eHealth Governance Initiative:

Joint Action JA-EHGov & Thematic Network SEHGovIA

DELIVERABLE

D8.1: Technical background of eID solutions

WP 8: ISM

(Interoperability, Standardization, Market)

Version:	1.00
Date:	16-03-2012

Project co-funded by the European Commission within the ICT Policy Support Programme and the Health Framework Programme

COVER PAGE	
Project Acronym	**eHGI**
Grant Agreement number	
Status*	**Final**
Dissemination level**	**CO**
Author(s) & Organization(s)	**ISM**
Contact	**falk.schubert@bmg.bund.de**

* Status: Draft / In Progress / Final
** Dissemination level: PU = Public or
CO = Confidential, only for members of the consortium and the Commission Services

ABSTRACT

In the European Union, existing eID solutions build a heterogeneous landscape of organizational concepts and technologies. That includes means of authentication, identity and attributes provider and identity management. Based on these realities, recommendations for the technical design, implementation and management of eID are derived.

Change History					
Version	**Date**	**Status**	**Author**	**Details**	**Review**
1.0	16/3/2012		Sören Bittins, Falk Schubert		ISM group

Statement of originality:

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

ABBREVIATIONS

eHGI	eHealth Governance Initiative
EU	European Union
eID	electronic Identification
ENISA	European Network and Information Security Agency
OSI	Open Systems Interconnection Reference Model
PIN	Personal Identification Number

LIST OF REFERENCES

Name of Author	Reference / Source
ENISA (2011)	European Network and Information Security Agency: Managing multiple identities http://www.enisa.europa.eu/activities/identity-and-trust/privacy-and-trust/library/deliverables/mami
TDL (2012)	Trust in Digital Life: Architecture serving complex Identity Infrastructures http://www.trustindigitallife.eu/uploads/Architecture%20serving%20complex%20Identity%20Infrastructures.pdf
ENISA (2012)	European Network and information Security Agency: Country reports. http://www.enisa.europa.eu/activities/stakeholder-relations/files/country-reports/

TABLE OF CONTENTS

Technical background of eID solutions 5
Means for authentication 5
Infrastructure 6
Identity and attribute provider 6
Identity management 6
User-centricity, privacy, inclusion 7
Proliferation of identities 7
Lifecycle of an identity 7
Pseudonymous transactions and unlinkability 7
Interoperability of eID solutions 7
1. ANNEX 9
Current situation on eID 9
Summary on the current Situation on eID in the EU 9

Technical background of eID solutions

In the European Union, existing eID solutions build a heterogeneous landscape of organizational concepts and technologies. Before discussing the existing approaches in Europe, its characteristics will be explained.

Means for authentication

In general, eID is based on the individual presenting a digital identifier plus the verification of the claimed identity.
That verification can be based upon:

- something a user has (a card, a key)
- something a user knows (password)
- something a user is (biometrics, fingerprint)
- something a user can do (signature)

A combination of two means is called two-factor-authentication. An example would be a bankcard (something the user has) and a PIN (something the user knows).
1. In the case of the "mobile identity", the phone's identification (phone number, but more likely the card number) is implementing the identity, while the possession of the phone/card is the means of authentication.
2. In the case of a combination of logon and password, the means of authentication is the knowledge of the password. Passwords typically do have little authentication strength i.e. if they are not properly chosen; they are often easy to guess by some algorithm. However no extra client hardware or software has to be deployed.
3. In case of biometric means, a digital identifier has to be provided and biometric measures help to authenticate it. Biometric authentication is generally recognised as a very reliable authentication method.
4. Certificate based approaches use different platforms but share the same characteristics.
So-called certificates combine identity and means for authentication. Both, identity and means for authentication are known to a secure token carrier (PC or smartphone or a smartcard), and therefore they are easy to use. Corruption is less likely because the secret is coupled to or hidden by the secure token carrier.

Infrastructure

The infrastructure for the handling of eIDs depends on the authentication method chosen. Generally speaking, that includes:

- eID means (software or hardware based, e.g. , software certificate, smart card) and authentication token (pin, password, biometric token),
- optional client software to access the eID or to initialize an authentication or identification process and
- additional hardware (e.g. card reader, USB-stick or mobile phone) if applicable.

On the service provider side (business and governments) the following applications will be necessary in general:

- a connection to the identity provider or the national public-key-infrastructure
- a trust broker / mediator if applicable
- an authentication or authorisation certificate if applicable.

Further requirements will be necessary on client and server-side depending on the current implementation.

Identity and attribute provider

The two main players within the identity assurance market are identity and attribute provider. An identity provider assigns the electronic identity to the real-world entity of a person or organisation ("Mr Schmidt") whereas an attribute provider assures the particular attributes, skills or eligibilities of that person or organisation ("Mr Schmidt is a medical doctor").
The separation and loose-coupling of both providers is recommended.

Identity management

The technical needs for an eID Infrastructure depend strongly on the basic principles of the organizational concept. The following aspects have been identified by the ENISA[1] and Trust in Digital Life Initiative as major issues in identity management:

- composable architecture
- open standards
- user centricity (attributes remain with the subject)
- user privacy, consent and correctness/accountability

[1] ENISA: http://www.enisa.europa.eu/act/it/privacy-and-trust/library/deliverables/mami

User-centricity, privacy, inclusion

User-centricity puts the user e.g. a citizen or a customer into the centre of all decisions. He or she controls his or her identity information. Electronic ID systems must be based on high quality and security standards. This will enhance trust and with that acceptance of an eID.
eID solutions should not be compulsory for patients.
Additionally a user-centric system should include all people, even those who are not able to use standard online processes.

