eID Interoperability for PEGS

NATIONAL PROFILE GERMANY

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

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 German eGovernment applications.

Table of Contents

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

In Germany, the political debate about an eIDM system is still in an early stage. There are neither concrete plans for a comprehensive and integrated system nor the legal, technical and organizational preconditions for developing such a system in the near future. The basic policy aims at digitizing the existing means for the definition, authentication and administration of identities of German citizens, i.e. the registers of residence and the personal documents. Beyond its primary purpose of checking the identity of the holder in vis-à-vis communication, the Electronic Identity Card (*Personalausweis*), planned for being issued from 2008/2009 onwards, shall be used for online authentication in the front offices in all sectors of eGovernment and beyond. The citizens' registers of residence (*Melderegister*) which are run by local governments, the municipalities, according to new legislation, expected for 2009, will be integrated at state and federal level and be made accessible to the back offices of other government services at all levels.

The integration of the front office authentication with the back office authentication is not part of these plans. In particular, the present policy does not aim at a comprehensive and integrated eIDM system based on a unique personal identity number (ID) used on the digital token as well as in all or most sectors of government. The main argument against this option is the census decision (*Volkszählungsurteil*) of the Federal Constitutional Court (*Bundesverfassungsgericht*) of 1984 and its interpretation by the Federal Parliament (*Deutscher Bundestag*) that according to this sentence the constitution does not allow a unique personal identity number.

Instead, natural persons are identified by a combination of attributes such as first and family name and date and place of birth. In horizontally defined sectors of government such as tax administration, there are sector-specific IDs such as the number for the German pension insurance fund (*Sozialversicherungsnummer*) or the recently introduced Tax ID (*Steuernummer*). For some sectors, digital tokens are in the process of being introduced, in particular the Electronic Health Card.

Regarding digital signatures, Germany was the first member state in the European Union to pass legislation in 1997, which has since been adapted to the European directive in 2001. However, German signature cards are not suited for authentication because they only contain first name and family name of the holder and no additional relevant attributes such as the date of birth.

Foreign citizens are registered in the Central Register for Aliens (*Ausländerzentralregister, AZR*). They are identified by a unique register number, called AZR number, issued by the Central Register at the time of their first registration. The Federal Office for Migration and Refugees (*Bundesamt für Migration und Flüchtlinge)* is responsible for it. In technical respect, the register is operated by the Federal Office of Administration (*Bundesverwaltungsamt*).

There are several registers of companies. Most important are the Commercial Registers (*Handelsregister*), which are run by the Local Courts (*Amtsgerichte*). Every company has to meet disclosure requirements which are laid down in specific business regulations depending on the legal status of a legal entity. As a complement, the Companies Register (*Unternehmensregister*) was introduced in 2007 providing additional information, which has to be published in the Official Federal

Gazette. The database is run by a private entity, the Publisher of the Federal Gazette (*Bundesanzeiger Verlag*). As a link between companies information from "*Bundesanzeiger*" and "*Handelsregister*" an internal identifier is used (*UnternehmensID*). Recently first steps have been made to set up IDs for companies across sectors using the Business Identification Number and the Turnover Tax Identification Number.

3.2 Background and traditional identity resources

Germany is a Federal Republic made up of 16 states (*Länder*) which have their own legislative and executive governmental bodies. Within the federal system, the municipalities (*Städte, Gemeinden, Kreise*) are the lowest level in the three tier administrative structure after the federal government and the states. They have their own local self-government authority and are responsible for their own financial management. Most government services for citizens and business have to be offered by municipalities, most of them according to state law, only a few according to federal law.

The boundaries of legislative authority between state and federal level have been changed by a Federalism Reform Agreement between the Federal Government and the 16 State Prime Ministers in 2006. Among other things the legislative authority for civil registration has been shifted from the state to the federal level. Thus identity management is now an issue of the federal government, which has to seek agreement with the state governments and municipalities, which still have the authority for technical and organisational implementation of the law.

Therefore only federal eGovernment initiatives and the cooperation between the different levels of administration will be dealt with in this report.

3.2.1 Federal eGovernment Programmes

In 2000 the Federal Government started its "BundOnline 2005"[3] initiative, which came to an end as planned in December 2005. As one important result, 440 of the Federal Government's administrative services were made available online. In September 2006 the Federal Government passed the new programme "E-Government 2.0"[4]. The content and basic idea is in line with the EU eGovernment action plan as part of the i2010 initiative[5].

