policy-level interoperability of Levels of Assurance (LoAs).

3.3.3 Government initiatives

Government agencies, projects or academic programmes provide a valuable contribution to the eID industry. This section describes some of the notable government activities in eID.

3.3.3.1 ENISA

The European Network Information Security Agency (ENISA)[59] was established in 2004 to achieve a high and effective level of Network and Information Security within the European Union. Together with the EU-institutions and the Member States, ENISA seeks to develop a culture of Network and Information Security for the benefit of citizens, consumers, business and public sector organisations in the European Union. Operative networks contribute to the smooth functioning of the Internal Market, and concretely affect the daily lives of the citizens and business alike, using broadband, online banking, ecommerce, and mobile phones.

ENISA's specific expertise in IT and network security has created published resources on 'Web 2.0 and e-Government,' 'Social Engineering,' 'Security Features of European eID cards,' and 'Technology-induced challenges in Privacy and Data Protection.' ENISA has more recently been looking at issues of interoperability on eID.

3.3.3.2 OECD

The Organisation for Economic Co-operation and Development (OECD)[60] brings together the governments of countries committed to democracy and the market economy from around the world to support sustainable economic growth, boost employment, raise living standards, maintain financial stability, assist other countries' economic development, and contribute to growth in world trade. The OECD has a specific Working Party on Information Security and Privacy (WISP)[61] that has published policymaker guidance papers on 'Digital Identity Management in the Internet Economy,' 'Online Identity Theft,' and 'Personhood and Digital Identity in the Information Society.'

---

51 http://www.dataportability.org/
52 http://projectconcordia.org/
53 http://www.projectliberty.org/
54 http://www.isoc.org/
55 http://informationcard.net/
56 http://www.terena.org/
57 http://www.internet2.edu/
58 http://www.incommonfederation.org/
59 http://www.enisa.europa.eu
60 http://www.oecd.org/
61 http://www.oecd.org/sti/security-privacy

3.3.3.3 CCD-COE

Estonia's Cooperative Cyber Defence Centre of Excellence (CCD-COE)[62] has a mission to enhance the capability, cooperation and information sharing among NATO, NATO nations and partners in cyber defence by virtue of education, research and development, lessons learned and consultation. Whilst the defence focus means that much of the cyber-security work will be aimed at Critical National Infrastructure (CNI) protection, it is anticipated that the CCD-COE will also produce insights into the role of eID across Europe.

3.3.3.4 tScheme

tScheme[63] is the UK's co-regulatory body for approving providers of electronic trust services (although it is not mandatory to obtain such approval to operate as a credential provider). tScheme's remit initially covered PKI providers, but more recently this has expanded to cover providers of generic identity credentials. tScheme operates 'service approvals' for ID providers to assure users of service integrity. It also works with central government to provide authenticated access to shared services.

The organisation has its roots in a group of trade bodies that came together in 1998 to promote identity assurance. It is funded by member organisations subscriptions and license fees from approved service providers. Current approved providers include:

- TrustAssured (Royal Bank of Scotland);
- Certificate Factory (Trustis);
- Managed PKI (BT);
- SecureMark;
- NHS_RootCA (National Health Service);
- ARTL (Registers of Scotland).

[62] http://www.ccdcoe.org/
[63] http://www.tscheme.org/

4 STAKEHOLDERS AND VALUE CHAINS

4.1 Introduction

As part of the broader eID market analysis, a desktop survey of key eID stakeholders was conducted. The researchers drew upon their own experience, and information provided by IPTS to facilitate the investigation. This information was then used to profile those stakeholders and drive the development of an eID stakeholder ecosystem model. This section describes the process and outcomes of the stakeholder analysis.

4.2 Stakeholder analysis

The stakeholder analysis used a desktop survey to identify 193 organisations operating in the eID sector. These were examined, classified, and the data was listed in a spreadsheet. The ***IPTS Stakeholder Analysis*** workbook comprises three sheets:

- ***Primary analysis:*** Those stakeholders for which information was readily available, either online or through interviews/questionnaires, and for which the most detailed analysis has been prepared;
- ***Secondary analysis:*** Those stakeholders for which less information was available, and as such have characteristics documented less completely than the Primary analysis stakeholders;
- ***Other stakeholders:*** Identified stakeholders, with nationality, which were not researched further. In the majority (but not all) cases, these organisations are smaller or less focussed on the eID market than those in preceding sheets;
- ***Outlying stakeholders:*** Stakeholders that are no longer trading, not relevant to eID, or have been acquired by another party, together with the reason for their inclusion on this sheet.

The headings for the ***Primary analysis*** are shown in ***Table 2***:

Heading	***Description***
Name / Title / Organisation / Email / Website	Stakeholder contact details
Country	Country in which organisation is headquartered
Status	Legal status of organisation
Category	Primary activity of organisation
Type	Type of primary eID activity as defined in FIDIS' categorisation of Identity Management Systems (IMS):[64] • ***Type 1:*** IMS for account management • ***Type 2:*** IMS for profiling of user data by an organisation • ***Type 3:*** IMS for user-controlled context-dependent role and pseudonym management • ***N/A:*** Organisation has various offerings or does not engage in IMS
Class	Class of primary eID activity as defined in FIDIS' categorisation of Identity Management Systems (IMS)[65]: • ***Class 3:*** Identity management is main functionality (or economic core) of the product • ***Class 2:*** The product is no genuine IMS, but IMS functionality is relevant • ***Class 1:*** The focus of the product has nothing to do with identity management, nevertheless IMS functionality is included • ***Class 0:*** The corresponding type does not apply to the IMS • ***N/A:*** Organisation has various offerings
Employees	Total employees in organisation ('000)
Turnover	Annual turnover (€m)
Established	Year organisation was established
Product/Service Names	Names of key eID products/services offered by the stakeholder
Technologies	Principal eID technologies used by the stakeholder
Activities	Primary eID activities of the stakeholder
Target Market	Primary market (business, government, consumer)
Position in Value Chain	Levels of the value chain model in which the stakeholder operates (policy / regulation / exploitation / infrastructure / technology / support). Where the organisation sets or holds technology/interoperability standards, these are classified as 'regulation'.
Partners	Key stakeholder partners
Key Revenue Source	Description of how the stakeholder generates revenue from eID

Table 2: Primary analysis headings

[64] http://www.fidis.net/interactive/fidis-wiki-on-ims/wiki/Typology%202009/

[65] http://www.fidis.net/fileadmin/fidis/deliverables/new_deliverables/fidis-wp3-del3.17_Identity_Management_Systems-recent_developments-final.pdf

4.3 Summary of findings

Thirty-nine stakeholders were identified in the primary analysis, 51 in the secondary analysis. ***Table 3*** shows the Types and Classifications of those stakeholders as defined in ***Table 2***.

Percentage	***Primary Analysis***	***Secondary Analysis***
Type 1	21%	20%
Type 2	10%	2%
Type 3	23%	25%
Type N/A	46%	53%
Class 0	5%	2%
Class 1	5%	10%
Class 2	10%	12%
Class 3	39%	31%
Class N/A	41%	45%

Table 3: Stakeholder analysis by type/class

Whilst there are, for both stakeholder groups, a significant number of organisations that cannot be readily assigned a Class or Type, the division is shown in ***Figure 7***.

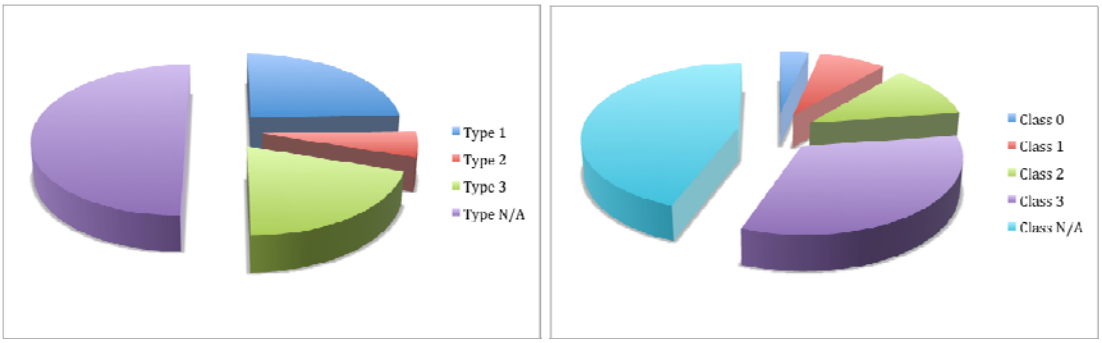


Figure 7: Stakeholder analysis by type/class

The vast majority of organisations analysed provide software and services, with other principal stakeholder groups covering foundations and research, smartcards, government, data brokerage and authentication services, as shown in ***Table 4***.

Accreditation services	1	Payments	1	Authentication services	3
Professional services	1	Data brokerage	2	Research	3
Domain names	1	Government	2	Foundation	4
Identity services	1	Smartcards	2	Software/services	17
Legal advice	1				

Table 4: Provision of services by primary stakeholders

Consideration was also given to target markets covered by primary stakeholders, as shown in ***Figure 8***.

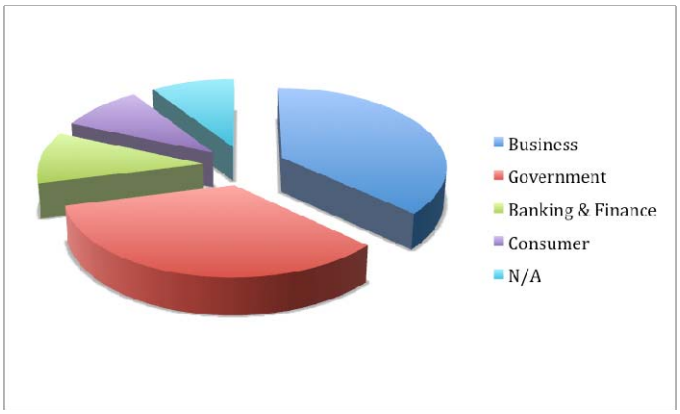


Figure 8: Target markets for primary stakeholders

Consideration of company size vs. type of product/service, and company size vs. importance of eID did not reveal any specific findings relevant to the research.

4.4 The eID ecosystem

The results of the stakeholder analysis were mapped against a single value chain model to better understand where those stakeholders sit in the ecosystem. The ecosystem is shown in ***Figure 9***:

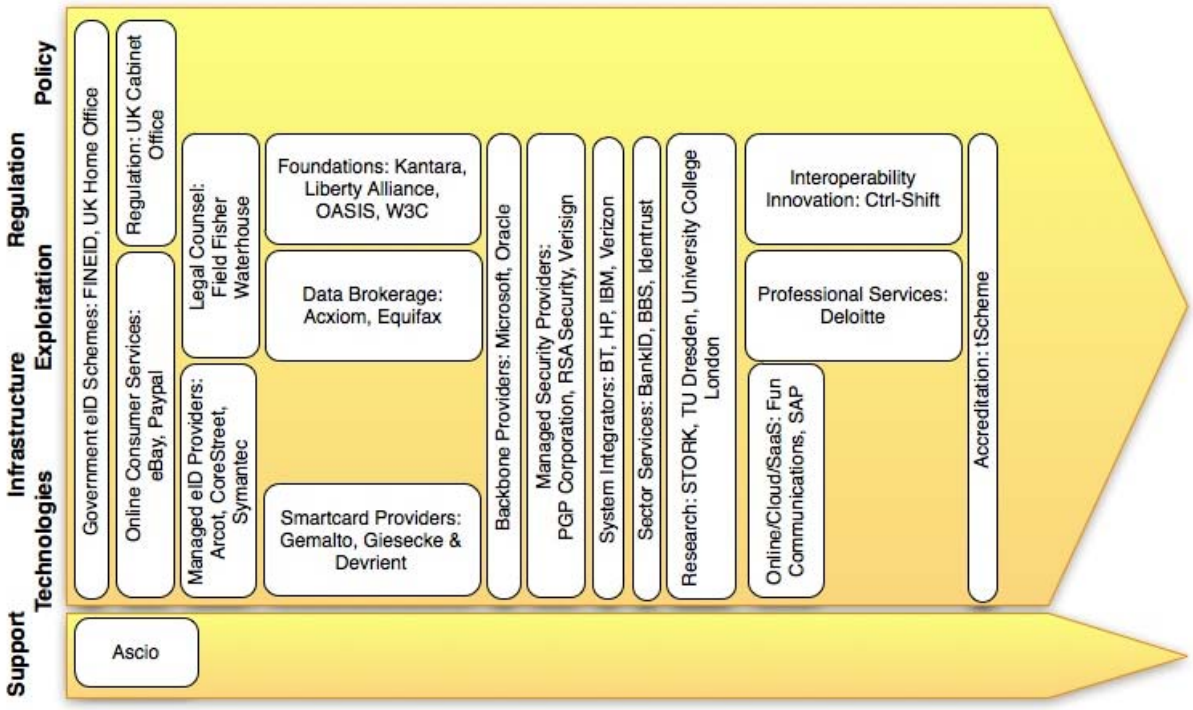


Figure 9: Primary eID stakeholder ecosystem

Figure 10 shows the spread of primary stakeholder organisations across the ecosystem; confirming that within the sample there are few operating in policy and support services, but a consistent spread across other levels of the model.

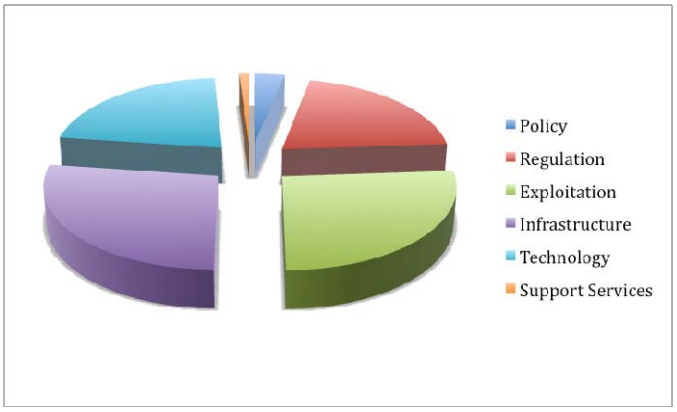


Figure 10: Division of analysed organisations by position in eID ecosystem

The ecosystem diagram does not take into account maturity or relative position in the value chain. By grouping the stakeholders according to their position, clear eID service groups are revealed, covering the areas shown in ***Table 5***:

Group	***Description***
Government eID schemes	National or regional eID schemes
Regulation	Policy and standard-setting bodies
Online Consumer services	Business to consumer websites
Legal Counsel	Legal support
Managed eID providers	Combined infrastructure/technology as a managed eID service
Foundations	Standard-setting bodies
Data brokerage	Firms gathering, selling or validating personal information
Smart card providers	Smart card manufacturers/vendors
Backbone providers	Organisations providing 'pervasive' information technology systems and services (e.g. enterprise desktop/server)
Managed security providers	Companies offering security as a service (with associated standard-setting or *de facto* standards)
System integrators	Organisations delivering bespoke enterprise systems
Sector services	Service delivery targeted at specific sectors
Research	Collaborative research and academic projects
Online/cloud/SaaS	Provision of outsourced software services
Interoperability innovation	Firms innovating in new eID applications and standards
Professional services	Consultancy
Accreditation	Certification of eID providers to ensure quality/interoperability

Table 5: eID ecosystem stakeholder groupings

Despite the volume of information collected about eID stakeholders, there was insufficient meaningful data to analyse the credential types and maturity in the manner defined in ***Sections 3.4 to 3.7.*** We anticipate that a significantly larger sample would be required, or that the sample should focus upon a single territory or market sector, in order to be able to apply this model to the analysis.

5 CREATING VALUE

5.1 Analysis of company activities

In the context of the eID ecosystem, value can be added both across the chain, and up and down through the layers: that is, as well as transmitting it along the chain, stakeholders can exploit added value by building on work on one level to move it to another (as is shown in ***Figure 11***). For example, by taking eID technologies and building them into an infrastructure, a vendor may create a value-added service. Likewise, taking policy or regulation developments may allow a vendor to exploit these into a new service offering.

