Electronic Signature Laws, PKI Projects and Time Stamping Technology in the European Union and Germany

Survey on the current status of Electronic Signature Laws, PKI Projects and Time Stamping in the EU and Germany

February 2005

INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN
Table of Contents

Table of Contents

1
1.1
2
2.1
2.1.1
2.1.2
2.1.3
2.1.4
2.1.5
2.1.6
2.2
2.3
2.4
3
3.1
3.2
3.3
3.4
3.4.1
3.4.2
3.4.3
3.5
3.5.1
3.5.2
3.5.3
3.6
3.6.1
3.6.2
3.6.3
3.6.4
3.6.5
3.7
3.8
Introduction
Document Purpose
Electronic Signature Law in Europe
Legal Framework
EU Directive on Electronic Signatures
EU Directive on electronic commerce
Minimum criteria to be taken into account
Directive on privacy and electronic communications
Publication of reference numbers
Scanned Documents
Legal and Market Aspects of Electronic Signatures
References
Related Links
Active PKI Projects in Europe
Non-regulated Electronic Signatures
Standardization
European Council Projects
E-Health Care Projects
European Challenges
Example: “Health On the Net”, the Winner of the eEurope Awards for eHealth 2004
Example: The Austrian eHealth card “e-card”
E-Business Projects
Example: e-BSN, the European e-Business Policies Portal
Example: e-Business W@tch, Analysing e-Business at the Sectoral Level
Example: eMarket Services, a Guide to Electronic Marketplaces
E-Government Projects
Example: The Austrian Citizen Card
Identity Cards Europe-wide
Example: Government Gateway in the United Kingdom
Example: Media@Komm-Transfer
Example: Electronic Marketplace - Czech Republic
E-Learning Projects
References and Related Links
4 Electronic Signatures Law in Germany
   4.1 Overview of Current Status of Legislation 19
   4.2 Main Changes of the Electronic Signatures Law 19
   4.3 Main Issues of the German Electronic Signatures Law 20
   4.3.1 General Objectives, Related Laws and Structure of the Signature Law 20
   4.3.2 Requirements for the Competent Authority 22
   4.3.3 Requirements for Certification Service Providers 25
   4.3.4 Requirements for Electronic Signature Products 34
   4.3.5 Requirements for Testing and Confirmation Offices 37
   4.4 References 40
5 Active PKI Projects in Germany 41
   5.1 E-Government Projects 41
   5.1.1 BundOnline 2005 41
   5.1.2 Administration PKI 42
   5.1.3 Service Provider Regulatory Authority for Telecommunications and Post (RegTP) 43
   5.2 E-Health Care Projects 43
   5.2.1 Overview 43
   5.2.2 Pilot Project to advance health professional cards for physicians in Sachsen (Germany) 44
   5.3 Public Key Infrastructures inside of Enterprises 44
   5.4 Joint Projects 45
   5.4.1 European Bridge-CA 45
   5.4.2 The Signature Alliance 45
   5.5 Research and Standardization 46
   5.5.1 ArchiSig / ArchiSoft 46
   5.5.2 TransiDoc 46
   5.6 References and Related Links 47
6 About Electronically Stored Documents in Germany 48
   6.1 Typical or important clauses 51
7 Conclusions about Signature Laws and PKI-Projects in Europe and Germany 52
8 Additional Information about Signature Laws and PKI-Projects in Europe and Germany 54
   8.1 List of Certificates in the EBCA TrustList 54
   8.2 List of Members of the Signature Alliance 55
   8.3 Comparison of the Definitions of Terms 56
   8.4 Comparison of Requirements for Qualified Certificates 59
   8.5 Electronic-to-Electronic and Paper-to-Electronic Document Transformations in Germany 60
   8.6 URLs Related to Legal Aspects of Document Transformation 71
## 8.6. URLs

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.6.1</td>
<td>URLs concerning European Law</td>
<td>71</td>
</tr>
<tr>
<td>8.6.2</td>
<td>URLs concerning taxes</td>
<td>72</td>
</tr>
<tr>
<td>8.6.3</td>
<td>URLs concerning insurances</td>
<td>74</td>
</tr>
<tr>
<td>8.6.4</td>
<td>URLs concerning Company Law</td>
<td>75</td>
</tr>
<tr>
<td>8.6.5</td>
<td>URLs concerning common Private Documents</td>
<td>75</td>
</tr>
<tr>
<td>8.6.6</td>
<td>URLs concerning Public Law</td>
<td>77</td>
</tr>
<tr>
<td>8.6.7</td>
<td>URLs concerning Electronic Signatures</td>
<td>78</td>
</tr>
<tr>
<td>8.6.8</td>
<td>URLs concerning Procedure Law</td>
<td>78</td>
</tr>
</tbody>
</table>

## 9 Adoption of the Qualified Certificate Profile in Germany

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.1</td>
<td>Relevant Documents</td>
<td>80</td>
</tr>
<tr>
<td>9.2</td>
<td>Profiling Structure</td>
<td>80</td>
</tr>
</tbody>
</table>

## 10 Technical Review

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1</td>
<td>Liaison between ETSI and IETF</td>
<td>83</td>
</tr>
<tr>
<td>10.2</td>
<td>Main Concepts of [RFC 3739]</td>
<td>83</td>
</tr>
<tr>
<td>10.2.1</td>
<td>Scope and Main Goal</td>
<td>83</td>
</tr>
<tr>
<td>10.2.2</td>
<td>Meaning of Qualified Certificate</td>
<td>83</td>
</tr>
<tr>
<td>10.2.3</td>
<td>Support of Qualified Certificates</td>
<td>84</td>
</tr>
<tr>
<td>10.2.4</td>
<td>Properties and Indication of Qualified Certificates</td>
<td>84</td>
</tr>
<tr>
<td>10.2.5</td>
<td>Identification of Certification Authorities</td>
<td>84</td>
</tr>
<tr>
<td>10.2.6</td>
<td>Identification of Natural Person</td>
<td>85</td>
</tr>
<tr>
<td>10.2.7</td>
<td>Additional Attributes of Natural Person</td>
<td>86</td>
</tr>
<tr>
<td>10.2.8</td>
<td>Key Usage</td>
<td>86</td>
</tr>
<tr>
<td>10.2.9</td>
<td>Biometric Information</td>
<td>86</td>
</tr>
<tr>
<td>10.2.10</td>
<td>Certificate Policies and Qualified Certificate Statements</td>
<td>87</td>
</tr>
</tbody>
</table>

## 11 Adoption of Qualified Certificates in the German Federal Government

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>11.1</td>
<td>Laws Supporting Electronic Signatures Based on Qualified Certificates</td>
<td>89</td>
</tr>
<tr>
<td>11.1.1</td>
<td>Overview of Relevant Laws</td>
<td>89</td>
</tr>
<tr>
<td>11.1.2</td>
<td>Laws for Forms of Documents</td>
<td>90</td>
</tr>
<tr>
<td>11.1.3</td>
<td>Tax Law</td>
<td>91</td>
</tr>
<tr>
<td>11.1.4</td>
<td>Health Care Law</td>
<td>92</td>
</tr>
<tr>
<td>11.2</td>
<td>Technical Base Standards Supporting Electronic Signatures Based on Qualified Certificates</td>
<td>92</td>
</tr>
<tr>
<td>11.2.1</td>
<td>Standards and Architectures</td>
<td>92</td>
</tr>
<tr>
<td>11.2.2</td>
<td>Specifications for Interoperable PKI Applications</td>
<td>92</td>
</tr>
<tr>
<td>11.2.3</td>
<td>Signature Card API</td>
<td>92</td>
</tr>
<tr>
<td>11.3</td>
<td>PKI-Projects and Applications Supporting Electronic Signatures Based on Qualified Certificates</td>
<td>93</td>
</tr>
</tbody>
</table>

## 12 Surveys on Practical Time Stamp Requirements

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>12</td>
<td>Surveys on Practical Time Stamp Requirements</td>
<td>94</td>
</tr>
</tbody>
</table>

## 13 Interview of Federal Government Ministries and Agencies

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>13</td>
<td>Interview of Federal Government Ministries and Agencies</td>
<td>94</td>
</tr>
</tbody>
</table>
13.1 Questions Asked to Federal Government Ministries and Agencies 94
13.2 Overview of Contacted Ministries and Agencies 97
13.3 Summary and Interpretation of Received Answers 98

14 Interview of Leading Time Stamp Vendors and Service Providers 104
14.1 Questions Asked to Leading Time Stamp Vendors and Service Providers 104
14.2 Overview of Contacted Time Stamp Vendors and Certification Service Providers 105
14.3 Summary and Interpretation of Received Answers 106

15 General Information about AuthentiDate 110

16 Time Stamp Solutions 111
16.1 OEM Time Stamp Products 111
16.2 Time Stamp Server 112

17 Functionality of the eTimestamp Module 112

18 Explanation of the “ArchiSig Project” 113

19 Abbreviations and Acronyms 116

20 References 117
1 Introduction

1.1 Document Purpose

This document provides

- the current status of electronic signature laws and active PKI-projects in the European Union and in Germany (Chapters 2 – 8)

- a report about the adoption of qualified certificates in Germany and a technical review on the IETF [RFC 3739] entitled "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile". (Chapters 9 – 11). The review focuses on main concepts of [RFC 3739] including:
  - The discussion of recognized issues of qualified certificates
  - The differences between [RFC 3039] and [RFC 3739], and
  - The adaptation of qualified certificates in the German Federal Government.

- the results of a survey on time stamp technologies (Chapters 12 – 17) that has been performed in order to get the current status of the
  - Needs and requirements in the federal government ministries and agencies that require time stamp technology
  - Degree of usage of time stamp services of leading vendors and time stamp service providers

- Additionally an explanation of the German ArchiSig project is given (Chapter 18)
2 Electronic Signature Law in Europe

2.1 Legal Framework

2.1.1 EU Directive on Electronic Signatures


The purpose of this Directive is to facilitate the use of electronic signatures and to contribute to their legal recognition. It establishes a legal framework for electronic signatures and certain certification-services in order to ensure the proper functioning of the internal market.

It does not cover aspects related to the conclusion and validity of contracts or other legal obligations where there are requirements as regards form prescribed by national or Community law nor does it affect rules and limits, contained in national or Community law, governing the use of documents.

2.1.2 EU Directive on electronic commerce

On 4 May 2000, the European Parliament approved the common position adopted by the Council with a view to the adoption of Directive of the European Parliament and of the Council on certain legal aspects of Information Society services, in particular electronic commerce, in the Internal Market. On 8 June 2000, the final version of the Directive was adopted. The Directive is being implemented by Member States. In pursuance of Article 9 of the Directive, Member States will have to remove barriers, such as legal form requirements, to electronic contracting. The directive is published in the Official Journal of the European Communities, L 178 (page 1 et seq.), 17.07.2000; refer to [EU-eComDir]. On [EU-eCommerce] you can find the directive also and additionally a first report (21.11.2003) providing the first assessment of the transposition and application of the Directive and its impact.

The Directive seeks to contribute to the proper functioning of the internal market by ensuring the free movement of information society services between the Member States.
The Directive approximates, to the extent necessary for the achievement of the objective set out in paragraph 1, certain national provisions on information society services relating to the internal market, the establishment of service providers, commercial communications, electronic contracts, the liability of intermediaries, codes of conduct, out-of-court dispute settlements, court actions and cooperation between Member States.

The Directive complements Community law applicable to information society services without prejudice to the level of protection for, in particular, public health and consumer interests, as established by Community acts and national legislation implementing them in so far as this does not restrict the freedom to provide information society services.

2.1.3 Minimum criteria to be taken into account


The purpose of this Decision is to establish the criteria for Member States to determine whether a national body should be designated as responsible for the conformity assessments of secure signature-creation-devices.

2.1.4 Directive on privacy and electronic communications


The Directive harmonises the provisions of the Member States required to ensure an equivalent level of protection of fundamental rights and freedoms, and in particular the right to privacy, with respect to the processing of personal data in the electronic communication sector and to ensure the free movement of such data and of electronic communication equipment and services in the Community.

The provisions of the Directive particularise and complement Directive 95/46/EC for the purposes mentioned in paragraph 1. Moreover, they provide for protection of the legitimate interests of subscribers who are legal persons.

The Directive shall not apply to activities which fall outside the scope of the Treaty establishing the European Community, such as those covered by Titles V and VI of the Treaty.
on European Union, and in any case to activities concerning public security, defence, State
security (including the economic well-being of the State when the activities relate to State
security matters) and the activities of the State in areas of criminal law.

2.1.5 Publication of reference numbers

On 14 July 2003, the European Commission adopted a Decision on the publication of
reference numbers of generally recognised standards for electronic signature products in
Communities, L 175 (page 45 et seq.), 15.07.2003; refer to [EU-Reference].

Reference numbers of generally recognised standards for electronic signature products are
laid down in the Annex of the mentioned document.

The Commission shall review the operation of this Decision within two years from the date of
its publication in the Official Journal of the European Union and report to the Committee
established under Article 9(1) of Directive 1999/93/EC.

2.1.6 Scanned Documents

We are yet not aware of any directives or commission decisions of the EU dealing with legal
issues of how to transform documents from paper form to an electronically form and vice
versa.

Two recently published documents in which the handling of scanned documents is mentioned
are:

L 98/9 (16.04.2003) The Court of Justice of the European Communities states in the section
Use of Technical means of Communications some rules how to deal with the electronic
transmission of documents. More precisely article 2 says that “Documents should be
scanned at a resolution of 300 DPI and, wherever possible, in PDF format (images plus text),
using Acrobat or Readiris 7 Pro software.”; refer to [EU-Practice].

L 251/9 (27.07.2004) The Commission of the European Communities has decided to add an
Annex to the Commission’s Rules of Procedure describing the Commission’s provisions on
electronic and digitised documents, the text is in [EU-Provisions]. These provisions determine
the conditions of validity of electronic and digitised documents for the Commission’s purposes.
They are also intended to ensure the authenticity, integrity and legibility over time of these
documents and of the relevant metadata. The provisions apply to electronic and digitised
documents established or received and held by the Commission. They may be made
applicable, by agreement, to electronic and digitised documents held by other entities
responsible for applying certain Community policies or to documents exchanged via data
transmission networks between administrations of which the Commission is part.
2.2 Legal and Market Aspects of Electronic Signatures

The European Commission has released on 20 October 2003 a detailed report on 'Legal and market aspects of electronic signatures', which brings some new insight regarding the use of electronic signatures in the EU, among other things for e-government services. The Report is available at [EU-Report].

The study was performed by a team of experts lead by researchers from the Interdisciplinary Centre for Law and Information Technology of the Catholic University of Leuven (KUL) in Belgium. This team was mandated by the Commission to assess the legal and practical issues concerning the implementation EU Directive 1999/93 of 13 December 1999 on a Community framework for electronic signatures, and the practical usage of electronic signatures and related services in Europe.

The report provides an analysis of national legislations implementing the directive in EU Member States as well as of e-signature legislations in the EU candidate countries and the EEA countries. It also provides a detailed analysis of the main practical and commercial usage of electronic signatures in the countries covered by the study, with a special focus on the technologies used, interoperability issues between products and services, and the use of common standards in this field. Based on both the legal and practical issues identified and analysed, the report contains a number of recommendations for a possible modification of the directive's scope in light of technology, market and legal developments.

In the field of e-government, the main finding of the report is that the public sector exception introduced by the directive lacks clarity and consistency and could be detrimental to the Internal Market. The article 3.7 of the directive provides that 'Member States may make the use of electronic signatures in the public sector subject to possible additional requirements'. This article therefore introduces what is called a 'public sector exception', allowing Member States to decide of specific 'additional requirements' to those contained in the directive for the use of electronic signatures for e-government applications. It is widely admitted an understood that public administrations need to have the possibility to specify more in details the requirements of their public key infrastructures (PKI) in order to achieve a sufficient degree of security, and of interoperability for e-government applications within one country. But the formulation of additional requirements on a general level for all kinds of e-government applications may infringe the e-signature directive as well as general EU competition rules.

As a matter of fact, most Member States have decided additional (security) requirements for the use of e-signatures in the public sector. Communicating electronically with public authorities is in many European countries possible only through the use of signatures based on Qualified Certificates (certificates providing the highest security guarantee for binding a public signature verification key with the identifier of a physical person) issued by an accredited CSP (certification service provider). The directive does not strictly forbid this but states that the requirement 'shall be objective, transparent, proportionate and non-
discriminatory and shall relate only to the specific characteristics of the application concerned'. As a consequence, Member States should only be able to impose the use of Qualified
Electronic Signatures for individual services and when this use is objectively justifiable. On the contrary, imposing the use of Qualified Certificates for all electronic relations between citizens and government in contradiction with Art 3.7 of the directive. Furthermore, such an imposition would also be contrary to the non-discrimination principle set in Article 5.2 of the directive. This article indeed states that an electronic signature cannot be denied legal effectiveness and admissibility as evidence in legal proceedings solely on the grounds that it is in electronic form, or not based upon a qualified certificate, or not based upon a qualified certificate issued by an accredited certification service-provider, or not created by a secure signature-creation device. Similarly, imposing the obligation to obtain an accreditation for Certification Service Providers (CSPs) as a condition to participate in e-government programmes is also in contradiction with the directive as it would limit the freedom for CSPs to adhere to an accreditation scheme of their choice. Such a measure would also have the effect of reducing the competition for certification services in a disproportionate way.

The main danger of the 'public sector exception', however, is that it could lead Member States to adopt additional requirements that could be detrimental to basic EU competition rules and to the internal market. In particular, such requirements could seriously affect competition on the market for electronic signature-related products and services and be in contradiction with article 4.2 of the directive that says: 'Member States shall ensure that electronic signature products which comply with this Directive are permitted to circulate freely in the internal market'. Member States should also make sure that they do not infringe EU competition rules when they intervene directly in the market for certification services. For example, a government can set up a PKI, alone or in partnership with private companies, to support the use of electronic signatures for its e-government applications. But the use of the same PKI for services outside the public sector would contradict EU competition rules as it would reduce competition in the market for certification services and would create barriers within the internal market in this area. Lastly, the definition of 'additional requirements' by national administrations may also be detrimental to the internal market if they end up creating different and contradictory rules between countries and therefore impede using e-government services across borders. They would then contradict the last sentence of Article 3.7 of the directive, which states that additional requirements 'may not constitute an obstacle to cross-border services for citizens'.

In order to address these issues and avoid the risks they represent, the report contains the following recommendations:

- The European Commission should clarify the conditions that are needed before Member States can use the 'public sector exception' of Art. 3.7 of the directive. It should also remind Member States that applying additional conditions can only be justified by objective reasons and should only relate to the characteristics of a specific application. Member States should also be made aware that the non-discrimination rule of Art. 5.2 of the directive applies not only to the private but also to the public sector.

- The Commission should examine in more details the compliance of some e-government initiatives not only with the Electronic Signature Directive's provisions but also with
general EU competition rules, particularly Art. 86 of the EC Treaty, which stipulates that competition rules of the EC Treaty shall apply to undertakings entrusted with the operation of services of general economic interest, "in so far as the application of such rules does not obstruct the performance, in law or in fact, of the particular tasks assigned to them").