The programme aims to define the major strategic objectives in the area of eGovernment for the coming years until 2010. Four major action areas have been identified:

- Portfolio: enhancement of the federal eGovernment services in terms of quantity and quality;

[3] http://www.bundonline2005.de/

[4] http://www.staat-modern.de/Anlage/original_1070438/E-Governemt-2.0-Das-Programm-des-Bundes.pdf

[5] http://europa.eu.int/information_society/eeurope/i2010/index_en.htm

- Process chains: establishing electronic collaboration between the public administration and the business community utilising common business process chains;
- Identification: introduction of an electronic Identity Card (eID Card) and development of electronic identification concepts;
- Communication: development of a secure communication infrastructure for citizens, businesses and public administrations.

As one of four action fields, the issue of e-identity has a high priority in the federal eGovernment strategy. The new eID card shall replace the traditional paper-based identity card (*Personalausweis*) and become a universal token for authentication on the Internet, for eGovernment as well as for eBusiness. Additionally, certified citizens portals (*Bürgerportale*) shall enable secure and anonymous online communication and serve as identity providers.

3.2.2 National eGovernment cooperation and coordination

"Deutschland Online"[6] is the concerted eGovernment initiative of Federal Government, states and municipalities. It was passed by the Federal Government and the heads of government of the federal states in June 2003[7] and supplemented in June 2006 by the "Deutschland-Online action plan"[8].

Deutschland-Online provides the framework for cooperation between all administration layers, based on five priorities:
1. Development of integrated eServices for citizens and businesses
2. Interconnection of Internet portals
3. Development of common infrastructures
4. Development of common standards
5. Experience and knowledge transfer

The action plan is implemented by the conferences of government ministers, coordinated by the working group of the Secretaries of State for eGovernment. The Federal Ministry of the Interior (*Bundesministerium des Inneren, BMI*) coordinates the Federal Government's involvement in the action plan.

Within the organizational structure of Deutschland Online a standard for the exchange of data from citizens registers of residence (*Melderegister*), called XMeld, has been developed (see chapter C.3.4.).

---

[6] http://www.deutschland-online.de/

[7] http://www.deutschland-online.de/Downloads/Dokumente/DeutschlandOnline%20Teil%201%20Beschluss%20St-Runde%20160503.pdf

[8] http://www.deutschland-online.de/Pressemitteilungen/aktionsplan_deutschland_online.htm

3.2.3 Traditional identity resources

In Germany there is no unique personal identity number as a central identity resource. However, in the former German Democratic Republic there was a central civil register and a unique personal identity number. Both have been abandoned in the Unification Treaty. This is due to the preceding census decision (*Volkszählungsurteil*) of the Federal Constitutional Court (*Bundesverfassungsgericht*) of 1984 and its interpretation by the Federal Parliament (*Deutscher Bundestag*) that according to this sentence the constitution does not allow a unified personal identity number. Neither are there ID cards which can be used for identification and authentication purposes in eGovernment or eBusiness services today. However, the federal government plans to introduce an electronic ID card in 2008 or 2009 which may serve these purposes (more details s. chapter D.1.).

Besides the mandatory Identity Card (*Personalausweis*), there are several sector-specific identity resources, in particular the passport as a travel document, a social security number, a federal tax number and others as well as several registers. Most relevant for the issue of eIDM are the citizens registers of residence (*Melderegister)*, the civil status registers (*Personenstandsregister*), the central aliens register (*Ausländerzentralregister*) and the business register (*Unternehmensregister*).

Personal Identity Card

In Germany every citizen aged 16 or older is obliged to have an Identity Card (*Personalausweis*). About 60 million paper-based cards have been issued. Since 1987, the German ID Card is issued in the ID-2-format (74 mm × 105 mm). The frontside contains a foto and a signature of the holder as well as name, first names, date and place of birth and a serial document number and the date of expiry. Name, first names, date of birth, document number and the date of expiry are repeated in machine-readable form in the two bottom lines of the document, which are used for border and police controls only.

The backside contains the residential address, the height and eye colour of the holder as well as the authority and date of issue. Therefore, when the residential address has changed, a sticker with the new data is applied to the document.