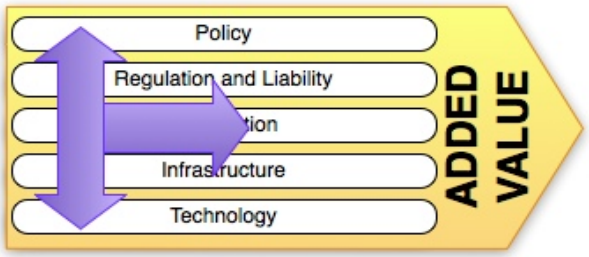


Figure 11: eID added/transmitted value

To develop this analysis further, the main activities of each company have been classified along this value chain. For each company included in the primary analysis, we have placed their three main activities in the most appropriate place in the model. While in a few cases it may be somewhat difficult to determine the most appropriate place for the concerned activity, in most cases it is a relatively straightforward process. The result of this analysis is shown in **Figure 12**, with each company represented by a particular colour (except for organisations which are only active within one segment), and in **Figure 13**, which groups together similar activities within each layer of the value chain. Figure 13 also introduces an additional element: the grouping of activities according to their degree of "sophistication", i.e. the degree to which they are composed of more applied services and/or the degree to which there are more basic services nedeed in that segment of the value chain.

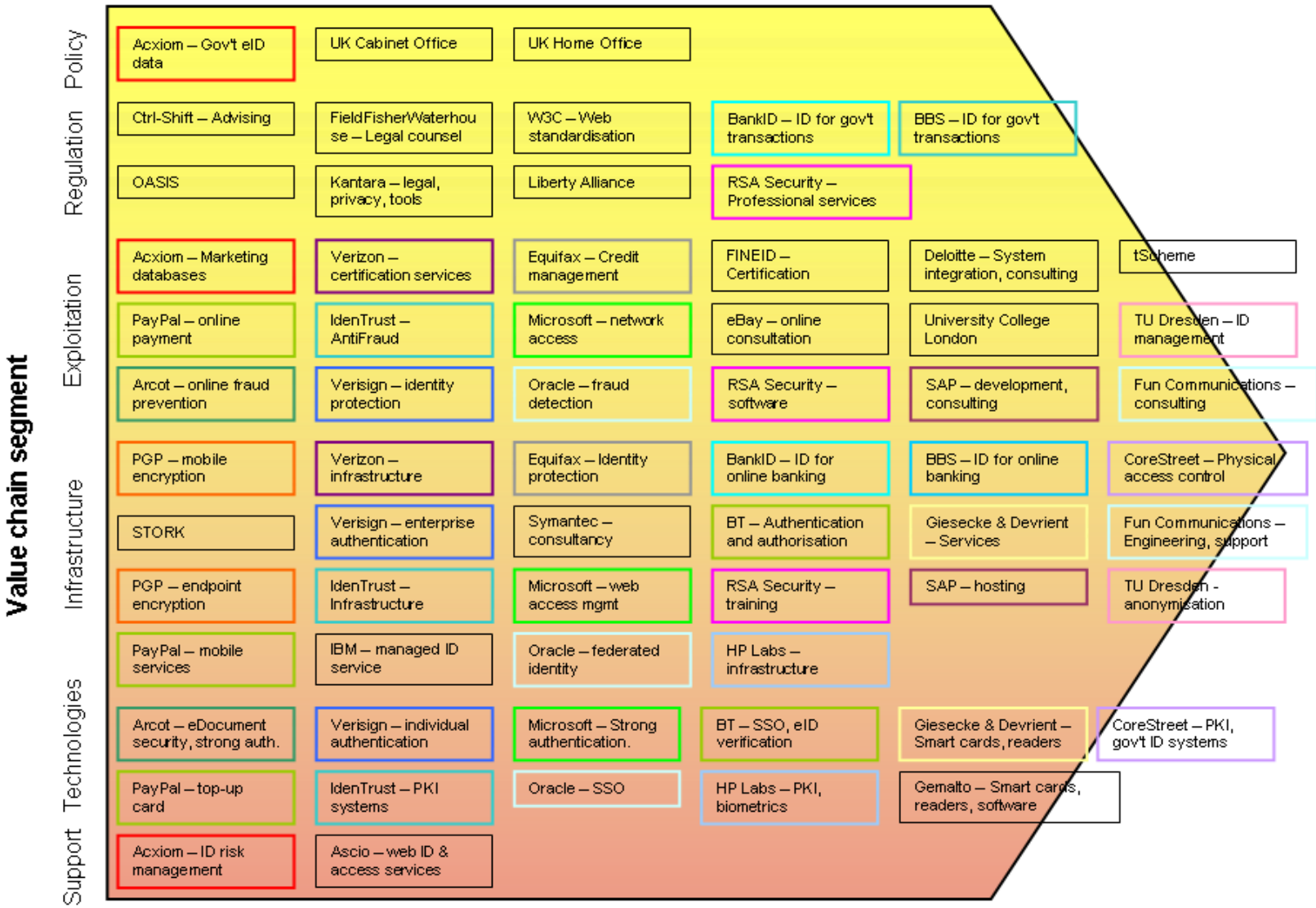


Figure 12: eID stakeholder activities in the value chain.

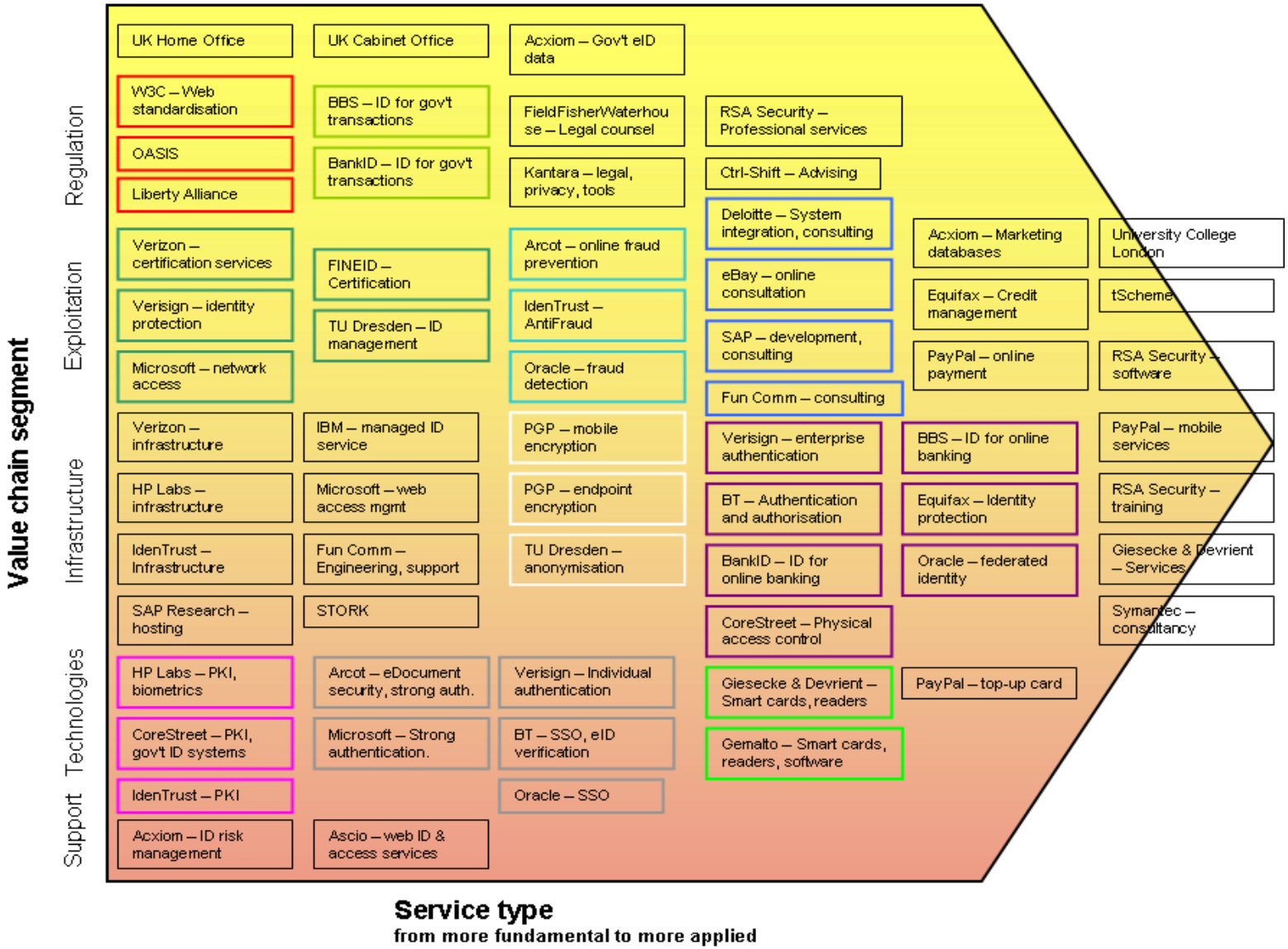


Figure 13: eID stakeholder activities in the value chain, grouped by activity

5.1.1 Types of company activities

We can draw several conclusions from the above value chains. First, it can be seen that most activities take place in the exploitation and infrastructure layers. The prevalence of exploitation products and services may reflect a certain degree of maturity in the marketplace: the underlying technologies are developed enough so that companies are able to create value-added services on top of them. For instance, different certification, antifraud and identity management services offered by the companies are all based on relatively robust identification technologies. The infrastructure products and services also rely on the availability of more fundamental technology solutions.

The technologies segment itself is somewhat smaller than the two above it. This may be due to the higher degree of technical expertise required by this segment of the value chain. Another possibility is the smaller size of the market, though lack of quantifiable data makes it difficult to say. Nevertheless, we can see that a variety of technological solutions are offered by the stakeholders such as: SSO (single sign-on), public key infrastructure (PKI), smart card products.

Clearly the smallest sections are policy and regulation, which is understandable given that these are typically not easily combined with other activities and are often composed of activities such as legal counsel or standardisation. Indeed, many of the organisations in these segments are not companies at all, but standardisation bodies or government departments. Nonetheless, this segment is vital for the industry as a whole since it provides the link between the core of the marketplace (the various technological and commercial solutions) and the public sphere, with its policy and regulatory activities.

It is also noticeable that a typical combination of products is either exploitation and infrastructure, or infrastructure and technologies. The provision of these kinds of services often complements each other; for example, by providing a technology infrastructure (or platform) an organisation may then find other uses for it or offer consultation services based on it; while a technology provider may be able to easily construct a more sophisticated infrastructure on top of it. Policy and regulation are much more specific services, which explains why they do not often go together with other layers, though in the case of government services, for example, there may be some correlation.

In some cases, we can notice companies operating in three separate segments. This is typically the case with large companies such as RSA Security, Oracle, or Microsoft. They are often able to leverage their existing offerings to cover a wide swathe of the value chain, and with a small or moderate additional investment expand into new segments. Many of these players may also try to actively connect their products and services in the different segments, thus seeking synergies and possibilities to offer significant added value to the client. For the smaller companies, the situation is different as they have more limited resources (financing, technical abilities, number of staff) at their disposal. Thus they may be forced to concentrate on one highly tailored product/service or business model, or to seek opportunities to exploit already existing infrastructure to facilitate their service provision.

It is also noteworthy that there are several companies offering consultation services in the eID market. On the one hand, this may show that the market is mature enough to allow the emergence of specific services designed to help companies better exploit the new opportunities offered by developments in eID. On the other hand, it may equally well be the case that there is so far too limited an understanding of how electronic identity based services could be commercialised, what opportunities and pitfalls there are, and how the industry is developing. At any rate, the emergence of consulting services shows that at least among some stakeholders there is an improving understanding of the industry.

5.1.2 Clustering of activities

If we then look at how activities are clustered within the segments, the following developments can be noted. First, in the policy and regulation layers the activities are quite dispersed. This is mostly due to the variety of activities within the segments. Standardisation organisations such as OASIS, W3C and

Liberty Alliance can, however, be loosely grouped together. Moreover, BankID and BBS both offer identity solutions for government transactions. Both of them have been developed for use by the public and companies in the marketplace as well as government organisations, which distinguishes them from other similar services. In addition, FieldFisherWaterhouse and Kantara are both active in the legal layer, albeit with different operational foci. Finally, Ctrl-Shift and RSA Security offer more advanced accordingly tailored services that seek to identify the particular problems and challenges that their customer companies face, and respond with concepts and advice.

In the exploitation section, we can see several service groups. Several institutions (Verizon, Verisign, Microsoft, FINEID, TU Dresden) offer certification and ID management services that verify the validity of the identities provided by other stakeholders. This function is fundamental in the sense that without reliable certificates, the other, more applied activities in this section cannot be realised. An example of this is the next cluster, where companies such as Arcot, IdenTrust and Oracle offer anti-fraud solutions addressing the growing threat of identity theft and abuse of electronic identities. Service solutions such as these utilise the identity and certification services offered by other companies, aiming to prevent the unauthorised use of existing identities and the use of false identities by using the established certificates as their starting point. A third major sector is the consulting services; while there is much more variation within this sector, all the companies seek to help their customers get the highest possible added value out of their portfolios by using them more efficiently or by introducing new, compatible services.

In the infrastructure section, the services offered tend to be more broadly defined or to be composed of a variety of elements. This makes it more challenging to group activities to specific clusters. However, we can still identify certain clusters of activities. Firstly, several organisations offer basic infrastructure or networking services, which are necessary to enable access to the more advanced services. Further, we can distinguish between encryption and authentication services: encryption merely packages the information into a secure format so it can only be accessed by appropriate stakeholders, while authentication includes the recognition and cross-checking of identity data used by individuals seeking to access a service.

In the technology section, where fewer companies participate, we can more readily divide it into groups as it is more clearly defined. There are a number of companies (CoreStreet, HP Labs, IdenTrust) offering public key infrastructure (PKI) technologies that create the actual keys and identification mechanisms used in the authentication. Further, there are five companies that offer specific authentication technologies such as SSO (single sign-on) and strong authentication. Finally, both Giesecke & Devrient and Gemalto offer smart cards and associated card readers and software. Since their portfolio includes a physical product, the smart card, as well as software, the complexity and thus the added value of the activities increase significantly.

Table 6 groups together the activities in each section of the value chain, highlighting the different service clusters.

Table 6: eID ecosystem stakeholder activities by segment of value chain and type of service

Layer	*Cluster 1*	*Cluster 2*	*Cluster 3*	*Others*
Policy	***Policy support***	***Data collection and management***		
	UK Cabinet Office	Acxiom – Gov't eID		
	UK Home Office			
Regulation	***Standardisation***	***Transactions***	***Legal***	***Advisory / services***
	W3C – Web standards organstion	BankID – ID for gov't transactions	FieldFisherWaterhouse – Legal counsel	Ctrl-Shift – Advising
	OASIS	BBS – ID for gov't transactions	Kantara – Legal, privacy, tools	RSA Security – Qualified services
	Liberty Alliance			
Exploitation	***Certification***	***Antifraud***	***Consultation***	***Applied services***
	Verizon – Certification services	Arcot – Online fraud prevention	Deloitte – System integration, consulting	Acxiom – Marketing databases
	Verisign – Identity protection	IdenTrust – AntiFraud	eBay – Online consultation	PayPal – Online payment
	Microsoft – Network access	Oracle – Fraud detection	SAP Research – Consult, development	Equifax – Credit Management
	TU Dresden – ID management			RSA Security – Software
	FINEID – Certification			University College London
				tScheme
Infrastructure	***Network***	***Encryption***	***Authentication***	***Services***
	Verizon – Infrastructure	PGP – Mobile encryption	Verisign – Enterprise authentication	PayPal – Mobile services
	IdenTrust – Infrastructure	PGP – Endpoint encryption	BT – Authentication and authorisation	Giesecke & Devrient – Services
	HP Labs – Infrastructure	TU Dresden – Anonymisation	BankID – ID for online banking	Symantec – Consulting
	SAP Research – Hosting		BBS – ID for online banking	RSA Security - Training
	IBM – Managed ID service		Equifax – Identity protection	
	Microsoft – Web access management		Oracle – Federated identity	
	Fun Communications – Engineering		CoreStreet – Physical access control	
	STORK			
Technologies	***Public key infrastructure (PKI)***	***Authentication technologies***	***Smart cards***	***Services***
	CoreStreet – PKI, gov't eID systems	Arcot – Strong authentication, eDocument security	Gemalto – Smart cards, readers, software	PayPal – top-up card
	HP Labs – PKI, biometrics	Verisign – Individual authentication	Giesecke & Devrient, Smart cards, readers	
	IdenTrust – PKI	Microsoft – Strong authentication		
		Oracle – SSO		
		BT – SSO, eID verify.		
Support	***Others***	***Others***		
	Ascio – Web ID & access services	Acxiom – ID risk management		

5.1.3 Linkages between segments of the value chain

It is also possible to identify several linkages *between* the different segments of the value chain. These linkages can be roughly grouped according to types of services they are associated with; the first of the linkages is clustered around **government services** and their supporting services. Different government departments (i.e. UK Home Office, UK Cabinet Office) and government eIdentity managers (i.e. Acxiom) are all involved in generating and maintaining eID information to be able to provide the policy support functions required of them. These stakeholders typically rely on lower-level services provided by companies such BBS and BankID, which offer identification services specifically for governmental transactions. In turn, these companies utilise certification and antifraud services from the exploitation layer, and authentication and authorisation services from the infrastructure layer, to provide the actual technical means for securely identifying the users for different kinds of use cases, environments and transactions. Antifraud and identity protection services are often especially important in the case of governmental services, due to the often very large sums of money and confidential nature of the information concerned. Finally, governmental organisations rely on companies such as CoreStreet to provide the technological base, e.g. in the form of the physical infrastructure, for the identification systems.

