eID Interoperability for PEGS

NATIONAL PROFILE LIECHTENSTEIN

November 2007

This report / paper was prepared for the IDABC programme by:

Author's name: Jos Dumortier - Hans Graux, time.lex

Company's name: Siemens - time.lex

Company's address (optional):

Company's logo (optional)

Contract No. 1, Framework contract ENTR/05/58-SECURITY, Specific contract N°3

Disclaimer

The views expressed in this document are purely those of the writer and may not, in any circumstances, be interpreted as stating an official position of the European Commission.

The European Commission does not guarantee the accuracy of the information included in this study, nor does it accept any responsibility for any use thereof.

Reference herein to any specific products, specifications, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favouring by the European Commission.

All care has been taken by the author to ensure that s/he has obtained, where necessary, permission to use any parts of manuscripts including illustrations, maps, and graphs, on which intellectual property rights already exist from the titular holder(s) of such rights or from her/his or their legal representative.

This paper can be downloaded from the IDABC website:

http://europa.eu.int/idabc/
http://ec.europa.eu/idabc/en/document/6484/5938

Executive summary

The project eID Interoperability for PEGS aims to propose a solution to the legal, technical and organisational issues related to the creation of an interoperable Pan-European identity management infrastructure. The EU Member States, Candidate Countries and EEA Countries are introducing more sophisticated ways to manage identities in the eGovernment area. Different member states are implementing different structures as their identity management solution. The main challenge for the eID Interoperability for PEGS project is to propose a general architecture that, while taking into account the existence of different models, is able to cope with them by obtaining the final goal of interoperability.

The project should conclude with several different proposals how to build interoperability without affecting member states' own existing infrastructures.

This document describes the current situation regarding the use of electronic authentication means in eGovernment applications in Liechtenstein.

Table of Contents

EXECUTIVE SUMMARY 3

1 DOCUMENTS 5

1.1 APPLICABLE DOCUMENTS 5

1.2 REFERENCE DOCUMENTS 5

2 GLOSSARY 6

2.1 DEFINITIONS 6

2.2 ACRONYMS 8

3 INTRODUCTION 9

3.1 GENERAL STATUS AND MOST SIGNIFICANT EIDM SYSTEMS 9

3.2 BACKGROUND AND TRADITIONAL IDENTITY RESOURCES 10

3.2.1 EGOVERNMENT STRUCTURE 10

3.2.2 NATIONAL EGOVERNMENT COOPERATION AND COORDINATION 10

3.2.3 TRADITIONAL IDENTITY RESOURCES 10

3.3 EIDM FRAMEWORK 11

3.3.1 MAIN EGOVERNMENT POLICIES WITH REGARD TO EIDM 11

3.3.2 LEGAL FRAMEWORK 11

3.3.3 TECHNICAL ASPECTS 11

3.3.4 ORGANISATIONAL ASPECTS 12

3.4 INTEROPERABILITY 12

3.5 EIDM APPLICATIONS 12

3.6 FUTURE TRENDS/EXPECTATIONS 12

3.7 ASSESSMENT 12

1 Documents

1.1 Applicable Documents

[AD1]	Framework Contract ENTR/05/58-SECURITY

1.2 Reference Documents

[RD1]	eGovernment in the Member States of the European Union – 5th Edition – May 2006 http://ec.europa.eu/idabc/servlets/Doc?id=24769
[RD2]	European Electronic Signatures Study http://www.law.kuleuven.ac.be/icri/itl/es_archive.php?where=itl
[RD3]	DIRECTIVE 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures http://europa.eu.int/information_society/eeurope/i2010/docs/esignatures/esignatures_en.pdf
[RD4]	Decision 2003/511/EC of 14 July 2003 on the publication of reference numbers of generally recognised standards for electronic signature products in accordance with Directive 1999/93/EC of the European Parliament and of the Council, OJ L 175, 15.7.2003, p.45 http://europa.eu.int/eur-lex/pri/en/oj/dat/2003/l_175/l_17520030715en00450046.pdf
[RD5]	DIRECTIVE 2004/18/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts http://eur-lex.europa.eu/LexUriServ/site/en/oj/2004/l_134/l_13420040430en01140240.pdf
[RD6]	IDABC Work Programme Third Revision http://ec.europa.eu/idabc/servlets/Doc?id=25302
[RD7]	DIRECTIVE 2004/17/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors http://europa.eu.int/eur-lex/pri/en/oj/dat/2004/l_134/l_13420040430en00010113.pdf

2 Glossary

2.1 Definitions

In the course of this report, a number of key notions are frequently referred to. To avoid any ambiguity, the following definitions apply to these notions and should also be used by the correspondents.

