eID Interoperability for PEGS

NATIONAL PROFILE AUSTRIA

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 Austrian eGovernment applications.

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 11

3.2.3 TRADITIONAL IDENTITY RESOURCES 11

3.3 EIDM FRAMEWORK 13

3.3.1 MAIN EGOVERNMENT POLICIES WITH REGARD TO EIDM 13

3.3.2 LEGAL FRAMEWORK 17

3.3.3 TECHNICAL ASPECTS 19

3.3.4 ORGANISATIONAL ASPECTS 23

3.4 INTEROPERABILITY 24

3.5 EIDM APPLICATIONS 25

3.6 FUTURE TRENDS/EXPECTATIONS 25

3.7 ASSESSMENT 26

3.7.1 ADVANTAGES: 26

3.7.2 DISADVANTAGES: 26

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

Austria has introduced a comprehensive eIDM approach referred to as Citizen Card (*Bürgerkarte*) with the eGovernment Act (*E-Government Gesetz*). Comprehensive information is available via the citizen card website at http://www.buergerkarte.at/index_en.html

The citizen card is a technology-neutral concept that allows for various different solutions. Both the public sector and the private sector issue citizen cards. To date, the most commonly used implementations are: (1) each bank card issued since March 2005, (2) the health-insurance card, which has been rolled out in 2005, or (3) mobile phones, which can be used as a two-factor authentication solution since March 2004. Further initiatives include universities that issue student service cards or federal ministries that roll out public servant's service cards. Generally, the tokens are prepared technically, the activation of a token as a citizen card is voluntary. An exception from the principal of voluntary activation may be public servant's service cards where the activation may be made compulsory as part of an official's duties.

The penetration, insofar publicly known, is listed below:

eIDM system	Potential user base	Actual penetration	Actual use
Bank cards	About 7 million[3]	About 6,5 million bank cards in use[4] (almost 80% of the population)	55.000 bank cards activated beginning of 2006[5] No public data for 2007 known.
Health insurance card	About 9 million[6]	9 million (100 %)	13.000 active cards as of March 2007
Mobile phone	About 7 million[7]	110%[8]	No statistics are publicly available
Federal public servant service cards	133.000 federal civil servants[9]	12.000 service cards issued by the Federal Ministry of Finance	12.000 (all service cards of the Federal Ministry of Finance)

[3] Juveniles and adults

[4] Source: press release 28.09.2005 at http://www.maestro.at

[5] Source: press release 20.03.2006 at http://www.a-trust.at/info.asp?node=710&ch=4

[6] Each Austrian citizen plus foreigners having health insurance

[7] Estimated as Austrians adults and juveniles

[8] Source http://www.rtr.at Telekom Monitor 1/2007. Penetration calculated as active SIM cards per capita.

[9] Source: Federal Chancellery, "*Das Personal des Bundes 2006*", December 2006.

The citizen card combines electronic signatures as a means of authentication and unique identification. For the latter, the concept is closely linked to the Central Register of Residents CRR (*Zentrales Melderegister*), which provides a unique source of identification for registered residents. A Supplementary Register for Natural Persons SRnP (*Ergänzungsregister für natürliche Personen*) allows for integration of foreigners or expatriates that are not covered otherwise. For legal persons, the Register of Company Names (*Firmenbuch*), the Central Register of Associations (*Zentrales Vereinsregister*), and a Supplementary Register of Other Data Subjects (*Ergänzungsregister für sonstige Betroffene*) complement the eGovernment base registers.

By applying cryptographic transformations, a sector-specific identification model that enforces data protection aspects for natural persons is used. The core element is a so-called identity link (*Personenbindung*). The identity link is an attestation signed by the authority that links a citizen's electronic signature to the unique identifier "sourcePIN" derived from the base registers. The sourcePIN may only be stored in the identity link in the citizen card, thus is under sole control of the citizen.

3.2 Background and traditional identity resources

3.2.1 eGovernment structure

The Austrian eGovernment structure is governed by horizontal and vertical coordination of activities. An ICT Strategy Unit has been installed at the Federal Chancellery. This group is responsible for the eGovernment Act and the Signature Act.

Coordination on the federal level and with provinces, municipalities and local authorities is carried out by the ICT Board. The ICT Board is composed of the Chief Information Officers of all the federal ministries and their deputies. A Federal CIO is installed that chairs the ICT Board.

An e-Cooperation Board allocates responsibility for the preparation of implementation projects and coordinates the implementation projects of the participating organisations (ICT Board, eGovernment working groups of the provinces and the public-administration bodies responsible for ICT). The two bodies ICT Board and e-Cooperation Board are coordinated by the ICT strategy platform "Digital Austria" which is led by the Federal CIO.

Thus, the eGovernment structure spans various levels.