A second linkage between layers of the value chain can be seen in what could be called **commercial add-on services**. Prime examples of these include marketing databases (Acxiom), credit management (Equifax) and online payment (PayPal). These exploitation-layer services make use of identification methods and technologies provided by other stakeholders, and create their own tailored products on top of them. Typically, the supporting infrastructure is composed of different authentication and encryption services, as well as access management and hosting solutions. The actual technologies used very much depend on the add-on service in question, but in many cases, single sign-on and/or strong authentication methods come in useful; in some cases, smart cards and their readers (provided by companies such as Gemalto and Giesecke & Devrient) may also be used as the means of identification.

A third group is the various **soft services** that use the different technical solutions just as the first building block of their services. In the regulation layer, these include legal counsel and advisory services (FieldFisherWaterhouse, Kantara, Ctrl-Shift). In the exploitation and infrastructure layers, typical soft services are consultation, training, and management services, offered by the likes of Deloitte, SAP, and Symantec. Key features of these services are a high added value, often enabling companies offering them to charge a premium for the services, and a high degree of flexibility in tailoring the services to match the needs of the individual customers. The technologies layer is less relevant in the case of soft services, but companies such as Acxiom in the support layer can be very important in providing the appropriate level and type of risk management for other companies.

As an example of existing linkages between companies, IdenTrust operates in many markets together with RSA Security, CoreStreet and Gemalto. The main activity of IdenTrust is offering authentication systems for the finance sector. Their system is based on PKI-based credentials that allow stakeholders in the financial sector to securely and reliably carry out large-scale transactions. However, since IdenTrust does not have all necessary competencies in-house, they partner with the three companies to be able to offer a full service to their customers. In this case, all the supporting companies have a quite clearly defined role: RSA Security offers high-level services (i.e. consultation and training) to help companies make the most of the eID system, CoreStreet is the company that controls the physical access to the system, while Gemalto provides the software that carries out the operations required by the system specifications.

5.2 Individual companies

5.2.1 Introduction

Private-sector activities deliver eID credentials that are immediately usable as products or services, given that there is a need for a clear return on investment. In many cases, they build upon the work of research projects and standards bodies. This section describes a number of notable private-sector eID schemes in an attempt to single out characteristics that may be useful for further analysis of the eID sector value-chain and operative business models.

5.2.2 BBS Global Validation Service

Acting as a "trust anchor", BBS Global Validation Service[66] helps customer organisations to manage risks associated with the acceptance of digital signatures and certificates while conducting global e-business. Owned by Nordic financial institutions, BBS is a leading provider of identity, banking, payments and information services, and works in partnership with solution providers and managed security providers. Key services include Managed PKI (on a national scale), managed one-time passwords, global validation, eArchiving, eInvoicing and eWorkflow. Technologies used by BBS include PKI, smartcards and tokens. BBS has operated national critical financial infrastructures since 1972 and identity solutions since 2000.

The validation service manages the process of verifying digital signatures and validating digital certificates (eIDs). The service relies on a risk-based assessment of credential quality and is currently in use by the Norwegian government procurement portal (HANDEL). The fact that these services are accepted by several governments in addition to the marketplace distinguishes the BBS service offering from other similar ones. This has the potential to be quite a significant development, given that governments in general are very wary of accepting commercial credentials and instead prefer to rely on their own solutions. As the security standards of the commercial products are constantly improving, this lack of acceptance may be more of an issue of suitability of commercial credentials for governmental purposes, rather than concerns about their lack of reliability.

In general terms, international companies need to handle the complexity of verifying different kinds of signatures and to validate certificates from various issuers worldwide. This is the main challenge that BBS seeks to address. They offer validation services that seek to solve the complex problem of offering signature verification and certificate validation as a service for the receiving party. In this way, their customer can obtain a solution designed to manage different signatures and certificates worldwide. Effective use of digital signatures, especially across national frontiers, reduces costs and complexity of using PKI in global e-business. The service also effectively helps to connect different closed eID communities. Ultimately, BBS aims to function as a single, independent trust provider, which offers one set of standards and one software package for processing of signatures and certificates, as well as effective risk management for using PKI in global business transactions.

BBS operates in two distinct segments of the eIdentity market: they offer multi-purpose ID schemes for heterogeneous citizen-merchant markets, and tailored PKI solutions, with more stringent security parameters, whose users are typically enterprise customers with transactions taking place in closed environments.[67] The most important product of BBS is the Identity Management Platform. Developed in 2008, it is used for issuing, managing and using digital certificates online. It can handle different Certificate Authority (CA) platforms and validation technologies, thereby providing BBS with the flexibility to adapt their certification to the specific needs of individual customers and transactions. The BBS Identity Manager is used to provide all their electronic ID services, including enterprise PKI, mobile PKI, EU-qualified (BBS PKI has been established in the EU-Compliant Qualified Certificate environment, allowing enterprises all over Europe to get PKI services and qualified certificates) and

[66] http://www.bbs-nordic.com/en/Solutions-and-Services/eSecurity/Global-Validation-Service/

[67] B. Choudhary, "European e-ID services: future trends and Nordic experiences," FST Europe (GDS Publishing Ltd., 2010), vol.

standard certificates. It can also be used to provide one-time passwords and validation of individual transactions. The BBS services allow for the use of identity in context- and transaction-specific ways, utilising different types and levels of security for specific use cases. In general, BBS services have been developed with a modular design, allowing their customers to choose the combination of identification mechanisms that is most appropriate for their needs.

The market activities of BBS are complemented by their participation in international standardisation and expert groups such as European Committee for Banking Standards (ECBS; Mobile Payments Workgroup), Mobey Forum (Mobile Authentication and Business Ecosystem), and European Payment Council (EPC). The participation in these bodies helps BBS to develop identity solutions that better address specific privacy and data protection issues, in addition to having a hand in shaping the future development of the eID industry.

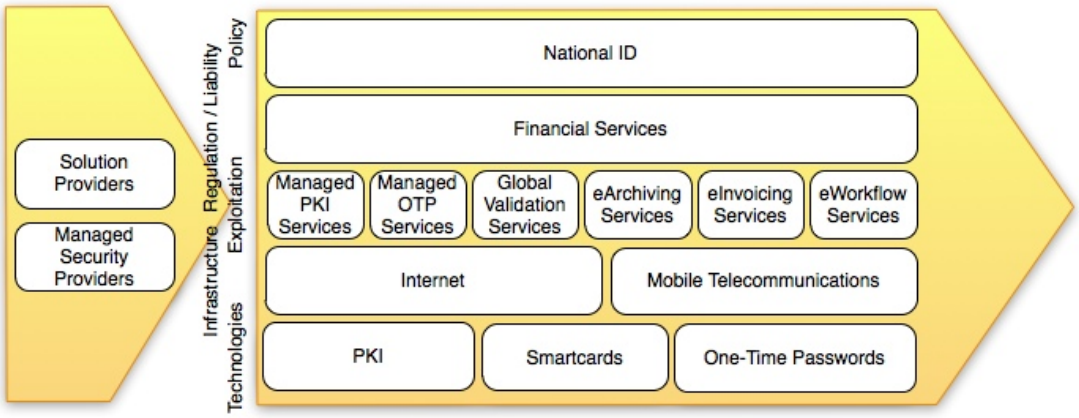


Figure 12: BBS Value Chain

An alternative way to analyse the activities of BBS (as well as other companies) is according to a business model framework developed by Osterwalder (2004),[68] where the elements underpinning the operations of a company are divided into nine categories. Below we present the nine categories and the way in which the BBS operations fit into them, displayed graphically in the following Figure 15.

- Customer segments – Who does the company create value for? BBS: Government departments, financial institutions, other private stakeholders who require reliable identification and validation services.
- Value proposition – What does the company offer to the market? BBS: Solution to the complexity problem of verifying different kinds of signatures and validating certificates from various issuers worldwide.
- Distribution channels – Which communication and distribution channels do the products and services reach the market through? BBS: Works as an independent trust provider whose products come in a modular design, meaning that their customers are able to purchase the type and level of service they need.

[68] Osterwalder, Alexander (2004). The Business Model Ontology: A Proposition in a Design Science Approach. PhD thesis, University of Lausanne.

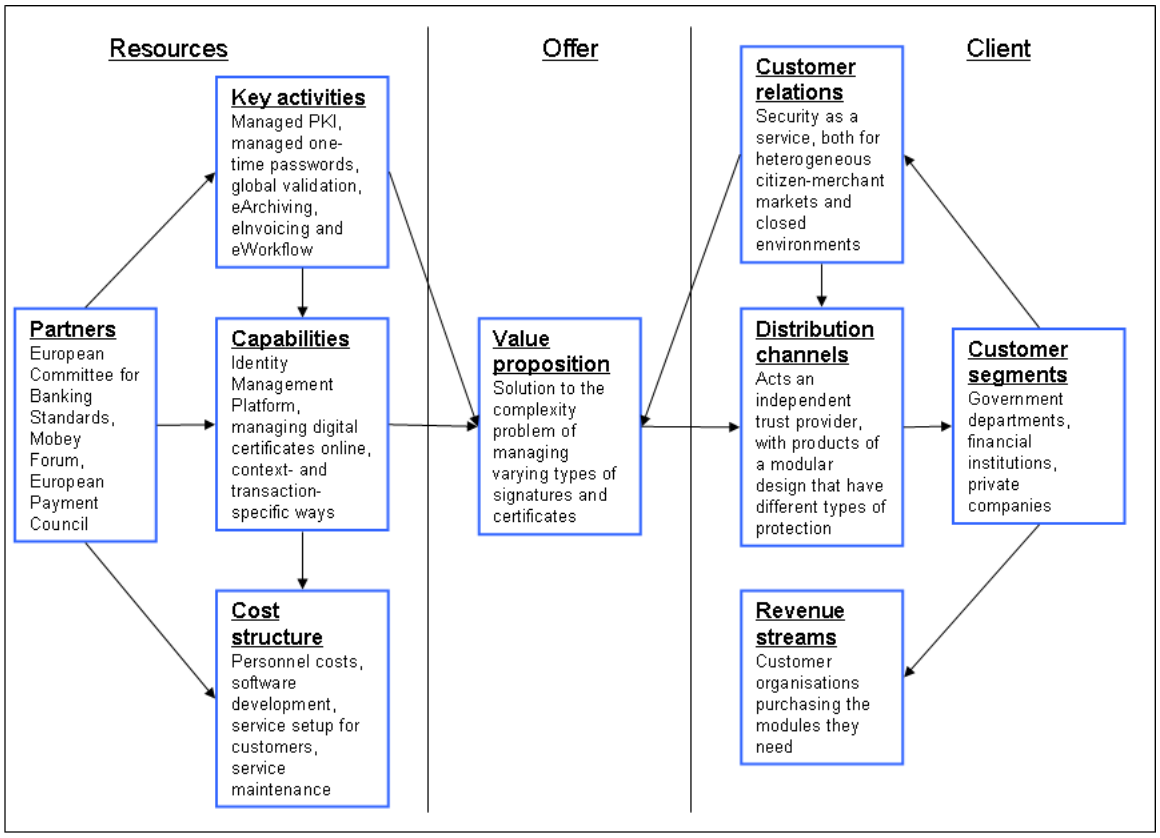


Figure 13: BBS Business Model

- Customer relationship – Which different customer relationships are developed and maintained in the business model? BBS: Offers security as a service, aiming at two separate segments of the eIdentity market: ID schemes for heterogeneous citizen-merchant markets and tailored PKI solutions for closed environments.
- Revenue streams – What are the key sources of revenue for the company? BBS: Revenues come in from customer organisations purchasing the product modules that fit their particular needs.
- Core capabilities – What are the key resources and capabilities of the company? BBS: Identity Management Platform, the ability to issue, manage and use digital certificates online, managing the use of identity in context- and transaction-specific ways.
- Value configuration – What are the main activities of the company that contribute to generating value? BBS: Managed PKI, managed one-time passwords, global validation, eArchiving, eInvoicing and eWorkflow.
- Partner network – Which partners does the company work together with? BBS: Participates in international expert groups such as European Committee for Banking Standards, Mobey Forum and European Payment Council.
- Cost structure – What are the most important cost elements for the company? BBS: Personnel costs, software development, service setup for customers, service maintenance.

5.2.3 CoreStreet[69]

CoreStreet is a US-based company delivering eID validation services at infrastructure and application layers in IT and physical security environments. The company operates in the EU through a network of partners. Key product areas include:

[69] http://www.corestreet.com/

- ***Public key infrastructure:*** Certificate validation technologies used to validate credentials of individuals for email and secure forms;
- ***Physical access control:*** Integration of physical access control systems with eID systems;
- ***Secure ID checking:*** Provision of technologies and infrastructure to check government ID credentials, particularly around ‘first responders’ in incident management and crisis control scenarios.

CoreStreet's aim is to improve security, speed, and efficiency in critical day-to-day applications, including PKI-based IT security, physical access control, and secure ID checking. CoreStreet technology, along with CoreStreet-compatible products and services from partners and integrators, are designed to facilitate the convergence of physical and IT security systems. CoreStreet products perform the twin functions of authentication (is the person or organization who he says he is) and validation (is the person or organization allowed to do what he is doing at this particular moment).

As to PKI services, CoreStreet’s certificate validation technology is currently deployed by the US Department of Defense and other organizations, public and private, around the globe. The CoreStreet technology is designed to validate the credentials of individuals as they interact with IT applications with a security component, including digitally signed email and secure forms. In doing so, users and administrators can have the highest level of trust in their secure communications and transactions. Based on the work of Dr. Silvio Micali, an MIT professor on cryptography, the CoreStreet PKI technology enables credential validation quickly in both online and offline environments. Examples of credential types include smart cards, ePassports, and driver's licenses.

As to physical access control, CoreStreet's Card-Connected technology is used to enhance the capacity of physical security products from infrastructure vendors. By integrating CoreStreet technology, companies are able to deliver solutions to their customers that increase the scope of any physical access system by allowing centralised management of both wired and standalone locations. In addition, CoreStreet technologies can be used to enable one-card access to all systems. CoreStreet's physical access systems represent a novel approach to security by utilising advanced smart cards that act as a network between wired and standalone locations.

As to mobile identity validation, CoreStreet offers the PIVMAN solution, which is a system for checking secure government IDs such as the government issued smart cards, ePassports, or driver's licenses in locations where network connectivity is either unavailable or difficult to obtain. Consisting of handhelds, desktops, and servers, the CoreStreet PIVMAN Solution is an end-to-end mobile identity verification solution that requires no network connectivity in order to check the validity of a credential. Applications include incident response, natural disaster, and border control.

5.2.4 Gemalto

Gemalto is a leading provider of security devices including smartcards, SIMs, e-passports, tokens and the necessary backbone services to manage these devices. The company is particularly engaged in public sector activities with more than 20 ePassport initiatives, 15 national eID programs, and various eHealth and e-driving/smart transport schemes. Gemalto operates worldwide from its home territory in France, using direct sales or partner organisations, in a model that varies according to local conditions. Technologies in use include polycarbonate or PVC contact/contactless smartcards, with Java and match-on-card biometric systems.

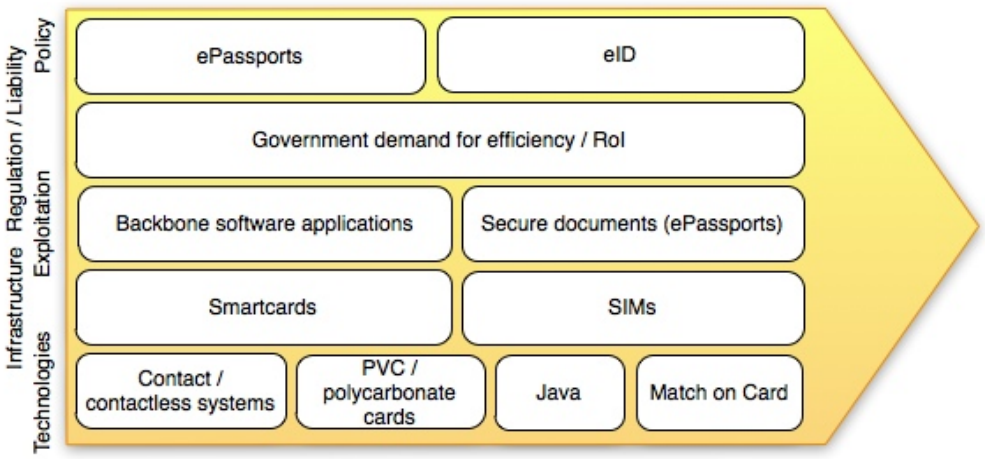


Figure 14: Gemalto Value Chain

5.2.5 IdenTrust

IdenTrust[70] is a bank-developed PKI authentication system that is primarily used by the finance sector and is recognised by government agencies and corporations around the world. IdenTrust issues credentials and provides a supporting infrastructure that incorporates policies, legal framework, operations and technology to facilitate authentication, encryption and digital signing between organisations. The company is headquartered in the US, but provides services to financial institutions across Europe.