- More generally, the Commission should perform a detailed study on the consequences of the e-government programmes of the Member States for the internal market, and on ways to avoid that these programmes could result in the erection of national barriers, increased fragmentation and lack of interoperability.

- Efforts towards improvement of interoperability between e-government programmes, and particularly between their electronic signature applications, should be supported or initiated at the European level.

2.3 References


[EU-Practice] Court of Justice Practice Directions relating to direct actions and appeals; L 98/1 (16.04.2003):


The Directive can be found on [EU-eComDir].

[EU-Notification] Status of notification of legal acts implementing the electronic signatures directive:

[EU-Report] The Legal and Market Aspects of Electronic Signatures (Study for the European Commission),
20.03.2003:

[Law-Survey] Digital Signature Law Survey (by Simone van der Hof):
http://rechten.uvt.nl/simone/DS-LAWSU.htm

2.4 Related Links


http://europa.eu.int/information_society/index_en.htm


http://europa.eu.int/information_society/topics/ecomm/all_about/todays_framework/privacy_protection/index_en.htm#security

http://europa.eu.int/information_society/topics/ecomm/useful_information/library/legislation/index_en.htm#dir_2002_58_ec

http://www.qlinks.net/quicklinks/digsig.htm

http://www.law.kuleuven.ac.be/icri/
http://www.law.kuleuven.ac.be/icri/it/elsig.php

http://www.enisa.eu.int/

http://www.dfn-pca.de/bibliothek/sigg/
3 Active PKI Projects in Europe

This chapter contains a brief description of relevant active PKI projects in Europe.

The survey is focused on the quality of the used electronic signature and the related law.

The projects are arranged according to their application domains.

3.1 Non-regulated Electronic Signatures

The widely-used application for electronic signatures and PKI in Europe is corporate and personal e-banking. But it is not regulated by the EU Directive. Traditionally personal e-banking ("consumer banking") is based on one-time passwords and tokens, but certificates by degrees are increasing in use. Besides using passwords and certificates for authentication purposes (secure login), electronic signing of transactions is on the rise. Smart cards are not widely-used in the context of personal e-banking but are increasing in use for business-to-business and inter-bank transactions.

3.2 Standardization

EESSI (the European Electronic Signature Standardization Initiative) was created in 1999 by ICT Standards Board (ICTSB) to co-ordinate the standardization activity in support to the implementation of EU Directive 1999/93/EC on electronic signature. Standardization activities were carried out in the CEN/ISSS E-sign workshop and the ETSI TC SEC/ESI. With the publication of a full set of standards, EESSI has fulfilled its mandate and consequently ICTSB decided to close EESSI WG in October 2004. New standardization work as well as maintenance of existing standards and specifications is still being carried out in ETSI TC/ESI. ETSI together with CEN and CENELEC, the three recognized European Standardization Organizations, was invited to contribute to the objectives set by the eEurope action plan because standardization is necessary for the successful implementation of the Information and Communications Technologies (ICT) that support the Information Society. The standardization work being carried out within Europe to achieve the targets of the European Commission's eEurope Action Plan is documented on [OL_EuroStd].

3.3 European Council Projects

According to the German initiative BundOnline 2005, described in chapter 5.1.1, the European Council has resolved the eEurope 2005 Action Plan [OL_Euro05].

It comprises more technical based projects like providing a widespread secure broadband infrastructure as well as more application oriented projects in the areas of eHealth, eBusiness, eGovernment and eLearning.
In the meantime the eEurope 2005 Action Plan has been supplemented by some issues for an Information Society policy beyond 2005, so called 2010 Challenges that should be more closely tailored to citizens’ needs and expectations.

3.4 E-Health Care Projects

3.4.1 European Challenges

Complementing the national eHealth projects in various European countries the European Council initiated a series of European Ministerial Conferences and the e-Health Awards for providers of Europe’s best e-Health solutions.

During the eHealth Conference and Exhibition 2004 in Cork, Ireland, 32 selected finalists of the eEurope Awards for eHealth 2004 presented their projects and eHealth solutions. The research report “Mapping the Potential of eHealth: Empowering the citizen through eHealth tools and services” was presented. It gives a brief history of eHealth, details potential challenges for the future of eHealth, gives recommendations how to meet them, and provides examples of European best practice. [OL_EuroAwards]

The Report appoints the following issues

- Citizens want more information
- Citizens want better information
- Healthcare delivery is safety-critical
- Europe is getting greyer (means elder)
- Healthcare costs are rising

Therefore eHealth requires the use of modern information and communication technology. But it also has to ensure secure access to accurate information for all parties concerned the citizens, the patients, the clinicians, and healthcare professionals and also the managers and regulators.

According to this intentions the providers of e-Health solutions were arranged under three themes

- eHealth information tools and services for citizens
- eHealth administrative support tools and services for citizens, and
- eHealth homecare and telemedicine tools.

More than half of the presented solutions refer to the theme “eHealth information tools and services for citizens”.

At current time information portals usually are split in a public and a private part. But certificates only are used for HTTPS (SSL/TLS) connections and not for authentication purposes. Private sites can be accessed using registration by login-name and password.
As an example for secure access to personal data and information tools using certificates have a look to the description of the Austrian e-card in chapter 3.4.3 and the German eHealth care projects in chapter 5.2.

3.4.2 Example: “Health On the Net”, the Winner of the eEurope Awards for eHealth 2004

The HON (Health On the Net) project submitted by the Health On the Net Foundation has been appointed as winner of the eEurope Awards for eHealth 2004 in the category “eHealth information tools and services for citizens”. The project is focused on online information quality addressing the providing of health information. The HON online platform includes an accreditation system for online information quality, a repository and a search engine. [OL_HON]

3.4.3 Example: The Austrian eHealth card “e-card”

In a first step the Austrian e-card will replace 42 millions paper bounded health insurance certificates. About 8 millions chip cards will be handed over to insured persons and their relatives.

The card is designed as a multifunctional card for the areas social insurance/ eHealth care and electronic Government.

In the area of health care on the one hand the card will contain the personal data of insured persons for identification and authentication on the other hand it will be possible to reload the necessary certificates to use it as a signature card that enables access to electronic information portals. Besides the insured persons staff members of the social insurance and physicians will be provided with the Austrian e-card. In a further step electronic health care will be extended to pharmacies (electronic prescription), hospitals and other domains.

3.5 E-Business Projects

The term ‘e-business’ covers both e-commerce (buying and selling online) and the restructuring of business processes to make the best use of digital technologies (cit. European Commission).

As part of the eEurope 2005 Action Plan the European Commission promotes the use of Information and Communication Technologies (ICTs) and e-business applications.

As a part of this initiative it was necessary to

- review relevant European legislation
- improve trust and confidence in e-business through establishing a European on-line dispute resolution mechanism, information systems on legal issues, trust mark requirements, and more
- ensure consumers’ trust and confidence in trading on-line
– ensure users’ privacy and consumer rights
– support the development of interoperable business solutions for transactions, security, signatures, procurements and mobile payments
– analyse “eSkills” supply and demand in Europe, and creating Europe-wide e-Skills definitions
– establish an e-business support network to strengthen and coordinate SME (Small and Medium Enterprises) e-business support actions
– raise awareness on the real benefits obtained by European SMEs by implementing advanced e-business solutions in the context of the IST programme with showcases interchange and organisation of the e-Challenges annual conference

Main instruments to fulfil the objectives in the area of e-business are economic analysis, policy co-ordination with EU Member States, public-private partnerships with non-profit organisations, and co-operation with European Standardisation Organisations.

3.5.1 Example: e-BSN, the European e-Business Policies Portal

The European e-Business Support Network for SMEs (eBSN) has been established by the European Commission in order to federate e-business experts in Europe and to share experience and good practice in support of e-business for SMEs [OL-eBSN]. It is open to all relevant policy initiatives in support of e-business for SMEs in the EU Member States, the acceding and candidate countries and the EEA states, which are willing to share experience and information.

In more detail the objectives of the eBSN initiative are

– to bring together real decision makers in the field of e-business, to share information, to discuss strategic policy orientation
– to validate existing e-business policies and to agree on targets for future e-business policies
– to provide a "one-stop-shop" for information about regional, national and European initiatives and funding possibilities for SMEs
– to organise special meetings of governmental e-business experts to share practical experience and to identify future challenges

The eBSN initiative is structured into a Steering Group, consisting of representatives of the Commission, the participating countries, academics and the business community, the eBSN portal linking all identified stakeholders and initiatives, and providing information, statistical data, best business practice, etc. Two - four thematic workshops per year, aiming at bringing together interested stakeholders to deepen the dialogue on specific issues of common interest, are hosted and organised by eBSN members.
3.5.2 Example: e-Business W@tch, Analysing e-Business at the Sectoral Level

The e-Business W@tch monitors the adoption, development and impact of electronic business practices in different sectors of the European economy. Since its starting, the e-Business W@tch has published e-Business Sector Studies on 17 sectors of the European economy, synthesis reports about the status of electronic business in the European Union, statistical pocketbooks and further resources (newsletters, presentations, special issue reports). These documents are all available on its website [OL_eBWatch].

3.5.3 Example: eMarket Services, a Guide to Electronic Marketplaces

The eMarket Services website is a collection of information, links, reports, case studies and contact persons in 21 European countries in the area of electronic marketplaces. [OL_eMplace]

The mission of eMarket Services is to make it easier for companies, particularly small and medium sized companies, to use electronic marketplaces for international business.

eMarket Services is a not for profit project, funded by the trade promotion organisations of Australia, Denmark, Holland, Iceland, Italy, New Zealand, Norway, Spain and Sweden. As of January 1st 2004 the EU Commission came into the project as a co-sponsor for a period of 2 years. eMarket Services is now the official European portal for information on e-marketplaces and aims to make it possible for companies in all EU member states to get answers in their own language.

3.6 E-Government Projects

E-government is the rapidly rising application for electronic signatures in Europe. In the near future it will dominate applications for electronic signatures that are regulated by the EU Directive.

3.6.1 Example: The Austrian Citizen Card

The Austrian Citizen Card project [OL_AuCC] was launched by the Austrian Federal Government in a cabinet council in November 2000. It is addressed to the citizens in order to enable a more easy access to the authorities and administrative proceedings. Citizen Cards shall become the “official identity documents” in the electronic administrative procedures but in a secure manner. Therefore the card has to meet the requirements signature and identification. For a transition period until end of 2007 the E-Government law [OL_AuSL] lays down that for public administration so-called “administration signatures” are equivalent to legally defined secure electronic signatures.
3.6.2 Identity Cards Europe-wide

Identity cards like the Austrian Citizen Card are a widespread application in Europe. You can find them also in Belgium, Estonia, Finland, France, Iceland, Ireland, Italy, Netherlands, Norway, Portugal, Slovenia, Spain, Sweden, Switzerland, and the United Kingdom [OL_IDEu]. Belgium and Sweden already established electronic identity cards.

In Germany the adoption is planned for the year 2007. It is intended that the electronic identity card has to be compatible to passport and electronic health card. The electronic identity card will contain digital biometric data like face- and fingerprint for unique identification of the holder. For optional use the card will contain a function to create qualified electronic signatures. The necessary certificates have to be reloaded under control of the holder.

In Germany the adoption of a multi functional citizen card e.g. is provided by the Signature Alliance described in chapter 5.4.2.

Actually a Working Draft that deals with the subject European citizen card is developed for CEN, the European Committee for Standardization, TC224, Working Group 15 [OL_CEN_STD].

3.6.3 Example: Government Gateway in the United Kingdom

Comparable to the German Federation’s service portal www.bund.de, described in chapter 5.1.1, the Government of the United Kingdom provides the Government Gateway, which is a centralised registration service for e-Government services in the UK.

Registering with the Government Gateway enables citizens to sign up for any of the UK Government's services that are available over the Internet.

Services that are available at current time are for instance

- National Blood Service - Blood Donor On-Line Trial: Currently the National Blood Service is offering a trial on-line service to a small group of blood donors with the hope to offer a full service in the future
- Council Tax - for individuals to view their Council Tax bills and accounts and to submit direct debit applications to pay their Council Tax
- Housing and Council Tax Benefits - for individuals to enquire on the amount of Housing Benefit and / or Council Tax Benefit to which they are entitled and to submit a variety of change of circumstances
- Animal Movements Licensing System (AMLS) - currently only available for use by Local Authority Trading Standards Departments and the devolved administrations
- Procedure for the Electronic Application for Certificates from the HMI (PEACH) - for importers, exporters and processors of whole fresh produce into and out of the EU
- Seed Certification - for companies and seed testing stations
– Department of Trade and Industry Export Licence Application - for exporters of items controlled for strategic reasons or because of sanctions
– Child Benefit Online - for individuals wishing to claim Child Benefit and those already in receipt of Child Benefit who wish to report changes in circumstances
– Employer Direct Online - Employer Direct Vacancy Notification (for employers who wish to place vacancies with JobcentrePlus)
– Job Warehouse – for Job Advertisers who wish to upload their vacancies to the Jobcentre Plus Internet Job Bank
– State Pension Forecast - for the full working age population - 16 years of age through to 4 months and 4 days from State Pension Age – currently 60 for women and 65 for men

and a number of other services [OL_UKGate].

The Government Gateway is a secure site. All information is transmitted through a 128-bit Secure Socket Layer connection (SSL).

Many government transactions require a digital certificate that needs to be approved for use with the Government Gateway. Citizens utilizing the services can buy certificates over the Internet from the following service providers

– BT Trust Services [OL_BTServ]
– Equifax [OL_Equifax]
– Chamber SimplySign [OL_CSSign]

3.6.4 Example: Media@Komm-Transfer

Media@Komm-Transfer [OL_MeKo] is a project initiated by the public administration of Germany in order to modernize government structures at municipal level. It is a successor project of the Media@Komm scheme and is based on the modules

– Standardization
  Standardization subjects are, for example, Internet portals and virtual town halls, virtual health networks, geographic information systems and so on.
  The OSCI (Online Services Computer Interface) and the interoperability specification ISIS-MTT for electronic signatures are obligatory standards used in German government. One of the intentions of the Media@Komm project is to introduce them into the EU.
– Regional distribution of E-Government projects
  Based on the standardized solutions local government initiatives will be linked to a nationwide network. At the international level, both municipalities and regions are being targeted.
– Internalization
  In the course of an EU-wide public procedure a transfer agency was commissioned by the German Federal Ministry of Economics and Labour (BMWA) to manage the project. The transfer agency provides the transfer of knowledge by organizing joint events, supplying concepts on how to implement E-Government solution, or giving direct support in
technical, organizational and legal issues for the establishing of such projects in an EU-wide scope.

3.6.5 Example: Electronic Marketplace - Czech Republic

The Ministry of Informatics of the Czech Republic has introduced an electronic marketplace [OL_EMcz] for all orders and purchases of information and communications technologies up to the amount of 62,500 €. By 2006 electronic marketplaces should be used for repeated and bulk purchases in the whole field of the public administration.

In September 2004 the Ministry of Informatics finalized a bill on electronic communications with the intention to transpose the new European regulatory framework into national law.

3.7 E-Learning Projects

A lot of projects have been established in the area of e-learning, both within the scope of the European Commission initiative eEurope 2005 and in the private sector. But not any one is using certificates for authentication but provides registration by login-name and password or free information access.

As an example have a look at “elearningeuropa.info”, a portal about the use of Information and Communication Technologies to improve learning, an initiative of the European Commission [OL_EU_PeL] or “The ELearning Guild” in the commercial sector [OL_ELGuide].

3.8 References and Related Links


[OL_eMplace] E Market Services, a Guide to Electronic Marketplaces,  
http://www.emarketservices.com/

[OL_UKGate] Central Registration Gateway for e-Government services in the UK,  
http://www.gateway.gov.uk/

[OL_BTServ] BT Trust Services,  

[OL_Equifax] Equifax,  
http://www.equifaxsecure.co.uk/ebusinessid/

[OL_CSSign] Chamber SimplySign,  
http://www.simplysign.co.uk/

[OL_MeKo] Media@Komm-Transfer,  
http://www.mediakomm-transfer.de/Content/en/Homepage/Homepage_node.html__nnn=true

[OL_AuCC] The Austrian Citizen Card,  
http://www.buergerkarte.at/index_en.html

[OL_AuSL] The Austrian Signature Law,  
http://www.a-sit.at/informationen/gesetzlich/gesetzlich.htm

[OL_IDEu] Electronic Identity in Europe,  

[OL_CEN_STD] CEN Standardization Group,  

[OL_EMcz] Electronic Marketplace - Czech Republic,  

[OL_EU_PeL] Portal about the use of Information and Communication Technologies to improve learning,  

[OL_ELGuide] The ELearning Guild,  
http://www.elearningguild.com/
4 Electronic Signatures Law in Germany

4.1 Overview of Current Status of Legislation

The first German digital signature law has been published on July 28th 1997. In order to achieve compatibility with the European electronic signature directive [EC DIR] and to remove inconsistencies this law has been amended and replaced with the new “Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations” [SigG] that came into force on May 22nd 2001. The German electronic signatures law thus also represents the implementation of the European directive in German legislation. In accordance with article 13 of the European directive, the member states had to bring into force the related laws, regulations and administrative processes that are necessary to comply with the directive before July 19th 2001.

Recently the Lower House of the German Federal Parliament has decided and issued a first amendment of the German signature law [SigG] on January 4th 2005. The purpose of the changes made in [SigG] is to

- harmonize the German signature law with the directives of the European Parliament, and to
- increase the number of applications and users for legal transactions, electronic communication and commerce in Germany.

4.2 Main Changes of the Electronic Signatures Law

Concerning the changes of the German electronic signatures Law the following measures in the amendment law [SigG] are of relevance:

- Amendments of the electronic signatures law [SigG]
  - The definition of the term “advanced electronic signature” has been brought into alignment with the definition in the European directive [EC DIR].
  - The liability to use pseudonyms can be excluded by contracts.
  - Information provided to applicants of certificates needs only to be presented in text form.
  - Further reasons for certificate revocation that are not part of the signature law can be defined by contracts.
  - The hand-written confirmation of certificate applicants that they have got information on security measures from certification service providers is no longer required.
  - The rules to disclose pseudonyms have been clarified.
  - Manufacturers of products for qualified electronic signatures are obliged to pass a manufacturer declaration to the competent authority.
• Amendment of the related signature ordinance [SigV]
  – The receipt of signature keys and identification data on a secure signature creation
device does not need to be confirmed by the applicant in written form or by means of a
qualified electronic signature.
For logical reasons the description of the changes listed above and their reasons have been
incorporated into the following sections.

4.3 Main Issues of the German Electronic Signatures Law

This section contains the description of the major concepts of the German electronic
signatures law [SigG] and the related amendment law [SigG*]. It provides the current status of
the German legislation on electronic signatures.

4.3.1 General Objectives, Related Laws and Structure of the Signature Law

The German electronic signatures law aims at creating frame conditions for electronic
signatures. The use of electronic signatures is voluntary as far as not specifically required by
law for specific applications. In this context, the law principally differentiates between
“electronic”, “advanced electronic”, “qualified electronic” signatures and “qualified electronic
signatures with provider accreditation”.

By "electronic signatures" the law generally means data in electronic form which are attached
to other electronic data or are logically associated with them and which serve for
authentication purposes.

