Board Meeting

Coöperatieve Vereniging: International Post Corporation U.A.

Date: 19 November 2010

Time: 08.00 – 11.30

Venue: Brussels, Belgium

7b

Creating Intelligence – Digital Business

Digital Business: Opportunities for Value Creation

eID Services

Date: 15 October 2010

Summary

The growth of activity in the virtual economy is increasing demand for secure electronic identity in commercial and government relations. Enhanced identity and authentication services underpin security and confidence in digital business activities and provide the legal validity of digital transactions.

To date, electronic security has developed in 'islands' with individuals holding and operating multiple electronic identities on multiple platforms, typically using a range of security methodologies for different applications.

A number of companies and organisations, leveraging their role in business and society, have introduced certification services. These typically included Government departments, postal companies, telecommunication companies and banking organisations.

Common legal frameworks have been slower to develop which in turn, has hindered the development of certification recognition between different providers.

The general perception is that there are a variety of market pressures leading to a demand for common electronic identities recognised by Trusted Third Parties (TTP). These can be used for multiple applications and confer on the user legally compliant electronic signature capacity with added features of non repudiation and validation.

Overall, market up-take has been slow due to a variety of factors including access to technology, legal considerations, user immaturity, and insufficient numbers of web-based applications. The high level of investment required to develop these services has resulted in considerable restructuring of the certification sector, with services being closed and new joint-ventures created. In-source and out-source partnerships enhanced the overall certification value chain.

A decade ago there was significant postal investment in identification services and platforms. However while the technology proved robust, the market was not sufficiently mature and there followed a period of disinvestment.

General consensus among IPC members is that the market has now matured, driven by Government pressure to move citizen service delivery into digital channels and mailers looking to improve business process efficiency.

Posts are responding with identity business concepts which share the same principles but are developing distinctively different business models. It is an open issue as to the market-driven demand for international inter-operability in the identity services arena.

To prepare for demand, there is a need to define a process which creates a platform/service to create inter-operability from technical, operational, legal and commercial perspectives.

1. Developments in Electronic Identity Services

1.1. With the growth of content and services offered over digital infrastructures, digital identities are vital in the way internet services are provided between administrations, businesses and citizens alike. Secure online identity management and reliable authentication are the foundations of a networked economy of the future with electronic identity (eID) as the key enabler of and catalyst for these transformations.

1.2. Early developments in this area were primarily linked to user name and password solutions. While these solutions are easy to use, with low barriers to adoption, these do not provide sufficient levels

of security or confidence for more sensitive data and applications. The increasing number of applications transacted over the web is driving the demand for application independent and high security authentication.

1.3. Identity transactions conducted across a range of intermediaries are based on an increasing number and variety of identity systems. Internet, mobile or other electronic transactions are not based on a single, interoperable open-standard identity platform. Today, a wide range of sector-specific solutions (based on e.g. SSL encryption, PIN, tokens) and e-services (e.g. based on PKI infrastructure with either strong or weak authentication) is the norm. There is a trend from centrally-controlled systems towards more open identity infrastructures.

Different Electronic Identities

1.4. In an era of digitalisation, government administrations as well as as providers of internet services, ICT companies and identity assurance providers play a part in defining and controlling people's identities. These intermediaries provide the credentials, identification, authentication and authorisation necessary to ensure the access to public and private services.

1.5. Today's citizens often already dispose of a set of 'personal digital identities'. These range from given government-issued eID to user-selected enterprise IT system authentication, bank identification, and internet identity systems that have evolved in parallel and in isolation. These identities are often complementary and overlapping to some degree, but as these are not interoperable and built to meet different needs, they are normally not trusted across sectors or national borders.

1.6. With the growth of social digital networks, a newer type of identity is emerging, 'ambient identity'. This concept describes the fact that increasingly, the level of data capture in sites and search engines creates an electronic trail, which can be used to identify individuals. With the use of IP addresses and geo-location software, individuals can be identified, often unknowingly. 'Ambient identity' expands and blurs the definition of electronic identity as defined today.

Different Levels of Security

1.7. The market for identification services has grown dramatically through the last decade both in terms of technology solutions available and the number of applications requiring high confidence authentication solutions.