German Identity Cards are issued by the municipality of the residence of the holder, but they are centrally produced by the Federal Printing Office (*Bundesdruckerei*). Stickers containing changed address data are produced locally and vary in size, typeface and quality. The first card is provided free of charge and valid for ten years. For renewal, a fee of 13 EUR is charged.

The document number is a unique serial number, which in fact constitutes a unique personal identity number. But according to § 3 Identity Card Act, it is explicitly forbidden to use this document number for accessing personal data in files or for linking data in different files. The special machine-readable code is technically not suited for online authentication. But this will change, when the present paper-based ID card will be substituted by a digital ID card from 2008 or 2009 onwards (see chapter D.1.)

Passport

In addition German citizens may apply for a passport, which is used most of all as a travel document into countries which do not acknowledge the German Identity Card for authentication at their borders. About 30 million German citizens possess a passport. Since November 2005 the paper-based passports are being gradually exchanged for a new digital passport (*Elektronischer Reisepass, ePass*).

This document looks very much the same as the old one, but in accordance with European Directive 2252/2004 it also contains an RFID chip with digital personal data, a digital photo of the face of the owner and from 2007 on also two digitized finger prints of the owner.

The fee for an electronic passport is 59 EUR for persons aged over 26 years, valid for 10 years, and 37.50 EUR for people under 26, valid for 5 years. Old and new passports carry a serial document number, which according to § 16 Passport Act (*Paßgesetz*) may not be used for the access to or the linking of personal data.

Thus the digital passport does not contain any function for online authentication beyond border controls, and therefore it is not part of an eIDM system. But is has to be mentioned as it sets standards for the use of biometric identifiers.

Sector specific identifiers

For natural persons in Germany there are several sector-specific identifiers, which are not systematically linked. Most relevant are the number for the pension insurance fund, the health insurance number, ID for draftees, customer number (Federal Labour Agency) and most recently the federal tax ID number which has been introduced in 2007 and shall be issued and assigned to natural persons by birth.

Citizens registers of residence

The civil registers of residence (*Melderegister*) in Germany are run by the local municipalities. There are more than 5,000 local registration offices.

Until 2006, data processing was regulated by state law based on a federal frame law (*Melderechtsrahmengesetz*). In 2006, legal authority was shifted to the federal level within a larger Federalism Reform. The Federal Ministry of the Interior is at present preparing a Federal Registration Act (*Bundesmeldegesetz*). The Act is expected for 2009 and will substitute the present federal frame act as well as the 16 state acts on citizens' registration. The Ministry of the Interior has set up a working group including representatives of some states and municipalities to elaborate the details

which will have to be regulated in the act. It most likely will lead to a Federal Civil Register (*Bundesmelderegister*), which has to be fed by the local registers. This central register will play an important role in the identification processes with many other government units at all levels. But details have not yet been published.

It is not expected, that the range of data of the registers will change.

According to § 2 Citizens Register Frame Act (Melderechtsrahmengesetz, MRRG) the following data are currently registered:

- family name,
- previous names,
- first names,
- doctoral degree,
- order name/stage name,
- date and place of birth,
- sex,
- legal representative (first and family name, doctoral degree, address, date of birth, date of death),
- citizenship,
- legal membership of a religious community,
- present and earlier addresses, main and ancillary residential home, when moving from abroad, also the last former inland address,
- date of moving in and out,
- family status, with married couples or partners additionally date and place of marriage or establishment of the life partnership,
- spouse or partner (first and family name, doctoral degree, date of birth, address, date of death),
- minor children (first and family name, date of birth, date of death),
- issuing authority, date of issuing, validity period and serial number of identity card/passport,
- blocking of communication,
- place and date of death.

Moreover, § 2 clause 2 MRRG allows the storage of further data for special purposes, e.g., for the preparation of elections. These special data, however, are not relevant for eIDM.

State law on civil registers of residence may allow the collection of additional data and procedural provisions. Most states allow the registration authorities to assign reference numbers in the register. These may only be used for special purposes and not as unique personal IDs. This is not possible, anyway, because each registration authority can assign their own ID numbers.

The most important attributes for identifying a natural person in the register of a local authority are family name, first name, date and place of birth. Experts estimate that 95% of natural persons can be found in the citizens registers by these data.