The IdenTrust Trust Network, which is their main product, provides both hosting and connectivity for authentication between institutions, for which participating institutions pay a joining fee, an annual subscription and a 'per-transaction' charge. The system forms part of the UK Critical National Infrastructure, for example in support of ACH BACSTel IP which handles direct debits and credits. In the US, IdenTrust provides digital certificates to the US Federal Government and is involved in the ACES/ECA programmes (critical infrastructure).

The IdenTrust credentials are designed to provide three key capabilities: authentication (provision of identity), encryption (safeguarding content, eliminating unauthorised access) and digital signature (user-level signatures of specific transactions). In addition, IdenTrust credentials are designed to comply with relevant anti-money laundering or other anti-abuse regulations (i.e. Sarbanes-Oxley and HIPAA health data regulations).

IdenTrust products enable companies make authentication an integral part of their business processes and so to be able to conduct their operations reliably and securely over the Internet beyond fulfilling their legal obligations. IdenTrust products rely on an open standard that can be used by financial institutions to gain interoperability and legal acceptance in 120 countries. The membership of the IdenTrust network is restricted to institutions that agree to abide by the conditions set by IdenTrust, thereby ensuring that the standard is utilised in an appropriate manner. IdenTrust policies govern who receives the identity and how each individual or business is vetted to guarantee they really are who they say they are, along with making certain that the process is done consistently everywhere around the world. IdenTrust identities encrypt and control the process flows, in order to prevent the interception or redirection of a transaction or a document, in this way combating phishing and man-in-the-middle attacks.

[70] http://www.identrust.com/

The Trust Network work flows as follows.[71] It first specifies how a digital identity certificate can be issued and how it is validated. The transaction data and signed certificate are exchanged between the stakeholders involved in the transaction. The messages related to the transaction data are exchanged between the customers on either end of the transaction. IdenTrust only validates the identities used by these customers, not the data associated with the transaction. The transaction data itself is never passed to IdenTrust; the only information IdenTrust receives and sends back to the banks is validation of participant identities. All individuals and systems using the network are identified using IdenTrust digital certificates.

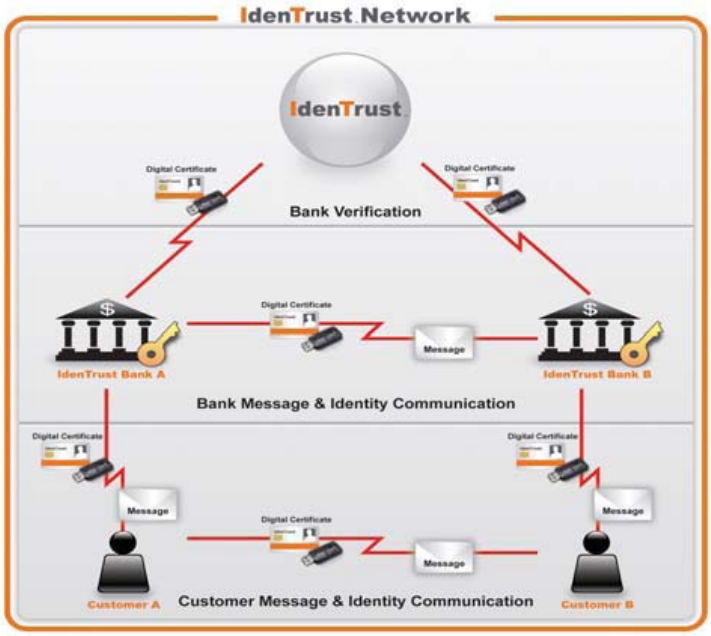


Figure 15: Functioning of IdenTrust Trust Network (Source: IdenTrust, ref. #78)

Overall, IdenTrust supplies the technology and legal mechanisms to allow companies to trust that their Internet trading partners are who they claim to be. The provision of verifiable identities makes it less risky for companies to operate over the Internet, hence reducing transaction costs and creating auditable records of their transactions. This means that IdenTrust products and services have an important role in supporting growth in the eIdentity market, even if the products are initially considered as simply a cost for the customer companies.[72]

---

[71] IdenTrust. The IdenTrust Rule Set:Providing Secure Identities While Protecting Privacy. (White Paper). London: IdenTrust, 2007. Available from <http://www.identrust.com/pdf/IdenTrust_Privacy_WhitePaper.pdf>.

[72] IdenTrust. Identity Authentication as a Critical Growth Strategy. (White Paper). London: IdenTrust, 2007. Available from <http://www.identrust.com/pdf/Identity_Authentication_CriticalGrowth.pdf>.

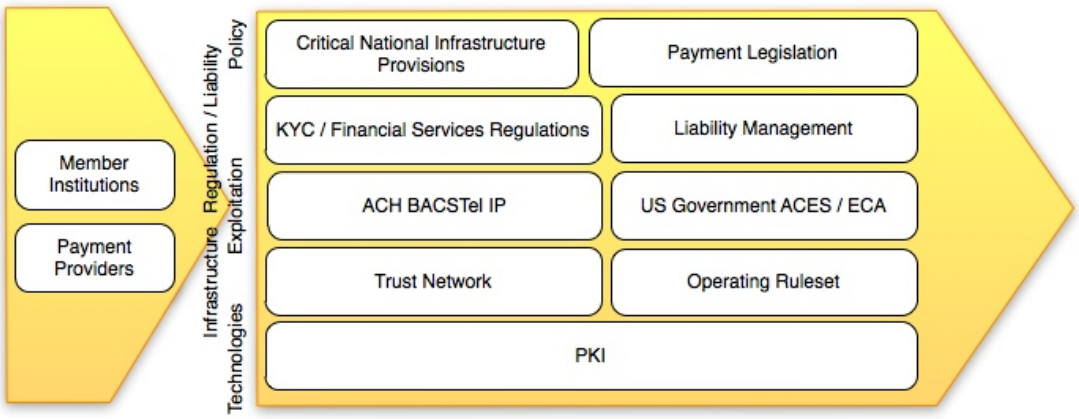


Figure 16: IdenTrust Value Chain

Given the wide range and complexity of IdenTrust's operations, we classify them below according to the Osterwalder model (see Section 6.2.1 and resulting graph in figure 19).

- Customer segments – Who does the company create value for? IdenTrust: UK government (forms part of UK Critical National Infrastructure), US government, financial institutions, corporations who need reliable and legally binding global authentication.
- Value proposition – What does the company offer to the market? IdenTrust: Enables organisations to conduct transactions electronically with an appropriate degree of reliability and security, providing verifiable identities to the participants of the transaction.
- Distribution channels – Which communication and distribution channels do the products and services reach the market through? IdenTrust: Utilises an open standard whose users agree to abide by a set of rules specified by IdenTrust.
- Customer relationship – Which different customer relationships are developed and maintained in the business model? IdenTrust: Customers are able to operate as members of the Trust Network, which guarantees that all members follow the same set of rules, thus promoting interoperability and generating trust in the market.
- Revenue streams – What are the key sources of revenue for the company? IdenTrust: Joining fee to the Trust Network, annual subscription fee, individual transaction charges.
- Core capabilities – What are the key resources and capabilities of the company? IdenTrust: Provides three key services: authentication (provision of identity), encryption (safeguarding content), and digital signing (user-level signatures of specific transactions).
- Value configuration – What are the main activities of the company that contribute to generating value? IdenTrust: Creating credentials, reducing transaction costs and creating an auditable record of transactions.
- Partner network – Which partners does the company work together with? IdenTrust: All the companies accepting the shared set of rules of the Trust Network.
- Cost structure – What are the most important cost elements for the company? IdenTrust: Personnel costs, hardware costs, software development, service setup for customers, service maintenance.

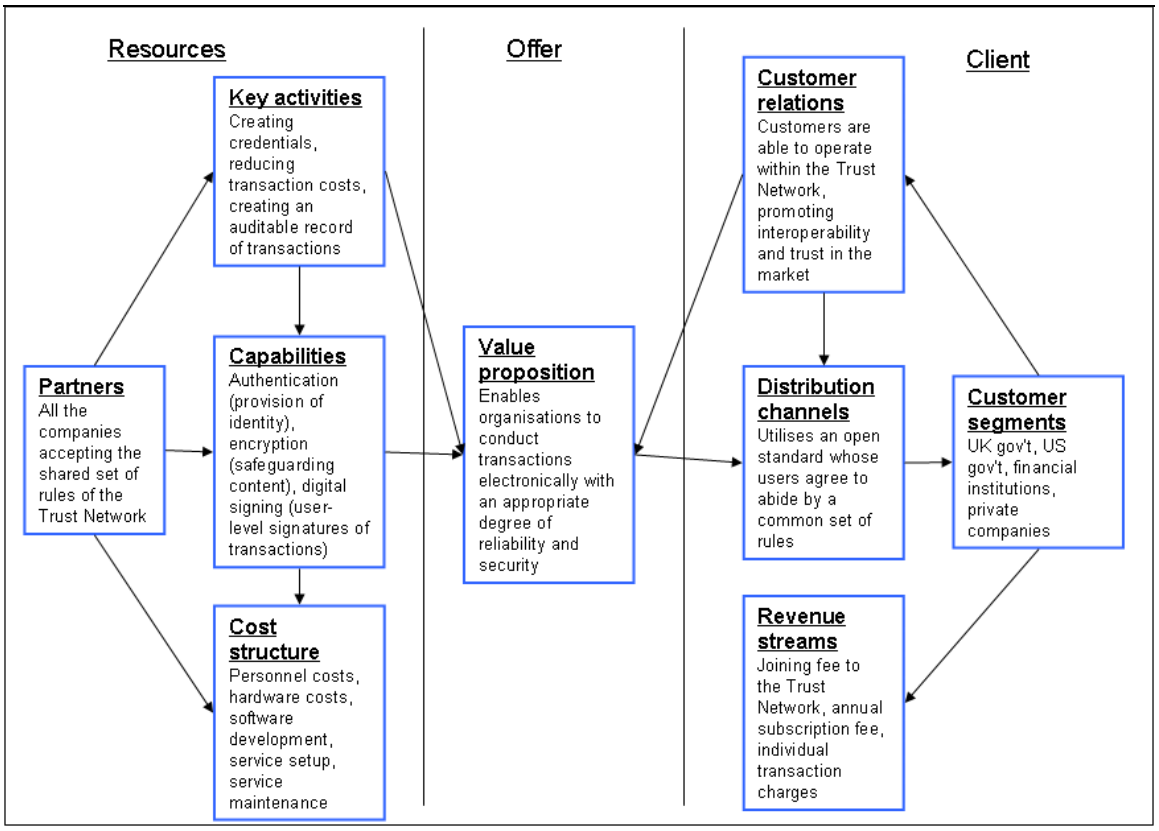


Figure 17: IdenTrust Business Model

5.2.6 RSA Security

Forming the Information Security Division of EMC[73] Corporation, RSA is one of the oldest providers of Information Security systems, services and support and has its roots in the synonymous algorithm (now reportedly embedded in over 1bn products worldwide). The 2000 employee division, headquartered in the USA with a significant presence in Europe, today provides encryption, authentication, access management, security information and event management and fraud control products, as well as consulting and professional services to over 35,000 organisations. Its technologies are used to protect 250m online Identities worldwide, in online banking and credit card transactions (via the provision of Verified by Visa[74] / Mastercard SecureCode[75] security systems)

RSA's range of technology, business and industry solutions are coupled with professional services as well as strategic partnerships with the relevant stakeholders in the industry. Furthermore, since companies must today fulfill a wide variety of regulatory requirements and recommendations that demand rigorous protection of identities and information, RSA provides services for helping their customer companies meet compliance requirements such as with the European Data Privacy Directive, Health Insurance Portability and Accountability Act (HIPAA), the ISO 27002 Standard and a variety of other US legislative measures.

RSA works throughout the eID value chain, from CA activities through to provision of a wide variety of authentication methods, including both software-based and hardware tokens. Strategically they anticipate a move away from perimeter centric and static security (e.g. tokens, PKI) to a more information centric and risk-based security, that analyse a host of parameters (e.g. IP address, machine characteristics, user behaviour) to make an optimal authentication choice, rather than the traditional

[73] http://www.emc.com/
[74] http://www.visaeurope.com/merchant/handlingvisapayments/cardnotpresent/verifiedbyvisa.jsp
[75] http://www.mastercard.com/us/personal/en/cardholderservices/securecode/index.html

binary ‘yes/no’ associated with authentication. In addition, it offers RSA SecurID USB Tokens[76] which combine a USB device with secure storage of digital credentials thus consolidating digital credentials onto a single device.

RSA provides solutions that apply appropriate controls to mitigate risk according to the value and criticality of data, applications, identities and transactions. With a range of identity assurance products, organizations can leverage information and new electronic applications to accelerate their business initiatives. Identity assurance products also support an information risk management process by helping define and enforce policy around users and access and providing the technology controls to mitigate risks related to unauthorized access. Overall, identity assurance products create trust by defining identity policy, verifying new identities and managing credential issuance. They also manage authentication, provide context for what a trusted identity can do, provide knowledge back to the enterprise of what an identity has done, alert on suspicious activity, and elaborate information on possible emerging threats.[77]

A significant part of RSA operations is the RSA Secured technology partner program. It is composed of over 1,000 strategic partnerships with relevant organizations, through which RSA is able to integrate its solutions into many diverse environments. The program focuses on interoperability certification activities as well as joint support strategies. Certification brings added assurance to customers that the solutions RSA provides are interoperable with industry-leading security products so that they can achieve faster time to deployment and lower total cost of ownership. In addition, RSA plays an active leadership role in standards development initiatives – such as Liberty Alliance, OASIS, IETF and WS-Security – to ensure the technical superiority and interoperability of their solutions. Their current portfolio supports a multitude of standards, including PKCS, RADIUS and SAML. One of the most important departments of RSA Security is RSA Laboratories,[78] which are researching enhanced user authentication techniques, RFID privacy and security, mobile phone personal authentication and cloud storage.

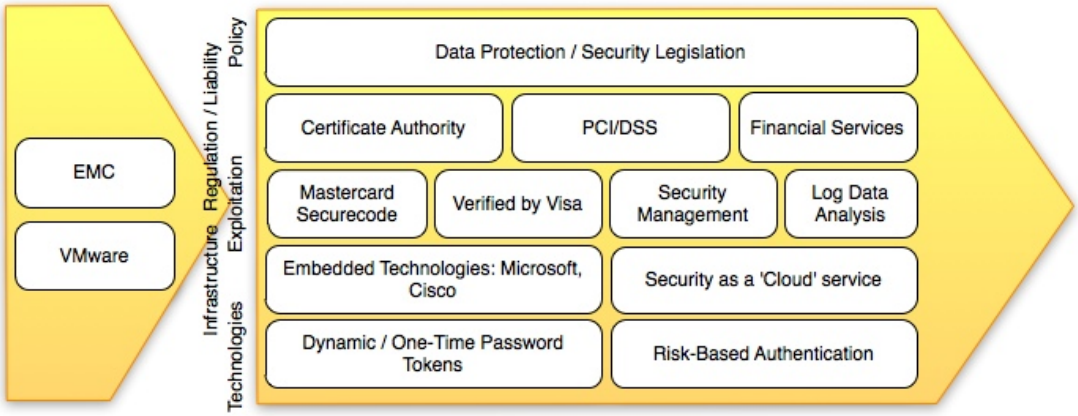


Figure 18: RSA Value Chain

5.2.7 BankID

The company, Financial ID-Technology, provides the service of electronic identities using the PKI technology to banks in Sweden. BankID[79] is the leading electronic identity in Sweden with a market share of 75%. BankID has been developed by a number of large banks for use by members of the

[76] http://www.rsa.com/products/securid/datasheets/2305_SID_DS_0709.pdf

[77] RSA-Security. Implementing Identity Assurance for Business Acceleration. (White paper), 2008. Available from <http://www.rsa.com/solutions/technology/overview/IA_OV_0208-final.pdf>.