- *Federal eGovernment*

  Federal eGovernment initiatives are coordinated by the ICT Board.

- *Regional and local eGovernment*

  eGovernement in the provinces (*Länder*), cities, and municipalities is under the responsibility of the respective authorities. Coordination is provided through the ICT Board and the e-Cooperation Board.

3.2.2 National eGovernment cooperation and coordination

Since the ICT Board had taken up its activities, great importance has been placed on cooperation between the federal government, the provinces, municipalities, and local authorities. The publication of decisions ensures compliance with the principle of transparency.

A reference server[10] has been set up by the provinces, which acts as a platform for communication between all levels of administration, on which proposals for working methods and concepts, contributions to discussions and conventions decided between the federal government and the provinces, are published.

Administrative tasks are for the most part performed by the provinces, regional councils, municipalities, and local authorities. Without basic coordination, the highly federal nature of the Austrian state would, in the long term, lead to differing approaches. Joint and coordinated action is therefore a principle ensuring the effective implementation of eGovernment.

In order to profit from synergies, IT activities at both provincial and federal level are coordinated in various working groups and priorities are set jointly. Working groups focusing on specific needs act together with the ICT Board to support the coordinating activities. This means that concepts and projects are agreed before decisions are adopted across all levels of administration. In this way, differences of opinion on an expert level can be avoided.

3.2.3 Traditional identity resources

Registration of residents used to be on the local level, in many cases based on paper registers. The Central Register of Residents CRR (*Zentrales Melderegister*) went operational on 1st March 2002 – the day when the new Registration Act (*Meldegesetz*) went into force. The CRR was based on data from a census that has been carried out in 2001.

The General Procedural Law (*Allgemeines Verwaltungsverfahrensgesetz 1991 – AVG*) defines for conventional oral applications or applications in writing that the identity of an applicant or the authenticity of the application needs to be proven in cases where there are doubts or in cases where

[10] http://reference.e-government.gv.at

the nature of the proceeding requires that. Supporting evidence can be official documents such as a birth certificate (*Geburtsurkunde*), a proof of citizenship (*Staatsbürgerschaftsnachweis*), or an official identification with a photo, such as a passport, a driving license, or other ID cards (a *Personalausweis* which is a Schengen travelling document or an *Identitätsausweis* that is no travelling document).

Note, that Austria has no obligation to carry or possess any official identity card. Identity witnesses (*Identitätszeugen*) are persons who are in close relationship with the person in question, such as a relative or spouse, and who possess an official identification with a photo. If a public document is to be validated with a notary and the person in question does not provide an official identification with a photo himself, one or two identity witnesses are needed[11].

Apart from the registration of residents, some sectoral or application-specific identity management systems and identifiers have grown over time.

For natural persons, the most widespread system providing unique identifiers used to be the health insurance and social security system: the social security number is a ten digit number *nnnc-ddmmyy* where '*nnn'* is a 3-digit consecutive number, '*ddmmyy'* is the date of birth and '*c*' is an error checking digit. In conventional proceedings the social security number legally got used in a few other sectors, such as inter alia taxes, scholarships (*Studienbeihilfe*), tracking education (*Bildungsevidenz*), or building and loan association (*Bausparen*).

A further example of a traditional sectoral identifier is the matriculation number of universities (*Matrikelnummer*) consisting of a 2-digit number indicating the year of matriculation and 5 digits from a university's quota.

For legal persons and self-employed natural persons the tax number is used. The tax number is assigned by the tax authorities on request. It consists of a 2-digit tax office identifier and a 7-digit number. Another tax identifier is the VAT number (*Umsatzsteuer-Identifikationsnummer* UID).

Further traditional unique identifiers for legal persons are the identifiers of legal persons in the Register of Company Names (*Firmenbuch, Firmenbuchnummer*) or the Central Register of Associations (*Zentrales Vereinsregister, ZVR-Nummer*).

[11] The number of witnesses needed depends whether the entity provides evidence, e.g. a birth certificate (*Geburtsurkunde*) or proof of citizenship (*Staatsbürgerschaftsnachweis*).

3.3 eIDM framework

3.3.1 Main eGovernment policies with regard to eIDM

Base Registers

With the eGovernement Act (*E-Government Gesetz*) a sector-specific eIDM has been introduced that relies on a number of eGovernment base registers:

- *For natural persons*
  - *Central Register of Residents (Zentrales Melderegister ZMR)* [12]

    The CRR is operated by the Federal Ministry of Interior. It went operational on 1st March 2002. Identity data and residence data are stored. The identity data consists of name, gender, nationality, place and date of birth, and travel document data (type, number, issuing state and authority) for foreigners. The residence data is the entity's address, type of residence (main or second residence), the date of registration or deregistration and the name of the house owner or leaseholder. Moreover, a unique identifier CRR-number (*ZMR-Zahl*) is stored. The CRR-number is a 12-digit decimal number.