Registration data have to be exchanged between the local registers in case of moving. And many governmental and private organizations are entitled to request registration confirmations (*Melderegisterauskünfte*). The Federal Directive for the interchange of registration data

(*Bundesmeldedatenübermittlungsverordnung*), based on the Citizens Registration Frame Act has recently been revised and a data exchange format (XMeld) has been made mandatory for all registration offices. They may keep their different software systems, but by adding a special interface these have to be able to import and export data according to the XMeld standard.

The standard is based on the more general interchange standard OSCI (Online Services Computer Interface) recommended for data interchange between German government units and included in the List of Standards, SAGA (Standards and Architectures for eGovernment Applications)[9]. OSCI deals with security features and is complemented by different sector-specific message families using the XML data exchange format and therefore are called XöV. „XöV" is an abbreviation for the use of XML in the German public administration (*Öffentliche Verwaltung*). XMeld includes a number of data sets for messages such as confirmation of new address after moving (*Rückmeldung*), registration request, and confirmation of a registration request.

The shift of the legislative authority for civil registers to the federal level will probably lead to a central register and make most of the direct interchange of register data between the local registers obsolete. But it is most likely that XMeld will still be used for interchange between central and local registers and the interchange with third parties.

Civil status registers

In Germany, the registration data of residence and the data on the civil status are not stored together, although the local authorities are responsible for both. Normally the city's registrar in the civil status office (*Standesamt*) is responsible for recording births, marriages and deaths. For data interchange between offices, a combination of the following attributes is used: name of office, name of civil status register (*Personenstandsbuch*) and entry number.

Until now, civil registration in Germany still depends on paper as storage medium for register entries. In February 2007 a new law was passed that marks a paradigm shift for data storage in civil status offices. The new Personal Status Law (*Personenstandsgesetz*) allows data storage in electronic form in civil status registers (*Personenstandsregister*) as of January 2009. Still there are no advanced plans for electronic identity management in civil registration.

Central Register for Aliens

Person-related data of foreign citizens are stored in the Central Aliens Register (*Ausländerzentralregister, AZR*). The Federal Office for Migration and Refugees (*Bundesamt für Migration und Flüchtlinge)* is responsible for it. In technical respect, the register is operated by the Federal Office of Administration (*Bundesverwaltungsamt*).

9 http://www.kbst.bund.de/cln_046/nn_837392/SharedDocs/Anlagen-kbst/Saga/saga__3__0__en.html__nnn=true

The register contains person-related data of foreigners:

- who are resident in Germany on a non-temporary basis,
- who have submitted an asylum application,
- for whom residence-related decisions have been taken,
- where there are objections against entry, or
- where other conditions specified in the act on the central register for foreigners are fulfilled.

The data are mostly supplied by the aliens registration offices, police, public prosecution authorities and other authorities. Some of these can directly transmit and change the data. The registration authority, in turn, transfers data to the aliens registration offices, the federal police, the enforcement agencies of the police, public prosecution authorities and further agencies who need these person-related data to fulfil their legal tasks like the customs authorities, the Federal Agency of Labour or organisations of social welfare. When exchanging person-related data, the AZR number is used as an identifier. It is assigned by the registration authority.

In summary, the central register for aliens can be understood as the identity provider for all people affected by the foreigners administration on behalf of the authorities responsible for the foreigners administration and further authorities such as the Federal Agency of Labour or organisations of social welfare.

Business registers

Public administration in Germany keeps a number of registers with business-related data:

- Basic information about every registered company in Germany can be found in the Commercial Register (*Handelsregister*). Responsible for those registers are the Local Courts (*Amtsgerichte*). Every company has to meet disclosure requirements which are laid down in specific business regulations depending on the legal status of a legal entity.[10] Since January 2007 the data of the Commercial Register is stored and administrated in electronic form.[11]
- As a complement to the Commercial Register, the Companies Register (*Unternehmensregister*) was introduced in 2007. The database is run by a private entity (*Bundesanzeiger Verlag*). The purpose of this register is mainly to disseminate information from the electronic *Handelsregister* and to combine it with data from the electronic Federal gazette (*Bundesanzeiger*), where further required disclosures are published. Basic information from the companies register is available free of charge on the Internet.[12] As a connective link between companies information from *Bundesanzeiger* and *Handelsregister* an internal identifier is used (*UnternehmensID*).