• “Advanced electronic signatures” are electronic signatures that are
  – uniquely linked to the signatory (owner of the private signature key),
  – capable of identifying the signatory,
  – created by means that the signatory can maintain under his sole control, and that are
  – linked to the data to which it relates in such a manner that any subsequent change of
    the data is detectable.
• “Qualified electronic signatures” are advanced electronic signatures that are
  – based on a qualified certificate valid at the time of their creation, and
  – created with a secure signature creation device.
• “Qualified electronic signatures with provider accreditation” are
  – qualified electronic signatures based on a qualified certificate
  – that has been issued by an accredited certification service provider.

The requirements for the equivalence of electronic signatures based on a foreign qualified
certificate issued by another member state of the European Union or signatory to the Treaty
on the European Economic Area with qualified electronic signatures compliant with the
German signature law have been explicitly defined in § 23 of [SigG]. A basic prerequisite for
equivalence is the fulfillment of article 5(1) of [EC DIR] on legal effects of electronic signatures.

Similar requirements hold for the equivalence with electronic signatures from third countries. The related certificates should have been issued publicly as qualified certificates by certification service providers in a foreign country and should have been designed for electronic signatures in the meaning of article 5(1) of [EC DIR].

The equivalence of foreign electronic signatures with qualified electronic signatures with provider accreditation requires a proof that foreign electronic signatures offer equivalent security.

The definitions of terms that are used in the German signature law are listed together with the related definitions of the European signature directive in table 1 of appendix 8.3. This table can be used to demonstrate the similarities as well as the differences between both legal frameworks. Concerning definition of terms the signature amendment law [SigG*] has only redefined the term signature-code owner (see item #9 in table 1 of appendix 8.3) as follows: “signature-code owners shall be natural persons who own signature codes; in the case of qualified electronic signatures the appropriate signature test codes must have been assigned to them in qualified certificates.” This redefinition was necessary in order to comply with the related definition in the European signature directive such that for advanced electronic signatures signature test codes must not have been assigned to signature-code owners in qualified certificates.

The German signature law does not specify individual requirements for specific forms of electronic data for which electronic, advanced or qualified electronic signatures will be created. The term electronic data is used in the signature law in a general and abstract fashion thus allowing any kind of electronic data to be used for any form of electronic signatures. Therefore, principally data objects like E-Mails, documents, contracts, medical records, or also digitally scanned documents can be used for electronic signatures. Other laws besides the signature law may specify further requirements for the usage or exclusion of electronic signatures. These laws define concrete forms of electronic data for which electronic signature can or must be used.

An example of these classes of laws is the law for modernization of the legal health insurance [GMG] in Germany that specifies requirements for the realization and usage of the electronic health card and their related application-specific electronic data, e.g. electronic prescription, medical emergency data records, or electronic patient record.

Other examples of these classes of laws in the German legislation are the following ones:

- Law on the adaptation of form requirements and other requirements for modern legal transactions [Form]
- Third law amending the administrative procedural requirements [E-FORM]
The first law [Form] establishes the legal effect for qualified electronic signatures in the civil law sector, whereas the second law [E-FORM] defines the “electronic form” in the public law sector. Both new laws provide the legal framework for the application of qualified electronic signatures in the civil administrative as well as in the public commerce sectors. They regulate the legal equivalence of electronic signatures to handwritten signatures and the legal effectiveness in legal proceedings thus also complying with the requirements of the European signature directive (see article 5 of [EC DIR]).

Basically the signature law consists of six parts. The first part describes the purpose of the law and contains definitions of terms used in the law. The second part formulates requirements for certification service providers (certification authorities, CAs). The third part regulates the preconditions for accredited certification service providers, while the fourth part contains technical requirements for signature products as well as requirements for the recognition of testing and confirmation offices. The fifth part states the rules for the supervision and control of the certification service providers obeying to the legal requirements. The last section contains regulations concerning fines as well as regulations for transitional periods.

For logical reasons the numerous requirements that have been specified in the signature law and the signature ordinance have been rearranged in the next sections using the following categories:

- Requirements for the competent authority,
- Requirements for certification service providers,
- Requirements for electronic signature products, and
- Requirements for testing and confirmation offices.

### 4.3.2 Requirements for the Competent Authority

#### 4.3.2.1 General Requirements

The tasks and the responsibilities of the competent authority comprises the following items:

- Issuance of licenses for CAs
- Issuance of certificates for CA signing keys
- Verification of CA compliance with the requirements of the signature law [SigG] and the signature ordinance [SigV]
- Taking over the documentation of a certification service provider that ceases its operation, if no other certification service provider takes that part
- Provision of information on the documentation in response to legitimate interest, if this is technically possible and does not require an over-proportionate amount of effort
- Voluntary accreditation of certification service providers
- Publication in the federal gazette of products for qualified electronic signatures that have been successfully tested and the time until which the confirmation at least is valid,
- Publication in the federal gazette of products for qualified electronic signatures whose confirmation has been withdrawn and the time from which this applies
- Publication in the federal gazette of algorithms and parameters suitable for creating signature keys, hashing of data, and for generating and verifying qualified electronic signatures
- Execution of supervision measures

The changes of the amendment signature law related to the competent authority have the following effects.

The signature amendment law (see [SigG] article 1, no.2) explicitly mentions the Regulatory Authority for Telecommunications and Post (RegTP, Regulierungsbehörde für Telekommunikation und Post) as the competent authority thus removing the link to the telecommunications law in the signature law (see [SigG] §3) and providing the independence of both laws.

### 4.3.2.2 Voluntary Accreditation of Certification Service Providers

The signature law specifies the following set of requirements and/or options for the competent authority regarding the voluntary accreditation of certification service providers (see [SigG] §15, and [SigV] § 11):

- Accreditation (if required with additional conditions) of certification service providers upon their request which has to be made in written form or as an electronic document with a qualified electronic signature
- Optional use of confirmation offices for the accreditation procedure
- Proof that the certification service provider complies with the signature law and signature ordinance
- Rejection of accreditation, if compliance with the signature law and signature ordinance cannot be proven
- Exhaustive and comprehensive evaluation of the CA security concept for its suitability and practical implementation
- Approval of the security concept by an confirmation office
- Repetition of testing and approval after the occurrence of any changes that greatly affect security, and at regular intervals of three years
- Revocation or withdrawal of an accreditation for the reasons listed in section 4.3.3.9
- Adequate testing of products for electronic signatures with state-of-the-art science and technology by an confirmation office
- Issuance of a quality sign to accredited certification service providers that confirms that the qualified electronic signatures (with provider accreditation) based on their qualified certificates offer comprehensively tested security
- Issuance of qualified certificates for the accredited certification service providers needed for their operations
- Optional issuance of the electronic certificates needed by the certification service providers or producers for the automatic authentication of products.
- Issuance and revocation of qualified certificates with the same requirements as listed in sections 4.3.3.2 and 4.3.3.6 for accredited certification service providers.
- Revocation of issued qualified certificates, if an accredited certification service provider ceases its operation, or if an accreditation is withdrawn or revoked.
- Provision of the following information that needs to be accessible and provable at any time by anyone via public communication links:
  - names, addresses, and communication links of the accredited certification service providers,
  - revocation or withdrawal of an accreditation,
  - issued qualified certificates, and their revocation, and
  - cessation of operations by an accredited certification service provider and a ban on these.

The signature amendment law [SigG*] did not change the general requirements related to voluntary accreditation of certification service providers as defined in the signature law [SigG].

4.3.2.3 Recognition of Testing and Confirmation Offices

The signature law specifies the following set of requirements and/or options for the competent authority regarding the recognition of testing and confirmation offices (see [SigG], §18):

- Recognition of a natural person or a legal entity upon request as a confirmation or as a testing and confirmation office
- Optional limited permission or permission for a period of time for operation as a confirmation or as q testing and confirmation office
- Optional limited permission with respect to the scope of the confirmation or the testing and confirmation office
- Optional additional conditions for the operation of the confirmation or testing and confirmation office
- Evaluation of the documentation of the executed tests and issued confirmations received from the test and confirmation offices at their start of operation

The signature amendment law [SigG*] did not change the general requirements for the competent authority regarding the recognition of testing and confirmation offices as defined in the signature law [SigG].

4.3.2.4 Supervision Measures

The signature law specifies the following set of requirements and/or options for the competent authority regarding the supervision measures (see [SigG], §19):
• Supervision of observance of the signature law and the signature ordinance
• Optional use of private entities to perform the task of supervision
• Start of supervision of certification service providers at start of their operation
• Definition of optional control steps in regard to certification service providers to ensure their compliance with the signature law
• Prohibition of the operation of a certification service provider for the following reasons:
  – missing reliability that is necessary to operate as certification service provider,
  – missing proof for the specialized knowledge required for the operations,
  – insufficient cover,
  – use of unsuitable products for electronic signatures, and
  – non-compliance with the signature law and the signature ordinance.
• Optional revocation of qualified certificates if
  – qualified certificates are forged,
  – qualified certificates are not sufficiently secure against forgery, or
  – secure signature-creation devices have security defects.
• Continuance of the validity of qualified certificates of the related certification service provider even for the following reasons:
  – ban on the CA operations,
  – cessation of CA operations,
  – withdrawal of an CA accreditation, or
  – revocation of an CV accreditation.
• Availability for anyone to access via public communication links the names of certification service providers that have been registered, ceased their operation or whose operations have been forbidden.

The signature amendment law [SigG*] did not change the general requirements for the competent authority regarding the supervision measures as defined in the signature law [SigG].

4.3.3 Requirements for Certification Service Providers

4.3.3.1 General Non-technical Requirements

The signature law specifies a set of basic pre-conditions for certification service providers for the following topics:

• Approval of operation
• Reliability
• Specialized knowledge
• Liability
• Cover
• Security concept
• Notification of start of CA operation
• Guarantees for operation
• Use of third party services

Approval of operation (see [SigG] §4)
In accordance with article 3 section 1 of the European directive, the operation of a CA shall not be made subject to prior authorization, i.e. it shall not require an approval under the current law.

Reliability of personnel (see [SigG] §4 and [SigV] §5)
CAs have to guarantee that they will observe and follow the legal regulations on the operation of the certification service. They have to provide procedures to assess and control the reliability of the personnel. In particular they can require the presentation of an actual certificate of good conduct of the Federal Central Register Act.

Specialized knowledge (see [SigG], §4, and [SigV], §1)
Certification service provider are obliged to prove that their stuff has the necessary technical, administrative and legal specialized knowledge, experience, and skills needed for this work.

Liability (see [SigG], §11)
Certification service provider are liable for reimbursement to a third party for any damage they suffered from relying on the data in a qualified certificate or a qualified time stamp or on related information.

Cover (see [SigG], §12)
Certification service provider are obliged for making appropriate cover provisions (minimum 250.000 €) for possible cases of reimbursement.

Security concept (see [SigG] §4 and [SigV] §2 and §6)
Certification service providers are obligated to present their appropriate and implemented measures to fulfill the security requirements of the signature law and signature ordinance to the competent authority in a security concept that contains the following information:
- a description of required technical, structural and organizational measures and their effectiveness,
- a list of products used for qualified electronic signatures including manufacturer declarations,
- the precautions taken in order to protect products used for qualified electronic signatures against unauthorized access,
- an overview of the CA organization and its operation procedures,
- the precautions taken and measures used to secure and maintain the CA operations (especially in the case of emergencies), and
- the evaluation and assessment of remaining security risks.

Notification of Start of CA Operation (see [SigG] §4, and [SigV] §1)
Certification service providers are obligated to submit a notification in written form or with a qualified electronic signature to the competent authority at latest when commencing operation including an appropriate proof that the required pre-conditions as described in this section have been met.

**Guaranteed operation (see [SigG], §4)**

Certification service provider have to fulfill the pre-conditions throughout the entire duration of operation as certification service provider, and to report circumstances that render this impossible to the competent authority without delay.

**Third party services (see [SigG], §4)**

Certification service providers have the option to use third party services, if this alternative is included in their security concept.

In the case of using parts of the CA service in an EU member state or in a third country further documents proving equivalent supervision of these foreign CAs have to be submitted to the competent authority. The use of CA services in other countries is only permitted in the framework of voluntary accreditation.

The signature amendment law [SigG*] did not change the general requirements for certification service providers as defined in the signature law [SigG].

### 4.3.3.2 Cooperation with the Competent Authority

The signature law specifies the following set of requirements for certification service providers related to the obligatory cooperation with the competent authority (see [SigG], §20):

- Permission for the competent authority and the persons acting on its behalf to enter their premises and workshops during normal operating hours
- Permission upon request for inspection the relevant books, records, vouchers, written material, and other relevant documents
- Supply of information and the necessary support.

The signature amendment law [SigG*] did not change the requirements for certification service providers related to the obligatory cooperation with the competent authority as defined in the signature law [SigG].

### 4.3.3.3 Requirements for Issuing Qualified Certificates

The signature law specifies the following set of requirements for certification service providers that issue qualified certificates (see [SigG], §5):

- Identification of natural persons
Prior to the issue and registration of qualified certificates CAs have to reliably identify the natural persons that apply for qualified certificates. The signature ordinance (see [SigV] §3) further requires that this personal identification has to be done by means of the national identity card or a passport or of documents with equivalent level of security. Applicants may be citizens of EU member states or of a state of the European Economic Area. The identification procedure may be omitted, if the certification request has been made with an electronic document confirmed with a qualified electronic signature of the applicant. CAs may re-use personal data that they have collected at an earlier point in time, if the applicant agrees and if these data guarantee his reliable identification (new option of the signature amendment law, see [SigG*] no. 3)

- Directory service (see also [SigV] §4)
  CAs have to guarantee that qualified certificates are accessible and verifiable by anyone at any time using public telecommunication links. Qualified certificates have to be kept in the directory from the time of their issuance for the period indicated within the certificate and at least for another five years from the end of the validity of the certificate.

- Accessibility of qualified certificates
  CAs must have the approval of the signature card owner that qualified certificates may be kept accessible.

- Approval of third party (see also [SigV] §3)
  If a qualified certificate shall contain data on the authorization of the applicant to act (i.e. to electronically sign) for a third party, a document of the third party is required as proof of approval. The third party has to be informed by the issuing CA about the contents of the related qualified certificate and its possibility for revocation. These exchanged documents shall be either documents with a qualified electronic signature or documents in written form.

- Confirmation of occupational-specific data (see also [SigV] §3)
  If a qualified certificate shall contain occupational-specific data (attributes) of the applicant, a document of by the office responsible for the occupational data is required for confirmation of its contents and authorization. This office has to be informed by the issuing CA about the contents of the related qualified certificate and its possibilities for revocation. These exchanged documents shall be either documents with a qualified electronic signature or documents in written form.

- Approval of other data (see also [SigV] §3)
  Other data (attributes) on the applicant may only be integrated into a qualified certificate if the applicant gives his explicit allowance.

- Pseudonyms
  CAs may use a pseudonym instead of the name in a qualified certificate, if this has been requested by an applicant.

- Security of qualified certificates
  CAs have to provide measures such that data for qualified certificates cannot be falsified or forged without detection.

- Secret generation and transfer of signature keys (see also [SigV] §4)
  CAs are required to perform a unique and secret generation and transfer of signature keys on and to the relevant secure signature creation device. They also shall take precautions to guarantee the secrecy of the card holder identification data transferred to the secure
signature creation device. The storage of signature keys and the card holder identification data outside the secure signature creation device has to be excluded.

- Suitable proof of possession (see also [SigV] §5 and [SigG] article 2)
The CA shall personally hand over the secure signature creation device including the generated signature keys and identification data to the applicant thus being sure that the applicant owns the relevant secure signature creation device. The handover has to be confirmed by the signature key holder by an electronic document unless a different handover has been negotiated.

- CA personnel and use of products
CAs shall employ reliable personnel and use products for qualified electronic signatures that meet the requirements of the signature law and signature ordinance.

The changes of the signature law related to the issue of qualified certificates (see [SigG] article 1 no. 3 and article 2) have the following effects.

Certification service providers are now allowed to use data for the purpose of identification of an applicant that they already have collected at an earlier point in time, if the applicant agrees to this simplified identification procedure. They also can use applicant identification data from third parties or they can shift the task of applicant identification to another company. This organizational lightening of the identification procedure decreases bureaucratic hindrances and unnecessary costs for the economy. Especially the banking sector will play a major role in the distribution of signature cards due to the fact of the existing infrastructures for banking and EC-cards. Under these conditions chip cards with qualified electronic signatures can be issued without personal identification. Applications for signature cards can be made electronically via the Internet and the produced signature cards can be sent to the applicant via post.

4.3.3.4 Requirements for Informing Applicants

The signature law specifies a set of requirements for certification service providers related to information that they shall pass to applicants or third parties if relevant (see [SigG] §6 and [SigV] §6). These requirements include the following types of information about the

- Storage and usage of secure signature creation device and appropriate measures in case of loss or suspicion of misuse
- Confidentiality of personal identification data
- Measures needed to increase the security of qualified electronic signatures and their reliable verification
- Necessity for re-signing data with a qualified electronic signature in cases where the security value of the current signature may be reduced by the passage of time
- Equivalent effect of a qualified electronic signature in legal transactions as a handwritten signature unless otherwise specified by specific law
- Existence of a voluntary accreditation scheme
- Procedures for revocation of certificates
Document in text form that has to be confirmed by the applicant in text form that he has read and taken note of this information as a pre-condition for the issue of a qualified certificate.

The changes of the signature law related to applicant information (see [SigG*] no. 4) have the following effects.

The confirmation of an applicant after the receipt of information from the certification service provider shall be done in “text form” which per civil code can be realized via simple E-Mail. This change supersedes the former requirement for hand-written confirmations and fully complies with the regulations in the European signature directive and with the signature laws in many other EU member states. It also simplifies the identification process.

4.3.3.5 Requirements for Qualified Certificates

The requirements related to the content of qualified certificates that are specified in the German signature law (see [SigG] §7) are listed together with the related requirements of the European signature directive in table 2 of appendix 8.4. This table can be used to demonstrate the similarities as well as the differences between both legal frameworks.

The signature ordinance defines the following further requirements for the content of qualified certificates and qualified attribute certificates (see [SigV] §14):

- Unambiguosness of data contained in qualified certificates
- Limitation of the validity period of qualified certificates to five years or shorter if the suitability of the applied algorithms and related parameters cannot be guaranteed
- Contents of qualified attribute certificate
  - unambiguous reference to the related qualified certificate,
  - qualified electronic signature of the certification service provider,
  - identification of algorithms required to verify the signature of the issuing certification service provider,
  - serial number of the attribute certificate,
  - name and country of the certification service provider,
  - indication as qualified attribute certificate, and
  - optional additional attributes.

The signature amendment law [SigG*] did not change the requirements for the contents of qualified certificates as defined in the signature law [SigG].

4.3.3.6 Requirements for Revocation of Qualified Certificates

The signature law specifies the following set of requirements for certification service providers related to the revocation of qualified certificates (see [SigG], §8 and [SigV] §7):
• Provision of a telephone number under which all authorized parties can request the revocation of a qualified certificate without any delay,

• The immediate revocation of a qualified certificate can be requested by the
  – competent authority,
  – issuing certification service provider,
  – signature-code owner,
  – representative of the signature-code owner,
  – third party if applicable, or
  – office responsible for the occupational or other data on the person, if applicable.