- *Entity:* anyone or anything that is characterised through the measurement of its attributes in an eIDM system. This includes natural persons, legal persons and associations without legal personality; it includes both nationals and non-nationals of any given country.

- *eIDM system*: the organisational and technical infrastructure used for the definition, designation and administration of identity attributes of entities. This Profile will only elaborate on eIDM systems that are considered a key part of the national eIDM strategy. Decentralised solutions (state/region/province/commune…) can be included in the scope of this Profile if they are considered a key part of the national eIDM strategy.

- *eIDM token (or 'token')*: any hardware or software or combination thereof that contains credentials, i.e. information attesting to the integrity of identity attributes. Examples include smart cards/USB sticks/cell phones containing PKI certificates, …

- *Authentication*[1]: the corroboration of the claimed identity of an entity and a set of its observed attributes. (i.e. the notion is used as a synonym of "entity authentication").

- *Authorisation*: the process of determining, by evaluation of applicable permissions, whether an authenticated entity is allowed to have access to a particular resource.

- *Unique identifiers*: an attribute or a set of attributes of an entity which uniquely identifies the entity within a certain context. Examples may include national numbers, certificate numbers, etc.

- *Official registers*: data collections held and maintained by public authorities, in which the identity attributes of a clearly defined subset of entities is managed, and to which a particular legal of factual trust is attached (i.e. which are generally assumed to be correct). This includes National Registers, tax registers, company registers, etc.

[1] For the purposes of this Profile, the notion of authentication is considered to be synonymous with 'entity authentication', as opposed to 'data authentication'. The notion of 'identification should be avoided to avoid confusion.

- *eGovernment application*: any interactive public service using electronic means which is offered entirely or partially by or on the authority of a public administration, for the mutual benefit of the end user (which may include citizens, legal persons and/or other administrations) and the public administration. Any form of electronic service (including stand-alone software, web applications, and proprietary interfaces offered locally (e.g. at a local office counter using an electronic device)) can be considered an eGovernment application, provided that a certain degree of interactivity is included. Interactivity requires that a transaction between the parties must be involved; one-way communication by a public administration (such as the publication of standardised forms on a website) does not suffice.

- *eSignature*: data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication with regard to this data. Note that this also includes non-PKI solutions.

- *Advanced electronic signature*: an electronic signature which meets the following requirements:

  (a) it is uniquely linked to the signatory;

  (b) it is capable of identifying the signatory;

  (c) it is created using means that the signatory can maintain under his sole control; and

  (d) it is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable;

  Again, this definition may cover non-PKI solutions.

- *Qualified electronic signature*: advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device, as defined in the eSignatures Directive[2].

- *Validation*: the corroboration of whether an eSignature was valid at the time of signing.

[2] See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML

2.2 Acronyms

A2A ..... Administration to Administration

A2B ..... Administration to Businesses

A2C ..... Administration to Citizens

CA ..... Certification Authority

CRL ..... Certificate Revocation Lists

CSP ..... Certificate Service Provider

eID ..... Electronic Identity

eIDM ..... Electronic Identity Management

IAM ..... Identity and Authentication Management

IDM ..... Identity Management

OCSP ..... Online Certificate Status Protocol

OTP ..... One-Time Password

PKCS ..... Public-Key Cryptography Standards

PKI ..... Public Key Infrastructure

SA ..... Supervision Authority

SOAP ..... Simple Object Access Protocol

SCVP ..... Server-based Certificate Validation Protocol

SSCD ..... Secure Signature Creation Device

USB ..... Universal Serial Bus

TTP ..... Trusted Third Party

XAdES ..... XML Advanced Electronic Signature

XML ..... eXtensible Markup Language

XML-DSIG ..... XML Digital Signature

3 Introduction

3.1 General status and most significant eIDM systems

As noticed by the eGovernment Observatory, section eGovernment Infrastructure/e-Identification Infrastructure, there is no specific eID infrastructure in place yet in Liechtenstein. The current e-Government portal is available under the following address: http://www.llv.li.

The legal framework is at this stage still fragmented (the basics are captured by the *Signaturgesetz* (Act on e-Signatures) and *Signaturverordnung* (Ordinance to the Act on e-Signatures)).

The popularity of the eGovernment portal can be rated as very high, with average portal access number rates around 60.000 visitors per month. With respect to the whole population figure of 34.000, this can be marked as a clear success indicator and points out the growing need for eGovernment services.

Currently there are only some certificates of A-Trust, Vienna, in usage, to fulfil aspects of Directive 2003/58/EC amending Directive 68/151/EEC, as regards disclosure requirements in respect of certain types of companies (Liechtenstein commercial register).

Within the scope of the e-ID eGovernment project in the near future smartcards, with qualified certificates from A-Trust, Vienna, will be used for the identification and authorisation processes for the execution of several eGovernment services.