1.8. With the global, but somewhat insecure Internet being the primary carrier of electronic commerce transactions, security is a concern for consumers as well as internet merchants. Web sites can be counterfeited, identities can be forged, and the nature of transactions can be altered.

1.9. A series of mechanisms are needed to make business transactions 'secure', including non-repudiation, authentication, integrity, and confidentiality:

- Non-repudiation assures that the parties in a transaction cannot deny it after the fact.
- Authentication refers to the ability to verify the identity of parties involved in transactions
- Integrity guarantees that the data transferred has not been modified in transit or in storage.
- Confidentiality ensures that when parties transmit a business contract over the Internet, no one else but the intended business partner can read it.

1.10. All of these requirements can be met by the use of encryption and digital signatures, -. Digital security must also provide an easy and safe process for revoking and renewing digital identities in case of identity loss or theft.

Different Electronic Identity Solutions

1.11. The banking sector, supported by private sector technology and service companies, has led the development of a variety of solutions are available today:

a) Transparent Solutions

- Digital Certificates based on x 509 standards and issued according to in-house certification rules. These can include soft and hard certificates using both smart card and USB token technology.
- IP geo-locator authentication based on location divergence profiles which create profiles of users.
- Device authentication based on device registration and challenge.

b) Physical Solutions

- One time pass tokens generators are used to create one time 8 digit codes (banking sector)
- Grid authentication co-ordinates
- One time past lists

c) Non- Physical Solutions

- Knowledge based
- Out of bounds identities sent to other media
- Soft tokens

d) Mutual Solutions

- Enhancement around SSL certificates using a variety of replay and locator identifiers

1.12. Different solutions emerged to address the need for enhanced authentication, identity, and security, based on Personal Key Identifier (PKI) technologies and X500 standards. The fundamental logic of the Personal Key Identifier (PKI) model is that a Trusted Third Party (TTP) authenticates an individual and provides them with an electronic identity. This electronic identity is used as a log–on identifier to multiple applications provided by many organisations which recognise the certificate. The certificate can be supported by a number of additional services such as time stamping and a digital signature.

1.13. Historically, posts have been active in this market, leveraging their trusted postal brand to create the basis for secure transactional, messaging and payment services. However, early innovators (Deutsche Post DHL, Posten AB, Royal Mail Group Plc and TPG (TNT)) undertook significant disinvestment as market estimates failed to meet revenue expectations. Today, there is a renewed interest in developing and implementing variants of these original services.

2. Current Market Trends and Stimuli

2.1. Technology networks, solutions and legal environments have matured. There is a belief that customer demand is now evolving and that the market will grow as electronic messaging begins to handle more sensitive transactions and information. There are a number of socio-technical trends which support the development of PKI based multi–application certificates.

Consumer Pull

2.2. Consumer resistance to multiple log-on and authentication procedures drives the potential latent demand for multi–application certificates.

Market growth and maturity

- Increased drive to grow e-Government services (e.g. e-Health, taxation, licensees and contracts, payments).
- Increased development for web-based hosted applications as well as networked and virtual organisations. Authentication of users and management of the different rights and access are critical to these business models.
- Increased trust in E- banking and online payment supporting the growth of online transaction services

Growth in E-Commerce

2.3. The availability of mutual authentication processes and trusted payments services drive growth in C2C activities (eBay), SME e-commerce and facilitate cross-border e-commerce

Explosion of Social Media

2.4. The massive adoption of social networks is changing the concepts of digital identities and may change the way digital identifiers develop into the future

eGovernment Policy and Initiatives

2.5. A key market driver for the development of electronic identities has been the development and implementation of e-Government services in many countries across the world. The ability to transact and share information digitally in a secure and confidential way with identified citizens and businesses is critical to the success of these new services.

2.6. While many governments have been implementing eGovernment services to address their local, regional and national administrative and information needs, the European Union has been working on the development of electronic identities and addressing issues of inter-operability between systems and countries over the past ten years.