• Possible reasons for revocation of a qualified certificate can be that the
  – certificate was issued on the basis of false data,
  – certification service provider has ceased to operate without continued operation by another certification service provider,
  – conditions for the occupational or other data on the person cease to apply after being included in the qualified certificate, and
  – further reasons for revocation can be negotiated by contract (see [SigG] article 1, no. 5).

• Revocation procedures
  – proof of the identity of the person authorized to revoke the certificate,
  – recording of the revocation in the directory,
  – inclusion of the official revocation time,
  – revocation with backdated effect is not permitted, and
  – if a qualified certificate was issued with false data, the certification service provider may also make this known.

The changes of the signature law related to the revocation of qualified certificates (see [SigG] article 1, no. 5) have the following effects.

The catalogue of revocation reasons is not limited to the reasons specified in the signature law and it can be extended by contract. This contributes to the principle of technical neutrality of the signature law. This change of the signature law also clarifies that the signature laws does not adopt a specific validity model. Instead the certification service provider has to demonstrate (see [SigG] §4) that his validity model complies with the rules of the signature law. It must especially be possible to check the validity of a certificate in accordance with the legal rules for a point in the past.

4.3.3.7 Requirements for Qualified Time Stamps

The signature law specifies the following requirement for certification service providers that also issue qualified time stamps (see [SigG] §9):

• CAs shall employ reliable personnel and use products for qualified electronic signatures that meet the requirements of this the signature law and signature ordinance.
Concerning long-term data security the signature ordinance (see [SigV] §17) defines requirements for the use of qualified time stamps. Data that have been secured with a qualified electronic signature and that need to be kept for a long period have to be re-signed, if the used algorithms and parameters turn-out to become weak. In this case the signed data and a qualified time stamp for these signed data have to be protected by a new qualified electronic signature using appropriate new algorithms and parameters prior to the time at which the suitability of the algorithms and parameters expires.

The signature amendment law [SigG*] did not change the requirements for qualified time stamps as defined in the signature law [SigG].

4.3.3.8 Requirements for Documentation

The signature law specifies a set of requirements for certification service providers related to documentation (see [SigG] §10 and [SigV] §8). These requirements include the following types of documentation:

- Documentation of the security concept, i.e. of the security measures taken to comply with the law and the ordinance
- Documentation of the specialized knowledge of the personnel
- Documentation of contractual arrangements made with the applicants
- Documentation of issued qualified certificates allowing that the integrity of the data can be verified at any time
- Documentation particularly related to the issuance and revocation of qualified certificates shall be made without delay and in such a manner that it cannot subsequently be altered without detection
- Documentation and data retained with regard to relevant applicants shall include
  - photo copy of submitted identity card, passport or other proof of identity,
  - issued pseudonym if applicable,
  - proof of provision of information to the applicant,
  - proof of the approval of the authorized persons if applicable,
  - confirmations of occupational offices if applicable,
  - list of qualified certificates that have been issued including the times of issuance, handover and time of inclusion in the directory,
  - list of revoked qualified certificates,
  - information related to data protection, and
  - handover confirmations for signature keys and identification data
- Documentation shall be maintained for the following periods:
  - five years for certification service providers,
  - thirty years for accredited certification service providers,
  - if required at court until the final verdict, and
  - twelve month for documentation related to data protection (disclosure of pseudonym)
- Provision of access for applicants to the data and the procedural steps concerning him
The signature amendment law [SigG*] did not change the requirements for certification service providers related to documentation as defined in the signature law [SigG].

### 4.3.3.9 Requirements for Cessation of Operation

The signature law specifies the following set of requirements for certification service providers related to the cessation of their operation (see [SigG] §13 and [SigV] §10):

- Delivery of report at latest two month prior to the cessation of operation to the competent authority,
- Delivery of immediate information to the competent authority of an application to open insolvency proceedings,
- Guarantee that qualified certificates will remain valid after cessation of operation, if the service will be taken over by another certification service provider,
- Guarantee that qualified certificates will be revoked, if requested,
- Delivery of information at least two month prior to the cessation of operation to the signature-code owners,
- Delivery of information at least two month prior to the cessation of operation to the signature-code owners that the qualified certificates are being taken over by another certification service provider,
- Delivery of existing documentation to the new certification service provider.

The signature amendment law [SigG*] did not change the requirements for certification service providers related to cessation of its operation as defined in the signature law [SigG].

### 4.3.3.10 Requirements for Data Protection

The signature law specifies the following set of requirements for certification service providers related to data protection (see [SigG] §14, and [SigG*] article 1 no.6):

- Only those personal data that are necessary to issue a qualified certificate may be obtained only from these persons,
- Data from third parties shall only be permitted with the consent of the person concerned,
- Data on the identity of a signature-code owner shall be handed-over the to the related federal authorities upon justified request such as
  - necessity for the prosecution of criminal acts or infringement of regulations,
  - avoidance of risk to public security or order,
  - fulfillment of the legal tasks of the constitutional protection agencies of the federal government and the individual states, the federal secret service, military defense, or the fiscal authorities, or
  - order by courts as part of proceedings pending and pursuant to the appropriate statutory provisions,
- Documentation of the information given to requesting authorities.
• The authority requesting the information shall inform the signature-code owner that his data have been revealed as soon as this will not restrict the performance of its legal duties, or if the interests of the signature-code owner in being informed outweigh the other considerations.

The changes of the signature law related to data protection [SigG*] have the following effects.

The obligation to disclose the identity of a signature-code owner towards federal authorities is no longer restricted to the exceptional case of pseudonyms. The extension of the obligation thus can create extra costs for certification providers, since currently this disclosure information has to be provided by CAs for free. The German government considers to regulate possible financial compensation for disclosure information from certification service providers within the framework of the telecommunications law.

4.3.3.11 Requirements for Accredited Certification Service Providers

The signature law and signature ordinance specify the following additional set of requirements for accredited certification service providers (see [SigG], §15):

• Exclusive use of tested and approved products for qualified electronic signatures in certification operations
• Issuance of qualified certificates only for persons with tested and approved secure signature creation devices
• Submission of information to the signature-code owners on tested and confirmed signature application components.
• Directory services (see also [SigV] §4)
  Accredited CAs have to guarantee that qualified certificates are accessible and verifiable by anyone at any time using public telecommunication links. Qualified certificates have to be kept in the directory from the time of their issuance for the period indicated within the certificate and at least for another thirty years from the end of the validity of the certificate.

The signature amendment law [SigG*] did not change the requirements for accredited certification service providers as defined in the signature law [SigG].

4.3.4 Requirements for Electronic Signature Products

The signature law explicitly mentions the following kinds of products:

• Secure signature creation devices
• Signature application components for signing
• Signature application components for verification
• Technical components for certification services for the generation and transfer of signature keys
• Technical components for certification services for managing qualified certificates
• Technical components for certification services for the generation of qualified time stamps

The signature law (see [SigG] §17) and the signature ordinance (see [SigV] §15) specify the following set of requirements for technical security:

• Secure signature creation devices (see also [SigV] §5)
  – storage of private signature keys,
  – generation of qualified electronic signatures,
  – reliable identification of forged signatures and false signed data,
  – protection against unauthorized use of the private signature keys, i.e. the private signature keys shall only be used after the identification of the key holder by means of possession and knowledge or of possession and one or more biometrical characteristics,
  – prohibition of storage of private signature keys outside the secure signature creation device,
  – prohibition of disclosure of private signature keys,
  – capability for the user to recognize any security-relevant changes in the component, and
  – compliant products need to be tested by an confirmation office

• Signature application components for signing
  – generation of a signature only when initiated by the authorized signing person,
  – clear indication of the start of the generation of a qualified electronic signature,
  – identification of the data to be signed,
  – optional appropriate visualization of the contents of the data to be signed,
  – prohibition of disclosure of identification data,
  – exclusive storage of identification data only on the secure signature creation device,
  – capability for the user to recognize any security-relevant changes in the component, and
  – declaration of the manufacturer of the compliant product for electronic signatures

• Signature application components for verification
  – reliable verification of qualified electronic signature including a proof of the correctness of the signature and appropriate indication,
  – reliable verification of qualified electronic signature including a clear decision whether the verified qualified certificates of the certification path were contained in the relevant certification service directories and not revoked at the given signing time,
  – identification of the data to which the signature to be verified refers,
  – indication whether the signed data are unchanged,
  – indication of the private signature key owner whose signature has been verified,
  – indication of the contents of the qualified certificate on which the signature is based, and of the appropriate qualified attribute certificates,
  – indication of the results of the subsequent check of certificates of the certification path,
  – optional appropriate visualization of the contents of the signed data,
- capability for the user to recognize any security-relevant changes in the component, and
- declaration of the manufacturer of the compliant product for electronic signatures

- Technical components for certification services for the generation and transfer of signature keys (see also [SigV] §5)
  - unique and secret generation and transfer of private signature keys on respectively to the relevant secure signature creation device,
  - guarantee that private signature keys cannot be derived from the related public signature keys or from generated signatures,
  - guarantee that private signature keys cannot be duplicated,
  - precautions to guarantee the secrecy of the card holder identification data transferred to the secure signature creation device,
  - prohibition of storage of private signature keys and the card holder identification data outside the secure signature creation device,
  - capability for the user to recognize any security-relevant changes in the component, and
  - test of compliant products of this type by a testing and confirmation office.

- Technical components for certification services for managing qualified certificates
  - accessibility and verifiability of qualified certificates,
  - protection from unauthorized alteration and unauthorized downloading of qualified certificates,
  - guarantee that the revocation of qualified certificates cannot be rescinded without being noticed,
  - guarantee that the information about the status of qualified certificates can be checked for genuineness,
  - information about the status of qualified certificates must include whether the verified qualified certificates were present in the relevant certification service directories and not revoked at the given time,
  - qualified certificates for which the owner has not given his allowance for publication must not be made publicly available for retrieval,
  - capability for the user to recognize any security-relevant changes in the component, and
  - declaration of the manufacturer of the compliant product for managing qualified certificates

- Technical components for certification services for the generation of time stamps
  - exclusion of forgery and falsification during the generation of qualified time stamps,
  - inclusion of the official time valid at the generation time of the qualified time stamp,
  - capability for the user to recognize any security-relevant changes in the component, and
  - declaration of the manufacturer of the compliant product for time stamps

With respect to the recognition of foreign products for electronic signatures the signature law (see [SigG] §23) specifies the following additional requirements:
• Products for electronic signatures of another EU Member State or another signatory to the Treaty on the European Economic shall satisfy the requirements of the European directive [EC DIR].
• Products for qualified electronic signatures of a state mentioned before or of a third country are regarded as equivalent if they can prove that they offer the same security as the products for qualified electronic signatures used by accredited certification service providers.

The changes of the signature law related to electronic signature products [SigG*] have the following effects.

The signature amendment law (see [SigG*] no. 8) further requires manufacturers to hand-over a declaration in written form to the competent authority at latest when the product is brought to the market. Manufacturer declarations must contain a precise designation of the issuer and the product and precise information about the individual requirements of the signature law and the signature ordinance to which the product conforms. Declarations compliant with the signature law and signature ordinance will be published in the official gazette of the RegTP (competent authority).

4.3.5 Requirements for Testing and Confirmation Offices

4.3.5.1 Non-technical Requirements

The signature law (see [SigG], §18) and the signature ordinance (see [SigV] §16) specify the following set of requirements and/or options for the testing and confirmation offices:

• Natural persons or legal entities may request to operate as a confirmation or as a testing and confirmation office under the control of the competent authority.
• An application for operating as a testing and confirmation office must include the following items:
  – name and address of the applicant and his legal representatives,
  – current certificates of good conduct of applicant and his legal representatives,
  – current extract from commercial register or equivalent document,
  – documents to prove the financial independence (minimum capital and comparable collateral), and the necessary technical, administrative and specialized legal knowledge for performing these tasks, of reliability.
• Submission of the documentation to the competent authority at start of operation

Details for requirements for testing and confirmation offices will be published in the official gazette of the RegTP (competent authority).

The signature amendment law [SigG*] did not change the general requirements for the testing and confirmation offices as defined in the signature law [SigG*]
4.3.5.2 Requirements for Testing Products for Qualified Electronic Signatures

The signature law (see [SigG] §15) and the signature ordinance (see [SigV] §11 and annex I) specify the following set of requirements and/or options related to the testing of products for qualified electronic signatures:

Basis for testing
The basis for testing shall be either the
- “Common Criteria for Information Technology Security Evaluation” [CC], or the
- “Information Technology Security Evaluation Criteria” [ITSEC]
in their current version.

Level of Evaluation
- Technical components for certification services for
t  - generation and transfer of signature keys:
The testing must cover at least the evaluation level EAL4 or E3.
t  - managing qualified certificates outside a specially secured area (trust centre):
The testing must cover at least the evaluation level EAL4 or E3.
t  - managing qualified certificates inside a trust centre:
The testing must cover at least the evaluation level EAL3 or E2.
t  - generation of time stamps outside a trust centre:
The testing must cover at least the evaluation level EAL4 or E3.
t  - generation of time stamps inside a trust centre:
The testing must cover at least the evaluation level EAL3 or E2.
- Secure signature creation devices
  - The testing must cover at least the evaluation level EAL4 or E3.
- Signature application components for signing and verification
  - The testing must cover at least the evaluation level EAL3 or E2.

Analysis of Weak Points
Evaluations against a high attack potential and a full misuse analysis shall be done for products with level E3 and E2.

Strength of Mechanisms
The strength of security mechanisms shall be categorized as high for products with level E3 and E2. The strength of mechanism for the purpose of identification with biometrical characteristics shall be categorized as mean for products with level E3 and E2 if these are used in addition to knowledge-based data.

Algorithms
The strength of security mechanisms shall be categorized as high for products with level E3 and E2. The strength of mechanism for the purpose of identification with biometrical
characteristics shall be categorized as mean for products with level E3 and E2 if these are used in addition to knowledge-based data.

Approval of Products for Qualified Electronic Signatures
The testing and confirmation office shall confirm the compliance of a tested product with the requirements of the signature law (see [SigG], §17) and the signature ordinance (see [SigV] §15). This confirmation shall include the following information:

- List of relevant requirements against which the product has been tested
- Algorithms and related parameters used and the time until which they are considered as suitable
- Evaluation level of the testing procedure and the achieved strength of security mechanisms

The testing and confirmation office has to deliver the test report, the assessment document and the confirmation to the competent authority.

The signature amendment law [SigG*] did not change the general requirements for the testing of products for qualified electronic signatures as defined in the signature law [SigG].
4.4 References


[SigG*] Bundesgesetzblatt (Federal Law Gazette) No. 1, p 2: First Law Amending the Signature Law, (Entwurf eines Ersten Gesetzes zur Änderung des Signaturgesetzes 1. SigÄndG), please note that currently an English version of this amendment law is not available, January 2005


5 Active PKI Projects in Germany

This chapter contains a brief description of relevant active PKI projects in Germany.

The survey is focused on the quality of the used electronic signature and the related law.

The projects are arranged according to their application domains.

5.1 E-Government Projects

5.1.1 BundOnline 2005

The German Government and Administration are preparing for the digital future with the e-government program BundOnline 2005 [OL_BuOn05]. The Federal Government's aim is to go online with all services which are suitable for the Internet by the year 2005. 403 services were scheduled to be offered online by this time. The services concern the citizens (administration to citizen), business (administration to business), and the authorities on the federal, state, and local level alike (administration to administration).

www.bund.de, the Federation's service portal www.bund.de is supporting the Federation's extension of online services into an overall e-government package. It covers the whole range of Internet services offered by constitutional organs, administrative bodies and other public sector institutions.

Some of the projects, developed within the scope of BundOnline 2005 are:

- BAföG-services online, New Internet service for students repaying their loans
- Virtual Labour Market, The Federal Institute for Employment offers comprehensive services on the Internet
- ELSTER, "Electronic Tax Declaration"
- BSV Direct, Internet Banking Service

As a joint programme for all federal authorities, BundOnline provides five so called “one for all services”, five joint basic components and four competence centres.

The central idea of the “one for all services” is to separate the rendering of services from the specific and different areas the ministries and the pertinent public agencies are responsible for. As an example the subsidy process is more or less the same in every ministry independent of the purpose of the grant. Hence the one for all service “profi project subsidy system” covers the identical IT support requirements of several public agencies.

With the same intention five basic components have been developed
The "payment transaction platform" basic component
The "content management system" basic component
The "form server" basic component
The "data security" basic component
The "www.bund.de portal" basic component

As a central service of the "data security" basic component the "virtual post office" for secure electronic communication is being developed. This component provides security functions like authentication, creation and verification of electronic signatures, encryption and decryption of messages.

Beside the services and components four competence centres have been established

- The "workflow management, processes and organization" competence centre
- The "payment transactions" competence centre
- The "data security" competence centre
- The "content management system" competence centre

The competence centres have been established to support the ministries and public agencies in introducing and integrating the corresponding basic components.

All functions and components have been developed in a standardized and modular manner. As an important basis the SAGA (Standards and Architectures for eGovernment Applications) has been defined by the Co-ordinating and Advisory Agency of the Federal Government for Information Technology in the Federal Administration (KSt) [OL_KBST_SAGA].

5.1.2 Administration PKI

The Administration-PKI [OL_APKI] started from the experimental SPHINX project in February 2001. The aims were to set up a PKI and to introduce interoperable products for secure message and document exchange. Since that time the Administration-PKI is used commonly by the federal, the states and the municipal administrations to secure their electronic communication.

The German IT Security Agency (GISA) runs the Policy CA (Root) of the Administration-PKI and a certification authority, called Administration-CA, which may be used as a certification authority by federal, state or municipal administrations. This Administration-CA is certified by the Policy CA. Another way to participate is to ask for certification services from a commercial trust center that is not located in the administration area but that also has a certificate from the Policy CA, what means it commits to be compliant with the Policy CA's policy in written form. The Administration-PKI commonly works with advanced certificates.

Trust centers and administrations, which actually are involved in the Administration-PKI, are
– Atos Origin GmbH (formerly SchlumbergerSema Competence Center Informatik GmbH)
– Bayerisches Landesamt für Statistik und Datenverarbeitung (The Bavarian State Office for Statistics and Data Processing)
– D-Trust (trust center)
– Datenzentrale Schleswig-Holstein (central service provider for the state Schleswig-Holstein operated by Dataport)
– Deutscher Bundestag (operated by Betrusted, formerly TC-Trustcenter AG)
– IVBB (operated by T-Systems GEI GmbH BU ITC Security; T-TeleSec)
– LIT Berlin (central service provider for the state Berlin)
– LIT Hamburg (State Office for Information Technology Hamburg, operated by Dataport)
– rip-Trust (operated by T-Systems GEI GmbH BU ITC Security; T-TeleSec)
– Betrusted (formerly TC-Trustcenter AG)
– TESTA (Trans-European Services for Telematics between Administrations, operated by T-Systems GEI GmbH BU ITC Security; T-TeleSec)

An X.500 directory run by IVBB (Informationsverbund Berlin-Bonn) [OL_IVBB] provides certificates and certificate revocation lists used in the Administration-PKI.