[10] http://www.handelsregister.de

[11] http://www.handelsregister.de

[12] http://www.unternehmensregister.de

- Local governments additionally run trade registers (Gewerberegister) within their offices of trade inspection (Gewerbeamt). They are not used for identification purposes.

As for natural persons, in Germany there are a number of sector-specific IDs, but no uniform ID for companies. A first test case for the introduction of a unique identifier for companies to be used by trade offices (*Wirtschaftsnummer-Erprobungsgesetz*, *Bundesgesetzblatt* I, p. 1644, 2002-05-22) in Bavaria showed that – regarding the given circumstances in 2002/2003 – there were no obvious advantages without a reform of the entire legal framework for business registration.

Nevertheless, first steps towards such a reform have recently been made including IDs for companies across sectors. Examples are the Business Identification Number and the Turnover Tax Identification Number.

The Business Identification Number according to the Tax Code (§ 139c *Abgabenordnung*, AO) shall serve for the identification of commercially active corporate bodies for their communication with the tax authorities and for the administration of tax data. However, a date of implementation has not yet been fixed. According to § 139c, clause 7 AO, using this number in other sectors is not excluded, if a legal basis exists.

Each company who wants to take part in the goods traffic of the European Union, i.e. to supply or purchase goods in the territory of the European Union, needs a so-called Turnover Tax Identification Number (§ 27a UStG). The Central Federal Tax Office (BZSt) assigns this number on application. According to § 5 clause 1 no. 6 TMG in connection with service provision, providers of tele-services have to publish their business number and their turnover tax identification number, if available.

3.3 eIDM framework

3.3.1 Main eGovernment policies with regard to eIDM

In Germany, the political debate about an electronic Identity Management System for German citizens is still in an early stage. There are neither concrete plans for a comprehensive and integrated system nor the legal, technical and organisational preconditions for developing such a system in the near future. The basic policy aims at digitizing the existing means for the definition, authentication and administration of identities of German citizens, i.e. the civil registers and the personal documents.

eCard strategy and eID Card

As described in the previous sections, eID cards do not currently exist in Germany. The Federal Government passed an eCard strategy in a cabinet decision on 9th March 2005. The aim of the strategy is to coordinate the projects carried out by different federal ministries. This mainly concerns the electronic passport (*ePass*), and the electronic health card and the electronic identity card (*ePA*).

The new electronic passport, as described in section C.3.1, includes a chip with some personal data including biometric data. But it is not intended for use in electronic communication beyond border control.

The Federal Ministry of Health (*Bundesministerium für Gesundheit)* is responsible for the electronic health card. To identify the patient, the card shall be provided with a photo. Optionally, an electronic signature shall also be possible. The electronic health card is intended to facilitate processes in the health system and to make the patient data digitally available to the physician. For this purpose, physicians shall authenticate themselves by their electronic signature on a special chip card, the Health Professionals Card.

The new eID Card (*elektronischer Personalausweis,* ePA) shall be used for visual inspection and, in addition, for universal identification and authentication on the Internet for eGovernment and eCommerce services[13]. For this purpose, features for electronic authentication and for digital signatures will be implemented. The chip on the card will contain the same information which is printed on the card today. The chip will also contain certificates to prove these data. Data from the chip can only be read if the holder agrees by entering a PIN beforehand.[14] As the card shall be used for authentication in the private sector as well, and because in different contexts different parts of the total data are necessary, there will be a function to allow the holder to control which data can be read in a specific situation[15]. For example, when an age control is required, only the data from the age field can be read.[16]

As with the Digital Passport already issued, biometric attributes, a digitized picture of the face as well as finger prints will most likely be included as well. The Ministry of the Interior emphasizes that because of the extended range of authentication in all sectors the security requirements have increased and should not be lower than for the travel document passport. In addition, the same technical infrastructure and equipment could be used for passports and identity cards which are often used as travel documents at border controls, e.g., within the European Union.

However, the complete range of functions and the set of data to be included in the chip have not yet been published. And there is still no draft for the revision of the Personal Identity Card Act (*Personalausweisgesetz*). Accordingly, the fee for the digital ID card has not yet been fixed. It is likely to be between the fee for the present paper-based card of 13 EUR and the fee for the electronic passport of 59 EUR.