2.7. i2010 Action Plan is the key pillar of EU strategy at achieving inclusive eGovernment, facilitating European public administrations to deliver public information and services in ways that are more easily accessible and increasingly trusted by the public. It emphasises interoperable electronic identification management (eIDM) for access to public services, electronic document authentication and electronic archiving. i2010 action points include: e-signatures; technologies for eIDM processes; a programme on cooperation on management, authentication and cross-border access to electronic records and archives in public administrations; and interoperability.

2.8. One of the priorities of the plan is the widespread adoption of electronic procurement by administrations: with cross-border e-procurement chosen as the first application.

2.9. While EU- initiated projects have successfully launched electronic services which aim to delivery efficient and cost-effective services, internal evaluation studies have noted that business and citizens' needs are 'indirectly' addressed. Greater emphasis on user-focussed development strategies in developing structures and services will deliver greater usage and adoption by businesses and citizens alike.

2.10. Initiatives linked to electronic identity and interoperability are not limited to Europe. Regular sharing of best practice sessions among governments from the EU, Japan and the US have been facilitated by the EU.

2.11. The electronic personal identity market will not be a monopoly and Government applications are likely to recognise certificates from multiple identification providers, as long as these conform to the desired authentication procedures.

Understanding Consumer and Business needs in eID services

2.12. A recent report prepared by Rand 'Study on eGovernment scenarios for 2020 and preparation of 2015 Action' (30 June 1010) provides insights in the current and future needs for e-Government services among citizens, business in a range of EU countries.

2.13. A multi-phase study was conducted in February and March 2010 in six countries (Austria, Germany, the Netherlands, Poland, Spain and the UK) among representative samples of citizens and businesses. A total of 7287 interviews were conducted: 6070 with online citizens, 300 with offline citizens and 917 with medium to large sized private companies with an annual turnover of 10 million Euros or less operating nationally.

2.14. Respondents were asked to rate on a scale of 1 to 10, their preferences for a range of pan-European services. A ranking of results provides a view on the value of potential services to be developed. Results in the table below indicate similar values of services for both citizens and businesses.

2.15. The top two most valued potential cross-country digital services for both citizens and businesses are a secure email access for all communication, followed by a European electronic identity card. Citizens third most valued eGovernment service is an online registry of job vacancies, whereas business would value a European standard for digital signatures.

Pan-European services preferences	Businesses	Citizens
Secure email channel for all formal communication	2	1
EU standard for digital signatures	1	3
EU electronic identity card	3	2
EU wide electronic platform for public procurement	4	Na
EU registry of available jobs and job seekers	5	4
EU index of health care providers	6	5
Services supporting portability of pensions etc	Na	6
eVoting, ePolling and participation services	Na	7
EU electronic patient record	7	8
Pan-European emergency services	Na	9
Online registration of EU wide work permits	Na	10
EU land and real estate registry	8	11

2.16. The most valued services reinforce trust and security. There are uncertainties linked to the level of trust people have in digital systems, and their willingness to adopt digital services. It is important for users to know that their personal information is kept securely and is not used for purposes other than those for which they were initially meant for. From a commercial perspective, many service providers with an extensive customer base who have invested in the required infrastructure to offer digital services, are looking for cheap access to as much information about their consumers. This raises issues of data protection, privacy, 'ambient identity' which need to be assessed and reviewed in terms of legislation

2.17. Overall, the results from the research indicate that citizens and companies seem, willing to interact with their governments over the Internet, and willing to do so more in the future. Barriers such as costs and concerns about use of personal data exist but in general people are open to overcome those, when benefits are clearly communicated to them.

2.18. A balance between the convenience to the end users and security in terms of electronic identity needs to be achieved. Currently, the general consensus is that it is unlikely that end users would be willing to pay a premium for security.

Role of Legislation

2.19. The development of eID services are intertwined with the development of data protection and privacy laws. Data protection and privacy guidelines need to address the extension of identity by digital means, the increasing number of players holding these identities, the multiplication of identifiers and the type of identifiers. Current legislation was designed to regulate static information and these may need to be reviewed when applied to the more dynamic nature of digital identities.

2.20. The European regulatory framework for electronic communications includes security-related provisions. In particular, the Directive on Privacy and Electronic Communications contains an obligation for providers of publicly available electronic communications services to safeguard the security of their services. Provisions against spam and spyware[5] are also laid down.