  - *Supplementary Register for Natural Persons SRnP* (*Ergänzungsregister für natürliche Personen ERnP*)

    The SRnP holds – upon request by the entity concerned – natural persons that are not required to be registered in the CRR (e.g. expatriates, foreigners with no residence in Austria). The source PIN Register Authority (cf. D.1.2 below) is responsible for the SRnP, it recourses to the services of the Federal Ministry of Interior. The unique identifier's format is the same as the CRR-number. The record and the identifier can be transferred from the SRnP to the CRR to maintain unique identification, e.g. in cases where expatriates return to Austria, foreigners take residence in Austria, or vice versa.

- *For legal persons*
  - *Register of Company Names (Firmenbuch)* [13]

    The Register of Company Names is a public trade register under the responsibility of the Federal Ministry of Justice. An electronic database provided by the Austrian Federal Computing Center started in 1991. The identifier is a 6-digit decimal number plus an error detection digit.

[12] http://zmr.bmi.gv.at

[13] http://www.justiz.gv.at/firmenbuch

- *Central Register of Associations (Zentrales Vereinsregister ZVR)* [14]

  The Central Register of Associations is maintained by the Federal Ministry of Interior. It went operational on 1st January 2006. The identifier '*ZVR-Nummer*' is a 9-digit decimal number.

- *Supplementary Register of Other Data Subjects (Ergänzungsregister für sonstige Betroffene)* [15]

  Entities not covered by registers mentioned before can apply for being registered in a further supplementary register. Examples for such entities are churches, public authorities, foundations, municipalities, etc. The register is maintained by the sourcePIN Register Authority that recourses to services of the Federal Ministry of Finance. A decimal number with at least 3 digits is assigned as an identifier.

Legal persons use the identifier (*Firmenbuchnummer* or *ZVR-Nummer*) in their communications both in conventional paper communication (e.g. letterheads), or in their electronic presence (e.g. an obligation to present the *Firmenbuchnummer* and the *VAT number* exists under the eCommerce Act).

For natural persons, however, the identifiers are under specific data protection constraints. The sourcePIN Register Authority plays an important role.

SourcePIN Register Authority, Electronic Representation

The duties of the sourcePIN Register Authority are taken care of by the Data Protection Commission. The main responsibilities are to implement the citizen card concept and the cooperation with its service providers.

The sourcePIN is a unique identifier that is derived from base register identifiers for natural persons, i.e. the CRR-number or the SRnP-number. Therefore the sourcePIN Register Authority applies a TripleDES encryption step to the base identifiers to create the sourcePIN (128 bit binary or 24 digit base64 number).

The sourcePINs are only stored in a so-called identity link in the citizen card. The identity link is a data structure that is created by the sourcePIN Register Authority during the issuance process of citizen cards. A signature of the sourcePIN Register Authority attests the link between the unique identifier 'sourcePIN' and an electronic signature provided to the entity by the citizen cardissuer. The identity also holds the name and data of birth. These data are frequently needed in official proceedings and intelligent forms can be pre-filled with the name and data of birth.

A further responsibility of the sourcePIN Register Authority is the issuance of electronic representations and mandates. Electronic mandates are XML records that hold the identifiers of both

[14] http://zvr.bmi.gv.at

[15] http://www.ersb.gv.at/

the constituent and the representative. The electronic mandate is signed by the sourcePIN Register Authority and stored in the citizen card of the representative. The scope of such mandates is specific and explicitly given in the mandate. It can thus also be a general power of attorney, if this is stated as such. The XML structure contains a textual field TextualDescription which describes the scope of the mandate, which can take any arbitrary content (human readable), essentially in the same way that a conventional paper mandate does. Depending on the complexity of this description and the context in which the mandate is being used, automatic recognition of such mandates may or may not be possible.

Sector-specific Identification, Authentication Process

The Austrian concept refers to identifiers as personal identification numbers (PINs). The eIDM model implemented using the citizen cards are sector-specific PINs that are derived from the sourcePINs. Using cryptographic one-way functions the sector-specific identifiers are calculated so that the citizen is uniquely identified in one sector, but identifiers in different sectors cannot be unlawfully cross-related.

The Sector Delineation Regulation (*E-Government-Bereichsabgrenzungsverordnung - E-Gov-BerAbgrV*) defines 26 sectors of State Activity so that within each sector using the same identifier no data protection issue is caused. Examples for such sectors are taxes, health, or sports. Nine further spanning delineators are defined that may involve or be used by distinct sectors, such as legal protection, electronic delivery, or human resource management.