5.1.3 Service Provider Regulatory Authority for Telecommunications and Post (RegTP)

The Regulatory Authority for Telecommunications and Posts (RegTP) [OL_RegTP] issues certificates according to Germany's signature law (SigG) for providers of certification services such as the Telekom Trust Center T-Telesec, DATEV eG or TC-Trustcenter AG (now Betrusted). This so called accredited trust centers for their part supply end customers with electronic certificates and signatures. The RegTP also operates a directory and certificate revocation list (CRL) service.

The complete list of all accredited trust centers is available on RegTP's website [OL_RegTP] following the “Electronic Signature”-Link.

5.2 E-Health Care Projects

5.2.1 Overview

As of 2006 the electronic health card will replace the medical insurance card for all people insured by Germany’s health insurance companies. The health card has been designed as a microprocessor card that will store data and also enable access to servers. Therefore it is necessary to provide authentication, encryption and digital signature. Data may only be accessed if doctors or dentists provide proof of their identity with their electronic Health Professional Card and the patient consents by entering a PIN.

To prepare the adoption of the electronic health card there are a lot of ongoing projects as well in the area of specification as in production of cards and in performance of pilot projects. One of the pilot projects is described in chapter 5.2.2.
About 72 millions patients, 350,000 doctors and dentists, 2,000 hospitals and 22,000 pharmacies will be integrated in the process of the adoption of the electronic health card and the electronic Health Professional Card.

5.2.2 Pilot Project to advance health professional cards for physicians in Sachsen (Germany)

620 hospital physicians in radiology departments of 5 hospitals in Sachsen are provided with a chip card, as a first step towards the health professional card (HPC) that allows doctors to store and retrieve patient data such as radiological diagnostic findings.

The used cards are crypto microprocessor smart cards with encryption offered by Giesecke & Devrient (G&D), a leading supplier of smart cards. The provided certificates are from TC TrustCenter (now Betrusted), a Certification Authority accredited by the Regulatory Authority for Telecommunications and Posts (RegTP) in accordance with the German Signature Act.

5.3 Public Key Infrastructures inside of Enterprises

In Germany a lot of large companies in various industrial sectors have established their own Public Key Infrastructures in order to provide their employees with digital signatures, e.g. the corporate groups Mannesmann, Siemens, Thyssen, Volkswagen, or the Fraunhofer Gesellschaft as well as federal, state or municipal administrations.

Large numbers of certificates are issued for internal corporate use but they are often issued from one specific service provider. (An initiative to join such PKIs is described in chapter 5.4.1, the European Bridge-CA.). The used certificates are simple or advanced ones. The identification of the certificate owner (the employee) is done by members of the local personnel administration either by appearance in person or with the aid of secure administration management systems. Certificates are distributed to employees both on chip cards and as software tokens. The most used certificate type is x.509v3. Each enterprise has defined a policy that is in force for the internal corporate use. Partially separate key pairs are used for signature, authentication and/or key and data ciphering. Certificates are used both to identify persons and electronic equipment (e.g. for client / server authentication purposes).

Applications using certificates are for example

- Identity card for internal enterprise wide use, e.g. for Secure Login and Single Sign on
- Electronic Mail
- HTTPS (SSL+TLS)
- Virtual Private Network
- Secure Administration Management Systems

As part of the PKI a directory service is operated by enterprises, where certificates and revocation lists are published for internal use. Enterprises, which participate in the European
Bridge-CA initiative, publish certificates and revocation lists partially by public LDAP- or Web-Services.

The requirements for long-term archiving of signed documents and time stamp services actually are mean but will increase in the future.

5.4 Joint Projects

5.4.1 European Bridge-CA

The European Bridge-CA (EBCA) [OL_EBCA] is an initiative of Deutsche Telekom AG and Deutsche Bank AG. It bands together existing Public Key Infrastructures of corporations and public administration units based on the S/MIME-Standard (with profiling ISIS/MTT) and offers testing in the this field. After registered with the European Bridge-CA a company can communicate securely with all other participating organizations without having to conclude bidirectional contracts.

The European Bridge-CA publishes its own Root Certificate, Signing Key and a Signed Certificate List which contains the CA Certificates of its participants.

The current members of the European Bridge-CA are for example the Administration PKI, Siemens AG, Deutsche Bundesbank, Deutsche Telekom AG and Deutsche Bank AG. The European Bridge-CA is operated by TeleTrusT Deutschland e.V.

A list of member certificates signed with the EBCA Signing Key you can find in chapter 8.1.

5.4.2 The Signature Alliance

The Signature Alliance (German: Signaturbündnis) [OL_SigA] has been established in April 2003 as a joint initiative of the business community and administrations. The aim of the Signature Alliance is that all citizens will be able to use a chip card based on a standardized technical infrastructure and issued by various providers. With this card citizens will be enabled to perform a wide variety of electronic operations involving government agencies and the private sector for authentication and encryption as well as signing documents. It is intended that the used certificates fulfill the requirements of advanced or qualified signatures, thus complying with German and European law.

Actually forty organizations are members of the Signature Alliance. You can find the list of members in chapter 8.2.
5.5 Research and Standardization

5.5.1 ArchiSig / ArchiSoft

The objective of the project ArchiSig was to extend an interdisciplinary co-operation existing archiving concepts by new technical components and organizational concepts such that they enable to preserve, securely and conclusively, digitally coded and signed documents over durations of 30 years and more.

Integration of verification data into signatures and signature renewal for long-term conservation purposes was not yet in adequate account of signature standards. Therefore this gap was closed with the aid of the ArchiSig project within the scope of the national standardization initiative ISIS-MTT [OLISIS_MTT_LT] and the international standardization activities of the Internet Engineering Task Force (IETF) Working Group “Long Term Archiving and Notary Services” (LTANS) [OL_IETF_LTANS].

In the context of the ISIS-MTT standardization initiative a legal opinion was commissioned that proves that the proposal “Long-Term Conservation of Electronic Signatures” complies with the German Signature Law. Both documents are published on the ISIS-MTT website [OLISIS_MTT_LT].

A detailed description of the ArchiSig project you will find in the Final Report “Practical Time-Stamp Requirements”, chapter 4, “Detailed Explanation of the ArchiSig Project”.

Subsequent to the ArchiSig project the Fraunhofer Institute SIT has developed the complete software package ArchiSoft as the practical implementation of the ArchiSig concept.

This software package allows enterprises to observe the legal requirements for archival and to streamline their archiving processes. Using ArchiSoft errors and additional costs resulting from transformation of paper based to digital signed documents are minimized. The software is easy to integrate into document management systems.

5.5.2 TransiDoc

TransiDoc – Legally Secure Transformation of Signed Documents – is a research project under the leadership of the Fraunhofer Institute SIT, founded by the German Ministry of Economics and Labour.

The problem under examination is the growing number of specialised document formats in all application areas. With digitally signed documents this leads to problems, since changing the format breaks the original signature. A similar problem occurs when paper based documents will be transformed into digital ones.

TransiDoc is tackling these problems by developing both concepts and concrete solutions for the practice in the areas of health care, public administration and the legal professions.
Guiding principle of TransiDoc is the development and specification of a seal for transformed documents which holds certain document data in cryptographically secured form. Such a transformation certificate can only be useful if it is accomplished in a trustworthy way and blends in seamlessly into diverse workflows.

TransiDoc handles all kinds of signatures simple ones as well as advanced and qualified signatures. Therefore apart from technical solutions TransiDoc has to take organisational procedures as well as existing and future law into account.

5.6 References and Related Links


[OL_KBST_SAGA] Latest SAGA Version provided on the KBSI's web pages, [http://www.kbst.bund.de/saga](http://www.kbst.bund.de/saga)


[OL_IVBB] IVBB Directory, [http://x500.bund.de/](http://x500.bund.de/)


[OL_SigA] Signature Alliance, [http://www.signaturbuendnis.de/](http://www.signaturbuendnis.de/)


6 About Electronically Stored Documents in Germany

The German Federal Government strives for citizens and enterprises to handle all everyday transactions via the internet. It wants enterprises to use electronic applications in the private sector and to continue their e-business applications towards communication with public administrations – without a media gap at the door of the town hall.

Generally declarations of intent are possible and legally binding in any form in both, the private and the public sector. However, in the past this was only true in principle. This general rule was subsidiary. Special regulations in all sectors overruled these. In particular cases a special regulation then often required written form, paper and handwritten signatures. In reality electronic acting was not admissible in many relevant cases.

To alter this situation and to achieve the above mentioned goal Germany enacted many new laws. These laws adjust the form clauses to enable legally binding electronic applications in both, the private and the public sector.

1. Private Law

The most important adjustment in the private sector was done by the Law adapting formal regulations of private law and other regulations to modern legal relations (Federal Law Gazette 18 July 2001 Part I page 1542; entry into force 19 July 2001) [Form]. It introduced in Art. 126 sec 3 Civil Code an electronic form as an equivalent for the written form. According to Art. 126 a Civil Code an electronic document is to be attached with a qualified certificate and signed with a qualified electronic signature in order to fulfil the electronic form.

Art. 126 sec. 3 and 126a Civil Code are blanket clauses. They are applicable to all regulations in the private sector. Wherever in the private law written form, e.g. paper document and handwritten signature, is required, the electronic form is allowed to be used also. On account of this blanket clause adjustments to the many regulations requiring written form were not carried through. Specific exceptions to these blanket clauses were regulated in about 35 articles of the Law adapting formal regulations of private law and other regulations to modern legal relations.

Therefore in Germany the general rule is effective that private documents may be used in electronic form. If there is no form requirement electronic documents can be used without additional electronic signature. If there is the requirement of written form electronic documents can be used with a qualified electronic signature. This rule is applicable to all general and specific laws in the private sector as for instance the other provisions of the civil code, the commercial code or the law on contracts of insurance.
Additionally to that Art. 126b Civil Code introduced a text form – a form for different kind of documents without the need of a handwritten or electronic signature. A text form comprises also electronic documents. The text form is admissible if a specific provision allows the usage of this form.

Exceptional rules which explicitly require written form are stipulated for instance for instance for consumer credit contracts according to § 492 Civil Code, for the notice of termination of employment contracts according to § 623 Civil Code or for certificates of employments according to § 630 Civil Code.

2. Administrative Law

The most important adjustment in the public sector was done by the Third Amendment of the administrative procedure law (Federal Law Gazette 27. August 2002 Part I page 3322; entry into force 1 February 2003) [E-FORM].

In Art. 3a sec. 2 of the administrative procedure law an electronic form for public law is set up in a blanket clause and compared with the written form. In order to fulfil the electronic form an electronic document is to be attached with a qualified certificate and signed with a qualified electronic signature. Wherever in the administrative law written form, e.g. paper document and handwritten signature, is required, the electronic form is allowed to be used also. On account of this blanket clause adjustments to the many regulations requiring written form are not necessary. Specific exceptions to this blanket clause were regulated in about 75 articles of the Third Amendment of the administrative procedure law. Exceptional rules which explicitly require written form are stipulated for instance for the issue of passports according to § 6 PassG (Passgesetz – Passport law), licences and confirmations for the conveyance of passengers as well as the revocation of licences and confirmations according to § 5 PBefG (Personenbeförderungsgesetz – Conveyance of passenger law) or documents dealing with citizenship affairs § 38a (Staatsangehörigkeitsgesetz – Citizenship Law) (URL No. 5.9).

Therefore in Germany the general rule is effective that private documents to provide to administrations may be used in electronic form. Generally the administrative procedure law determines the administrative procedure to be carried through simply, suitably and promptly, it is not bound to any specific forms. According to this citizens and public authorities can also act in electronic forms without electronic signature. If specific regulations require written form an electronic document with a qualified electronic signature may be used. This rule is applicable to all general and specific laws in the public sector as for instance the building code, the industrial code, registration laws or environmental protection laws.

3. Tax Law and Social Security Law

The same rule is applicable for both other general laws in the public sector, the tax code and the social security code. Like the administration procedure law they comprise a blanket clause which determines the electronic form equivalent with the written form. This is regulated in Art. 87 sec. 3 tax code and Art. 36a first book of the social security code. Therefore also in the cooperation with tax administration and with social security administration the general rule is effective that private documents to provide to administrations may be used in electronic form.
Exceptional rules which explicitly require written form are stipulated for instance for certain notifications of courts or other institution dealing with the confirmation of documents concerning acquisition of real estate according to § 18 sec. 1 GrEstG (Grunderwerbssteuergesetz - Tax on acquisition of real estate Act) (URL No. 2.13) or for notifications of courts and other institutions regarding documents and events influencing inheritance tax according to § 7 – 10 Erbschaftssteuerdurchführungsverordnung (Executive Decree of the inheritance tax).

4. Procedure Law

In the field of court procedures the German Federal Government has passed a draft of a judicial system communication law in summer 2004. It is expected to be enacted in 2005. According to that filing a lawsuit in electronic form will be admissible. Providing electronic documents as evidence are already admissible today. There is also a specific rule for an assumption of evidence according to qualified electronic signature in Art. 292a of the civil procedure code.

5. Requirements of electronic documents

The Federal Government of Germany intends to make enterprises to use electronic documents in the cooperation with administration in order to foster electronic government. They will have to use electronic documents and will not be allowed to use paper documents from 2005 and 2006 respectively onwards for instance for the tax card of employees, declaration of turnover tax, declaration of income tax of employees, certificates of employment, certificates of income of employees and so on. This is the prerequisite to establish the two electronic government programs of “ELSTER” and “BundOnline2005”.

6. Blanket Clauses

In the past the mainly used form ist the written form. In order to allow the replacement of the written form by an electronic form many modern German laws use the same wording of a blanket clause. In a losse translation this wording is: „A written form required by law can be replaced by electronic form, if there is no exclusion by another regulation. In case of replacing the written form a qualified electronic signature may be used.” In the attached document “Typical or important clauses“ the important regulations using this clause are listed. In most of the documents mentioned in appendix 8.5 or in appendix 8.6 or in this section this clause is used.

Appendix 8.5 lists document types and related legal systems that apply to electronic-to-electronic and to paper-to-electronic document transformation processes.

Below the typical wording of the blanket clauses allowing electronic form and of the introducing clauses of administration and procedure law is loosely translated. For demonstration purposes the German text of the different corresponding clauses is added. The nearly identical wording is marked by italics.
6.1 Typical or important clauses

Below the typical wording of the blanket clauses allowing electronic form and of the introducing clauses of administration and procedure law is loosely translated. This section contains relevant laws existing only in German language. For key regulations an English translation is provided.

Blanket clauses (wording used for § 126, 126a BGB, § 3a VwVfG, § AO, SGB I)

Translation of the blanket clauses:
„A written form required by law can be replaced by electronic form, if there is no exclusion by another regulation. In case of replacing the written form a qualified electronic signature may be used”

- (Civil Code) BGB § 126 Schriftform (Written form)
- (Civil code) BGB § 126a Elektronische Form (Electronic form)
- (Tax code) AO § 87a Elektronische Kommunikation (Electronic communication)
- (First book of the social security code) SGB I § 36a [1] Elektronische Kommunikation (Electronic communication)

Wording of clauses introducing electronic form into process or administration law (e.g. § 86a sec. 1 VwGO, § 46b sec. 1 ArbGG, § 125a sec. 1 PatG)

Translation:
If the written form is destined for […] enumeration of documents], the recording as an electronic document will comply with this form, if the document is appropriate to the processing by the [name of the institution concerned by the law]

- (Civil Procedure Code) ZPO § 130a [1] Elektronisches Dokument (Electronic document)
- VwGO § 86a [1] [Elektronisches Dokument] (Electronic document)
- ArbGG § 46b [1] Einreichung elektronischer Dokumente (Submission of electronic document)
- PatG § 125a [1] [Einreichung elektronischer Dokumente] Dokumente (Submission of electronic document)
7 Conclusions about Signature Laws and PKI-Projects in Europe and Germany

Electronic Signatures Law in Europe

The report presents the most relevant EU directives and commission decisions concerning electronic signature law in the EU. The study [EU-Report] describes in detail the legal and market aspects of electronic signatures in the EU in general and also in each member state. Unfortunately there are no relevant documents regarding a discussion how to deal with digitally scanned paper documents.

Electronic Signatures Law in Germany

The German legislation with its electronic signatures law [SigG] and first amendment of the electronic signatures law [SigG*] has created the necessary frame conditions for the use of electronic signatures in legal transactions, electronic communication and electronic commerce in Germany. It has been designed in a way that complies with the requirements of the European electronic signatures directive [EC DIR] reaching a high level of harmonization. In addition to the electronic signatures law other new laws have been issued that regulate the legal equivalence of electronic signatures to handwritten signatures and the legal effectiveness in legal proceedings. These are the “Law on the adaptation of form requirements and other requirements for modern legal transactions” [Form] that establishes the legal effect for qualified electronic signatures in the civil law sector, and the “Third law amending the administrative procedural requirements” [E-FORM] that defines the “electronic form” in the public law sector.

PKI Projects in Europe

Many projects related to PKI technology and applications using electronic signatures are currently performed in Europe in the scope of the European Council’s eEurope 2005 Action Plan. These European PKI projects can be classified as

- Corporate and personal e-banking,
- Standardization initiatives,
- E-health care projects,
- E-business projects,
- E-government projects, and
- E-learning projects.

E-government is the rapidly rising application for electronic signatures in Europe and is connected with the applications in the area of E-health care.
PKI Projects in Germany

Many projects related to PKI technology and applications using electronic signatures have
been recently initiated in Germany and are currently active and are further improved to get
into efficient operation. These German PKI projects can be classified as

- E-Government projects,
- E-Health Care Projects,
- Enterprise PKIs,
- Joint Projects, or
- Research and standardization projects.

Among these projects the e-government program BundOnline2005 and the e-health care
project can be evaluated as the projects with the highest effect to promote the use of
electronic signatures in Germany.

The e-government project will provide about 400 online services in the public sector for
"administration to citizen", "administration to business" and "administration to administration"
communication.

The e-health care project specifies the introduction, realization and the use of the health
professional card and the electronic health card for the health care area from 2006 on for all
people insured by German health insurance. About 72 millions patients, 350,000 doctors
and dentists, 2,000 hospitals and 22,000 pharmacies will be integrated in the process of the
adoption of the electronic health card and the electronic Health Professional Card.

About Electronically Stored Documents in Germany

The German Federal Government strives for citizens and enterprises to handle all every day
transactions via the internet. It wants enterprises to use electronic applications in the private
sector and to continue their e-business applications towards communication with public
administrations – without a media gap at the door of the town hall.

Generally declarations of intent are possible and legally binding in any form in both, the
private and the public sector. However, in the past this was only true in principle. This general
rule was subsidiary. Special regulations in all sectors overruled these. In particular cases a
special regulation then often required written form, paper and handwritten signatures. In
reality electronic acting was not admissible in many relevant cases.