2.21. In order to be able to go one step beyond: i.e. electronic exchange of relevant and correct information between authorised authorities, legal barriers and semantic barriers need to be overcome An example of such a legal barrier is the usage of national identity numbers, cross border. DIGID, the Dutch citizen's electronic identification system, is based on the national identity number. As this number represents the identity of the citizen, it is well protected: it is illegal to use it for other services than government services, and only for people who are registered inhabitants of the Netherlands. Whereas the number is now in use for identification for multiple services, like student allowances, it cannot be used by Dutch students who do not officially live in the Netherlands. In other countries, such as Germany, the current legal framework does not allow the transfer of identities between applications.

3. Postal Value Propositions and Business Drivers

3.1. The technological infrastructure, legal framework and implementation of eID is a reality today, used and adopted to varying degrees by administration and businesses. The predicted growth in electronic identity services will be primarily driven by trust-in and ease of use for citizens. Their needs in terms of service applications, including mobile access, are changing and subject to continued research. It is certain however, that there is the political and business will to move into the digital space and this will require authenticated electronic identities.

3.2. Posts have key assets which can be leveraged in the electronic identity market:

- Trusted brands and reputations
- Existing intermediary role in commerce, communication and payments
- Retail networks facilitate registration function
- Relationships with Government
- Potential to bundle identity with digital mail application

3.3. The factors behind the limited success of early forays in electronic identity services by postal companies relate to issues of technology, market entry strategies and process, at a time of a developing and fast changing digital environment. Over the last decade, there is an increasing acceptance of the benefits of digital transactions and therefore it is relevant for posts to review these markets again.

3.4. Market opportunities for a postal personal electronic identity are primarily country specific. In some countries (e.g. Sweden) the space is already occupied by the development of multi-use bank identities. E-Government policies and the implementation of an active communication portal with citizens (e.g. Government Gateway in the UK) are key in shaping the general acceptance and adoption of identity certificates from postal organisations.

3.5. Interviews with IPC members identified a range of services which could use a postal digital identity:

- Secure electronic messaging (e.g. eBoxes)
- Electronic bill payment and presentation
- Electronic identity and identity cards
- Basis for e-Government services
- Distribution of social benefits payments to citizens
- Logistics, tracking and tracing
- Be the underlying Certification Authority for private Certification Authority domains

3.6. Posts, as providers of secure transaction and identity services in the physical world, have the opportunity to position their organisation as a natural Trusted Third Party. This creates the space for posts to leverage their intermediary or mutuality role and become certification authorities in digital identity services, controlling policies and processes.

	Experience	Key Lessons
CA PROVIDER	• CA provider has to have credibility in market • CA polices have to balance liability usability and value • Joint ventures reduce costs and increase value	• Posts, Telecoms and Banks are often seen as TTPs • Government seek provider rather than be TTP • Best practice polices now available • Joint venturing growing
CA PRODUCTION	• Complex to establish • Deviation from standards expensive • Economies of scale critical	• Seek established CA technology partner to provide core production • Ensure data centre competences • Develop Outsource –Insource migration to follow volumes
CA REGISTERING	• Balance integrity with usability • Overly complex registration slows down use • Leverage existing assets	• Design user friendly procedures • Explore distributed trust model • Seek registration partners
CA CERTIFICATES	• Hard certificates were to complex • Soft Certificates became norm key • Issue different classes of certificates with different level of authenticity	• Fit certificate policy and technology delivery to establish utilisation in the local market • Ensure that certificate standards meet local law and are compliant with international directives
APPLICATIONS	• Failure has often been linked to no joint launch of applications • Applications will drive revenue	• Service needs to have applications when launched e.g banking, government, secure messaging ,notary, identity management • Recognise the need for mutual cross recognition and that government is unlikely to have a monopoly provider of CA services
PRIVATE CAs	• Closed user group CA have been major growth market with CA technology being used for corporate identification and access and permissi0n services	• Establish potential for this market • Develop interoperability rules between private hierarchy certificates and public certificates • Also recognise the value of the SSL market and provision of non PKI based authentication routes

4. Certification Value Chain

4.1. In the online environment, identities can be forged much more easily than in the physical world. Authenticating the content creators therefore becomes a paramount concern for business transactions. Certification authorities (CA) have emerged to provide this type of services. Major players include VeriSign, GTE CyberTrust, and IBM VaultRegistry.