The eIDM model is open for the private sector. Companies can use the citizen card to derive private sector-specific PINs that are unique within their sphere, but cannot be cross-linked with identifiers of other entities. The company's identifier (e.g. *Firmenbuchnummer*, cf. D.1.1 above) is used as a delineator during the cryptographic calculations similar as the sectors described above are used for calculating sector-specific PINs for the public sector.

The citizen's experience during the authentication process is that she or he gets presented a statement "With my signature I, <*givenName*> <*surname*> born <*date of birth*> request access to <*application*>", which she/he is requested to sign. Name and date of birth are taken from the identity link. The sector-specific PINs are transparently calculated using the identity link. Depending on the technological implementation or the citizen's choice, the identity link may by protected by a chosen PIN.

Citizen Cards

The Austrian Citizen Card is a concept rather than a specific token. It defines minimal requirements that an eID token needs to fulfil. Major requirements are electronic signatures and storage of the identity link or electronic mandates. Quality criteria are defined such as security requirements for the electronic signatures,[16] or the interface between Web-applications and the citizen card[17].

[16] Qualified signatures fulfill the requirements. For an interim period until end of 2007 other electronic signatures referred to as "administrative signatures" are admissible

To implement the functionality, usually software components accompany the hardware tokens. This middleware is referred to as 'citizen card environment' (*Bürgerkartenumgebung*). The Federal Chancellery has procured a general licence of one product that is made available to citizens for free for major platforms[18]. Another vendor make his middleware available for free.

As a general principle, eID tokens are prepared for being activated as a citizen card. However, it is the citizen's choice whether to actually activate the citizen card[19], which usually consists of the creation of electronic signature certificates by a certification service provider and creation of an identity link during the certificate creation process.

The major issuers of citizen cards or certification service providers can be both from the public sector or the private sector:

- *Major public sector issued citizen cards*
    - *Health insurance card 'e-card'*

      The health insurance smartcard has been issued to each citizen in 2005. The Main Association of Social Insurance Organisations is the public sector certificate service provider[20].

    - *Public servant service cards*

      Some federal ministries issue service cards or plan to issue such smartcards. So far the Federal Ministry of Finance has reached 100 % coverage by issuing service cards as citizen cards to its 12.000 officials. A-Trust[21] as a private sector certificate service provider is relied on in that issuance process.

    - *Student service cards*

      Several universities have issued student smartcards as citizen cards. The private sector certification service provider A-Trust issues cards and certificates.

- *Major private sector issued citizen cards*
    - *Bank cards, A-Trust cards*

      Each Austrian bank card can be activated as citizen card. The certification service provider A-Trust also issues other qualified signature smartcards as citizen card.

---

[17] Technical details are available at http://www.buergerkarte.at/en/technik/index.html

[18] To date, Windows, MacOS and Linux versions are available

[19] An exception may be public servant's service cards where the activation may be compulsory as part of an official's duties

[20] http://www.sozialversicherung.gv.at

[21] http://www.a-trust.at

- *Mobile phone signature*

  Using the administrative signature approach, the mobile phone service provider A1 offers a service where secure servers provide electronic signature and citizen card services. One-time SMS codes sent to the subscriber's mobile phone together with a chosen username password are used as two-factor authorisation.

3.3.2 Legal framework

The main legal framework (currently being amended, with legislative reforms expected to enter into force as from 1 January 2008) for the eID card is:

- the E-Government Act came into force 1st March 2004; the law is an overall legal basis for the instruments used to provide eGovernment. Regarding eIDM the law defines the citizen card concept and its use in the public sector using sector-specific PINs and in the private sector using private sector-specific PINs, respectively

- the Federal Act on Registration of 1991, last amended 2006; the Law defines the Central Register of Residents

- the Source PIN Register Regulation has been enacted on 2nd March 2005, its part 4 on electronic representation went into force 1st July 2005; it defines the activities of the sourcePIN Register Authority that are necessary to implement the citizen card concept, inter alia the creation of the identity link or electronic representation

- the E-Government Sectors Delimitation Regulation has been enacted in 2004; it defines the sectors of State activity that are distinguishable in the sector-specific eIDM model

- the Supplementary Register Regulation of 1st August 2005 defines the operation of the Supplementary Registers to include natural or legal persons that are not covered by existing registers

- the Administrative Signature Regulation has been enacted 16th April 2004; it defines the technical requirements for citizen cards that, in an interim period until end of 2007, need not be based on qualified signatures

Other relevant legislation includes:

- the Signature Act which went into force 1st January 2000, last amended in 2001

- the Signature Order of 2nd February 2000, last amended in 2004

The Signature Act has transposed the e-Signature Directive. Electronic signatures are defined for natural persons only.

The eGovernment Act defines two identification levels, as follows:

- *Unique identity*: "*designation of a specific person by means of one or more features enabling that data subject to be unmistakably distinguished from all other data subjects*"

- *Recurring identity*: "*designation of a specific person in a way which, while not ensuring unique identity, enables this person to be recognised by reference to a previous event, such as an earlier submission*"

As from 1 January 2008, the recurring identity concept will cease to exist and the eGovernment Act will know only the unique identity.