[78] http://www.rsa.com/rsalabs/

[79] http://www.bankid.com/en/What-is-BankID/

public, authorities and companies. The services vary from online banking, e-trade to tax declaration and are provided by government, municipality, banks and companies. BankID is used both for identification as well as electronically signing. The customer's identification is guaranteed by the bank issuing the BankID. According to Swedish law, signatures with BankID are legally binding within the EU. BankID is available on smart card, soft certificate and since 2010 on mobile phones (mobile BankID).

The first BankID was issued in 2003. At the moment 9 banks acts as issuers (Certification Authorities) of BankID to their customers. Together they represent about 5.6 million online bankers (Sweden has about 7.3 million citizens above the age of 18). BankID illustrates the potential of crossover between banking credentials and public sector services; the most important element underpinning this potential is its liability model.

5.2.8 VeriSign

VeriSign is one of the world's largest providers of authentication and certification services based on PKI technologies. They and their partners provide Domain Naming System (DNS), Secure Socket Layer (SSL), Public Key Infrastructure (PKI), and other authentication services. At the moment, VeriSign facilitates up to 50 billion DNS queries a day. Their service offering includes global registries, data centres, and infrastructure whose aim is to provide secure and scalable authentication services worldwide. One product area of particular interest in the eID arena is Verisign's National PKI Program.[80] This is designed to provide an infrastructure for the creation of PKI schemes at a national level, and is being promoted – particularly in the US – as the foundation for an open eID scheme. The company is worldwide, with European headquarters in Geneva, and offices in the U.K., Sweden, Switzerland. Products and services include PKI, Fraud Detection Service (FDS), and One-Time-Password (OTP) software, services.

The VeriSign product offering covers four separate areas:

(a) global registries which are able to store information in secure and easily accessible formats. The registries provide a certifiable record of all contents, enabling companies to monitor and record how and by whom the data are accessed and used. The key registries offered by VeriSign are the Global Domain Name Registry (stores IP addresses and domain names, facilitating service to Internet, email, FTP and other addresses), the Network Routing Directory (a master repository of subscriber and network information), and the Object Naming Service (stores critical information that allows authorized individuals to track products across global supply chains using RFID and other tags).

(b) different types of networks that allow their customer companies to transfer information securely and reliably, using different protocols and physical infrastructure. The Signaling System 7 (SS7) Network, enables the provision of advanced digital services among different types of companies, including telephone operators, cable operators, ISPs, wireless providers, and wired/wireless advanced digital network database providers.

(c) data centres that provide the physical security and backup capabilities required from the infrastructure. VeriSign maintains a number of data centres providing different services such as monitoring the global DNS systems, managing customer networks, hosting Internet and telecommunications systems, and monitoring and securing network traffic.[81]

(d) a single platform for provisioning, managing and using multiple authentication credentials named VeriSign Unified Authentication[82]. The platform supports strong authentication using smart cards, the Secure Storage Token, the USB Token, a device-generated One-Time Password (OTP) Token and digital certificates. It also supports PKI-based encryption, digital signing, and non-repudiation.

[80] http://www.verisign.com/static/national-pki-government-trust.pdf
[81] VeriSign, "VeriSign Internet Infrastructure: An Overview," (2007), vol.
[82] http://www.verisign.com.au/guide/unified-authentication/uniauth_datasheet.pdf

Overall, VeriSign enables companies and consumers rely on an Internet infrastructure that lets them communicate and conduct commerce with confidence. For this purpose, they provide encryption and authentication services to Web sites, intranets, and extranets, protect digital identities with strong authentication mechanisms, develop online fraud detection services, as well as maintain the authoritative registry of all .com, .net, .cc, and .tv domain names.

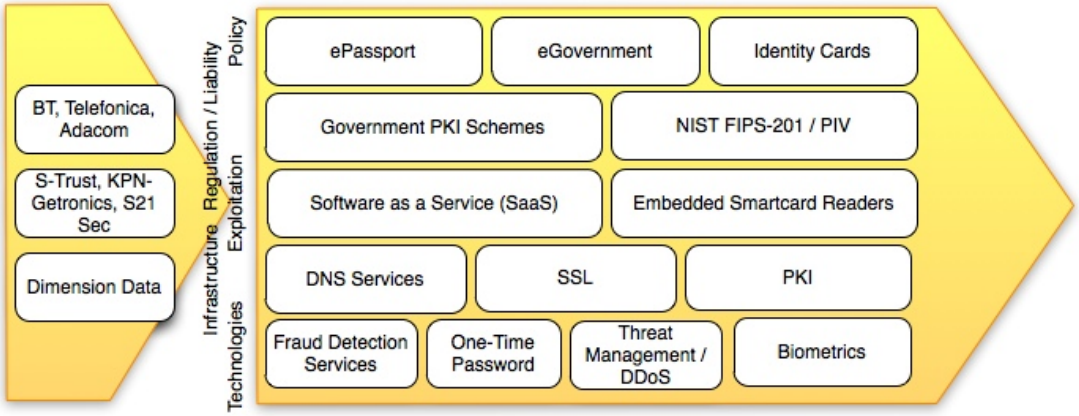


Figure 19: Verisign Value Chain

5.2.9 Giesecke & Devrient[83]

Giesecke & Devrient (G&D) is a leading international technology provider and a global market leader and pioneering innovator in banknote production and processing, smart card solutions for telecommunications and electronic payment, and security documents and identification systems, headquartered in Munich, Germany . In the eID market, their products can be divided into three main groups: smart cards, management of personal data, and security solutions:

(a) smart cards, manufactured by G&D, are used worldwide in various environments. G&D provides end-to-end solutions in the intelligent debit and credit cards area, for instance. G&D smart cards, based on secure smart card operating systems and conforming to the latest EMV standards, can incorporate different applications on a single smart card adding features and extra applications to existing payment cards of various kinds.

(b) means for the secure acquisition and processing of personal data. G&D equips passports, ID cards, health care cards, and driver's licenses with sophisticated security features to prevent their misuse, and also enables the use of integrated chips, which may also contain biometric data, in these cards to provide additional security. Such products follow the requirements of EC Directive CEN TC 224 WG15, which describes a universal standard for security and data protection on the so-called European Citizen Card (ECC). The ECC standard ensures easier access to e-government and local administrative services by citizens, through the use of IAS services (identification, authentication, digital signature).

(c) integrated systems and solutions for network authentication, e-mail encryption, and single sign-on. G&D also offer security solutions for protecting brands and sensitive documents.

5.2.10 PGP Corporation[84]

PGP Corporation is a US-based company that specializes in email and data encryption software used for data protection in both fixed and mobile environments. The most important part of the PGP product offering is the PGP Encryption Platform, which provides a single, scalable architecture for addressing privacy and data protection issues while reducing IT operational costs. Unlike point

[83] http://www.gi-de.com/
[84] http://www.pgp.com/

solutions that address specific threats, the PGP Encryption Platform delivers an integrated encryption framework across a broad range of encryption applications.

Based on a unified key management and policy infrastructure, the PGP Encryption Platform offers a set of integrated applications for enterprise data security. PGP platform-enabled applications allow organizations to address current needs and expand as security requirements change for email, laptops, desktops, instant messaging, smart phones, network storage, file transfers, automated processes, and backups. This approach enables IT to develop a proactive encryption strategy to mitigate risks before they affect operations or threaten the corporate brand and reputation. PGP encryption solutions are currently used by more than 110,000 enterprises, businesses, and governments worldwide. Customers use PGP solutions as part of a regulatory and audit compliance solution, to protect confidential information, secure customer data, and safeguard companies' brands and reputations.

5.2.11 Arcot Systems[85]

Arcot Systems is a US-based company that offers online fraud prevention, strong authentication and eDocument security solutions. Their products and services are used to prevent fraud and identity theft in Internet transactions and online access by over 100 million consumer, enterprise and e-Commerce users. Financial institutions, pharmaceutical companies, eShopping sites are some of the most important sectors that use Arcot's solutions. Arcot aims to make their solutions easily deployed, low-cost, and highly scalable; this entails enabling organizations to protect their users from fraud without changing user behavior or requiring expensive hardware.

Organizations can deploy Arcot solutions either in the cloud (through remote hosting) or on the premises of the customer company, addressing its particular requirements for cost, convenience, and level of security. Arcot's services are hosted in a certified, PCI DSS-compliant data center, which provides the highest level of cloud security currently standardized by the industry. Arcot offers a two-factor authentication software-only midrange solution[86] called WebFort, designed to deliver a balance of cost, convenience, and strength for a lower cost of ownership than alternative solutions. This can be achieved through the use of the ArcotID which is a software credential which combines the protection for digital IDs (like a hardware smartcard) with the lower cost and simplicity of a software solution. It can be integrated with various existing infrastructures, with support for standards such as RADIUS-based OTP and PKCS#11. In addition to strong authentication, the ArcotID enables PKI applications such as electronic document signing, secure email, and secure ecommerce.

5.3 Further research to make sense of the eID market

A number of steps could be taken to enhance our understanding of the functioning and future development of the eIdentity market. First, in relation to the economics of the eID market, it would be essential to find more *quantitative* data, both about the individual companies and the market as a whole. This would give us an indication of the economic significance of the eID market and the relative roles of the various stakeholders. However, this kind of research would constitute a very significant additional effort, both in terms of resources and time.

From a more theoretical perspective, we think that economics of identity can be understood according to four distinct schools of thought. Each of these four schools allocates specific dynamics to economics of identity; we believe that these dynamics should be mapped out and their impact on how the eIdentity market functions should be researched. Based on this work, the ensemble of company activities could then be studied according to each school of thought as appropriate. The four schools of thought are identity as a consumption good, identity as a capital asset, identity as a social good, and identity simply as a cost. The first possibility, **identity as a consumption good**, means that users

[85] http://www.arcot.com/

[86] In between simple, inexpensive but insecure, traditional username/password mechanisms and very secure but expensive hardware-based one-time password tokens, biometric, smartcard, and PKI systems

choose their identity on a case-by-case according to how and where they want to use it. In this case, identity results from *explicit* choices by the individual. Viewing **identity as a capital asset**, where identity is regarded a property that can be publicly traded means that identity will have a changing value over time and space, because people's valuation of their identity changes with time and social context. When identity is understood as property, the value of pieces (i.e. value in different contexts) does not equal the value of all. The third way to analyse economics of **identity** is **as a social good** (where the esteem and reputation of a person have economic externalities). In this case, identity is understood to have network effects, meaning that identity increases in economic value by its increased use (by companies, by people). Finally, the conventional way to understand **identity** is purely **as a cost**. This means that the economic value of identity is only recognized as far as it incurs costs for the different stakeholders (governments, companies, consumers).

Secondly, it would be important to look more closely at how different companies are positioned along the value chain, and what business models they use to operate. This would entail a more detailed look at the activities of each company, analysing how exactly they create value, how these activities are linked with those of other companies, which companies and stakeholders form partnerships, and how and why they do it and what is the specific role that each company fulfils in the value chain. This would provide us with a much more detailed understanding of the dynamics of the eID market and the way different types of companies can work together to increase the added value of the whole value chain. This analysis could be combined into a look at the competitive dynamics of either the whole market or some segments of it: what kind of strategies and ways of operation do companies with similar offerings use to best address the needs of the customers and to gain a competitive advantage over each other?

Thirdly, it would also be worthwhile to find out more about the role of social networking sites (SNSs) for the eID market. As the role of stakeholders such as Facebook, mySpace, and Google is constantly growing, both in terms of use of the sites and economic importance, their role both as individual players and as contributors to the overall eID market (how they contribute to the growth of the sector, how their prominent role supports smaller companies in the field, etc.) should be better understood.

Finally, a regional-level analysis, analysing similarities and differences of the national and regional markets, combined with insights into the particular drivers and barriers, and respective growth rates, would result in a much more granular understanding of the eID market.

6 EID MARKET TRENDS AND FINDINGS

6.1 Introduction

Whether offering secure smart card based authentication, software-based credentials or PKI-based interoperable services, the market for eID products and services is in rapid transition. Existing and emerging technologies shape developments, while new applications and partnerships raise new opportunities. Moreover, organisational and institutional changes elicit stakeholder strategies within an evolving legal and regulatory framework. Not all of these developments can be monitored or predicted using quantitative approaches; important qualitative factors must also be considered. This section describes some of the key changes in eID technologies, applications and marketplace developments, analyses them and elaborates possible market drivers and barriers.

6.2 Key technology and usage developments

Relatively robust identification and authentication technologies exist and have come to support a range of value-added services. Still many activities take place in the exploitation and infrastructure layers as businesses and Members States alike intend to facilitate access to new services. Technology and usage developments in the eID arena can be considered as short-term (up to three years) and long-term (beyond three years).

6.2.1 Short-term developments

In the short term, eID technology will develop onto more robust or standardised implementations; that is, well-known technologies (i.e. Single-Sign-On, Public-Key-Infrastructure, smart cards) will be made more practical through improved product development and commercialisation. Relatively large companies (i.e. RSA, Verizon, Microsoft) are expected to be making most progress in the short-term.

6.2.1.1 Greater federation

The next three years will see an increase in use of federated technologies for eID (i.e. SUN/Oracle with Liberty Alliance, Microsoft with WS-Federation) as cross-enterprise applications become more mainstream. In addition, as trust in both the technology and the issuers grows, traditionally 'competing' providers will become more willing to rely on each others' credentials within a federated space. This follows a shift in emphasis from underlying eID technology to value-added services (i.e. consulting, marketing databases, online payment). Interoperability of existing schemes is a current focus for development by the likes of Kantara (3.3.2.1), which will in turn improve adoption rates.

6.2.1.2 Embedding eID in the infrastructure

Increasingly, eID technology is embedded either in the infrastructure (i.e. biometric access to portable devices) or into the broader technology infrastructure ('across the layers')[87] through collaborative development and strategic partnerships. Organisations – such as Verisign – embedding eID into the infrastructure aim to deliver an integrated, holistic, service-centric product model through integration with key infrastructure vendors (e.g. Microsoft, Cisco, Oracle) so that own security and identity technologies become part of the fabric of the Internet. This is in a way a return to the origins, when SSL was shipped with the first Netscape browsers. However, the whole process is delayed by known challenges in relation to open vs. proprietary standards and organisational innovation barriers.

[87] For instance, the case of privacy-aware eID across layers, work conducted in preparation of the FIA 2010 event: http://security.future-internet.eu/images/c/c5/WS_3March_final_report1.pdf

Embedding eID technologies in the Internet and mobile infrastructure will be critical to the development of broader eID applications, which are likely to emerge as a 'critical mass' of enabled infrastructure becomes available.

6.2.1.3 Enhanced tokens

A current challenge for eID is credential delivery through existing tokens, mainly due to the need for enhanced security (i.e. RSA SecurID USB token 5.2.6, Verisign Unified Authentication 5.2.8). At present, where two-factor authentication is required, the user has to carry a token for each credential; for example, a credit card for each credit card account, or a passport, driving license, and health card when dealing with central government. This is inconvenient for the individual and inefficient for the market. This is due to lack of interoperability between ID schemes; competition between commercial providers (in particular financial institutions which wish to keep their logo in the customer's wallet); regulatory limitations; market inertia; and perceived cost of integrating credentials.

Technologically, existing EMV[88] schemes can already handle multiple accounts per token, and it is probable that financial institutions in particular will wish to consolidate the number of cards issued in order to reduce costs. In some countries (i.e. Finland 3.1.2.3) this has already occurred (e.g. checking, savings and credit accounts accessible from a single token), whilst in others such as the UK this is yet to achieve.

The availability of enhanced token devices that consolidate existing multiple tokens and offer users additional functionality through local card readers (or embedded equivalents) will lead to greater adoption of certificate-based services and the incorporation of two-factor authentication into a wider range of identity relationships.

A second problem with current tokens concerns online use, away from a card reader infrastructure. Some countries, such as Belgium and Estonia, have built an infrastructure for the domestic use of smart card credentials, but this is not the case in the majority of European Member States. This has hindered growth and increased fraud, since where card readers are not available, users have to fall back on manual processes – and credit card numbers and magnetic stripes provide low-security attack channels for fraudsters.

This problem may be addressed through the provision of domestic or portable smartcard readers. Belgium, for example, has encouraged PC manufacturers to integrate card readers into all new PCs, and has an accreditation logo so that vendors can demonstrate compatibility of their equipment. However, banks have traditionally been reluctant to foot the cost of providing readers for their customers; in part, this is due to the perception that customers would require a card reader per provider, rather than a single reader for all cards from all providers.

One innovative solution to this is the EMUE[89] approach of integrating the card reader with the card; by providing an embedded PIN reader in a card that has multiple wallets (the card can store ten different credentials), it is possible to offer high-value authentication across multiple credentials from a single trusted device. The card can also generate challenge/response codes as dynamic passwords where required.