To alter this situation and to achieve the above mentioned goal Germany enacted many new
laws. These laws adjust the form clauses to enable legally binding electronic applications in
both, the private and the public sector. Appendix 8.5 lists document types and related legal
systems that apply to electronic-to-electronic and to paper-to-electronic document
transformation processes.
8 Additional Information about Signature Laws and PKI-Projects in Europe and Germany

8.1 List of Certificates in the EBCA TrustList

![Certificate List](image-url)
8.2 List of Members of the Signature Alliance

- Atos Origin GmbH
- Bayerische Hypo- und Vereinsbank AG
- BKK Bundesverband
- Bremen-Online-Services GmbH & Co. KG
- Bundesagentur für Arbeit
- Federal Ministry of Defense
- Federal Ministry of the Interior
- Federal Ministry of Finance
- Federal Ministry of Economics and Labour
- Bundesnotarkammer
- Bundesverband der Deutschen Volksbanken und Raiffeisenbanken
- Bundesverband Deutscher Banken e.V.
- Bundesverband öffentlicher Banken
- Federal Insurance Institute for Salaried Employees
- Commerzbank AG
- Curiavant Internet GmbH
- Datenzentrale Baden-Württemberg
- DATEV eG
- DE-CODA GmbH
- Deutsche Bank AG
- Deutsche Post Com GmbH
- D-TRUST GmbH
- Gesamtverband der Deutschen Versicherungswirtschaft e.V.
- Hessisches Ministerium des Innern und für Sport
- Infineon Technologies GmbH
- Informatikzentrum Niedersachsen
- LASA Brandenburg GmbH
- SAP AG
- secunet AG
- Siemens AG
- Sparkassen-Finanzgruppe
- SUN Microsystems GmbH
- TC Trustcenter
- T-Systems International GmbH
- Ventasoft GmbH
- Verband Deutscher Rentversicherungsträger
- Verein Media@Komm Esslingen e.V.
- Wilken GmbH
- Winter AG
- Zentralverband des Deutschen Handwerks
8.3 Comparison of the Definitions of Terms

This appendix contains the definitions of terms that have been used in the European directive on electronic signatures (see [EC DIR], article 2), and in the German electronic signatures law (see [SigG], §2). The following table can be used to show the similarities as well as the differences between both legal frameworks.

Table 1: Definition of Terms

<table>
<thead>
<tr>
<th>#</th>
<th>European Directive</th>
<th>German Signature Law</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>electronic signature</strong> means data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication;</td>
<td><strong>electronic signatures</strong> shall be data in electronic form that are attached to other electronic data or logically linked to them and used for authentication</td>
</tr>
<tr>
<td>2</td>
<td><strong>advanced electronic signature</strong> means 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;</td>
<td><strong>advanced electronic signatures</strong> shall be electronic signatures as in 1. above that a) are exclusively assigned to the owner of the signature code b) enable the owner of the signature code to be identified c) are produced with means which the owner of the signature code can keep under his sole control and d) are so linked to the data to which they refer that any subsequent alteration of such data may be detected;</td>
</tr>
<tr>
<td>3</td>
<td>Note that there is no explicit definition of this term in the directive. However article 5 can be used as an implicit definition. It reads as follows: Member States shall ensure that advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device: (a) satisfy the legal requirements of a signature in relation to data in electronic form in the same manner as a handwritten signature satisfies those requirements in relation to paper-based data; and (b) are admissible as evidence in legal proceedings.</td>
<td><strong>qualified electronic signatures</strong> shall be electronic signatures as in 2. above that a) are based on a qualified certificate valid at the time of their creation and b) have been produced with a secure signature-creation device;</td>
</tr>
<tr>
<td></td>
<td><strong>signature-creation</strong> data means unique data, such as codes or private cryptographic keys, which are used by the signatory to create an electronic signature;</td>
<td><strong>signature codes</strong> shall be unique electronic data such as private cryptographic codes that are used to create an electronic signature;</td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td>---</td>
</tr>
<tr>
<td>5</td>
<td><strong>signature-verification-data</strong> means data, such as codes or public cryptographic keys, which are used for the purpose of verifying an electronic signature;</td>
<td><strong>signature test codes</strong> shall be electronic data such as public cryptographic codes that are used to test an electronic signature;</td>
</tr>
<tr>
<td>6</td>
<td><strong>certificate</strong> means an electronic attestation which links signature-verification data to a person and confirms the identity of that person;</td>
<td><strong>certificates</strong> shall be electronic certificates assigning signature test codes to a person and confirming his or her identity;</td>
</tr>
<tr>
<td>7</td>
<td><strong>qualified certificate</strong> means a certificate which meets the requirements laid down in Annex I and is provided by a certification service-provider who fulfils the requirements laid down in Annex II;</td>
<td><strong>qualified certificates</strong> shall be electronic certificates pursuant to 6. above for natural persons that fulfill the requirements in Section 7 and are issued by certification service providers who meet at least the requirements under Sections 4 to 14 or Section 23 of this Law and the provisions of the statutory ordinance pursuant to Section 24 that are based on this Law;</td>
</tr>
<tr>
<td>8</td>
<td><strong>certification service-provider</strong> means an entity or a legal or natural person who issues certificates or provides other services related to electronic signatures;</td>
<td><strong>certification service providers</strong> shall be natural persons or legal entities who issue qualified certificates or qualified time stamps;</td>
</tr>
<tr>
<td>9</td>
<td><strong>signatory</strong> means a person who holds a signature-creation device and acts either on his own behalf or on behalf of the natural or legal person or entity he represents;</td>
<td><strong>signature-code owners</strong> shall be natural persons who own signature codes and to whom the appropriate signature test codes have been assigned in qualified certificates;</td>
</tr>
<tr>
<td>10</td>
<td><strong>signature-creation device</strong> means configured software or hardware used to implement the signature-creation data;</td>
<td><strong>secure signature-creation devices</strong> shall be software or hardware products used to store and apply the respective signature code, that meet or exceed the requirements of Section 17 or Section 23 of this Law and the provisions of the statutory ordinance pursuant to Section 24 that are based on this Law, and that are designed for qualified electronic signatures;</td>
</tr>
<tr>
<td>11</td>
<td><strong>signature-verification device</strong> means configured software or hardware used to implement the signature-verification data;</td>
<td><strong>signature-application components</strong> shall be software and hardware products designed to a) assign data to the process of producing</td>
</tr>
<tr>
<td>12</td>
<td><strong>Electronic-signature product</strong> means hardware or software, or relevant components thereof, which are intended to be used by a certification service-provider for the provision of electronic-signature services or are intended to be used for the creation or verification of electronic signatures;</td>
<td><strong>Technical components for certification services</strong> shall be software or hardware products designed to a) create signature codes and transfer them into a secure signature-creation device b) keep qualified certificates available for testing and, if necessary, downloading by the public, or c) produce qualified time stamps;</td>
</tr>
<tr>
<td>13</td>
<td>Note that there is no explicit definition of this term in the directive.</td>
<td><strong>Products for qualified electronic signatures</strong> shall be secure signature-creation devices, signature-application components, and technical components for certification services;</td>
</tr>
<tr>
<td>14</td>
<td>Note that there is no explicit definition of this term in the directive.</td>
<td><strong>Qualified time stamps</strong> shall be electronic certificates issued by a certification service provider that meet or exceed the requirements under Sections 4 to 14 and Section 17 or Section 23 of this Law and the provisions of the statutory ordinance pursuant to Section 24 that are based on this Law, and that confirm that certain electronic data have been presented to it at a certain time;</td>
</tr>
<tr>
<td>15</td>
<td><strong>Voluntary accreditation</strong> means any permission, setting out rights and obligations specific to the provision of certification services, to be granted upon request by the certification service-provider concerned, by the public or private body charged with the elaboration of, and supervision of compliance with, such rights and obligations, where the certification service-provider is not entitled to exercise the rights stemming from the permission until it has received the decision by the body.</td>
<td><strong>Voluntary accreditation</strong> shall be a procedure to issue a permit that authorizes the operation of a certification service and confers specific rights and obligations.</td>
</tr>
</tbody>
</table>
### 8.4 Comparison of Requirements for Qualified Certificates

This appendix contains the requirements for the content of qualified certificates that have been used in the European directive on electronic signatures (see [EC DIR], annex I), and in the German electronic signatures law (see [SigG], §7). The following table can be used to show the similarities as well as the differences between both legal frameworks.

<table>
<thead>
<tr>
<th>#</th>
<th>European Directive qualified certificates must contain:</th>
<th>German Signature Law a qualified certificate shall contain the following data:</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>the advanced electronic signature of the certification service-provider issuing it;</td>
<td>and bear a qualified electronic signature</td>
</tr>
<tr>
<td>2</td>
<td>the name of the signatory or a pseudonym, which shall be identified as such;</td>
<td>the name of the signature-code owner, to which a supplement shall be added if there is a possibility of confusion with another name, or an unmistakable pseudonym assigned to the signature-code owner and recognizable as such;</td>
</tr>
<tr>
<td>3</td>
<td>signature-verification data which correspond to signature-creation data under the control of the signatory;</td>
<td>the assigned signature-test code;</td>
</tr>
<tr>
<td>4</td>
<td>the identity code of the certificate;</td>
<td>the current number of the certificate;</td>
</tr>
<tr>
<td>5</td>
<td>an indication of the beginning and end of the period of validity of the certificate;</td>
<td>the start and end of its validity;</td>
</tr>
<tr>
<td>6</td>
<td>the identification of the certification service-provider and the State in which it is established;</td>
<td>the name of the certification service provider and the state in which he is domiciled;</td>
</tr>
<tr>
<td>7</td>
<td>limitations on the scope of use of the certificate, if applicable; and limits on the value of transactions for which the certificate can be used, if applicable.</td>
<td>information on whether the use of the signature code is limited to certain applications by nature or extent;</td>
</tr>
<tr>
<td>8</td>
<td>an indication that the certificate is issued as a qualified certificate;</td>
<td>information that this is a qualified certificate; and</td>
</tr>
<tr>
<td>9</td>
<td>provision for a specific attribute of the signatory to be included if relevant, depending on the purpose for which the certificate is intended;</td>
<td>if necessary, attributes of the signature-code owner. Attributes may also be included in a separate qualified certificate (qualified attribute certificate). In a qualified attribute certificate, the data under (1) may be replaced with clear</td>
</tr>
</tbody>
</table>
reference data from the qualified certificate to which it refers, where this is not needed to use the qualified attribute certificate.

8.5 Electronic-to-Electronic and Paper-to-Electronic Document Transformations in Germany

The URL numbers given in the columns of the following table refer to the numbering in Appendix 8.6.

<table>
<thead>
<tr>
<th>Type of document</th>
<th>Electronic→electronic (electronic storage when produced electronically)</th>
<th>Paper→electronic (electronic storage when produced in paper)</th>
<th>Legal systems (year enforced, etc)</th>
<th>Technical requirements, etc</th>
<th>remarks (reference, etc)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Income-tax return (tax declaration) (Form)</td>
<td>Filing electronically allowed.</td>
<td>Not provided.</td>
<td>§ 87a AO (Abgabenordnung – tax law), entry into force: 28 August 2002; If not signed with a qualified signature a concise income-tax return in paper is necessary.</td>
<td>Compatible software to ELSTER (ELSTERFormular)</td>
<td>Project ELSTER (Electronic tax return) URL: No. 2.1 Preferential treatment at some federal states. STDUeV URL No. 2.4; AO URL No. 2.7</td>
</tr>
</tbody>
</table>

financial statement, etc.
<table>
<thead>
<tr>
<th>Records, receipts connected with Income tax return</th>
<th>If the documents are originally in electronic form, an electronic dissemination should be possible.</th>
<th>Where an electronic return is possible, the connected records (the electronic and the paper ones) must be archived and can be requested by the revenue authority.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employ-ment tax: - Certificate of employment tax deduction - tax card</td>
<td>Confirmation of paid income tax (Certificate of employment tax deduction) shall be filed by employer electronically. But the income tax card is still existing in paper. Shall be abolished in 2006.</td>
<td>Not provided. § 41b sec 1 ESIG Compatible software to ELSTER Project ELSTER (Electronic tax return) URL: No. 2.1</td>
</tr>
<tr>
<td>Advanced Employ-ment tax return</td>
<td>Allowed. Since 2005 only electronic (with exceptions for certain cases)</td>
<td>Not provided § 41a sec. 1 ESIG, § 87a AO ELSTER-Formular Project ELSTER (Electronic tax return) URL: No. 2.1, ESIG URL No. 2.5</td>
</tr>
<tr>
<td>Yearly turnover tax return</td>
<td>Allowed</td>
<td>Not provided § 87a AO Encryption by ELSTER Software “ELSTER Formular” Project ELSTER (Electronic tax return) URL: No. 2.1</td>
</tr>
<tr>
<td>Service Type</td>
<td>Approval Conditions</td>
<td>Certifications</td>
</tr>
<tr>
<td>------------------------------</td>
<td>---------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Advanced Turnover Tax return (§ 18a USiG)</td>
<td>Allowed (Since 2005 only by electronic means, with exceptions for certain cases)</td>
<td>Encryption by ELSTER Software  “ELSTER Formular”</td>
</tr>
<tr>
<td>Trade tax return (§ 14a GewStG; § 25 GewStDVO (Decree on trade tax procedure))</td>
<td>Allowed.</td>
<td>§ 87a AO</td>
</tr>
<tr>
<td>Beer tax return</td>
<td>Allowed, but not realized by Hauptzollamt Stuttgart</td>
<td>§ 17 sec. 1 BierStV; § 8 BierStG</td>
</tr>
<tr>
<td>Coffee tax declaration</td>
<td>Allowed, but not realized by Hauptzollamt Stuttgart</td>
<td>§ 9 KaffeestG; § 8 KaffeestV</td>
</tr>
</tbody>
</table>
| Motor vehicle tax return     | Allowed                                                                                | § 15 KraftStG; § 3 sec. 1 KraftStDV 2002; Reference to § 87 a AO                 | Reduced qualified signature required. KraftStDV URL No. 2.12; KraftStG URL No. 2.13
<table>
<thead>
<tr>
<th>Description</th>
<th>Status</th>
<th>Requirements</th>
<th>URL No.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tax on acquisition of real estate return</td>
<td>Allowed</td>
<td>§ 19 sec. 5 GrESIG (Grunderwerbsteuer-gesetz - Tax on acquisition of real estate Act); § 87a AO</td>
<td>GrESIG URL No.</td>
</tr>
<tr>
<td>Books, receipt, order form, bill, other transaction documents.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bills in respect of turnover tax</td>
<td>Allowed</td>
<td>§ 14 sec 3, 14 b USIG, in force since 1.1.2004 (Art. 5 No. 15, 17, Art. 25 sec. 4 Second law for amending taxation rules (2. StAndG 2003); Art. 28 h sec. 3 c) Directive 2001/115/EC</td>
<td>StAndG URL No. 2.3; USIG URL No. 2.6; Directive 2001/115/EC URL No. 1.2 Qualified electronic signature: SigG 2001 (Digital signature act 2001) URL No. 7.1; Directive 99/93/EC URL No. 1.6</td>
</tr>
<tr>
<td>Electronic accountancy</td>
<td>If accountancy is stored electronically, it can be reviewed electronically by local inspectors.</td>
<td>§§ 146 sec 5, 147 sec 2, 5, 6, 200 sec 1 AO; § 14 sec 4 USIG; GDPdU</td>
<td>GDPdU URL No. 2.2</td>
</tr>
</tbody>
</table>

Electronic Signature Laws, PKI Projects and Time Stamping in the European Union and Germany 63
<table>
<thead>
<tr>
<th>Financial statements, inventories, books of account, annual statements of accounts</th>
<th>allowed</th>
<th>allowed</th>
<th>§ 257 sec 3 HGB (German Commercial Code), § 147 sec. 2 AO</th>
<th>HGB URL No. 4.1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Records of public accountants according to § 51b WiPrO (all documents, that the accountant received by or for his client)</td>
<td>Allowed</td>
<td>Allowed</td>
<td>§ 51 b sec 5 WPO (Code of conduct for public accountants)</td>
<td>WPO URL No. 5.5</td>
</tr>
<tr>
<td>Insurance policy</td>
<td>allowed</td>
<td>allowed</td>
<td>§§ 3, 4 VVG Versicherungsvertragsgesetz (Law on contracts of insurance); § 126</td>
<td>VVG URL No. 3.1</td>
</tr>
<tr>
<td>Financial report of insurances</td>
<td>In principle allowed, but depending on rules of the Bundesaufsichtsamt für Versicherungswesen (Federal Supervisory Office for the Insurance Industry).</td>
<td>§§ 54d, 55 VAG (German insurance supervision act)</td>
<td>VAG URL No. 3.2</td>
<td></td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------------------------------------------------------------------------------</td>
<td>-------------------------------------------------</td>
<td>------------------</td>
<td></td>
</tr>
<tr>
<td>Mandatory Social Insurances</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Records of Social Insurances</td>
<td>Allowed</td>
<td>§§ 110a, 110d SGB IV (Sozialgesetzbuch - Code of Social Law IV)</td>
<td>SGB IV URL No. 3.3</td>
<td></td>
</tr>
<tr>
<td>(e.g. compulsory health insurance, statutory pension insurance, employment promotion)</td>
<td>allowed</td>
<td>§ 110d SGB IV: Record is utilisable for administrative actions only with qualified electronic signature.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Contract in social affairs</td>
<td>Allowed</td>
<td>§ 56 SGB X; § 36a SGB I (Code of social law X and I)</td>
<td>SGB I URL No. 3.7; SGB X URL No. 3.6</td>
<td></td>
</tr>
<tr>
<td>Performance of Notification requirements concerning the mandatory medical insurance (§ 198 SGB V, §§ 28 a,b,c SGB IV)</td>
<td>Allowed (depending on directives of the different insurance companies)</td>
<td>§ 28c Nr. 8, 28b sec. 2 No. 4 SGB IV, § 36a SGB I</td>
<td>SGB IV URL No. 3.3; SGB V URL No. 3.4</td>
<td></td>
</tr>
<tr>
<td>Performance of Notification requirements concerning the social insurances (§ 28a SGB IV)</td>
<td>Allowed (depending on directives of the different associations of insurance companies)</td>
<td>§ 28b sec. 2 No. 4 SGB IV, § 36a SGB I</td>
<td>SGB IV URL No. 3.3</td>
<td></td>
</tr>
<tr>
<td>Order to pay of social insurances</td>
<td>Allowed</td>
<td>Allowed</td>
<td>§ 7 SVRV (Decree on monetary transactions, accounting and financial statements of social insurances)</td>
<td>Qualified electronic signature required.</td>
</tr>
</tbody>
</table>