4.2. Certification organisations authenticate the identity of each trading party in a transaction by issuing digital certificates based on public key cryptography and digital signatures. Security concerns such as confidentiality, message integrity, and user authentication are addressed by using digital certificates in business transactions. The benefit for a small business to carry a digital certificate is to increase consumer confidence that they are dealing with a business entity that has been authenticated.

4.3. Posts can take multiple positions in the certification services value chain. Today, the majority of Posts who are currently offering full Certification Authority (CA) services do so in joint ventures.

Postal Role	Registration Authority	Certificate Authority	Certificate Production	Comments
Basic	X			• Posts simply act as the registration authority on behalf of one or more companies offering CA services • Posts are only liable for the accuracy of the authentication process • Revenue is limited to a transaction fee for processing the authentication • The resulting certificate may be accepted by the Post to be used in own applications (e.g. e-Box services) • There are opportunities for co-branding and white labelling in this positioning
Service Lead	X	X		• Posts are the Certificate Authority responsible for issuing and managing the certificates and certificate polices over it life cycle, and ensuring compliance with legal requirements. • Registration is carried out at postal counters but certificate authorities (posts) could also leverage trust hierarchies, other agents and online functions to manage registrations • The certificates open postal applications, digital communications and other commercial services. Posts can act as the Trusted Third Party (TTP) for other applications most notably e- Government services. • Revenue accrues from the fee for providing the certificate as well as any related services linked to the certificate. Pricing is determined by market norms and strategic decisions. If linked to e-Box authentication, certificates are usually free to end users. • However the actual technical production of the certificates is outsourced to a certificate provider, managed through contracts, SLA agreements and auditing.
Full	X	X	X	• As above however, Posts in-source the production operations and have direct control of all aspects of the value chain. • These operations increasingly build on standard technology modules from leading specialist software providers.

5. Development of eID Models among IPC members

5.1. Five IPC members (bpost, Norway Post, Swiss Post, Poste Italiane and P&T Luxembourg) currently offer full Certification Authority services. A further two members (CTT Correios de Portugal and Deutsche Post DHL) provide receivers with a full authenticated electronic certificate as part of the registration process for digital mail services. The challenge for these posts is to grow the acceptance of the postal certificates in other applications.

5.2. The area of electronic identity services is currently being explored by a further five members.

Post	CA	Face to face registration for eBox	Comment
An Post			Exploring related to digital mail
Australia Post			
Canada Post			Exploring related to digital mail
Correos y Telegrafos			

CTT de Portugal			• De-facto certificate with eBox
Cyprus Post			
Bpost			
Deutsche Post DHL			• Exited CA • De-facto certificate with eBox
Hellenic Post ELTA			
Iceland Post			
Itella			• Exited CA • Acceptance of other certificates
Magyar Posta			
New Zealand Post			• Exploring related to digital mail
Norway Post			
Österreichische Post			
Poste Italiane			• De-facto certificate with eBox
P & T Luxembourg			• Shareholder in Luxtrust
Posten Norden			• Exited CA • Acceptance of other certificates
Royal Mail Group		Exploring related to digital mail	• Exited CA business
Swiss Post			
TNT		Exploring related to digital mail	• Exited service • Exploring
USPS			

6. Future eID Business Drivers

Vision 2020 – European Union Developments

6.1. ELSA (European Large Scale bridging Action) for electronic identity is an EU strategic initiative to achieve long-term objectives set for eID in Europe. Stakeholder involvement is facilitated by a Thematic Network which engages public and private entities in order to collaborate in the preparation for the deployment of the eID management infrastructure.