The eIDM system in Liechtenstein will be based on the future Liechtenstein e-ID Card, a mandatory electronic identity card to facilitate access to eGovernment services for all Liechtenstein citizens. Further information about the Liechtenstein eGovernment portal, actions and strategy may be obtained under

http://www.portalinfos.llv.li.

A potential user base of 70 % of the population would result in a figure around 24.000. Obviously there are no figures of the actual penetration or usage.

3.2 Background and traditional identity resources

3.2.1 eGovernment structure

The public administration of Liechtenstein, particularly the *Amt für Personal und Organisation* (Office of Human Resources and Administration) coordinates the development of eGovernment applications at national level. EGovernment projects tend to a vertical integration, within the same area of competence, such as tax or social security. Nevertheless, steps will be taken towards horizontal integration covering several departments and local municipalities.

One of the purposes of horizontal integration will be to share information so as to avoid requesting it twice. This is the so-called “authentic source” principle: once information has been requested from the user, it should be stored in a single authentic source. All other eGovernment services are then expected to access the information through the authentic source whenever possible, rather than requesting it multiple times.

3.2.2 National eGovernment cooperation and coordination

The need for integrated cooperation between the various levels will be specified in an agreement between the national public administration and regional authorities, such as communities (Liechtenstein has 11 communities), for the setting up and exploitation of a common platform on public eGovernment services for administrations, business and citizens. This agreement will stress the need for a strong legal and interoperability framework at the organisational, semantic and technical level. For the area of electronic signatures, essential requirements must be met to avoid isolated use of a signature solution and to increase trust in the signature.

The framework used in Liechtenstein will be compatible with the European Interoperability Framework (EIF).

3.2.3 Traditional identity resources

Liechtenstein established a *Zentrale Personenverwaltung* (ZPV, Central Administration of Data of Individuals), in order to accumulate all information as regards Liechtenstein citizens and all persons either residing or working in Liechtenstein. The ZPV, therefore, facilitates the administrative procedures, and is one of the main working instruments for the State Administration (within the limits as set out by the data protection Directive 95/46/EC).

Liechtenstein relies mostly on a system of civil registers (*Zivilstandsregister*), in which life events such as birth, deaths and marriages. Registered data includes full name, date and place of birth, parent's names, gender and place of residence..

There is a non-mandatory identity card in Liechtenstein, but it is not electronic. It contains the name and first name, signature, date of birth, place of residence and issuance, size, eye colour, validity duration, photo of the bearer and card number.

3.3 eIDM framework

3.3.1 Main eGovernment policies with regard to eIDM

The Government of Liechtenstein decided in June 2007 to free the necessary means within the e-ID project for the elaboration of the specifications of the e-ID card, the blank cards and the foreseen usage of A-Trust certificates. Deployment of this card will start in spring 2009.

The chip will contain two certificates, allowing the authentication of the citizen and the use of a qualified electronic signature.

3.3.2 Legal framework

With regard to the legal framework, internal discussions are still ongoing. Most presumably a new e-Government Act will be enacted. Legal fragments, such as the e-Signatures Act and the Ordinance to the Act on e-Signatures, as well as the *Personen- und Gesellschaftsrecht* (Persons and Companies Act) are already in force.

3.3.3 Technical aspects

The e-ID card is based on PKI technology, and will incorporate two certificates: one for authentication, and one for electronic signatures, with only the latter being considered as qualified. Each private key is dependent on the use of a PIN-code. The definition of the use cases around the task "e-ID-Card issue", will be done within the mentioned projects.

The hardware specifications will be mainly based on the indications given by A-Trust, Vienna, to comply safely with the involved PKI-infrastructure and a wide range of smartcard readers.

The technical aspect of the specific middleware is based on guidelines, EIF-specifications and standards.

Procedures will be put in place to suspend or revoke certificates when the e-ID card is lost or destroyed. Card holders will be informed of their obligation to notify their local police in case of loss or compromise of the card, and an e-ID card stop telephone number will be provided.

3.3.4 Organisational aspects

As mentioned the organisational aspects will also be handled within the e-ID project and actually no statement about these issues can be made yet.

3.4 Interoperability

The step towards the European information society requires interoperable delivery of e-Government services throughout Europe. Relying to the European EIF-model it enables an interoperable e-Government infrastructure, providing public services to the European citizens.

3.5 eIDM Applications

Currently, no eIDM applications are in place.

3.6 Future trends/expectations

The Liechtenstein approach will be strongly centred around e-ID cards. The e-ID cards will become the standard for authentication services in e-Government processes.

3.7 Assessment

It remains to be seen whether the future implementation will meet the end user's needs, and in particular if and how the system will be made accessible to nationals and non-nationals.