Proliferation of identities

The concept of username and password in a strongly connected world as today becomes a major challenge. Today individuals have numerous identities for a variety of purposes. Users tend to use the same combination of username and password or passwords that are easy to guess. An alternative would be to derive multiple identities from a generic identity.
Additionally, new eID concepts have to use more secure identifiers like smartcards, certificates or mobile IDs.

Lifecycle of an identity

As each person, each object and each service undergoes changes throughout its lifetime, so does their digital identity. As it is impossible to guarantee absolute life-long security the lifespan of an identity influences the security standards that can be considered and vice versa.

Pseudonymous transactions and unlinkability

Privacy-enhancing technologies like pseudonymisation should be applied whenever possible. Identifiers should be health-specific in order to hinder the linkage between transactions from different aspects of life (e.g. different identifiers for shopping-, health- and tax-related transactions).

Interoperability of eID solutions

For technical and organizational interoperability a common set of mature open standards and contractual agreements needs to be defined. The standard should incorporate abstraction and encapsulation. Best practice on achieving interoperability is a layered approach as it was defined by the OSI seven-layer model.
eID solutions in healthcare and their interfaces should always be based on open standards in order to achieve cost-effective, maintainable and safe systems.

1. ANNEX

Current situation on eID

Summary on the current Situation on eID in the EU

The following table is picturing the current situation and potential deployment of eID solutions across Europe. It does not include eHealth-specific eID means (e.g. health insurance cards or health professional cards).

Country	ID Manda-tory	eID Manda-tory	Source	eID Introduc tion	eHealth with eID	eSignatu re Act	Costs for eID	National Identifier	Valid	Biometri c	eID planned
Austria	Yes, over 14	No	Bürgerk arte	2003	Yes	Yes, 1999	Free of charge	Sector specific	5 years	No	Available
Belgium	Yes, over 12	Yes	.beID	2004	Yes	Yes, 2000	min 12 EUR	Yes	5 years	No	Available
Bulgaria	Yes, over 14	-	lichna karta	-	No	Yes, 2001	BGN 50	Yes	10 years	Yes	Yes
Cyprys	Yes, over 12	-	Civil identity card	-	No	Yes, 2004	Cy £5,00	-	-	-	Yes
Czech Republic	Yes, over 15	-	civic certificat e	-	No	Yes, 2004	-	Yes	-	No	Yes
Denmar k	No	No	OCES	-	-	Yes, 2000	-	Yes	-	-	No
Estonia	Yes, over 15	No	id.ee	2002	No	Yes, 2000	25 EUR	Yes	10 years	No	Available
Finland	No	No	FINEID	2000	-	Yes, 2009	51 EUR	Yes	5 years	Yes	Available
France	No	-	INS	-	No	Yes, 2000	-		10 years	Yes	Yes
German y	Yes	No	Online-Ausweisf unktion	2010	No	Yes, 2001	28,80 EUR	No	10 years	Yes	Available
Greece	Yes, over 12	-	ID card	-	No	Yes, 2001	-	Several	-	No	Yes
Hungary	Yes, over 14	-	ID card	-	No	Yes, 2001	-	Yes	-	-	Yes
Ireland	No	-	ID card	-	No	Yes, 2003	-	Yes	-	-	Yes
Italy	Yes, over 15	No	Carta d'Identit à Elettroni ca	2001	No	Yes, 1997	25 EUR	Yes	10 years	Yes	Available
Latvia	Yes, over 15	-	ID card	-	No	Yes, 2003	-	Yes	-	Yes	Yes, in 2012
Lithuani a	Yes, over 16	No	Personal Identity Card	2009	No	Yes, 2002	-	Yes	10 years	Yes	Available

Country	ID Mandatory	eID Mandatory	Source	eID Introduction	eHealth with eID	eSignature Act	Costs for eID	National Identifier	Valid	Biometric	eID planned
Luxembourg	Yes, over 15	No	LuxTrust cards	-	-	Yes, 2000	-	Yes	-	-	No
Malta	Yes, over 18	-	Karta ta' l-Identità	-	-	Yes, 2001	-	-	-	Yes	Yes
Netherlands	Yes, over 14	No	DigiD	2007	No	Yes, 2003	42,85 EUR	Yes	5 years	Yes	Available
Poland	Yes, over 18	-	pl.ID	-	Yes	Yes, 2001	Free of charge	Yes	10 years	Yes	Yes, in 2013
Portugal	Yes, over 16	No	Cartão de Cidadão	2007	-	Yes, 2003	12 EUR	4 main identifier	10 years	-	Available
Romania	Yes, over 14	-	Carte de identitate	-	-	Yes, 2001	-	Yes	-	-	Yes
Slovakia	Yes, over 15	-	Občiansky preukaz	-	No	Yes, 2002	-	2 main identifier	-	No	Yes
Slovenia	Yes, over 18	-	Osebna izkaznica	-	-	Yes, 2000	-	Yes	-	-	Yes
Spain	Yes, over 14	No	e-DNI	2006	No	Yes, 2003	10,10 EUR	Yes	-	-	Available
Sweden	No	No	ID-kort	2005	No	Yes, 2000	-	Yes	5 years	Yes	Available
UK	No	-	-	-	-	Yes, 2000	-	Sector specific	-	-	No

Table 1: eID across Europe EU-27[2]

[2] Source: http://www.enisa.europa.eu/act/sr/files/country-reports/; as well as by the links incorporated in the table