Electronic Identities – a brief introduction[1]

[1] This document is intended purely as a discussion paper exclusively for the internal, non-public use of the recipients. Although every effort has been made to ensure the accuracy and relevance of the contents, they do not in any way represent the official position or policy of the European Commission

Table of Contents

1. **DEFINITION AND CONTEXT** 3
2. **GENERAL AMBITION** 3
3. **ELECTRONIC IDENTITIES VS. NATIONAL ID CARDS VS. BIOMETRICS** 3
4. **MAIN BENEFITS** 4
5. **ISSUES** 5

1. DEFINITION AND CONTEXT

In a generic way, an "Electronic identity" is a means for people to prove electronically that they are who they say they are and thus gain access to services. The identity allows an entity (citizen, business, administration) to be distinguished from any other.

Citizens, businesses and administrations face common problems regarding their electronic presence:

- They all need to have an electronic presence, protected from abuse and misuse, confirming unequivocally who they are in electronic transactions. Their electronic identity should also be able to take different forms according to the citizens' wishes. In certain circumstances (see **Error! Reference source not found.**), a person might wish to present himself as the CEO of a company and in a separate context as the beneficiary of a health insurance.

- They all need to have available descriptions of themselves. Whether it is a citizen filling in an online administrative form, a business offering a service or preparing a tender, or an administration wishing to share information, they should all be able to dispense with the time-wasting and cost involved in forever answering the same questions in ever more forms; it is also advisable that the corresponding data be trusted and considered as authentic.

2. GENERAL AMBITION

The ability to link a set of information to a user (citizen, business, administration) and the effective and secure handling of user-related data are essential to numerous different interactions. To this end, organisational and technical infrastructures are developed to define, designate and administer the identity related to specific groups of people, such as customers, patients or citizens. These infrastructures are identity management systems.

In all EU Member States several initiatives are underway to introduce electronic identities (eID) for public services. At EU level, the current ambition is that any European citizen should be able to cross European borders and access local services as seamlessly as access local voice services via their mobile phones. In practice, there is a need for an interoperability framework to address eID requirements at an EU level and which is reflected in the eGovernment action plan, adopted by the European Commission on 25 April 2006. The following commitment was made to this end:

> *The Commission, in cooperation with the Member States, will pursue policies to grant safe access to services EU wide. When citizens travel or when they move they want easy access to services. EU governments have agreed to facilitate this process by establishing secure systems for mutual recognition of national electronic identities for public administration web-sites and services. The Action Plan foresees a full implementation by 2010. The Commission will help make this happen by supporting wide-scale cross-border demonstrators, identifying common specifications for electronic ID management during 2007 and by reviewing the rules of electronic signatures in 2009.*

Multiple e-Government application areas are strong candidates for integration into a European wide e-Government services framework and require therefore interoperability of the identity mechanisms on a cross border basis: Identity card schemes, Government procurement, Social security, Pensions, Health, Companies registration, Certificates and licences (Drivers and vehicles), Taxation (VAT) …

3. ELECTRONIC IDENTITIES VS. NATIONAL ID CARDS VS. BIOMETRICS

An electronic identity (eID) is distinct from a digital identity card even if in some cases, the two concepts could converge. An electronic identity is a means for people to prove electronically that they are who they say they are and thus gain access to a panel of services. From an electronic identity perspective, one person is usually involved in multiple sectors (e.g. taxation, social security, education, telephony services,

banking services) and also often fulfils different roles (e.g. a civil servant, a lawyer or a father) depending of the context. Therefore, the corresponding data should be managed/accessed in an independent way. Dealing with this content-rich electronic identity will require adequate legal provisions in terms of data-protection and personal control over personal data by the individual.

National identity cards (current or proposed) and passports are primarily issued by member states in order to address a specific sector: the necessity to have travel documents. The authorities retain control over its usage. For such specific usage, a digital identity card is a natural replacement. The digital identity card is a physical token containing personal information used for proving that the holder is a specific person, a citizen of a given country.

Depending on the type of use, an electronic identity does not necessarily imply the use of a physical item such as a smart card or a USB token (e.g. an identifier in a population register might be sufficient). Additionally a person's identity exceeds the duration of a specific physical item: while an electronic identity card has an expiration date, the identity of a natural person does not expire. Conversely, a digital identity card can be considered a one potential physical container, among others (USB stick, mobile phone, bank card…), to deliver an electronic identity. Beyond the sectoral use as travel document, the digital identity card can also be used as container for additional sector-specific identities (e.g. social security). Combined implementations of the electronic identity and the digital identity card can be beneficial, but it is a matter for Member States to decide if and how they may be related and/or bound to each other.