[88] http://www.emvco.com/
[89] http://www.emue.com/site/home.htm

6.2.1.4 Portability of credentials

There are various examples of credential use, typically in the banking/financial services area as well as in the public sector (see examples quoted in section with brief country reports 3.1). However, following the Belgian and Estonian examples, the next three years will see increasing use of 'portable' or hybrid credentials in both public and private sector eID schemes. Portability brings forward two aspects:

- ***choice of delivery channels:*** consumers will be able to embed eID certificates in a broader range of devices than currently available. Rather than being constrained to a single smartcard, certificates will be widely embedded in multiple cards or EMUE devices, PCs, mobile phones or even vehicles. The likes of the BankID scheme offer this approach, but many countries lack this flexibility. The Estonian eID scheme even provides a real-time counter of the number of certificates downloaded.[90] Portability of both public and private sector credentials onto mobile platforms will be particularly well received as smart phones are personalised for diverse service offerings. With security standards improving, acceptance of such systems will be mainly an issue of trust.
- ***alternative authentication channels:*** where existing smartcard-based schemes suffer fraud, particularly in cardholder not present transactions, one effective solution is to use a separate channel for the authentication process. For example, a credit card number may be presented for an Internet transaction, but the authentication is done via a challenge/response over SMS to the cardholder's registered mobile telephone number. The hybrid use of channels creates an additional layer of security, since an attacker has to intercept two channels to successfully attack the transaction.

> Increased portability of credentials and use of alternative authentication channels would result in a higher take-up and more extensive use of eID solutions, thus contributing to market growth.

6.2.1.5 'Zero-proof' eID

Microsoft's acquisition of Credentica[91] and its U-Prove eID technology ought to be mentioned as a development in eID. U-Prove allows asserting parties to verify personal information with relying parties without actually revealing information; and where information is revealed, it cannot be used for onward purposes without the asserting party's consent. Even where relying parties collude, there is no mechanism for them to undermine the asserting party's privacy. Microsoft is now integrating U-Prove into Windows and Infocards, and as it becomes increasingly available on the desktop it is likely that providers will exploit the toolkit and build commercial implementations.

6.2.2 Long-term developments

In the longer term (three years and beyond), key technology developments will come from improved use of identity credentials.

6.2.2.1 Governments accepting commercial credentials

In general, governments/public authorities do not accept commercial credentials as sole identifiers when authenticating individuals and instead rely on proprietary sources; while a range of commercial breeder documents (e.g. utility bills) are used to make a risk judgement on identity, they are not used as the sole credential. Conversely, commercial providers will generally trust government-issued credentials even if these are used out of context – a passport is not designed for opening a bank account, but will be accepted for doing so.

[90] http://www.id.ee/
[91] http://www.credentica.com/

A centrally-regulated framework to provide identity assurance for government use of commercial credentials both within and between European Member States would promote eID interoperability and create new eID market opportunities.

However, as private sector providers issue more trusted credentials, and there is greater interoperability between private and public sector schemes both within and between nations, governments are increasingly likely to accept commercially-issued or foreign credentials, with less dependence upon their own issued documents. This will create new market opportunities for commercial providers as their services move into high-value and cross border use cases. The existence of an appropriate common legal/regulatory framework in all Member States would help in the use of intra-operable credentials which would, as mentioned, facilitate further market take-up of advance services.

6.2.2.2 Tighter integration with mobile telecoms

A critical move in the acceptance of eID has been the provision of portability of identity between platforms: the ability to embed a certificate in multiple devices to facilitate use over different channels (6.2.1.4). For example, a user logs on to their online banking from an Internet café; the bank uses SMS to send a challenge code to the user's registered mobile phone. The user enters the number, and a PIN, into a trusted application on the handset which generates a response to the bank, and a one-time PIN for the user to enter into the PC. The bank can then authorise the login. As eID implementations become more interoperable and tightly integrated, mobile telecommunication providers will take on roles of greater importance.

Use of mobile alternative authentication channels would promote eID interoperability, user convenience and security. For this to happen telecommunications standardisation bodies and industry regulators across Europe could work closely with mobile telecoms on rollout of interoperable digital certificates.

Those countries such as Belgium and Estonia that have delivered portability in national eID schemes have benefitted from embedding certificates in mobile devices. New developments include those by Vodafone and Gemalto[92] which have proven the concept of embedded certificates. But the next stage will be to fully integrate certificates into the device's SIM card. This will permit high-value authentication of the device – and therefore the user – and provide an infrastructure that can support beyond e-Banking, e-Voting, Telemedicine and other critical services. In addition, portable credentials on mobile tokens reduce the risk of identity theft as there are no high risk, centralized repositories of personal identity information; they also deter social engineering attacks as they would have to be executed one by one and thus can not be automated.

6.2.2.3 Acceptance of biometrics

To date, biometric authentication technologies have not achieved much penetration of commercial markets. This is due to multiple factors: high cost of biometric infrastructure provision, historic concerns about the reliability of enrolment and authentication and cultural acceptability.

Enhanced biometric technologies that are portable and affordable would encourage widespread adoption of 3-factor authentication and help to address phishing and impersonation attacks.

[92] http://www.betavine.net/bvportal/home.html

However, recent developments have pointed the way for a much more widespread implementation of biometric technologies:

- Continued falling prices of biometric readers, coupled with improved usability and reduced size of equipment, are making the technology more attractive for commercial use.
- Increasing reliability of biometric readers (in particular fingerprint); mass trials and implementations mean that the false accept / false reject rates are much more clearly understood. Thus systems can be designed with a proper understanding of the consequences of failures, and where these occur, more reliable technologies can be introduced.
- Untraceable biometrics[93] and biometric encryption techniques are delivering privacy-friendly biometric systems that are more likely to gain trust and widespread public acceptance, moving public attitudes from 'Big Brother' towards a less intrusive and more socially acceptable technology medium.

6.2.3 The impact of virtualisation and cloud computing

Possibly, the most significant influence on the eID market will be the growth in virtualisation and cloud computing. Virtualisation – including virtualisation of the data centre and of the broader infrastructure, as well as of individual machines and processes – can be thought of as the 'entrance' to cloud computing. If security, identity and privacy controls are integrated into the virtual machine, then the physical or logical location of that device becomes irrelevant from a trust perspective.

> Virtualisation/cloud computing eID 'nodes' require technology-specific operation and protection (since all security effectively moves to the end-point in this model), and new management tools and licensing models even where existing technologies and products are used.

Cloud computing – which implies moving storage and processing into a fully virtualised and often outsourced infrastructure – takes virtualisation challenges to the next level. In many cases an organisation will not be aware of the physical location of critical information assets, including identity data, when they are in the 'cloud'. Whilst this delivers compelling cost-savings, it also gives rise to concerns about possible security and integrity problems. Once again, existing technologies are finding new growth channels through the provision of management tools and licensing models.

In addition to provision of existing eID services when systems are virtualised or moved into a cloud computing model, this movement creates the opportunity for virtualisation of eID services themselves – that is, provision of eID to organisations or communities through a fully-outsourced service that can bind together the organisation's infrastructure without being present within that infrastructure.

> Whilst deliverable with existing technologies, the challenge for vendors will be to convince clients that an outsourced eID infrastructure can be trusted: this has long been a challenge for vendors when selling other security outsourcing services.

6.3 Emerging eID applications

Beyond technological developments, opportunities are created in the market that aim to satisfy actual and latent demands. As a result numerous, novel eID applications are being developed and tested. While most relate to the provision of enhanced security identity services and online fraud prevention, new services related to online payments and credit management are also making progress, such as

[93] http://www.ipc.on.ca/images/Resources/untraceable-be.pdf

services offered by US-based Paypal[94] and Equifax. The availability of cross-border and cross-sector interoperable infrastructure will no doubt aid new applications' development and diffusion. Developing embedded applications, hiding the security complexity in the underlying infrastructure (i.e. smart card readers on PCs that can read multiple vendor cards) are a way of promoting innovation in eID applications. More sophisticated applications, for instance those providing access to marketing databases[95], or those that allow a 'plug-and-play' approach with several eID components combined to offer a personalised customer experience are yet enriching the market. Finally, additional 'soft' applications/services offered by specialist partners that combine focused technical solutions with expert advice as to how to use them to make most of their benefits, could also enrich the market. While most emerging applications are in the 'services to businesses' segment, it is expected that many new applications will emerge in the 'services to individuals' segment, where users are likely to be the main innovation motor for their development[96].

6.3.1 Social media and self-assertion

A dominant trend is the growth of eID systems based on 'user'-driven or 'self-asserted' identities, particularly those used in social media. Individuals' Facebook Connect, Googlemail and eBay credentials are becoming as important to them as government-issued documents. Self-assertion regards:

- ***credentials:*** e.g. I-names,[97] OpenID,[98] domain names, email accounts;
- ***personae:*** e.g. Facebook, LinkedIn, chi.mp;
- ***attributes:*** e.g. Volunteered Personal Information (VPI) / Vendor Relationship Management (VRM).

The Internet is moving towards a model where users depend less upon trusted service providers and build up their own peer-to-peer relationships, often based upon self-asserted or reputation-based credentials. These multi-party relationships are much harder to define and classify than 'traditional' two-party trust relationships and there are questions about whether basic ID concepts – such as those discussed – remain valid in this case.

> Self-asserted credentials are gaining significant public trust and adoption, and must be taken into account in any eID interoperability consideration.

The growth in self-asserted ID gives rise to key questions such as: 'what is an identity?'; 'does it have to depend on a trusted third party or a credential issuer?'; 'how do identities, personae and attributes relate to each other?'; 'do one person's different personae actually have to be consistent?' These are issues that must be addressed if the role of self-assertion is to be properly understood in the eID model.

6.3.1.1 OpenID

OpenID is probably the most successful self-asserted cross-provider eID scheme in use today. Created and managed by the open source community, the scheme provides a federated eID for use across multiple relying parties, which trust assertions from OpenID rather than requiring a relationship with the end user. This in turn allows users to access new participating services without having to register

---

94 PayPal offers online payment services on top of secure eID service provision by Verisign and Equifax offers Credit management services also secured by Verisign.

95 Acxiom is an interactive marketing services company.

96 Alluding to a possible customer relations management in a user-to-user environment.

97 http://www.inames.net/

98 http://openid.net/

or provide additional personal information each time they wish to do so; the precise information revealed to a new provider remains under the user's control. OpenID claims to have over 1bn enabled user accounts and over 50,000 participating websites, and already has a substantial commitment from key Internet companies, including the likes of Google, Yahoo, Blogger, myspace, Wordpress, Flickr, Orange and AOL.

6.3.1.2 Government use of self-asserted ID

Governments have yet to make widespread use of self-asserted ID; it is a concept that defies the tenet of government being the issuer of credentials of the last resort. This may be about to change: the US government is proposing to use OpenID as a citizen credential in 'low assurance', low-trust scenarios, leveraging existing industry solutions (the evolution path to using IDs in a higher-trust scenario is as yet unclear).[99] Plans are as yet at a very early stage, and are being debated mainly between government security architects and technologists, but if they turn into an implementation, then this will clearly have implications for the EU eID landscape.

> Governments have yet to make widespread use of self-asserted eID schemes, but it is likely that such approaches will become increasingly important in the near future.

6.3.1.3 Volunteered Personal Information

Not only is the basic model for trust changing, but also the way in which data is shared in trust relationships. The growing trend towards Volunteered Personal Information (VPI) (also known as Vendor Relationship Management (VRM) or Personal Information Brokerage (PIB)), in which individuals release information about themselves in response to requests from relying parties (as opposed to placing that information with those relying parties and authorising them to use it when required) is shifting trust models away from the concept of a 'trusted third party'.[100] Organisations are decreasingly seen as the authoritative source of identity/attribute data, and new models rely on trusting the data subject with that role. This may have an effect of disintermediation on traditional identity providers, but leaves an opportunity for those providers of underlying identity infrastructures that can accommodate these new trust models.

> Self-assertion and volunteered personal information (VPI) are shifting the balance of power in identity relationships away from traditional providers and back to data subjects. This will result in disintermediation for third parties who are no longer required, and lead to new business models for eID.

6.4 Market developments

The stakeholders analysed in this Report are involved in a wide variety of activities collateral to eID; partly, this comes as a result of the fact that eID services have a cost that few are willing to assume. A manner to diffuse the cost is to bundle eID with other complimentary but more lucrative services, such as security, anti-fraud, or to embedded in the infrastructure; both ways are considered as necessary for the further development of an eID market. Consequently, the eID market relies heavily on the information security market for its development, and many of the key organisations and technologies originate from the information security industry. Such offerings include both 'traditional' vertical technology solutions (security as a 'bolt on' approach) and embedded solutions; for instance Verisign has developed strategic partnerships with other vendors to deliver an integrated, holistic, service-

[99] See http://www.idmanagement.gov/drilldown.cfm?action=openID_openGOV
[100] See http://kantarainitiative.org/wordpress/2009/06/iain-henderson-the-personal-data-eco-system/

centric product model hiding in the process their secure identity technology in the underlying infrastructure.

> Whilst infrastructural development supporting embedded eID capability is market driven, governments may be able to accelerate the process by providing incentives to embedded eID standardisation and innovation.

Most of the companies identified take part in the exploitation of the eID products and services in the lower layers of the value chain. In the exploitation layer, many of the companies analysed offer identity management or antifraud services. For instance, Arcot systems (5.2.11), provides its clients with a risk-based Web identity fraud solution that in real-time assesses the fraud potential of every online transaction. What seem to be lacking are companies providing more sophisticated services that take existing identity infrastructures as a base and utilise them to offer novel services. Some such services include marketing databases by Acxiom and online payment by PayPal; other companies offering a particular service on top of the existing infrastructure were not encountered in the research. However, if the eID market is to develop into full maturity, there will be a significant need for sophisticated services which have a much higher added value than simple technology-based ones.

Typically larger companies (such as Oracle, Microsoft, SAP) that have the necessary financial, personnel and knowledge resources to operate simultaneously in multiple segments of the value chain, have emerged to offer products and services there. If these companies will be able to combine their offerings across different segments, they may be able to create significantly higher added value than the sum of the constituent parts. In addition, many of the companies analysed offer full solutions that address discrete customer needs across the value chain, providing all necessary components required to offer the service. Often in these cases, the solution may be tailored case-by-case, thus creating even higher added value for the customer company.

> To drive the growth of the eID market, there is a need for more advanced eID services that take existing technologies as a starting point and, building on them, create novel services that offer a higher added value.

We also note the emergence of a cluster of 'soft' services such as consultation, training, and management (traditionally Services to Business, according to NACE categorisation). This trend points to the increasing maturity of the industry: as both public and private stakeholders begin to realise the importance of eID solutions but do not know how to make the most of them, specialist companies that offer these services have emerged. A particularly common development is the coupling of identification solutions with professional services; by providing the technical solutions while at the same time offering expert advice on how to make the most of them, companies are able to make it significantly easier for their customers to make use of eID infrastructure in a reliable and cost-efficient manner. In some cases, eID companies are already partnering with each other, with each company in the partnership operating in the activities they are most proficient in.

> The emergence of softer services, such as consultation and training, has provided additional value to existing eID solutions; these are an important driver in keeping the industry on a growth path.

Although many companies operate in the infrastructure layer, some important technological developments are not yet addressed by many. One of these developments is federated identity, which allows individuals and companies to utilise the same identification to access networks managed by

different organisations in order to conduct transactions. In this way, users can share information and applications with no need for separate identification for each service. While federated identity offers significant potential for further market growth several factors slow down its uptake. The most significant of these is security and privacy concerns, such as security of storage, retention period, data minimisation and secondary usage of data kept. There are also challenges in finding a common set of identity attributes (identifiers) for federated identities, i.e. attributes that are suitable for the purposes of all the stakeholders taking part in the federated identity scheme. Finally, many of today's federated identity schemes seem to be limited to web services, and do not allow access to proprietary services.

> The commercial availability of federated eID solutions – shared and trusted by both private and public actors – will further drive market growth; however, it will require addressing security and privacy concerns.

Another significant development in the infrastructure section is the portability of credentials. Particularly important in this sense are governments accepting commercial credentials and their portability into the mobile sector. These developments would make it possible for companies to offer the same product or service for a wider market, thus significantly improving the potential of the business case. However, so far there are limited possibilities for companies to offer interoperable eID solutions. While some companies such as BankID and BBS offer solutions that are accepted for certain purposes by governments, in general they are very wary of accepting commercial credentials and instead prefer to rely on in-house solutions. As the security standards of the commercial products are constantly improving, it may be that this lack of acceptance is more of an issue of perceived suitability of commercial credential for governmental purposes. In some cases there may also be issues of trust.