Corporate Law

<p>| Reports to the board of directors | Allowed | Allowed | § 90 sec. 4 AktG (Companies Act); § 126b BGB (Civil Code) | No requirements. | AktG URL No. 4.2; BGB URL No. 5.2 |
| Account books | Allowed | Allowed | § 239 sec. 4, § 257 sec. 3 HGB | | HGB URL 4.1 |</p>
<table>
<thead>
<tr>
<th>Real estate register</th>
<th>The electronic storage of documents is allowed.</th>
<th>The electronic storage of documents is allowed.</th>
<th>§ 126 GBO Grundbuch-ordnung (Real estate register law)</th>
<th>Accredited qualified electronic signature.</th>
<th>GBO URL No. 5.3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conveyance of property of real estate</td>
<td>Not allowed. Change possible by entry in force of JKomG.</td>
<td>For storing at the land registry electronic storage is allowed.</td>
<td>§§ 925 sec. 1, 128 BGB (Civil Code). But Storing at the land registry: § 10a GBO (Real estate register law).</td>
<td>Qualified electronic signature.</td>
<td>GBO URL No. 5.3; BGB URL No. 5.2</td>
</tr>
<tr>
<td>Complaint at the real estate register</td>
<td>Allowed</td>
<td></td>
<td>§ 73 sec. 2 GBO, § 130 a sec. 1 ZPO (Civil Procedure Code)</td>
<td>Qualified electronic signature</td>
<td>GBO URL No. 5.3; ZPO URL No. 8.2</td>
</tr>
<tr>
<td>Commercial register</td>
<td>The electronic storage of documents is allowed.</td>
<td>The electronic storage of documents is allowed.</td>
<td>§ 8a HGB (German Commercial Code); Art. 2 Directive 2003/58/EC</td>
<td>Accredited qualified electronic signature.</td>
<td>HGB URL Nr. 4.1; Directive 2003/58/EC URL No. 1.1</td>
</tr>
<tr>
<td>Documents given to the real estate register or to the commercial register</td>
<td>Planned</td>
<td>Planned</td>
<td></td>
<td>Accredited qualified electronic signature.</td>
<td>Draft JKomG URL No. 8.1</td>
</tr>
<tr>
<td>Complaints or documents directed to the register of shipment (kept by the local courts)</td>
<td>Allowed where the Land government has used the delegated power to render a permitting decree.</td>
<td>Allowed (Reference to § 126 GBO (Real estate register law))</td>
<td>§ 89 sec. 2 SchiffRegO (Register of shipment code)</td>
<td>SchiffRegO URL No. 5.9</td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>-------------------------------------------------</td>
<td>-------------------------------------------------</td>
<td>-------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Patent application; Trade mark application</td>
<td>Allowed</td>
<td>Allowed</td>
<td>As written form is required (§ 34 VI PatG, § 2 PatAnmV)(§ 95a sec. 1 MarkenG (trade mark act), it can be replaced by electronic form according to § 3a VwVfG. Realized by ErvGewRV (decree on electronic communication concerning legal protection in commercial affairs)</td>
<td>Qualified electronic signature required.</td>
<td>URL PatG No. 5.4; URL PatAnmV No. 5.5; ErvGewRV URL No. 5.10; MarkenG URL No. 5.11</td>
</tr>
<tr>
<td>Administrative procedures, especially procedures of environmental law</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Writings, Documents directed to the administration</td>
<td>Allowed. If an administrative authority has opened an account, written form or less is required and no exception is existent.</td>
<td>Allowed</td>
<td>§ 3a VwVfG (Administrative Procedure Code)</td>
<td>Qualified electronic signature to replace written form.</td>
<td>VwVfG URL No. 6.2</td>
</tr>
<tr>
<td>Offer in a tendering procedure</td>
<td>Allowed</td>
<td>Allowed</td>
<td>§ 15 VgV (Vergabeverordnung – Tendering procedure law)</td>
<td>Qualified electronic signature and encryption required.</td>
<td>VgV URL No. 6.4</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>--------</td>
<td>---------</td>
<td>-------------------------------------------------------</td>
<td>------------------------------------------------------</td>
<td>----------------</td>
</tr>
<tr>
<td>Application regarding pollution control (§ 3, 4, 4a ff 9. BImSchV)</td>
<td>Allowed</td>
<td></td>
<td>As written form is required (§ 3 9. BImSchV) it can be replaced by electronic form according to § 3a VwVfG</td>
<td>Qualified electronic signature required.</td>
<td>VwVfG URL No. 6.2; 9. BImSchV URL No. 6.3</td>
</tr>
<tr>
<td>Application for a permission for the use of water (§ 7 WHG Water Resources Law))</td>
<td>Allowed</td>
<td>Allowed</td>
<td>§ 3a sec. 1 VwVfG</td>
<td>VwVfG URL No. 6.2 ; WHG URL No. 6.7</td>
<td></td>
</tr>
<tr>
<td>Documents of the body responsible for a project concerning an assessment of environmental effects (§ 6 UVPG)</td>
<td>Allowed</td>
<td>Allowed</td>
<td>§ 3a VwVfG</td>
<td>UVPG URL No. 6.8</td>
<td></td>
</tr>
<tr>
<td>Applications in atomic energy affairs</td>
<td>Allowed</td>
<td></td>
<td>§ 2b sec. 1 AtG (Atomic Energy Act)</td>
<td>Qualified electronic signature required. For administrative acts a accredited qualified electronic signature is required.</td>
<td>AtG URL No. 6.5</td>
</tr>
<tr>
<td>Others (electronic form admitted)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Records stipulated by § 10 SigG</td>
<td>Allowed.</td>
<td>§ 10 SigG</td>
<td>Qualified electronic signature required</td>
<td>SigG URL No. 7.1</td>
<td></td>
</tr>
<tr>
<td>--------------------------------</td>
<td>----------</td>
<td>-----------</td>
<td>---------------------------------------</td>
<td>-----------------</td>
<td></td>
</tr>
<tr>
<td>Documents regarding lawsuits filed by parties or thirds</td>
<td>Allowed.</td>
<td>Allowed.</td>
<td>Art. 2, 5 No. 2, 6b, 7, 8, 9 Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr (Law adapting formal regulations of private law and other regulations to modern legal relations); § 130 a sec. 1 ZPO (Code of civil procedure)</td>
<td>Qualified electronic signatures required.</td>
<td>Adapting Law URL No. 5.1; ZPO URL No. 8.2</td>
</tr>
<tr>
<td>Criminal information</td>
<td>Allowed</td>
<td>Allowed</td>
<td>§ 158 StPO (Criminal Procedure Code)</td>
<td>A criminal information can be done verbally, so it is possible electronically, if an electronic access is given.</td>
<td>StPO URL No. 8.3</td>
</tr>
<tr>
<td>Ban of an association</td>
<td>Allowed</td>
<td>Allowed</td>
<td>§ 3 sec. 4 VereinsG (Association Law)</td>
<td>The ban has to be sent from the administration to the appropriate court. An accredited qualified electronic signature is required</td>
<td>VereinsG URL No. 6.6</td>
</tr>
</tbody>
</table>
8.6 URLs Related to Legal Aspects of Document Transformation

8.6.1 URLs concerning European Law


Commission Recommendation of 19 October 1994 relating to the legal aspects of electronic data interchange 94/820/EC
http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=EN&numdoc=31994H0820&model=guichett


Community framework for electronic signatures

VAT and Electronic Commerce (Activities of the European Union – Summaries of legislation)

8.6.2 URLs concerning taxes

Project ELSTER (Electronic tax return) (english information site)
https://www.elster.de/ssl/main-pro-info-english-01.htm

Grundsätze zum Datenzugriff und zur Prüfbarkeit digitaler Unterlagen – GDPdU (Principles for
data access and for the ability to review digital records) 16. July 2001 (only available in German
language)
http://www.bundesfinanzministerium.de/Anlage8440/BMF-Schreiben-vom-16.07.01.pdf

Steueränderungsgesetz 2003 - StÄndG 2003 (Law amending tax laws 2003) (only available in
German language), of 15 December 2003, promulgated 19 December 2003 at the Federal Law
Gazette Part I page 2645.

Steuerdaten-Übermittlungsverordnung (StDUEV) (Taxation data interchange decree) (only
german) Decree in force since 5. February 2003
http://www.bundesfinanzministerium.de/Anlage17161/Steuerdaten-Uebermittlungsverordnung-StDUEV.pdf

Einkommenssteuergesetz – EstG (Income tax law) (only available in German language)
Umsatzsteuergesetz – UstG (Turnover Tax Law) (only available in German language)

Abgabenordnung – AO (Tax Law) (only available in German language)

Biersteuergesetz – BierStG (Beer tax law) (only available in German language)

Biersteuerverordnung – BierStV (Decree on beer tax) (only available in German language)

Kaffeesteuergesetz – KaffeestG (Coffee tax law) (only available in German language)

Kaffeesteuervorordnung – KaffeestV (decree on coffee tax) (only available in German language)

Kraftfahrzeugsteuer-Durchführungsverordnung – KraftStDV (Motor vehicle tax executive order)
(only available in German language)

Kraftfahrzeugsteuergesetz – KraftStG (Motor vehicle tax law) (only available in German language)

Grunderwerbssteuergesetz – GrESTG (Tax on acquisition of real estate Act) (only available in German language)
Gewerbesteuergesetz – GewStG (Trade Tax Law) (only available in German language)

Gewerbesteuer-Durchführungsverordnung (Decree on trade tax procedure) (only available in German language)

8.6.3 URLs concerning insurances

Versicherungsvertragsgesetz – VVG (Law on contracts of insurance) (Only available in German language)

Versicherungsaufsichtsgesetz – VAG (German Insurance Supervision Act)
http://www.bafin.de/gesetze/vag.htm
http://www.iuscomp.org/gla/ (english translation)

Sozialgesetzbuch IV – SGB IV (Code of social law IV) (only available in German language)

Sozialgesetzbuch V (Code of social law V) (only available in German language)

Verordnung über den Zahlungsverkehr, die Buchführung und die Rechnungslegung in der Sozialversicherung – SVRV (Decree on monetary transactions, accounting and financial statements of social insurances) (only available in German language)
http://217.160.60.235/BGBL/bgb1/1/b199038f.pdf

Sozialgesetzbuch X – SGB X (Code of social law X) (only available in German language)
Sozialgesetzbuch I – SGB I (Code of social law I) (only available in German language)

8.6.4 URLs concerning Company Law

Handelsgesetzbuch – HGB (German Commercial Code) (only available in German language)

Aktiengesetz – AktG (Companies Act) (only available in German language)

8.6.5 URLs concerning common Private Documents

Gesetz zur Anpassung der Formvor-schriften des Privatrechts und anderer Vorschriften an den modernen Rechtsge-schäftsver-kehr (Law adapting formal regulations of private law and other regulations to modern legal relations), Federal Law Gazette 18 July 2001 Part I page 1542; entry into force 19 July 2001 (only available in German language)

Bürgerliches Gesetzbuch – BGB (Civil Code) (only available in German language)

Grundbuchordnung – GBO (Real estate register law) (only available in German language)

PatentG – PatG (Patent law)
http://www.gesetze-im-internet.de/bundesrecht/patg/index.html
http://www.wipo.int/clea/en/ (English translation)
Patentanmeldeverordnung – PatAnmV (Patent application decree) (only available in German language)
http://www.ip-firm.de/patanmvo.pdf

Gesetz über eine Berufsordnung der Wirtschaftsprüfer - WPO (Code of conduct for certified accountants or Law Regulating the Profession of Wirtschaftsprüfer) (only available in German language)
http://www.wpk.de/english/publications/publications.asp (english translation, under construction)

Communication of the chamber of public accountants regarding the accreditation as certification service provider (only available in German language)
http://www.wpk.de/berufsregister/elektronische-signatur.asp

Registerverfahrensbeschleunigungsgesetz – RegVBG (Acceleraration of register procedures law) (available only in German language)
http://www.jura.uni-sb.de/BGBI/TEIL1/1993/199321821.HTML

Schiffsregisterordnung – SchiffRegO (Register of shipment Code) (available only in German language)
http://www.uni-mannheim.de/fakul/jura/ls/otte/transportrecht_content/1070026947.pdf

Verordnung über den elektronischen Rechtsverkehr im gewerblichen Rechtsschutz – ErvGewRV (Decree on electronic communication concerning legal protection in commercial affairs) (available only in German language)
http://217.160.60.235/BGBL/bgb1f/bgb103s1558.pdf

Markengesetz – MarkenG (Trade mark act)
Nachweisgesetz – NachwG (Law on the evidence of contract terms concerning employment contracts) (available only in German language)

8.6.6 URLs concerning Public Law

Neue gemeinsame Geschäftsordnung des Bundesministerien (GGO) – Grundlage für eine zeitgemässe Steuerung (Joint Rules of Procedure of the Federal Ministries), in force since 1 September 2000

Verwaltungsverfahrensgesetz – VwVfG (Administrative Procedure Act) (only available in German language)


Vergabeverordnung – VgV (Tendering procedure law) (only available in German language)

Atomgesetz – AtomG (Atomic Energy Act)

Vereinsgesetz – VereinsG (Association Law) (only available in German language)
Gesetz zur Ordnung des Wasserhaushaltes – WHG (Water Ressources Law) (only available in German language)

Gesetz über die Umweltverträglichkeitsprüfung – UVPG (Assessment of environmental effects law) (only available in German language)

Staatsangehörigkeitsgesetz – StAG (Citizenship Law) (only available in German language)

8.6.7 URLs concerning Electronic Signatures

Signaturgesetz – SigG (Digital signature act), from 16 May 2001, amended caused by European directive 99/93/EC (new version from 2001 only available in German language)
http://www.bundesrecht.juris.de/bundesrecht/sigg_2001/
http://www.iid.de/iukdg/english.html (inofficial current version)

Signaturverordnung – SigV (Ordinance on Electronic Signatures) of 16 November 2001
http://www.iid.de/iukdg/gesetz/SigV161101-engl.pdf (English translation)

8.6.8 URLs concerning Procedure Law

Entwurf eines Gesetzes über die Verwendung elektronischer Kommunikationsformen in der Justiz (Justizkommunikationsgesetz – JKomG) (Governmental draft of a law regarding the application of electronic communication at the judicial system) (only available in German language)
Zivilprozeßordnung – ZPO (Civil Procedure Code) (only available in German language)

Strafprozeßordnung – stop (Criminal Procedure Code)
http://www.iuscomp.org/gla/ (English translation)
9 Adoption of the Qualified Certificate Profile in Germany

9.1 Relevant Documents

In addition to [RFC 3739] and [RFC 3039] the following set of standards, specifications and legal requirements are of relevance within this review:

- **ITU-T|ISO/IEC and IETF Area**
  - [X.509] Information Technology — Open Systems Interconnection — The Directory: Public-Key and Attribute Certificate Frameworks, and

- **European Area**
  - [TS 102 280] X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons,
  - [TS 101 862] Qualified Certificate Profile, and

- **Germany**
  - [ISIS-MTT] Certificate Profile for Certificates Issued to Natural Persons,
  - [SAGA] Standards and Architectures for eGovernment Applications, and
  - [SigG] Law Governing Framework Conditions for Electronic Signatures (Signature Law — SigG).

9.2 Profiling Structure

Profiling of standards are the means to use existing standards and to create new standards in which

- all mandatory conformance requirements defined in the input standards have to be used without any changes, and in which
- further restrictions and/or extensions on the optional and/or conditional requirements, defined in the input standards, may be specified.

An overview of the profiling structure of relevant certificate standards and their relationship is illustrated in figure 1.

Figure 1: Overview of Related Certificate Standards and Their Relationship
**Profiling Aspects of [RFC 2459] and [RFC 3280]**

The IETF [RFC 3280] specification is built on [X.509] and profiles the formats and semantics of certificates and certificate revocation lists for facilitating the use of X.509 certificates and technology. It replaces its predecessor [RFC 2459].

**Profiling Aspects of [RFC 3039] and [RFC 3739]**

The IETF [RFC 3739] specification is built on [RFC 3280] and provides a certificate profile for identity certificates issued to natural persons. It defines further technical requirements for certificates that can be used within a defined legal framework in order to declare these certificates as Qualified Certificates. [RFC 3739] replaces its predecessor [RFC 3039].

**Difference between [RFC 3739] and [RFC 3039]**

In [RFC 3739] all references to the obsolete [RFC 2459] have been replaced with references to [RFC 3280].
PROFILE ASPECTS OF [TS 102 280]

The ETSI [TS 102 280] technical specification is built on the IETF standards [RFC 3280], [RFC 3739], and on the ETSI technical specification [TS 101 862] for generic profiling of X.509 and for the implementation of the requirements (for qualified certificates in Annex I, for certification-service-providers issuing qualified certificates in Annex II) of the electronic signature directive [EC DIR].

PROFILE ASPECTS OF [TS 101 862]

The ETSI [TS 101 862] technical specification is built on the IETF standard [RFC 3739] and profiles the qualified certificate statements extension of [RFC 3739] to facilitate the issuance and usage of qualified certificates as defined by the electronic signature directive [EC DIR] (annexes I and II).

PROFILE ASPECTS OF [ISIS-MTT]

The German [ISIS-MTT] specification is built on IETF standards (RFCs of the PKIX and the SMIME working groups), and on technical specifications of W3C and of ETSI. It profiles these standards and technical specifications in order to facilitate interoperable PKI applications. As a basic approach [ISIS-MTT] consequently distinguishes among requirements that have to be fulfilled during the generation or the processing of particular objects (e.g. email, certificate, OCSP request, XML signature, ...). [ISIS-MTT] also contains an optional profile for the implementation of the legal requirements of the German Signatures Law [SigG].
10 Technical Review

10.1 Liaison between ETSI and IETF

The old [RFC 3039] has been updated and replaced with the new [RFC 3739] as a consequence of the liaison between the related IETF working group responsible for the qualified certificates profile and the ETSI STF 220 Task 3 working group responsible for the development of the technical standard for certificate profile. The ETSI activities during the production of their new technical specifications [TS 102 280] on "X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons" and [TS 101 862] on "Qualified Certificate Profile" have identified a set of issues and solutions in order to improve [RFC 3039]. The ETSI input has been taken into account by IETF resulting in the production of [RFC 3739].

10.2 Main Concepts of [RFC 3739]

10.2.1 Scope and Main Goal

[RFC 3739] is a profile that provides conventions and technical information in order to support the issuance of identity certificates for natural persons. Primarily it facilitates the issuance of so-called qualified certificates.

Difference between [RFC 3739] and [RFC 3039]

[RFC 3039] has defined a set of aspects that are generic for both qualified certificates as well as certificates to natural persons that are not qualified ones. Examples of these aspects are defined attributes, the biometric information extension, and aspects of the qualified certificate statements extension. Therefore the scope of [RFC 3039] has been modified in order to more clearly reflect this situation.

10.2.2 Meaning of Qualified Certificate

In this context it is important to note that a certificate compliant with [RFC 3739] can only be categorized as qualified if it

- is used to identify a person with an appropriate high level of assurance, and if it
- also fulfills the relevant legal requirements within a defined legal framework.
10.2.3 Support of Qualified Certificates

[RFC 3739] directly supports classes of certificates for which legal frameworks exist. Examples of legal frameworks, in which requirements for qualified certificates are defined, are

- the European Electronic Signatures Directive [EC DIR], or
- the German Electronic Signatures Law [SigG].

In order to make efficient use of [RFC 3739] further technical specifications based on [RFC 3739] are required to implement and fulfill the relevant legal requirements. In Europe the ETS specification [TS 101 862] and in Germany the ISIS-MTT specification support this class of qualified certificates.

10.2.4 Properties and Indication of Qualified Certificates

[RFC 3739] only makes a minimum set of assumptions concerning the properties of qualified certificates, whereas in legal frameworks complete sets of legal requirements are defined for qualified certificates and certification authorities issuing qualified certificates.

The key assumption in [RFC 3739] is that a qualified certificate issued by a certification authority to a natural person contains information that indicates that the purpose of this certificate is that of a qualified certificate. Further requirements for qualified certificate contents are:

- the indication of a certificate policy, and
- the inclusion of a name or a pseudonym of the certificate owner.

10.2.5 Identification of Certification Authorities

[RFC 3739] requires that the name of a certification authority issuing a qualified certificate shall be the officially registered name of this organization. It proposes a set of [X.520] attributes ("domain component" defined in [RFC 2247], "country name", "state or province name", "organization name", "locality name", and "serial number") that can be used in the issuer certificate extension field to identify the issuing certification authority without disallowing the use of further [X.520] attributes. The concrete semantics of the name attributes need to be expressed in the associated certificate policies and/or the certificate practice statements of the issuer.