All Austrian citizen cards in use provide unique identification, as the identity is linked to the base registers' unique identifiers.

Access to data in the base registers is provided as follows: An entity's record in the Central Register of Residents (*Zentrales Melderegister*) can be accessed[22] – except for the CRR number (*ZMR-Zahl*) – if the requestor is identified and certain data of the entity in question is known (first name, surname, and another attribute such as the date of birth, or the current or former address). The Register of Company Names (*Firmenbuch*), the Central Register of Associations (*Zentrales Vereinsregister*), or the Supplementary Register of Other Data Subjects (*Ergänzungsregister für sonstige Betroffene*) are public registers that can be queried.

The sourcePIN Register Authority provides services in connection with the sector-specific eIDM model. In particular, this includes the calculation of sector-specific PINs of other sectors, if the name and the date of birth together with the sector-specific PIN of the requesting sector are provided. The sector-specific PIN is encrypted for the target sector. This allows data exchange between sectors without involvement of the citizen where such data exchanges are admissible.

The unique identifiers *sourcePIN* and also the *sector-specific PIN*s are legally protected by the eGovernment Act. Storing the sourcePIN is prohibited for any application; only the citizen card holds the sourcePIN in the identity link. The sector-specific PINs may only be stored by the sector that has created the identifier. The same holds for private-sector specific PINs.

Representation of non-natural persons is handled using electronic mandates. The power to represent is checked by the sourcePIN Register Authority during issuing the electronic mandate.

[22] An entity can apply for blocking inquiries for up to two years if a legitimate interest can be shown

3.3.3 Technical aspects

The citizen cards currently in wide use can be divided into smartcard-based systems and the mobile phone signature. The smartcard-based systems can be further divided into two major types depending on the certification service provider issuing the card.

All citizen card systems are PKI-based. They have two key pairs – a qualified signature[23] for authentication and the second key pair for electronic signatures or encryption. The certificates are either provided by the private sector certification service provider A-Trust as qualified certificates, or by the Main Association of Social Insurance Organisations.

All smartcard-based systems are secure signature–creation devices (SSCDs) as of the signature directive 1999/93/EC. Common Criteria certifications at EAL4+ for the ChipOS and EAL5+ for the chip platform together with a formal confirmation of the notified body A-SIT[24] are available. The health insurance card 'e-card' uses 192 bit elliptic curve cryptography (ECDSA) for both key pairs. The A-Trust issued cards use 192 bit elliptic curve cryptography (ECDSA) for the qualified signature and 1536 bit RSA for the second key pair. Different chip-platforms are in use for both types.

ID1 format contact-cards are used. None of the citizen cards are travel documents or have an ICAO logical data structure. No biometrics are used or stored. Depending on the issuer, other applications such as health card certificates for the health insurance card or ATM and electronic burse functions for the bank cards are provided. Typical EEPROM sizes are 36k.

The middleware 'citizen card environment' integrates the various tokens. Access is provided via native ChipOS interfaces.

For the mobile phone signature, RSA is used. The signatory's keys and the identity link are protected by hardware security module (HSM) keys together with the signatory's username and passwords.

Both PKIs the one of the Main Association of Social Insurance Organisations and the company A-Trust use LDAP as directory service. A-Trust uses CRLs and optionally OCSP as revocation service. For the health insurance card OCSP is the only option. The contents of the certificate for the various eIDs are:

Health Insurance Card Signature Certificate					
	OID	Include	Critical	Value	
Certificate					
Version				2 (Version 3)	

[23] or an administrative signature that for the citizen card function is treated equivalent to qualified signatures in the interim period until end of 2007