Citizens' portals

[13] cf. http://www.bmwi.de/BMWi/Navigation/Presse/pressemitteilungen,did=60006.html

[14] s. Engel, Christian (2006): Auf dem Weg zum elektronischen Personalausweis. In: *Datenschutz und Datensicherheit* 30 (2006) 4, p. 209

[15] ibid.

[16] ibid.

Citizens' portals (*Bürgerportale*) may become a further relevant component in the German Identity Management System. The term is misleading as one might expect a one-stop portal for citizens' access to government services. But according to the E-Government 2.0 Programme, the Federal Government is planning quite the opposite: Portals integrating identity data of citizens and providing authentication services.

At present, basic ideas have been published[17] and tenders for feasibility studies are about to be launched early in April 2007. The following description is therefore preliminary.

Citizens' portals are intended to offer citizens a fixed space on the Internet. The Federal Ministry of the Interior conceives them as a bundle of online services with costs which shall be offered by certified providers such as the big portals, e.g., T-Online, or today's Free-Mail providers. Citizen shall be registered with the provider of their choice. The provider is obliged to check the identity of the citizen through the citizens register of residence, and to store certain attributes which are required for unambiguous identification (first name, surname, date of birth, address, etc.). If the new electronic identity card is used, the citizen can register online, otherwise they have to register in person and show their ID card.

Citizens' portals shall fulfil different functions:

As an authentication service, they shall play the role of a trustworthy third party (TTP) and confirm respectively make verifiable the identity of a citizen in electronic communication.

As a communication gateway, they shall provide citizens, in addition to their officially registered address in the real world, also with an officially registered address on the Internet, and thus will result in an increased reliability for sender and recipient of a message. The appearance of the address shall already indicate that the message was sent from a citizens' portal. Then the recipient can be quite sure that the address of the sender is correct. Vice versa, registered citizens will be provided with an electronic post box, which allows them to receive signed documents with a confirmation of receipt. There will be three security levels: the highest level is reached by documents signed with qualified digital signatures or with successful authentication of acknowledged tokens such as the eID Card. On the medium level there are documents which come from another account on a citizen portal. Any other document is assigned to the lowest security level. Currently, there are considerations whether the address of the postbox on the citizens' portal should be stored on the new identity card as an "electronic register address". Corporate bodies shall also be able to use this service. In this case the postboxes will be called "organisation postboxes". A company may declare several natural persons as authorized representatives, who may jointly access the postbox.

As a data safe, citizens' portals shall provide a safe storage place for important documents. By special services, the readability of file formats as well as the validity of electronic signatures shall be ensured. Moreover, the citizen shall be enabled to allow third parties the access to certain records and certificates which he has stored on the citizens portal.

[17] Stach, Heike (2007): Bürger-Portale: Für eine sichere und verbindliche Präsenz von Bürgerinnen und Bürgern im Internet. In: Zechner, Achim (ed.): Handbuch E-Government. Strategien, Lösungen und Wirtschaftlichkeit.Stuttgart, pp. 155-163.

The idea of citizens' portals represents a new way of identity management in electronic communication, supplementary to the usual eID cards. The Ministry of the Interior emphasizes the relevance of these portals for the further diffusion of eGovernment services, not only for authentication purposes but, equally important, for the receipt of electronic documents. eGovernment is not complete when at the end of a process documents are printed and sent by ordinary mail. To registered citizens, e.g., notifications of an authority could be sent electronically in digital form. Therefore the Ministry is interested in a high registration rate. Under the present privacy legislation this cannot be reached by making the registration mandatory. Rather it will be voluntary and users agree individually with the storage and processing of their personal data according to the rules of the portal. By getting private business on board, the Ministry is trying to make these portals as attractive as possible.