6.2. The new 2015 action plan will be an evolution from the previous phases of work rather than a radically new approach to eGovernment policy at EU level with a focus continued focus on electronic identity with a view on addressing longer term needs rather than immediate operational demands. The mid-term vision has been stated as:

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

6.3. The following objectives have been identified and will be refined for attainment by 2015.

- Establish personal identity frameworks that allow citizens to be in control of their
- digital selves and their personal data, respecting data protection requirements in a way that
- respects cultural differences.
- Develop electronic identity which is available to all citizens and provides consistent user experiences.
- Citizen's national eID should work seamlessly across sectors and borders
- Establish a communications and promotional actions to increase the understanding of the benefits among the general public of eID benefits and risks.
- Establish a Europe-wide architecture and model that meets the needs of citizens, business and administrations. The architecture should encompass the current range of approaches to eID, and that anticipates emerging approaches to eID to the greatest extent possible, offering interoperability at technical, semantic and organisational levels.
- Established world-class European knowledge and skills in eID management ecosystem (technology, business models, cost benefit analysis) and gain leadership position on the global eID scene.
- Adopt a proactive eID governance at country and European level based on cooperation, exchange of and promotion of best practice solutions.
- Develop a regulatory/governance framework for eID at European level to guide and facilitate
- eIDM in public and private sectors, including data protection aspects.
- Meet the needs of non-citizens residents inside the EU, as well as the needs of businesses and
- citizens who interact with extra-EU entities, must both be taken into consideration.

6.4. The European commission is supporting this new framework through research, testing, and deployment of projects. Results are expected by 2014 and significant budgets (300-400 million EUR) have been committed to achieving these goals, in collaboration with the Member States and including via partnerships with the private sector.

6.5. Despite a strong vision and sustained investment in further development and implementation of cross-border digital identities, the ELSA Thematic Working Group Report on Electronic Identity Management Infrastructure (January 2010) documented key barriers which will need to be addressed in order to stimulate widespread uptake of electronic identities. Although these have been identified for Europe, these factors apply to varying degrees, in all countries and as such provide a direction in achieving interoperability.

Technological barriers:

- Lack of interoperability at the technical, semantic, organizational and legal levels
- Complex and fragmented standards landscape
- New challenges related to scalability, connectivity and bandwidth
- Lack of bullet-proof reliability and redundancy
- Lack of framework to provide expected (and uniform) levels of security and privacy protection
- Manage the complexity of multiple electronic identities
- Lack of harmonized eID middleware implementations in existing operating systems distributed by major vendors
- Lack of services architecture and meta-model capable of accommodating different channels and eID types/sources, and covering public/private sector, etc.

Societal barriers

- Lack of citizen trust in areas of privacy: loss of anonymity, persistence of activity traces
- Lack of citizen capabilities to effectively use and protect their electronic identities
- Lack of ease of use of eID
- Lack of citizen awareness of benefits of the use of eID including a lack of understanding/appreciation of the *role* of eID, i.e. the value and place of anonymous/pseudonymous communications.
- Cultural Resistance to the use of eID in some regions and for some types of activities

Economic barriers

- Need for large up-front investments in leading edge technologies
- Need for significant investments to meet new legal obligations
- The cost for businesses to setup or migrate to use of eID in their standard
- business activities
- Potentially high (prohibitive) transaction costs in some cases

Legal barriers

- Lack of framework for assessing liability in cases of misuse (fraud, theft, etc.) of eID
- Lack of legal framework addressing the multitude of sources of eID (issuers, verifiers, etc.), how they are to be used, etc.
- Instability in transaction cost structure in the short- and medium-terms leading to uncertainty
- Limitations on re-use of nationally issued eID's in some countries/jurisdictions
- Lack of uniformity in MS Data Protection expectations and policies, perhaps even incompatibilities
- Lack of information on the differences between national laws on personal data protection, especially for users
- Lack of information on the proof requirements for electronic signing in a member state other than one's own

Political barriers

- Difficulties arising from the presence of certain administrative boundaries
- Need for high levels of cooperation between various public administrations, and even private operators when things go wrong with eID (identity theft, infrastructure problems, etc.)