Another element in the landscape is the limited number of states in Europe that rely on interoperable infrastructure, which may mean that identities accepted by some governments may not be accepted by others. This reduces the incentives for the private sector to provide such interoperable solutions for governments. As for the mobile sector, currently there is little evidence of mobile phone services using electronic identities from other sources, despite the significant potential of the market. As of today, developments in this area seem to be limited to patents and pilots, and there may be questions as to the technological maturity of these solutions.

> Those markets that have yet to adopt greater portability of credentials should be encouraged to do so through provision of appropriate Certificate Authorities, permitted use of government root certificates, and regulations to permit certificate use in mobile devices.

Specific solutions for single sign-on, public key infrastructures and smart card equipment are already offered by many companies. One of the most significant technological developments of late, cloud computing, is being widely discussed at the moment, but not many companies operate in the field yet. For example, none of the stakeholders included in the primary analysis was active in this segment. It can be expected that cloud computing emerges as a significant sector of the eID market in the coming years. Currently, however, 'Identity as a Service' is in an infant state with players such as Zimory[101] or CloudSigma[102] starting to offer cloud computing solutions. Zimory offers more efficient data storage through cloud computing, and CloudSigma has only recently started to offer cloud hosting.

[101] http://www.zimory.com/
[102] http://www.cloudsigma.com

Governments remain one of the most important stakeholders in the development of the eID market. Government departments in most EU countries increasingly deploy eID infrastructures to make it possible for citizens to have digital access to services, which makes them the largest individual customers of eID products and services. Governments' purchasing power alone gives them a high influence on the direction to which the market develops, for instance as to what features are required, what are the acceptable standards of trust and reliability and what identification methods will be used. The decisions and actions taken in different governmental bodies will thus be instrumental for the development of the eID industry.

> Governments are in a key position to drive the development of the eID market, both due to their position as the single largest customers of eID solutions and their role as the regulator of the market.

Furthermore, most eID solutions can at present only be used in discrete national markets, especially in EU27, despite the single market framework. This compartmentalisation is mainly due to the lack of a common legal framework defining the responsibilities and liabilities of various stakeholders (governments, solution providers, customer companies, citizens) using eID solutions. To unify the currently fragmented eID markets, it would be necessary to enable the use of a single electronic identity across national borders and in different use contexts, so that there would be an overarching set of general rules; this would promote economies of scale and customer trust in electronic identification.

Finally, the issue of trusted service provision still reigns in the market. The Microsoft's 'Passport' scheme is a prime example of the failure of a technically robust eID system to gain wide-spread adoption . Originally designed to provide an SSO to Microsoft services, including the Hotmail email platform, the company pitched Passport as an access tool to all online services: a definitive, centralised eID for the Internet. Soon, user concerns emerged about privacy and liability: fears of Microsoft's ability to profile users through their web access (initially denied by the company, but subsequently shown to be technically possible, even if Microsoft wasn't doing so) caused protests, and providers backed away from trusting a service that did not offer any practical solution to perceived problems in the event of failure.

> For an eID scheme to succeed, the provider must deal with likely abuse or misuse issues even if these are not a result of poor product development and thus raise the trust of all parties in the relationship.

Microsoft eventually pared Passport back to access to the company's own services (Hotmail and online support), and the lesson spurred their investment in Infocard technologies, including the development of the 'Laws of Identity'[103] which include specifications that identity providers must not themselves become 'inappropriate third parties' in an identity relationship.

6.5 Catalysts and barriers to market growth

Although quantitative statistics as to market size were not found, there is a strong belief that the eID market is growing; anecdotal evidence refers to an increasing number of organisations entering the marketplace. One vendor indicated that the problem is defining what the eID market really is; since there is no standard accepted definition, different vendors and analysts calculate market size (and therefore growth) in different ways. However, that particular vendor was confident that even in the recession, growth exceeds 10% year on year.

[103] http://www.identityblog.com/stories/2004/12/09/thelaws.html

6.5.1 Catalysts for growth

The growing movement towards citizen-centric public services – that is, structuring government services around individual citizens and allowing them to download information and services from a single web portal – is driving growth in the public sector. Whilst the recession has slowed overall growth, it has driven procurement towards specific vertical markets: in particular, the recession has (anecdotally) fuelled growth in fraud, and vendors report seeing the emergence as 'fraud as a service': the provision of packaged fraud services available online. This has pushed organisations towards the purchase of anti-fraud tools in preference to other security/eID mechanisms.

Vendors report major opportunities in those countries which are engaged in radical modernisation of their infrastructure (Estonia is an example of a country which has achieved this; Turkey one that is currently going through the process) where legacy approaches are abandoned and innovative eID solutions are adopted. In those countries where eID schemes are designed to serve the State, rather than a spectrum of stakeholders, and solutions incorporate legacy systems, ideas and processes (such as the UK), eID schemes appear to be less popular and adoption rates are disappointing.

6.5.2 Influencing growth

6.5.2.1 Policy innovation

Interviewees felt that growth of the eID market will come from innovation in policies rather than in new technologies. In order to fight market fragmentation as a result of the private sector creating piecemeal schemes rather than generic, interoperable infrastructure, Governments should provide those components of trusted infrastructures that are too risky or costly for private sector organisations to develop: for example, enrolment of the population into an authentication scheme, or underwriting financial losses arising from use of an ID scheme.

6.5.2.2 Federated eID

eID market growth could be encouraged by government encouraging greater use of federated ID schemes across the private sector. For instance in the case that a national eID scheme provides an 'open' interface for commercial exploitation (within a framework of regulation/accreditation) so that commercial stakeholders are encouraged to interface with the scheme rather than to develop proprietary ones in isolation. This could be achieved by public authorities that are willing to invest in, and then use, trusted federated credentials. BankID is a good example of this: by providing a trusted central database and underwriting the overall scheme, private companies have an infrastructure on which they can build trust services. Public authorities accept BankID credentials for specified purposes.

6.5.2.3 Tougher regulation and enforcement

Interviewees expressed the opinion that (with some exceptions) many EU Member States do not enforce sufficiently rigorously existing regulations, which would encourage the growth or operation of trusted eID. For instance, Directives encouraging organisations to use Privacy Enhancing Technologies (PETs) seem to have no mandatory requirement and no associated penalties, and are perceived as floundering. Moreover, Data Protection Commissioners lack, or choose not to use, the means and powers they need to enforce compliance with data protection regulations. The role, operation and powers of Data Protection Commissioners in regulating eID and ensuring a 'level playing field' across all borders and sectors is fundamental in the success of interoperable eID deployment.

In the majority of cases, the only effective regulations are those that are industry-specific, for example PCI DSS[104] or other financial regulations where the appropriate regulators are well-funded and

[104] https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

equipped with the ability to penalise non-compliance. It was also pointed out that this is not the case in the US, where regulators generally possess rigorous, prescriptive standards, and punitive powers to enforce them.

6.5.2.4 Enhanced smart card infrastructure

One of the challenges for growth in eID is the provision of portable access to eID certificates across platforms and locations: since most government eID schemes and payment cards rely on smartcard readers as the primary channel to access credentials, the lack of a smartcard reader infrastructure is a consistent problem. For example the Belgian and Estonian governments have encouraged vendors to embed readers in all new PCs, and have made readers available to citizens. The proliferation of smartcard reader devices among the citizens of these two Member States has without doubt been a key factor in the success of the eID schemes of these countries', and one that should be encouraged on a pan-European scale.

6.5.2.5 Dispute resolution and liability management

One of the obstacles to eID growth has been determining who – or which organisation – is responsible for what happens when things go wrong. Where interoperability is established, emerge issues of dispute resolution (agreeing the authority that has the ultimate decision on resolving problems) and liability management (a legally binding framework to ensure that all parties understand who will recompense what level of loss arising from failures in the system). If these issues are not addressed, trust in interoperability will eventually be eroded as disputes grow. A central European authority to resolve disputes and enforce liability decisions would become a powerful force in encouraging interoperable eID growth.

6.5.2.6 Public-private partnerships

It is common sense that commercial partners are essential to ensure that large-scale deployment objectives are pragmatic, real stakeholder needs are considered throughout development, and that the cost of the programme is proportionate to the value of the deliverables. As a result, it is also common sense that, where governments create national eID schemes, public-private partnerships can be critical for their success as opposed to where eID schemes are developed by the public sector in isolation.

6.5.3 Barriers to growth

6.5.3.1 Unclear policy for Government adoption of eID

On a pan-European scale, the lack of a commonly-understood authentication policy hinders eID growth. Private organisations are reluctant to speculatively invest in technology or infrastructure where there is a possibility that future government standards may select an alternative approach. In other words, the provision of firm and committed standards for government adoption of eID technologies will clear the way for greater commercial investment in eID.

6.5.3.2 Poor government investment

Just as government holds the key to influencing growth of eID, a lack of investment by government can be the greatest barrier to growth. For example, a lack of will by the UK government to implement high quality, remote authentication of individuals, even though that could help the provision of commercial eID solutions, has hindered eID growth in the UK.

6.5.3.3 Initial cost of user enrolment

For individual market players, one of the key barriers to growth is the up-front investment cost of initially enrolling individuals into eID systems in a trusted manner. This may require a face-to-face interview to take biometric details; checks on provided credentials; background checks with law

enforcement authorities or credit reference agencies; binding of payment details to the profile; and addition of other attributes to the user's profile. This can be prohibitively expensive for most organisations, which in consequence will either refrain from entering the market, or 'cut corners' in establishing credentials, which undermines the credibility of the eID credentials further along the value chain as fraud enters the system.

Governments can incentivise growth of eID usage by providing population-scale enrolment mechanisms (in much the way that Estonians can download certificates from their national eID) and thus prevent competitive/fractured approaches from commercial providers that divide investment into diverse schemes. However, care ought to be taken to do this in a scalable way allowing for cultural or regional specificities of EU27 Member States.

6.5.3.4 Lack of business case

The majority of eID systems in use today are specific to particular applications, communities, or nations. In the absence of a well-defined and accepted business case that proves the value in harmonisation and interoperability of eID, no organisation or government is willing to speculatively invest in the necessary standards and 'pump priming' to catalyse the eID market. For instance, banks often see security as a potential competitive advantage, but not nearly as important as customer retention: they are reluctant to share eID services with competitors for fear of losing customers. Governments would be well advised to identify and raise consensus on a compelling business case for investment in eID technologies – one which breaks down current 'competing' approaches – so as to 'steer' companies towards more collaborative eID schemes.

6.5.3.5 Usability

Usability of eID can be a challenge, particularly in public sector implementations, where eID is often integrated into complex citizen-facing applications, and becomes difficult to use. This is not unique to eID: usability is not generally well-understood in government systems, and user experience can be poor, leading to a lack of confidence in eID itself.

6.5.3.6 Over-dependence on national security needs

In many national eID implementations, national security is the driving objective behind the business case: where a large initial investment is required, often without the prospect of a clear return, governments have used national security needs to justify the cost. From the perspective of encouraging adoption and interoperability, this can lead to a number of fundamental flaws in the approach, including addition of security features that discourage interoperability or access by other stakeholders, failure to provide for commercial stakeholder needs, and end-user views that eID is only for government interaction.

For instance, the UK government's own report[105] into identity assurance recommended that national security needs should be seen as secondary in any scheme; that if the scheme is designed around end-user requirements, then the resulting rapid adoption will deliver secondary national security benefits as the eID infrastructure becomes pervasive.

6.6 Summary of tech-apps and market trends and barriers

Recent developments in eID technologies and markets have been presented and analysed in this chapter, demonstrating on the one hand a wide-spread consensus on the role of eID as a lubricant enabling new services for citizens and on the other a systematic monetisation of users' eID related data. While we still need further analysis of the social dynamics of the European eID market and specifically more research to better understand the economics of eID, in this section we will present a

[105] http://www.hm-treasury.gov.uk/identity_assurance_index.htm

'roadmap' of eID evolution as a result of the findings presented in this chapter. The objective of this exercise is to identify those activities that may be used to signal a maturing market. As such this 'roadmap' is a brief synthesis of trends, initiatives and activities that which are likely to materialise over the next 10 years (up to 2020[106]). In the next chapter we will propose a number of policy options that may help overcome some of the barriers.

In essence, and presented graphically in Figure 20, the findings identified in the previous sections have been categorised in three areas (technology, market and policy) and over time (today, 2015, 2020) making up nine groups of entries. On the horizontal axis, we distinguish technology related, market related and policy related developments. On the vertical axis we report the three main stages of temporal developments, between now and 2020. A few entries cross the groups' time borders, indicating that: (a) the entry will take more time to develop (i.e. a common legal framework); or (b) it will take more time for consensus to be raised before this entry shapes the area (i.e. in the case of "Data Subject in control"). While the entries are neither new nor surprising, they clearly point to a logical evolution path into the future that is not the result of extrapolation techniques but follows bottom-up analysis of market activities, in view of the evolution in separate policy/regulatory, business/market and technology/knowledge network areas. In this fashion, the evolution towards the foreseen objectives is likely to occur even though the barriers are not removed at once.

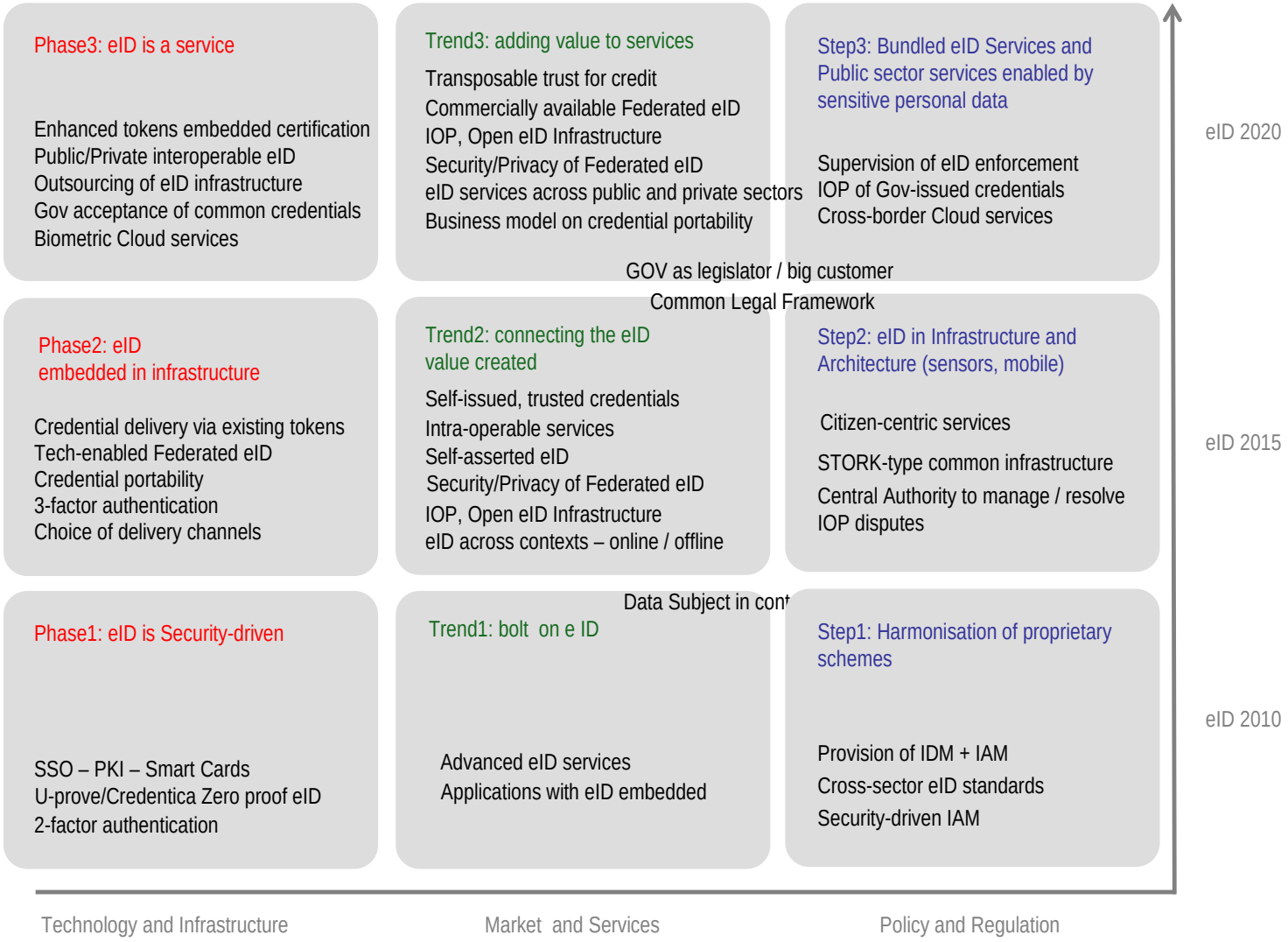
In essence, today's (2010) spectrum of activities comprises security-driven technological evolution, regulatory activity in harmonisation of proprietary eID systems and market activities that aim to add value through marrying eID systems to specific applications or infrastructure. This position may be interpreted as a "wait-and-see" position for the market players under the general uncertainty as a result of the lack of clear business models and of open standards as well as the ongoing and unresolved battle between security-driven and citizen-centric eID services. The lack of available data on successful cases only makes decision-taking more difficult, both for market players and for regulators.