3.3.2 Legal framework

The most important legal provisions with regard to IDM have been mentioned in the previous sections:

- Design and use of identity card and passport are regulated in the Identity Card Act and the Passport Act. If these documents are to be designed differently, for example, in order to be able to use them for electronic communication, these acts will have to be changed correspondingly.
- The authorities responsible for the identity cards keep records on identity cards (§ 2a of the Identity Card Act). Among others, these local registers issue the identity cards and verify their authenticity. A nation-wide data file will not be established.
- The passport register is regulated parallelly (§ 21 Passport Act). The passport register is kept by the passport authorities who issue passports and verify their authenticity, the identity of the person who owns the passport or for whom it has been issued, and who executes passport law.
- The civil registers of residence are currently regulated by the Citizens Register Frame Act, which is complemented resp. concretised by state law. The reform of the German federalism passed by the Federal Parliament and the Federal Council in 2006 redistributes the legislative authority among the federal government and the state governments. It has come into effect on 1 September 2006. Among others, a change of the constitution (Art. 73 Abs. 1 Nr. 3 GG) enables the Federal Government to issue a common registration act. This law will certainly not be enacted before 2009.
- The civil status registers are regulated by the Personal Status Law, which now also allows the electronic storage of these data.
- The Central Register for Aliens is based on an ordinance passed by the Allied Countries. After the census sentence (s. below), a legal basis for the practice of keeping records with the Federal Administration Office was created by passing the Central Register for Foreigners Act. Since 2001, when fighting terrorism became more relevant, the Central Foreigners Register was extended to a comprehensive information system and networked with the administrative intelligence services.
- The statutory basis for commercial registers and company registers are laid down in § 8 and § 8b of the Commercial Code (Handelsgesetzbuch).

Federal Constitutional Court, judgement on census

Every law has to comply with the principles regarding the protection of the basic right to informational self-determination which the Federal Constitutional Court laid down in its judgement on census in 1983.

Late in 1983, the Federal Constitutional Court deduced the right to informational self-determination (BverfGE65, 1: census) from Article 2 in conjunction with Article 1 subsection 1 GG (constitution). This "census decision" is generally opposed to introducing a uniform personal code number or a central register which the authorities can use.

Closure of the Central Residents Register of the GDR / Cancellation of the Personal Code Numbers by the Unification Treaty

Also the decision for the closure of the Central Residents Register of the GDR after the accession of the new German states argues against central personal databases and personal code numbers for the whole of Germany. The corresponding section of the Unification Treaty (Anlage I Kap. II Sachgeb. C Abschn. III, BGBl. II 1990, S. 889, 918, dort 4. c) aa) was attached to the Citizens Register Frame Act as Appendix EV.

Special Standards on Data Storage, Data Exchange and IDs

The 2003 tax amendment act of 15 Dec. 2003 introduced an unambiguous identification number for each taxable person in order to enable clear identification for tax procedures (§ 129b tax code). The nation-wide identification number replaces the income tax number eTIN. It is stored in the residents register.

Each company that wants to take part in the goods traffic of the European Union, i.e. to supply or purchase goods on the territory of the European Union, needs a so-called Turnover Tax Identification Number (§27a Turnover Tax Act, *Umsatzsteuergesetz*, UStG). The Central Federal Tax Office (*Bundeszentralamt für Steuern*) assigns this number on application.

The business identification number (§ 139c Tax Code, *Abgabenordnung*, AO) shall identify legal entities engaged in business during their contact with the finance authorities and for the administration of tax data. The date of implementation has not yet been fixed.

Thus the intention is that for the time being both identification numbers for legal entities are used for purposes of finance and tax administration.

According to § 139c subsection 7 AO, their use in other sectors has not been excluded, if a legal basis exists.

According to § 5 subsection 1 No. 6 Tele Media Act (*Telemediengesetz*, TMG) providers of tele-services have to publish their business and turnover tax identification numbers in connection with their service provision, if applicable.

Signature Act

In Germany, regulations on electronic signatures are mainly to be found in the Signature Act (SigG dated 16 May 2001, BGBl. I dated 21 May 2001, p. 876).

Administrative Procedures Law: The federal and state administrative procedure law stipulates that, in administrative procedures, the written form can be replaced by qualified electronic signatures according to the signature act (e.g., § 3a subsection 2 of the Federal Administrative Procedures Act).

Replacement of the written form in the civil code: for private law, § 126a Civil Code (*Bürgerliches Gesetzbuch*, BGB) regulates that the statutory written form can be replaced by the electronic form if the qualified electronic signature according to the signature act is applied.

Although there are regulations on electronic signatures in Germany already since 1997 (however, the signature act of 22 July 1997 spoke of "digital" signatures), this technology is still hardly used (see for example the late "Report on the Application of Directive 1999/93/EG on common framework conditions for electronic signatures" according to Art. 12 of the directive 1999/93/EG, KOM(2006) 120 fin. 15 March 2006).