[24] http://www.a-sit.at

SerialNumber		X		Provided by CSP	Dynamic
Signature Algorithm	1.2.840.113549.1.1.5	X		SHA-1 with RSA Encryption	Fixed
Issuer distinguished name					
CommonName	{ id-at-3 }	X		VSig CA 2	Fixed
organizationName	{ id-at-10 }	X		Hauptverband österr. Sozialversicherungs.	Fixed
CountryName	{ id-at-6 }	X		AT	Fixed
Validity					
NotBefore		X		Certificate generation date/time	
NotAfter		X		Certificate generation date/time + 5 years	
Subject					
commonName	{ id-at-3 }	X		First name(s) + Surname	Dynamic
organizationName	{ id-at-10 }	X		Hauptverband österr. Sozialversicherungs.	Fixed
organizationalUnitName	{ id-at-11 }	X		VSig	Fixed
countryName	{ id-at-6 }	X		AT	Fixed
Public Key					
SubjectPublicKeyInfo	1.2.840.10045.2.1	X		EC public key	Fixed
SubjectPublicKeyInfo	1.2.840.10045.3.1.1	X		NIST P-192, X9.62 prime192v1	Fixed
Bit String		X		Public Key	Dynamic
Standard Extensions	OID	Include	Critical	Value	
subjectAltName	{id-ce 17}				
SubjectAltName				Email-Address	Optional
authorityKeyIdentifier	{id-ce 35}	X			
KeyIdentifier		X		0100 + last 60 Bit of SHA-1 of Public Key	Dynamic
subjectKeyIdentifier	{id-ce 14}	X			
KeyIdentifier		X		0100 + last 60 Bit of SHA-1 of Public Key	
KeyUsage	{id-ce 15}	X	TRUE		
digitalSignature		X		Set	Fixed
nonRepudiation		X		Set	Fixed
CertificatePolicies	{id-ce 32}	X		N/a	
policyIdentifier		X		1.2.40.0.10.1.4.1.102.0	Fixed
Private Extensions	OID	Include	Critical	Value	
autorityInfoAccess	{id-pe 1}	X			
accessMethod		X		OCSP	
AccessLocation		X		http://ocsp.ecard.sozialversicherung.at	Fixed

Bank Card Qualified Signature Certificate					
	OID	Include	Critical	Value	
Certificate					
Version				2 (Version 3)	
SerialNumber		X		Provided by CSP	Dynamic
Signature Algorithm	1.2.840.113549.1.1.5	X		SHA-1 with RSA Encryption	Fixed
Issuer distinguished name					
CountryName	{ id-at-6 }	X		AT	Fixed
organizationName	{ id-at-10 }	X		A-Trust Ges. f. Sicherheitssysteme im elektr. Datenverkehr GmbH	Fixed
organizationalUnit	{ id-at-11 }	X		a-sign-Premum-Sig-nn (nn varies)	Fixed

CommonName	{ id-at-3 }	X		a-sign-Premum-Sig-0X (nn varies)	Fixed
Validity					
NotBefore		X		Certificate generation date/time	
NotAfter		X		Certificate generation date/time + max. 5 years (currently + 4 years)	
Subject					
countryName	{ id-at-6 }	X		Country that issued the identity document (AT for Austria)	Fixed
commonName	{ id-at-3 }	X		First name + Surname or a pseudonym	Dynamic
Title	{ id-at-12 }	X		Title	Dynamic
Surname	{ id-at-4 }	X		Surname (if no pseudonym)	Dynamic
givenName	{ id-at-42 }	X		First name (if no pseudonym)	Dynamic
serialNumber	{ id-at-5 }	X		CIN number of signature card	Dynamic
Title	{ id-at-12 }	X		Title	Dynamic
organizationName	{ id-at-10 }	O		Optional: Organisation	Dynamic
organizationalUnitName	{ id-at-11 }	O		Optional: Unit	Dynamic
Public Key					
SubjectPublicKeyInfo	1.2.840.10045.2.1	X		EC public key	Fixed
SubjectPublicKeyInfo	1.2.840.10045.3.1.1	X		NIST P-192, X9.62 prime192v1	Fixed
Bit String		X		Public Key	Dynamic
Standard Extensions	OID	Include	Critical	Value	
authorityKeyIdentifier	{id-ce 35}	X			
KeyIdentifier		X		0100 + last 60 Bit of SHA-1 of Public Key	Dynamic
CertificatePolicies	{id-ce 32}	X		N/a	
policyIdentifier		X		OID 0.4.0.1456.1.1 ETSI: itu-t(0) identified-organization(4) etsi(0) qualified-certificate-policies(1456) policy-identifiers(1) qcp-public-with-sscd (1)	Fixed
CPSuri		X		qualifier http://www.a-trust.at/docs/cp/a-sign-Premium	Fixed
policyIdentifier		X		OID 1.2. 40.0.17.1.11 (A-Trust)	Fixed
CRLDistributionPoints	{id-ce 31}				
distributionPoint		X		ldap://ldap.a-trust.at/ou=a-sign-Premium-Sig-nn,o=A-Trust,c=AT?certificaterevocationlist?base?objectclass=eidCertificationAuthority (nn variable, see issuer CN / OU)	Fixed
subjectKeyIdentifier	{id-ce 14}	X			
KeyIdentifier		X		0100 + last 60 Bit of SHA-1 of Public Key	
keyUsage	{id-ce 15}	X	TRUE		
digitalSignature		X		Set	Fixed
nonRepudiation		X		Set	Fixed
subjectAltName	{id-ce 17}				
SubjectAltName		O		Optional RFC822-Name=Email-Address	Optional
basicContraints	{id-ce 19}	X			
CA		X		FALSE (End entity)	
pathLengthConstraints				None	
SubjectAltName	{id-ce 17}				
subjectAltName		O		RFC822-Name=Email-Address	Optional