Tomorrow's (~ 2015) activities comprise services developed on top of eID embedded in the available infrastructure – apparently the market stakeholders envisage that all possible architectures would be available and that the legal/regulatory framework would be changed so as to create the necessary trust for broad implementation – where the efforts of the market players tend to connect eID applications to extend the reach of the services on offer. This position may be interpreted as "feel the environment" when market players make use of the 'trusted' eID-enabled access but explore and test the applications since the market is not deemed mature yet. At this stage, there will be a degree of opening of government-related services to industry-managed and individual managed credentials, and an increasing degree of open co-ordination of commercial schemes.

Further developments (~ 2020) will completely hide eID requirements in terms of tools an technologies; these will be both embedded and bundled and, in essence, eID will become a service. Such identity-layer services will be, naturally or by intervention of he policy-maker, independent of the owner of the infrastructure (functional separation, as is the case with most physical network operations) and the emphasis will be in adding value to the services on offer. This will be so much so that the public sector may not only intermediate to safeguard sensitive personal data but also use them to offer rich content services, in a sheltered, regulated setting.

[106] Market stakeholders interviewed considered that a 10 year span is adequate for all these changes to occur.

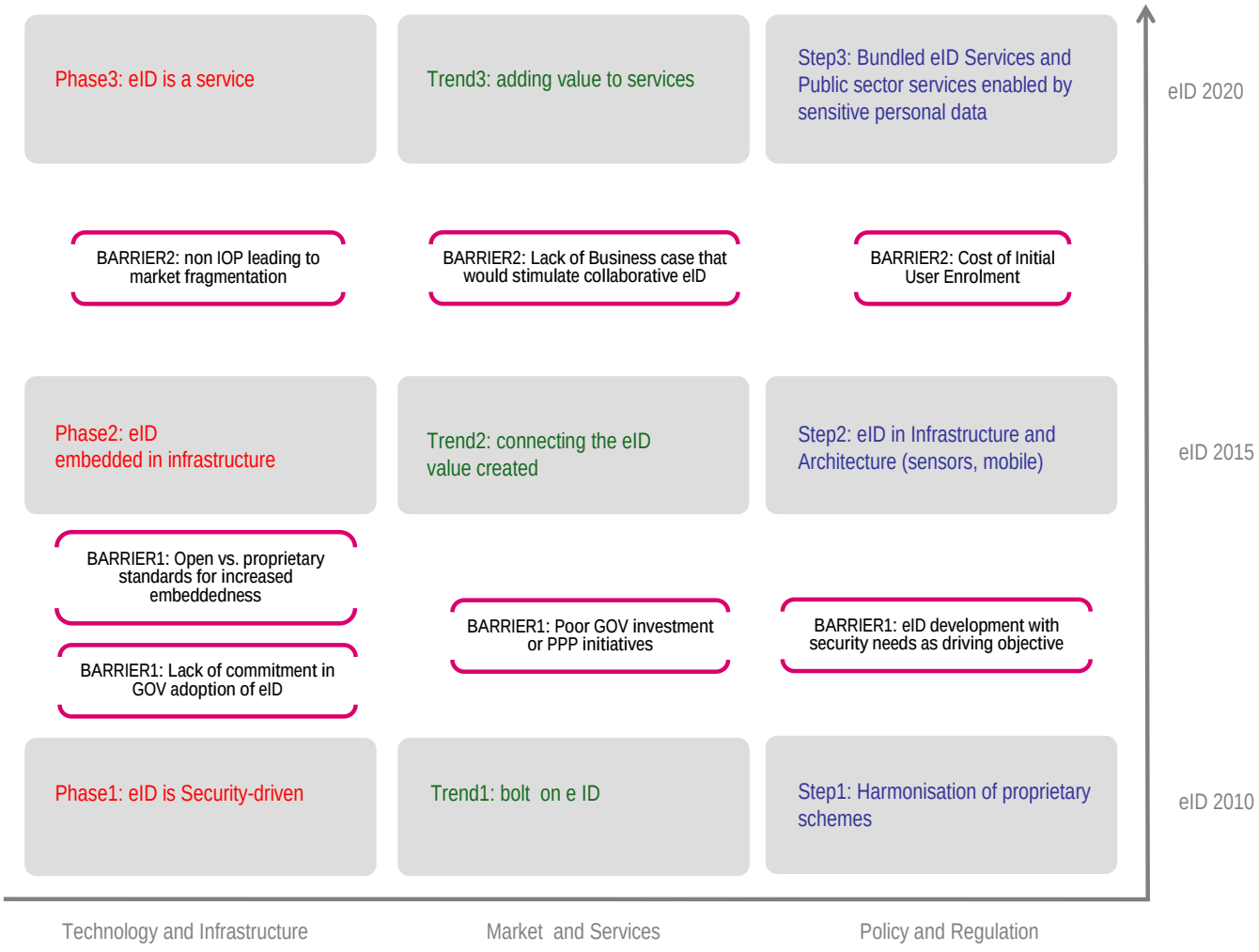
Figure 20: Road Map of eID evolution in Technological, Market and Policy areas



By then, the market would be sufficiently mature for eID to be considered as 'plumbing' by all stakeholders involved; eID-enabled access will be highly interoperable and sufficiently based on sufficiently open open-standards so as to support innovation and competition in added-value services.

In Figure 21, the gist of activities pertaining to each group is defined by a brief, descriptive title. Also represented in the same graph are the barriers to the development of the eID ecosystems which have been examined in the previous sections.

Figure 21: Road Map including Barriers



7 CONCLUSIONS AND RECOMMENDATIONS

Based on the analysis of the evolution foreseen in the Road Map, we draw a number of general conclusions:

1. The portability of credentials, both amongst and between public and business players, and the development of a wide choice of channels for delivering eID would facilitate the embedding of eID into the existing infrastructure.
2. Further development of biometrics would enable 3-factor authentication, which in turn could a) ease the evolution from security-driven to citizen-centric eID and b) enhance trust so as to facilitate the transition to eID as a service.
3. As market stakeholders are in stand-by mode in relation to what infrastructure eID would be embedded in, much more should be done to try-out federating processes and embedding eID into applications using open standards. More information on successful business cases should be circulated freely to enable the use of eID across contexts and public/private sectors.
4. While we cannot predict the future evolution towards an eID-enabled centrally overseen, public infrastructure and/or an affordable and trusted private sector eID-enabled, cloud infrastructure, the role of Government both as a legislator and as a promoter of open standards, (including its power as a first buyer of eID services), should be further explored.
5. Finally, in all circumstances, more needs to be done to promote the wider use of existing standards and to oversee the implementation of the embedding of eID in the infrastructure, as well as to offer a solution to the problem of user enrolment, currently a costly and safety-dependent procedure.

Drawing on the findings on the European eID market and innovation dynamics, a set of recommendations are presented below, that aim to promote the development of a mature, integrated EU27-wide eID ecosystem.

7.1 eID governance

Three main policy-related barriers are limiting the growth of the eID market. First, there is a lack of suitable standards for interoperable eID, meaning that personal identity data and electronic identities are unlikely to be technically usable. Even if these standards existed, it is unlikely they would be used in practice across borders. Second, as eID objectives vary between EU Member States, market development cannot be steered uniformly, thus potentially resulting in Member States policies and practices with conflicting aims. Third, there is hardly any trusted, consistent eID market data upon which governments can base their policy and organisations make decisions to invest in eID. Therefore, a coordinated pan-European approach to the development of a harmonious eID environment requires Member States and the European Commission to work together to

- ***raise consensus on standards:*** commit to consistent technology, application and policy approaches for government adoption of eID so as to promote interoperability across national boundaries and thus incentivise commercial investment in eID;
- ***harmonise objectives:*** raise consensus on shared objectives for eID schemes so that the systems delivered are not in fundamental conflict; in particular, national security should not be relied on as a key driver but treated as a secondary, measurable benefit. Relying mainly on national security generates fundamental design conflicts between schemes built around national security, and those built around citizen-centric services;
- ***collect, harmonise and make available information:*** develop and make publicly available authoritative data about eID markets to support commercial decision-making processes. This

could be accompanied by business case models to help justify investment and break down competitive barriers.

7.2 eID regulation layer

First, there are significant inequalities in regulatory approaches to eID across the EU27. Different countries apply different principles and methods in regulating their eID environment, making the business operating environment in the EU27 very varied. Often, this means it is difficult for companies to operate in multiple markets. Second, because of the current lack of a central authority in Europe for eID issues, there is no standard approach to matters such as cross-border use of identities, which hampers a more widespread adoption of eID services. Third, as there is a tendency towards proprietary, rather than interoperable national eID schemes, there is no commonly shared understanding of how national eID schemes should function. This also limits the possibilities of using national identities across national borders. Fourth, significant variations between eID standards in use across Europe mean that, even from a technological standpoint, the various eID solutions may not be compatible. For eID interoperability to succeed, regulatory bodies will need to provide a 'level playing field' across participating countries, and in particular prepare:

- ***regulatory parity:*** seek greater parity in the role, operation and powers of Data Protection Commissioners (or equivalent authorities) to supervise enforcement of eID;
- ***centralised leadership:*** establish a central European authority to manage interoperability, resolve disputes and enforce liability decisions between national ID schemes and, potentially, commercial schemes as well;
- ***interoperable government eID:*** European nations should prioritise greater interoperability of government-issued credentials, both inside and outside Europe;
- ***standardisation:*** work with relevant standards bodies to promote harmonisation of eID technology and infrastructure approaches.

7.3 eID technology layer

First, better end-user tokens that can handle multiple operating environments and use cases are needed. Currently, existing technologies may not be sufficiently versatile to support the variety of emerging eID services that may require particular, granular functionalities. Second, in order to improve credential portability, the ideal would be for consumers to be able to store their personal identity data in a device other than a smartcard. Third, there is a need for pervasive and portable biometric technologies to fight the growing risk of identity-related fraud.

Whilst there is no specific need for government intervention to develop new eID technologies, and citizens are not calling for greater use of biometrics at this time, certain technologies should be encouraged to promote eID growth, including:

- ***enhanced tokens:*** providing tokens that can consolidate multiple tokens and functions, or incorporate card reader/PIN technologies to promote use of dynamic passwords and two-factor authentication;
- ***certificate portability:*** allowing portable or multiple certificates so that they are not embedded solely in a smart card, but rather in the secure token of the user's choice;
- ***improved biometrics:*** enhanced biometric technologies that are portable and affordable would encourage widespread adoption of 3-factor authentication where needed and help to address phishing and impersonation attacks.

7.4 eID infrastructure layer

Governments can incentivise growth of eID usage by undertaking functions and supplying elements that are deemed too risky or costly for the private sector to develop (such as initial enrolment of individuals). thus preventing fragmentation of approaches. This would also provide an easy way for citizens to start using new eID based services in a variety of use cases. In this context, there is a need to incorporate eID technologies into other products and services so as to create a 'critical mass' of infrastructure based on the possibility of reaching a greater user base for a multiplicity of eID-enabled services.

In addition, the provision of and support for pervasive smartcard interface technologies could facilitate portable access to eID certificates across platforms and locations, ensuring enhanced access to credentials. There is also a need for greater use of federated database technologies to improve interoperability, as many eID developments tend to be limited in scope to a single country or an individual sector or application. Finally, there is a significant lack of trust between commercial eID initiatives, witness the existing wide variety of incompatible commercial solutions that enjoy only limited user trust.. The nurturing of an interoperable eID infrastructure which will in turn promote eID commercial exploitation can be achieved through:

- ***user enrolment :*** centralised or coordinated enrolment of users into authentication schemes would incentivise smaller innovative businesses to enter the market while ensuring credibility of eID credentials thus collected further, also along the value chain as fraud enters the system;
- ***embedding eID:*** governments may be able to accelerate eID development by incentivising key vendors to embed standardised eID mechanisms into their products;
- ***promoting federation:*** greater use of federated ID schemes across the private sector could be encouraged by governments if in turn public authorities would declare to be willing to use, trusted federated credentials.

7.5 eID exploitation / services layer

Actual public-sector eID schemes are quite inflexible and do not allow for new developments to emerge from outside the current paradigm. On the other hand, there is a requirement for open access to eID schemes by industry via open standards, and greater collaboration between public and private stakeholders. In view of these requirements and given the key position of governments to influence eID developments, a higher degree of cooperation between industry and government departments would be a positive development. Such cooperation could result in:

- ***innovative approaches:*** public authorities in particular should embrace innovative eID models that incorporate self-asserted credentials and volunteered personal information (VPI) models;
- ***open interfaces:*** government eID schemes should provide open access for industry to utilise public systems (with or without incurring licensing fees), and support that use by encouraging a range of Certification Authorities to grow around government schemes;
- ***public-private partnership:*** governments should work with commercial partners to ensure that objectives are pragmatic; that stakeholder needs are considered throughout development; and that the cost of the programme is proportionate to the value of the deliverables.

7.6 eID research

Finally, while the expectations of the eID market stakeholders we reported may never materialise, continued research of the European eID market and more reliable quantitative and qualitative information are needed, so as to be able to support evidence-based decision making. A first issue to consider is the availability of authoritative data on eID markets. During our research, interviewees

referred to analysts' reports on eID, indicating a preference for Gartner[107] and IDC[108] as the most credible sources. However, commercial organisations tend to rely on their own internal research and instincts – largely driven by customer opportunity – to inform their decision making. In some cases qualitative information is of greater value than quantitative information – vendors will consider the nature of a chain of trust to identify commercial opportunities. They may tend to privilege vendor-customer tactics and equilibria, rather that looking at general market welfare and, even less, social welfare. Legitimately, interviewees reported developing their own business cases for eID initiatives, rather than relying upon external information. In this light, there is a clear need for extensive, independent and authoritative data on eID markets, to be collected through a methodologically appropriate and transparent process, and made publicly available so as to support commercial and public decision-making processes. A final issue, in relation to the previous, is that of adequately publicising and diffusing the existing consensus on the state of the eID market. Public private collaboration and partnership, assisted by EU institutions, chiefly the European Commission, will be needed to develop measures to achieve this objective.

[107] http://www.gartner.com/
[108] http://www.idc.com/

European Commission

EUR 24567 **EN – Joint Research Centre – Institute for Prospective Technological Studies**

Title: The State of the Electronic Identity Market: technologies, stakeholders infrastructure, services and policies

Authors: Toby Stevens, John Elliott, Anssi Hoikkanen, Ioannis Maghiros, Wainer Lusoli

Luxembourg: Publications Office of the European Union2010
EUR – Scientific and Technical Research series – ISSN 1018-5593
ISBN 978-92-79-17206-9
doi:10.2791/4851

Abstract

Authenticating onto systems, connecting to mobile networks and providing identity data to access services is common ground for most EU citizens, however what is disruptive is that digital technologies fundamentally alter and upset the ways identity is managed, by people, companies and governments. Technological progress in cryptography, identity systems design, smart card design and mobile phone authentication have been developed as a convenient and reliable answer to the need for authentication. Yet, these advances are not sufficient to satisfy the needs across people's many spheres of activity: work, leisure, health, social activities nor have they been used to enable cross-border service implementation in the Single Digital Market, or to ensure trust in cross border eCommerce. The study findings assert that the potentially great added value of eID technologies in enabling the Digital Economy has not yet been fulfilled, and fresh efforts are needed to build identification and authentication systems that people can live with, trust and use. The study finds that usability, minimum disclosure and portability, essential features of future systems, are at the margin of the market and cross-country, cross-sector eID systems for business and public service are only in their infancy. This report joins up the dots, and provides significant exploratory evidence of the potential of eID for the Single Digital Market. A clear understanding of this market is crucial for policy action on identification and authentication, eSignature and interoperability.

The mission of the JRC is to provide customer-driven scientific and technical support for the conception, development, implementation and monitoring of EU policies. As a service of the European Commission, the JRC functions as a reference centre of science and technology for the Union. Close to the policy-making process, it serves the common interest of the Member States, while being independent of special interests, whether private or national.

JRC
EUROPEAN COMMISSION

LF-NA-24567-EN-N

ISBN 978-92-79-17206-9