Identification and Authentication

According to § 2 SigG German law differentiates between identification and authentication: "In the sense of this law

1. "electronic signatures" are data in electronic form which are attached to or logically linked with other electronic data and which serve for authentification;

2. "advanced electronic signatures" are electronic signatures according to 1. which

a) are assigned solely to the holder of the signature key,

b) enable the identification of the holder of the signature key ..."

During identification (2.b), a reference to personal characteristics is made which is not required for authentification. Also a pseudonymous or anonymous authentification is possible as long as it is ensured that the information comes from a determined sender and is not changed on the transmission route.

Data Protection Issues

For data processing by public authorities, the Federal Data Protection Act (*Bundesdatenschutzgesetz*) stipulates the following principles: legal reservation, limitation of use to specific circumstances and data reduction and data economy. This means that it has to be guaranteed that only data are collected or used, which are necessary and which are permitted by the law.

Representation of legal entities

Legal entities such as limited liability companies or public companies are capable of acting only through their managers resp. their managing board. §164 et seqq. of the Civil Code and other regulations specific for the legal form (GmbHG, AktG, etc.) apply.

3.3.3 Technical aspects

The technical details of the components of the German eIDM infrastructure (eID Card and citizens' portals) known so far are described in chapter D.1. Further information on the technical implementation is currently not available.

3.3.4 Organisational aspects

The organisational details concerning the components of the German eIDM infrastructure (eID Card and citizens' portals) known so far are described in chapter D.1. Further information on the organisational implementation is currently not available.

3.4 Interoperability

The most important resource for the identity of the citizens are the 4,000 local citizens registers of residence. As described in section C 3.4, interoperability between the local registers has been achieved by making the data exchange format X-Meld mandatory.

The digital personal identity card scheduled for 2008/2009 shall serve as a universal token for authentication. Questions of interoperability mainly concern transborder usage. As there are no concrete technical specifications available, interoperability on the different levels cannot yet be assessed. However, in presentations of the plans and in EU working groups, people responsible for this project in the Federal Ministry of the Interior (*Bundesministerium des Innern*) stress that technical specifications will be in line with CEN and ISO standards and that they aim for pan-European interoperability on the application layer as well. The BMI takes part in the ad hoc group for eIdentity within the eGovernment Expert Group. The Procurement Office within the Federal Ministry of the Interior participates in a pilot application for interoperability in transborder e-procurement within the GUIDE project. Further, the Ministry is considering joining the consortium for the Large-Scale Pilot for interoperable eIDM.

The goals are in line with the eIDM roadmap, which aims for a federated structure with mutual recognition of the different technical systems.

3.5 eIDM Applications

As there is no nation-wide eIDM system so far, there are no applications either.

However, there is one regional application in the city and state of Hamburg, the Hamburg Gateway, which should be mentioned.[18] As many other large cities, the Free and Hanseatic City of Hamburg offers a wide range of online services. Hamburg Gateway is a one-stop access point to these services and offers a central authentification for registered citizens. The lower security level one can be achieved by online registration with user name and password. Security level two requires registration in person at any of the decentralized customer centers, based on the presentation of the personal identity card. Authentication on level two is also carried out by user name and password. In November 2006, 60,000 citizens were registered on security level one, only 840 on security level two.

In any case, this system will only be temporary; it will switch to the digital identity card when it is introduced in 2008/2009.

3.6 Future trends/expectations

Plans and trends for registers and identity cards have been described in the preceding sections.

An issue to be mentioned here is the implementation of Article 8 of the Services Directive (2006/123/EC). Member states shall provide single contact points where service providers can electronically complete all requirements and procedures for registering in that country. Given the federal structure of the German government, it is not yet decided whether there will be single points of contact on the state level or on the national level as well. At the national level, the Ministry of Economic Affairs and the Ministry of the Interior are currently clarifying their authority and discussing with the respective state ministries in parallel.

3.7 Assessment

Given the early stage of development of eIDM in Germany, an evaluation of the planned evolutions is not yet possible.

[18] There is an extensive case description which has been produced as part of the MODINIS study on interoperability at local and regional level, available at http://www.egov-goodpractice.eu/download.php?&fileid=1084.