Conceptual barriers

- Lack of a common societal view on the concept of electronic identity,
- including ownership of attributes
- Lack of a common long-term vision on eID
- User interface issues: lack of a uniform and simple-enough interaction paradigm
- The 'Not Invented Here' syndrome, wherein interesting and/or useful approaches, tools, practices, etc., are rejected, to the detriment of the overall objectives, due solely to their origin

Organisational barriers

- Lack of appropriate public/private collaboration structures involving all relevant stakeholders
- Digitally agnostic persons, citizens without access to technology
- Lack of complete, clear set of scenarios to be supported by the eID infrastructure
- Lack of an EU-wide eID infrastructure capable of supporting all of the above
- Lack of global governance on eID issues
- Rollout challenge due to scale

6.6. The future challenge will be in creating a model of eID Management which has real business appeal and meets the needs of both end users and service providers.

Development of Postal Electronic Identity Services

6.7. There are currently no common business models or monetization strategies in services linked to electronic identity among postal organisations. Implementation models include stand alone authentication services as well as authentication services embed in digital mail applications (e.g. eBoxes). .

6.8. A review of postal experiences undertaken by IPC identifies clear market development strategies. Posts need to:

- Identify relevant partnerships opportunities so as to reduce investment costs and build credibility in the digital security space
- Leverage standard solutions and source technology from leading player (e.g. VeriSign. Entrust, etc)
- Seek to develop Certification Authority operations with strong local partner (e.g. telecoms, banks, clearing houses)
- Ensure certificate interoperability with key market players
- Support both public and private domains
- Recognise importance of providing hard and soft certificates
- Create useable and pragmatic registration policies
- Ensure that identity and authentication services are linked to business applications
- Recognise related market opportunities to lever trusted brand status in other identity markets (e.g. SSL certificates)

6.9. The postal services currently being developed based on identification and digital mail are primarily domestic in orientation. These provide access and authorisation to e-Government services and transactional mail applications to large postal customers.

6.10. However, there is an interest among IPC members to explore how these domestic systems could become interoperable in order to support the growth of international flows of authenticated digital mail, cross-border commercial services including e-commerce and to support an increasingly mobile population requiring access to government services in several countries.

6.11. The need and market potential for cross-border personal digital identity services is a yet not quantified. Three fundamental questions require further investigation prior to undertaking cross-border interoperability between domestic systems:

- Can posts accommodate international inter-operability without diluting the closed user authentication value proposition in their domestic markets?
- Will the level of legislative co-operation between governments grow to create sufficient demand from potential users?
- Is there a way to effectively monetize the demand from digital service providers?
- Can posts work with EU to meet the needs of the community in terms of cross-border identity services?

7. Consultation Process

7.1. Having identified eID services as potential area for international postal innovation and collaboration (Expert Meeting – June 28 2010) and to further explore the potential of developing interconnectivity between the different models of eID services among its members, IPC undertook a detailed consultation process in order to assess value and need. The following activities were undertaken:

July – August 2010: Benchmarking postal eBox and Secure Identity developments

7.2. This information collection exercise was conducted in conjunction with Adrian King from Strategia and involved individual interviews with experts in digital services among ten IPC members.

September 2010: Establishing a framework for evaluating the value to Posts, customers and end-consumers in facilitating international eBox and secure identity services

7.3. This framework was reviewed and approved by participating Posts. The analysis included a range of roles for IPC in bringing value to members in this area.

24 September 2010: Digital Services Workshop

7.4. This one day workshop centred around reaching consensus on the value of establishing international e-Box and Secure Identity services and the different roles for IPC in supporting members achieve these goals.

7.5. These additional activities requested by the IPC Board were funded from a central budget 'Innovating for Profit'.

8. Outcomes from Consultation Process

8.1. In its capacity as intelligence provider to the postal industry, IPC published in October 2010, a series of documents relating to Digital Services, which are available to all members at www.ipc.be

- Developments in Postal Digital Services: A Review of Business Innovation in e-Services
- IPC e-Box Concepts and Market Developments
- IPC e-Identity Concepts and Market Developments
- Value of International e-Services and Potential Roles for IPC

9. Need and Value of International Interconnectivity

9.1. IPC members participating in the consultation process identified the need for assessing the potential for inter-operability between electronic identity services offered by posts. There is a clear understanding that inter-operability and leveraging commonalities, including defining acceptable minimum international technical standards, is a pre-requisite for any future developments in this area.