Biometrics is referred to as a number of methods to prove that persons are who they say they are using their physical features (such as photo, fingerprints, hands scans, eye patterns, ear patterns…) or behaviour (such as voice recognition, signatures…). Several countries are currently implementing passports and electronic identity cards including biometric information for proving that the holder is a specific person.

4. MAIN BENEFITS

By 2010, citizens, business and administrations should benefit from an online presence that they can trust: i.e. secure, authentic, reliable and durable. The deployment of a cross-border electronic identity management will make available a foundation on top of which transactional online public services can be built. Examples of this are online tax declarations, social security or e-procurement.

From an Administration / Business standpoint, the main drivers for a pan European interoperable eID can be summarized as:

- ***Supporting e-services.***

An interoperable electronic identity is an ideal access tool for all kinds of e-services of any Government. They open the doors for customized service-delivery both in the public and in the private domain. Examples are dedicated access to government databases, personalized access to websites. Without eID eGovernment will not go beyond granting access to generic information.

- ***Improving security in terms of accountability***

An interoperable and largely deployed electronic identity is a key enabler for a better accountability: there is a direct trusted link between a person and an action within an application or website.

- ***Improving national security***

ID's and Passports/Visa will not stop terrorists. However, it is a building block to be relied upon.

- ***Building a more inclusive European society***

Like with the Euro currency it helps people to understand that they belong to a greater European community. A seamless use of eID should contribute to a citizen's general feeling of trust and security and also offer European-wide service provision whenever they are on-line.

- ***Generating economies of scale***

Electronic identity is part of an 'infrastructural approach'. An eID infrastructure which can support various applications at marginal costs will stimulate the introduction of new eServices. The banking sector with its Single European Payment Area Concept is already working on a similar concept.

- ***Increasing administrative efficiency and reducing cost***

The use of electronic identities facilitates the deployment of fully transactional systems diminishing the needs of manual/repetitive work and interactions.

From a citizen standpoint, the main drivers for a pan European interoperable eID can be summarized as:

- ***Reducing the burden when engaging with the administration***

Cross-border systems supporting an electronic identity will simplify the identification of the adequate counter and forms to submit a request. It will enable automated inter-administrations BackOffice information exchanges and will lead to minimal face-to-face and on-site interactions.

- ***Limiting possibilities for fraud, identity theft and phishing***

ID fraud is an increasing problem with an estimated impact of several billons Euro a year. Identity theft, phishing and fraud are serious threats that governments need to guard against in order to maintain public confidence in their e-services. An adequate basic security level is needed and can be delivered by an electronic identity.

- ***Supporting mutual recognition of documents and certificates in cross-border situations.***

From a citizen's perspective, having to produce certified documents in cross-border situations is really painful as it implies a loss of time and unnecessary travels. Solutions based on electronic identities would simplify this and would also help avoiding languages issues leading to certified translations.

- ***Facilitating mobility***

The European citizen enjoys free movement in the European domain and is entitled to avail of government services wherever here or she is, permanently or temporarily residing. All this will contribute to the social inclusion of the European citizen.

5. ISSUES

- ***Costs and benefits***

An Electronic Identity Infrastructure is expensive. Moreover it's not only the costs of the system components that count, it's also the organisational costs such as card issuance and enrolment of the cardholder. The corresponding business case must include the benefits resulting from multiple projects, both for the Government and the private sector.

This is currently addressed by the identification of adequate business cases and the implementation of a large-scale pilot.

- ***Interoperability***

Multiple identity schemes are being deployed on a per-sector / per-country basis. At this stage, interoperability is not guaranteed: there is a multitude of standards and a lack of a commonly accepted standard, the mapping of identity information in cross border transactions is not direct and the physical containers used to store electronic identities vary (smart card, bank card, SIM/mobile phone …).

Infrastructural requirements will be addressed as part of the i2010 eID roadmap. This includes a clear conceptual framework (including common specifications), the definition of authentication levels, the choice of data formats and standardisation issues.

- ***Legal difficulties***

The current legal frameworks differ on a per-country basis. Furthermore, eID cards are outside of the European legal competence.

However, a specific task has been identified as part of the eID i2010 roadmap to address the legal issues.

- ***Privacy***

Privacy is a big concern for the end users. The individual is losing control when confronted to activities such as profiling, behavioural targeting, social sorting, dynamic pricing, blacklists, constant surveillance… The use of a unique identifier encompassing several sectors (e.g. taxation - bank, social security - insurances …) could make this even worse.

However, when setting up architectures based on identities there are possibilities to give the users control over the information they share with services. Furthermore, privacy-enhancing tools can be embedded in the design of eID infrastructures to clearly segregate the different sectors where the user is active. As part of the eID i2010 roadmap, a personal data ownership/stewardship model will be developed that also takes into account privacy requirements mapped on a Member State level.