subjectDirectoryAttributes	{id-ce 9}				
SubjectDirectoryAttributes		O		Date of Birth	Optional
Private Extensions	OID	Include	Critical	Value	
autorityInfoAccess	{id-pe 1}	X			
accessMethod	{ id-ad 2 }	X		calssuers	Fixed
AccessLocation		X		http://www.a-trust.at/certs/a-sign-Premium-Sig-nnx.crt (nn variable, see issuer CN / OU)	Fixed
accessMethod	{ id-ad 1 }	X		OCSP	Fixed
AccessLocation		X		http://ocsp.a-trust.at/ocsp	Fixed
Qualified Certificate					
qcStatements	{id-pe 3}	X	TRUE	Indicates qualified certificate (RFC3739)	Fixed
eGovernment OID					
	1.2.40.10.1.1.1	O		Indicates Austian public authority	Optional

A1 Mobile Phone Signature Certificate					
	OID	Include	Critical	Value	
Certificate					
Version				2 (Version 3)	
SerialNumber		X		Provided by CSP	Dynamic
Signature Algorithm	1.2.840.113549.1.1.5	X		SHA-1 with RSA Encryption	Fixed
Issuer distinguished name					
countryName	{ id-at-6 }	X		AT	Fixed
organizationName	{ id-at-10 }	X		mobilkom austria AG & Co KG	Fixed
organizationalUnit	{ id-at-11 }	X		A1.net	Fixed
commonName	{ id-at-3 }	X		A1 SIGNATUR	Fixed
Validity					
NotBefore		X		Certificate generation date/time	
NotAfter		X		Certificate generation date/time + currently 3 years	
Subject					
givenName	{ id-at-42 }	X		First name	Dynamic
Surname	{ id-at-4 }	X		Surname	Dynamic
commonName	{ id-at-3 }	X		First name + Surname	Dynamic
Public Key					
SubjectPublicKeyInfo	1.2.840.113549.1.1.1	X		rsaEncryption (2048 bit)	Fixed
Bit String		X		Public Key	Dynamic
Standard Extensions	OID	Include	Critical	Value	
keyUsage	{id-ce 15}	X	TRUE		
digitalSignature		X		Set	Fixed
nonRepudiation		X		Set	Fixed
basicContraints	{id-ce 19}	X	TRUE		
CA		X		FALSE (End entity)	
pathLengthConstraints				None	
subjectKeyIdentifier	{id-ce 14}	X			
KeyIdentifier		X		160-bit SHA-1 hash of subjectPublicKey	
CRLDistributionPoints	{id-ce 31}				

distributionPoint		X		http://www.A1.net/signatur/crl/currentcrl.crl	Fixed
authorityKeyIdentifier	{id-ce 35}	X			
KeyIdentifier		X		0100 + last 60 Bit of SHA-1 of Public Key	Dynamic

To integrate the citizen card into an application, i.e. to 'plug in' to the eIDM system, modules for online applications (MOAs) have been procured by the federal government and are made available for free to the public sector and the private sector in an open source program[25]. The 'MOAs' include modules for the identification process (MOA-ID), for electronic representation and mandates (MOA-ID+ and MOA-VV), for electronic delivery (MOA-ZS), and for server-side signature creation and signature validation (MOA-SS/SP).

Interoperability is provided by take-up of widely used standards. SAML is used for the identity link and during the identification and authentication process via MOA-ID. Access to the middleware is provided using HTTP. The electronic signatures follow XMLDsig or CMS.

3.3.4 Organisational aspects

Each resident in Austria – both Austrians and foreigners – is registered in the Central Register or Residents. Some exceptions exist such as under privileges and immunities of international organisations, which would need registration in the Supplementary Register for Natural Persons. Thus, the data basis for integration into the eIDM system exists for the vast majority of residents. Moreover, practically each resident possesses one token or several tokens (a bank card, a health insurance card, or a mobile phone) that can be activated as citizen card.

The activation process depends on the actual token used:

- Bank cards require the activation process for qualified certificates. Application for the certificate can be made via the Internet. Registration requires physical presence at a registration office (banks, notaries) and showing a photo ID.

- The health insurance card can either be activated via the Internet where identification is proven via a registered letter in a quality that requires showing a photo ID to the post official, or with physical presence at a registration officer (social insurance organisations).

- To register a mobile phone as citizen card, the application is made via the Internet. Registration requires physical presence at a registration office of the mobile phone service provider.

- Other tokens such as student service cards or public servant service cards can involve delegation of the registration officer duties to personnel departments or student offices.

[25] http://www.cio.gv.at/onlineservices/

All registration processes require identification of the applicant at a defined quality level and documentation by the issuer.