9.2. An initial step would be to conduct a detailed mapping of how inter-operability could be achieved on a technical and operational level. A decision for progressing to implementing cross-authentication of digital certificates would be made to the IPC Board.

10. Certification Authority Services and Inter-Operability

10.1. There are a series of technical issues which need to be assessed, understood and resolved to achieve international inter-operability of certificates.

Directory Issues	• Developing inter-operability between directory services and between individual postal CAs
Certificates and Certificate Policy	• Ensuring that there is a common set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements • Instrumental in forming the basis of inter-operability between two or more PKI domains
Levels 1-3 Consistent Definition	• Ensuring that a common set of rules and definitions exist
Naming Conventions	• Need to agree a set of conventions to cover naming issues that may arise in cross-certification
Boundary and Range Issues	• Ensuring that one CA can recognise certificate serial numbers, names and paths of certificates issued by another CA
Failure Procedures	• Development of a standard set of procedures that are initiated in a case of compromise to the system
Authentication	• Authentication is the process by which the electronic identity of a client is asserted to, and validated by, an information system for a specific occasion using a credential issued following a registration process. • Need to ensure that common processes are adhered to by postal CAs
Registration	• Registration is the process by which a client gains a credential such as a digital certificate for subsequent authentication. Registration can be associated with a real-world identity or can be anonymous or pseudonymous. • Need to ensure that common processes are adhered to by postal CAs
Physical Issuing	• Set of procedures to ensure that the certificate is not compromised at any stage between production and distribution to the end-user
Revocation	• A CA maintains a list of certificates that have been withdrawn prior to their normal expiry date (certificate revocation list). Certificates presented by a relying party are checked against this list to ensure that they are valid. • Need to ensure that common rules around certificate revocation are in place

10.2. The mapping exercise would identify similarities and differences between systems, establish how these could be resolved and further explore the potential for cross-border business applications. IPC could support its members achieve commercial and technical interoperability through either a mutual cross certification scheme or a bridge certification authority function.

10.3. The value to IPC members in understanding and documenting the technical and operational issues in achieving inter-operability of digital certificates has key implications for the future positioning of posts in the digital world

- Participating in the development of a key enabler to the future digital economy
- Leveraging postal values of trust and confidentiality in the digital world
- Harnessing postal relationships with administrations and businesses as a credible partner in facilitating digital information exchange and transactions
- Creating the basis for an infrastructure which accommodates international dimensions and therefore can meet these needs as they arise.

10.4. The use of ICT and networks is approaching new maturity levels, world-wide. Technical issues such as the ability to exchange data between systems and/or applications that held developments back in the past are becoming less relevant as issues of inter-operability are addressed. The ground for offering public e-services is becoming more fertile, and organisations such as posts need to align themselves to participate in these developments.

11. Future Activities for IPC in 2011

11.1. IPC proposes to conduct an inter-operability mapping exercise identified in the consultation process in early 2011. The timing of this information gathering exercise is critical in order to understand the ability of postal operators to play a role in the eID Management systems envisioned at European and global level.

11.2. In response to the member needs identified in the consultation process, IPC will continue its information support with regard to digital services in general, as well as with a specific focus on the development of electronic services linked to eID services.

12. Resources required from IPC

12.1. IPC will identify, in conjunction with interested members, specialist partners or contractors in order to access the required expertise. IPC will provide the project management resource to define, manage and deliver the report.

13. Budget

13.1. No additional funding - to be reviewed with IPC members at the SEF on Postal Electronic Products in March 2011 to determine whether members wish to pursue this.

14. Risks of not taking action

14.1. Today, there is high pressure on governments to focus on priorities other than ‘getting organised’ and therefore eGovernment Services are likely to move to a lower priority as they currently apply only to a small proportion of citizens. Decreasing budgets would make it more difficult to support the development of digital services today, although payback of those investments over time is expected.

14.2. New digital services or public e-services are now offered by parties that are not necessarily close to government and therefore may not meet national interests. Without a level of centralised direction, this may lead to further fragmentation of eID services, increasing the complexity of communicating and doing business in the future.