A primary source of the eIDM system is the Central Register of Residents that determines the data quality. The registration authorities (the mayors) have an obligation to maintain the data and to correct errors under the Registration Act (*Meldegesetz*).

3.4 Interoperability

Austria has considered access for non-nationals and interoperability in the design of the eIDM system from the beginning. Three options exist, depending on the residence of the entity and whether a foreign eID token is used:

- *Non-national with residence in Austria; Austrian eID*

  In this case, the entity is usually registered in the Central Register of Residents[26]. An Austrian eID can be activated. In practise, if having a residence in Austria the entity is likely to already possess either a health insurance card[27], a bank card or an Austrian mobile phone that can be activated as citizen card. If not, an SSCD that can be activated as citizen card can be purchased by the certification service provider A-Trust.

- *No residence in Austria; Austrian eID*

  In the case of non-nationals that do not have a residence in Austria or that do not fall under registration obligation, the entity can enrol to the Supplementary Register for Natural Persons. An Austrian eID can be activated than, such as an SSCD of the certification service provider A-Trust[28].

- *Using foreign eID tokens*

  A non-national may use his home-country's eID. At least smart card like foreign eID solutions can be integrated into Austrian citizen card concept the same way as the different Austrian smart cards (bank card, health insurance card, student cards, etc.). From a technical point of view, the integration into the Austrian eID middleware 'citizen card environment' has already been done for eID cards from Belgium, Estonia, Finland, and Italy. From the legal point of view, a regulation will clearly define which foreign eID cards are accepted.

Aside the integration of foreign tokens or allowing non-nationals to activate an Austrian citizen card, adhering to open standards such as SAML is considered to at least ease further interoperability steps. Lacking a widely agreed and proven European eID interoperability framework it remains to be seen whether that assumption and the chosen standards turn out fruitful.

---

[26] If the entity has a residence in Austria but no registration obligation, such as under privileges and immunities of international organisations, the case of an entity with no residence in Austria applies.

[27] If working in Austria or if for other reasons falling under Austrian compulsory health insurance

[28] Enrolment to the SRnP or registration of the qualified certificate requires showing identity documents, i.e. in practice personal presence in Austria at least once.

3.5 eIDM Applications

A multitude of applications use the citizen card concept. This includes private sector applications. Some of the applications can be used only with a citizen card, others allow for the citizen card in parallel to legacy and traditional identification and authentication approaches such as username/password or transaction numbers.

Listing all applications that support the citizen card is not possible. Many are on the regional and local level where, depending ion the region or commune, the service may not yet be offered. Thus a representative selection is given:

- *Applications that require a citizen card*
    - Electronic delivery that replaces registered letters[29]
    - Electronic certificate of enrolment (Central Register of Residents)[30]
    - Electronic Register of Convictions certificate[31]
    - E-Reporting certain crimes (child porn, repeat offence, ...)
- *Applications that support the citizen card (together with other methods)*
    - Tax declarations online (FinanzOnline)[32]
    - Several Internet banking solutions
    - Social security (statement of social security terms, application for premature retirement, …)[33]

3.6 Future trends/expectations

Given the already high penetration of tokens that a citizen may activate as a citizen card (bank cards, health insurance cards, mobile phones), together with the continuously increasing number of

[29] http://www.zustellung.gv.at

[30] https://meldung.cio.gv.at/egovMB/

[31] https://apps.egiz.gv.at/strafregister/

[32] https://finanzonline.bmf.gv.at/

[33] https://www.sozialversicherung.at/applikationen/

applications, an increasing number of citizens are expected to make use of these services. Even tough further tokens are expected as citizen cards, such as ministries issuing cards to their officials.

3.7 Assessment

3.7.1 Advantages:

- *Technology neutrality*:

  The approach of defining the citizen card on a high abstraction level has proven advantageous:

  - Technology steps have already been experienced which did not require changes in the approach an allowed of the co-existence of technologies. E.g., the first citizen cards have been RSA-based, the new generations use ECDSA
  - Solutions not thought of or known at the beginning could be integrated. I.e. integration of foreign eID tokens or mobile phones as citizen cards

- *Open specifications*

  Allow for adoption of the approach by the market

  - Three providers of citizen card environments so far (two client middleware software, the mobile phone solution)
  - Private sector application take-up, e.g. Internet banking portals
  - Different issuers of citizen cards also given the citizens a choice

- *Open source basic modules*

  Server side integration is supported by open source modules for online applications (MOAs) ease integration by communes or the private sector.

3.7.2 Disadvantages:

While no immediate disadvantage pops up, some argue that take up by the citizens has been below original expectations. A reason may be that relatively few government contacts – on average less than 2 per year – might not stimulate the use just for eGovernment, the given synergies with the private sector – Internet banking or eCommerce – may turn out fruitful.