[TS 102 280] specifically mandates the presence of the "country name" and the "organization name" attribute in the issuer field for compliance with the European Electronic Signatures Directive [EC DIR]. These mandatory attributes in the issuer extension shall serve for the following purposes:
the “organization name” attribute shall contain the full registered name of the certificate issuing organization, and
the “country name” attribute shall contain the country in which the certificate issuing organization is registered.

10.2.6 Identification of Natural Person

[RFC 3739] requires that the name of a certificate owner shall be a distinguished name being composed of an appropriate subset of [X.520] attributes (“domain component” defined in [RFC 2247], “country name”, “common name”, “surname”, “given name”, “pseudonym”, “serial number”, “title”, “organization name”, “organizational unit name”, “state or province name”, and “locality name”) that can be used in the subject certificate extension field to identify the certificate holder without prohibiting the use of further [X.520] attributes.

[RFC 3739] requires that at least one of the alternative attributes “common name”, “given name” or “pseudonym” shall be contained in the subject field, whereas [TS 102 280] only considers the two alternatives “common name” or the combination of “surname” and “given name” as relevant. At first glance the choice “given name” in [RFC 3739] without “surname” seems to be confusing, however [RFC 3739] is a general profile for identity certificates for which a subject may only have a “given name”. For qualified certificates “given name” in deed is not sufficient and instead the combination of “surname” and “given name” as specified in [TS 102 280] is an appropriate choice of attributes. On the other hand the omission of the “pseudonym” attribute in [TS 102 280] seems to be a mistake, since it does not comply with the [EC DIR] requirement of its annex (c) that reads “Qualified certificates must contain the name of the signatory or a pseudonym, which shall be identified as such”. In the current version [TS 102 280] a “pseudonym” attribute can only be contained in the subject field together with the “common name” or the combination of “surname” and “given name” attributes.

Difference between [RFC 3739] and [RFC 3039]

In [RFC 3739] the set of attributes within the subject field has been updated. Specifically the requirements for the “postal address” and the “title” attributes have been modified for the following reasons:

The “postal address” attribute has been removed from the list of attributes in the subject field since it is not supported in [RFC 3280] and since it is a structured attribute not appropriate for use as a RDN (relative distinguished name).

The “title” attribute has been included in the list of attributes in the subject field since it often supported and since the common place to put this attribute is in the subject field.
10.2.7 Additional Attributes of Natural Person

[RFC 3739] allows the use of further [X.520] attributes (e.g. “date of birth”, “place of birth”,
“gender”, “country of citizenship”, and “country of residence”) in the subject directory
attributes extension that may be used for other purposes than identification of the certificate
holder.

Difference between [RFC 3739] and [RFC 3039]

The “title” attribute has been removed from the list of attributes in the “subject directory
attributes” extension since the subject field was considered to be the preferred place for it.

10.2.8 Key Usage

The requirement of having the non-repudiation key usage bit exclusively set has been
removed from [RFC 3039] since it has been considered as too specific and restrictive,
causing confusion concerning for which cases this applies and for which cases is does not.
This has shown to diminish the use of other functions of [RFC 3039] in certificates where
[RFC 3039] in general applies. This problem has been resolved in [RFC 3739] which explicitly
allows the definition of further requirements on key usage settings in accordance with [RFC
3280] that satisfy local policy and/or local legal requirements.

ETSI [TS 102 280] for example specifies the following three types of allowed key usage bit
combinations for qualified certificates satisfying the requirements of the European electronic
signatures directive [EC DIR]:

- Type A non-repudiation bit exclusively set,
- Type B non-repudiation and digital signature bits set, and
- Type C digital signature bit exclusively set.

The type A or type B combinations shall be used, if the qualified certificate is intended to be
used to validate commitment to signed content in electronic signatures on agreements and/or
electronic signatures on transactions. Specifically the use of type A is recommended.

Difference between [RFC 3739] and [RFC 3039]

The requirement of having the non-repudiation key usage bit exclusively set has been
removed from [RFC 3039].

10.2.9 Biometric Information

The optional and non-critical private extension “biometric information” can be used in a
qualified certificate to include biometric information for authentication purposes that is also
suitable for human verification. The syntax of the “biometric information” extension defines the following four components:

- the mandatory type of the biometric data as a choice of either a predefined type (picture or handwritten-signature) or a biometric data object identifier,
- the mandatory hash algorithm that is used to calculate the hash value of the biometric source data,
- the mandatory calculated hash value of the biometric source data, and
- an optional universal resource identifier using the HTTP or HTTPS scheme that can be used to obtain the source file. This optional feature may be useful for applications that want to display the graphical images of biometric information that is not stored inside the extension because of limiting the size of certificates.

10.2.10 Certificate Policies and Qualified Certificate Statements

[RFC 3739] has defined the optional extension “qualified certificate statements” that can be used to indicate aspects and properties of qualified certificates in the form of qualified certificate statements. Per ASN.1 definition qualified certificate statements represent a sequence of individual qualified certificate statements of the type “QCStatement” that is composed of a “statement identifier” and an optional “statement information” component. The “statement identifier” component is an object identifier (OID) that uniquely identifies an individual qualified certificate statement. The optional “statement information” component can be used to provide additional qualifying information. Its type is defined by the related statement identifier.

[RFC 3739] currently provides the two qualified certificate statements “qcStatement-1” and “qc-Statement-2” that indicate compliance with [RFC 3039] (Version 1) or [RFC 3739] (Version 2) respectively. Both statements may optionally include “semantics information” with the optional components “semantics identifier” and “name registration authorities”. The purpose of the “semantics identifier” component which is an object identifier is to define semantics for attributes and names used in certificate basic fields and extensions. The purpose of the “name registration authorities” component is to list the names of registration authorities that are in charge of registration of names or attributes of a natural person.

Certificate policies and qualified certificate statements are related items. If policy related statements are contained in the “qualified certificate statements” extension, then these should also be contained in the certificate policy extension.

[Ts 101 862] further profiles the qualified certificate statements of [RFC 3739] to facilitate the issuance and usage of qualified certificates as defined by the electronic signature directive [EC DIR] (annexes I and II). It defines the following four statements: “qualified certificate compliance”, “qualified certificate limit value”, “qualified certificate retention period”, and “qualified certificate secure signature creation device”.

The “qualified certificate compliance” statement can be used to indicate that a certificate has been issued as a qualified certificate complying with the requirement of [EC DIR] (annexes I (a)) for electronic signatures and complying with the legal requirements of the country specified in the issuer field. This statement together with the inclusion of a certificate policy, that also defines this quality, represents the implementation of the [EC DIR] requirement. The use of the “qualified certificate compliance” statement in qualified certificates is mandatory in Europe that will be issued after June 30th 2005.

The “qualified certificate limit value” statement can be used in a qualified certificate to indicate the limits on the value of transactions. This statement represents the implementation of the [EC DIR] requirements as defined in annex I (j), annex II (h), and article 6 complying with the legal requirements of the country specified in the issuer field. The use of the “qualified certificate limit value” statement in qualified certificates is optional. The advantage of its use however is to limit the costs for CAs that are liable for damages in cases where they acted negligently.

The “qualified certificate retention period” statement can be used in a qualified certificate to indicate how long beyond the end of the validity period an issuing CA will guarantee the availability of information relevant to the use of and the reliance on the qualified certificate. This statement represents the implementation of the [EC DIR] requirements as defined in annex II (i). The use of the “qualified certificate retention period” statement in qualified certificates is optional. However it may be useful for example in case of a dispute in order to get further information from the issuing CA to identify a natural person for which a pseudonym instead of a common name was included in the qualified certificate.

The “qualified certificate secure signature creation device” statement can be used in a qualified certificate to indicate that the private key related to the certified public key resides in a secure signature creation device. This statement represents the implementation of the [EC DIR] requirements as defined in annex III complying with the legal requirements of the country specified in the issuer field. The use of the “qualified certificate secure signature creation device” statement in qualified certificates is optional. The advantage of its use however is to indicate to relying parties that a high security level for electronic signatures is applied.

Difference between [RFC 3739] and [RFC 3039]

In [RFC 3739] the defined scope of the qualified certificate statements extension has been modified and adapted to its current and potential use.
11 Adoption of Qualified Certificates in the German Federal Government

The German Federal Government has made a great effort to initiate and support the development and use of electronic applications in the private, economic, public and administrative area. These activities also serve for the purpose of a wider use of qualified certificates and their adoption in Germany. In this context the following areas have to be mentioned that will be described in the following sections.

- Laws Supporting Electronic Signatures Based on Qualified Certificates
- Technical Base Standards in Germany
- PKI-Projects in Germany

11.1 Laws Supporting Electronic Signatures Based on Qualified Certificates

11.1.1 Overview of Relevant Laws

Qualified certificates are one of the required means to promote electronic signatures. Several laws have been established or amended in Germany in order to enable and support legal electronic transactions in the private, economic, public and administrative sector in order to provide the legal framework for the use of electronic data with signatures. Among these laws the following groups and subsets of laws represent the most important selection with respect to legal transactions:

- Electronic Signatures
  - Law Governing Framework Conditions for Electronic Signatures [SigG]
  - First Law Amending the Signature Law [SigG*]
  - Ordinance on Electronic Signatures [SigV]
- Forms
  - Law on the adaptation of form requirements and other requirements for modern legal transactions [Form]
  - Third law amending the administrative procedural requirements [E-FORM]
- Tax and Social Security Laws
- Health Care Law (Law for Modernization of the Legal Health Insurance [GMG])

The main issues and basic principles of laws on electronic signatures have already been presented in chapter 4 of the document “Electronic Signature Laws and PKI Projects in European Union and Germany”. The German signature law does not specify individual requirements for specific forms of electronic data for which electronic, advanced or qualified electronic signatures will be created. The term electronic data is used in the signature law in a general and abstract fashion thus allowing any kind of electronic data to be used for any form
of electronic signatures. Therefore, principally any kinds of electronic data like E-Mails, documents, contracts, medical records and digitally scanned documents can be used for electronic signing.

Other laws besides the signature law may specify further requirements for the usage or exclusion of electronic signatures. These laws define concrete forms of data for which electronic signatures can, must or must not be used. These remaining laws and their relevance for adoption of qualified certificates in Germany will be considered in the following sections.

11.1.2 Laws for Forms of Documents

11.1.2.1 Convergence Clauses

In the German legislation the most frequently kind of “form” was the so-called “written form” which means paper documents and handwritten signatures. In order to cope with the issues of electronic government many modern German laws now include an equivalence clause that explicitly allows the replacement of the written form by an “electronic form”. In these cases the general rule applies that “A written form required by a law can be replaced by an electronic form, if the written form is not exclusively mandated by other regulations”. It also has the effect that the related electronic documents have to be complemented with qualified certificates and signed with qualified electronic signatures in order to comply with the requirements for the electronic form.

All laws that contain an equivalence clause provide the legal means to increase the use and adoption of qualified certificates in Germany.

11.1.2.2 Civil/Private Law Sector

The law on the adaptation of form requirements and other requirements for modern legal transactions [Form] establishes the legal effect for qualified electronic signatures in the civil law sector. It includes an equivalence clause (see [Form] §126) that defines the electronic form as an equivalent for the written form. The law explicitly states that the electronic form can be used for all cases where in the civil law the written form is required. In cases where no form requirement is mandated by law electronic data can be used without additional electronic signatures.

This law thus provides the legal framework for the application of qualified electronic signatures in the private sector. It regulates the legal equivalence of electronic signatures to handwritten signatures and the legal effectiveness in legal proceedings.

The law on form regulations is applicable to all general and specific laws in the private sector e.g. civil code, commercial code or the law on contracts of insurances. For these areas the use of qualified certificates will also be triggered increasing the adoption of qualified certificates in Germany.
The law on the adaptation of form requirements and other requirements for modern legal transactions (see [Form] §126) also defines the so-called “text form” for a kind of documents including electronic documents for which neither handwritten nor electronic signatures are required. The use of the text form must be explicitly allowed by specific regulations.

11.1.2.3 Administrative/Public Law Sector

The third law amending the administrative procedural requirements defines the "electronic form" in the public law sector as an equivalent for the “written form” (see [E-FORM] §3a). In this context an electronic document has to be complemented with a qualified certificate and signed with a qualified electronic signature in order to comply with the requirements for the electronic form. The law explicitly states that the electronic form can be used for all cases where in the administrative law the written form is required except for those cases that explicitly require the written form.

The law also regulates that private documents to be submitted to administrations may be forwarded in electronic form. Citizens and public authorities can also exchange documents in electronic forms without electronic signatures. If specific regulations require the written form then electronic documents with qualified electronic signature based on qualified certificates may be used.

The administrative procedure law thus provides the legal framework for the application of qualified electronic signatures in the public sector and the exchange of electronic documents between citizens and administrations. It regulates the legal equivalence of electronic signatures to handwritten signatures and the legal effectiveness in legal proceedings.

The administrative procedure law on administrative procedural requirements is applicable to all general and specific laws in the public sector e.g. building code, industrial code, registration laws or environmental protection laws.

For these areas the use of qualified certificates will also be triggered increasing the adoption of qualified certificates in Germany.

11.1.3 Tax Law

The tax law also includes an equivalence clause that explicitly defines the equivalence of the electronic form with the written form.

This law thus provides the legal framework for the application of qualified electronic signatures in the public sector and the exchange of electronic documents between citizens, enterprises and administrations. It regulates the legal equivalence of electronic signatures to handwritten signatures and the legal effectiveness in legal proceedings.

Enterprises have to use electronic documents and will not be allowed to use paper documents from 2005 on that have to be submitted to the tax administrations. Examples of
these documents are declaration of income tax of employees, certificates of employment, or certificates of income of employees.

These applications will increase the use of qualified certificates leading to a wider adoption of qualified certificates in Germany.

11.1.4 Health Care Law

The law for modernization of the legal health insurance [GMG] in Germany that specifies requirements for the realization and usage of the electronic health professional card and electronic health card for citizens and their related application-specific electronic data, e.g. electronic prescription, medical emergency data records, or electronic patient record. The [GMG] law explicitly requires the use of qualified certificates in electronic health professional cards and also mandates the capability for the inclusion of qualified certificates of citizens in their electronic health cards. These electronic health cards will be distributed and used from 2006 on.

Since millions of people (citizens, physicians, pharmacists and others working in the health care area) in Germany will be equipped with electronic health cards the use of qualified certificates will be strongly effected leading to a wider adoption of qualified certificates in Germany.

11.2 Technical Base Standards Supporting Electronic Signatures Based on Qualified Certificates

11.2.1 Standards and Architectures

Within the framework of the so-called BundOnline 2005 initiative, whose intention and goal is the promotion of Internet-enabled administration services in Germany, the Federal Government has supported the development of the “Standards and Architectures for eGovernment Applications” [SAGA]. This document provides a comprehensive description of standards, processes, methods and products that are relevant to eGovernment applications.

11.2.2 Specifications for Interoperable PKI Applications

[SAGA] identifies [ISIS-MTT] as a mandatory standard that has to be taken into account within eGovernment applications that support electronic signatures using qualified certificates. Concerning qualified certificates [ISIS-MTT] itself is fully compatible with the requirements as specified in [RFC 3739] and [TS 101 862] and [TS 102 280].

11.2.3 Signature Card API

A third base standard that is important in this context is the document “Specification of the Application Programming Interface to the Signature Card” [SigBü] that has been developed by the signature alliance group (Signaturbündnis, SigBü). The aim of the signature alliance
group is to provide a signature infrastructure such that all users will be able to use a SigBü
chip card with as many as possible applications that require electronic signatures.

11.3 PKI-Projects and Applications Supporting Electronic Signatures Based on Qualified Certificates

The adoption of qualified certificates in Germany is affected by many PKI projects and
applications that have been initiated by the German Federal Government and that are using
electronic signatures for securing electronic transactions. These projects require the use of
qualified certificates either as a mandatory capability or as an option. Qualified certificates are
in use when the secured electronic transaction has to meet the requirements of national
legislation.

The main issues and basic principles of these projects and activities have already been
presented in chapter 5 of the document “Electronic Signature Laws and PKI Projects in
European Union and Germany”. The quality of the used certificated is associated with the
described project whenever possible.
12 Surveys on Practical Time Stamp Requirements

Both federal government ministries and agencies on the one hand, and leading vendors and time stamp service providers on the other hand have been interviewed. For both groups of interview partners two distinct lists of questions have been prepared as questionnaires. The lists of selected interview partners, the questionnaires, the collected answers and their analysis and interpretation are presented in the following chapters:

- Chapter 13 contains the information related to the interview of federal government ministries and agencies.
- Chapter 14 summarizes the information related to the interview of leading vendors and time stamp service providers.

13 Interview of Federal Government Ministries and Agencies

Information related to the interview of federal government ministries and agencies is given in the following sections, containing

- Questions asked to federal government ministries and agencies
- Overview of contacted ministries and agencies
- Summary and interpretation of received answers

13.1 Questions Asked to Federal Government Ministries and Agencies

The interview of the federal ministries and agencies included the following questions listed in table 1.
Table 1: Questionnaire for interviewing ministries and agencies

<table>
<thead>
<tr>
<th>Requirements for Using Time Stamps</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Question 1</td>
<td>Answers</td>
</tr>
<tr>
<td>Are there any requirements in your ministry/agency that mandate the usage of time stamps?</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Types of Legal Requirements for Using Timestamps</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Question 2</td>
<td>Type</td>
</tr>
<tr>
<td>What kinds of legal requirements on the usage of time stamps do exist in your ministry/agency that have to be satisfied?</td>
<td>2a) Law</td>
</tr>
<tr>
<td></td>
<td>2b) Ordinance</td>
</tr>
<tr>
<td></td>
<td>Further types of legal requirements if applicable</td>
</tr>
<tr>
<td></td>
<td>2c)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Types of Applications with Requirements for Time Stamps</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Question 3</td>
<td>Application</td>
</tr>
<tr>
<td>For which applications in your ministry/agency are time stamps needed?</td>
<td>3a) E-Mail</td>
</tr>
<tr>
<td></td>
<td>3b) Signature renewal for long-term archiving</td>
</tr>
<tr>
<td></td>
<td>3c) Transformation of documents</td>
</tr>
<tr>
<td></td>
<td>Further types of applications if applicable</td>
</tr>
<tr>
<td></td>
<td>3d)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Current Need for Time Stamps</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Question 4</td>
<td>Strength of Need</td>
</tr>
<tr>
<td>How strong is the current need in your ministry/agency for using time stamps?</td>
<td>4a) low</td>
</tr>
<tr>
<td></td>
<td>4b) mean</td>
</tr>
<tr>
<td></td>
<td>4c) high</td>
</tr>
</tbody>
</table>
### Current Usage of Time Stamps

<table>
<thead>
<tr>
<th>Question 5</th>
<th>Answers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does your ministry/agency currently make use of time stamps?</td>
<td></td>
</tr>
</tbody>
</table>

### Frequency of Usage of Timestamps

<table>
<thead>
<tr>
<th>Question 6</th>
<th>Answers</th>
</tr>
</thead>
<tbody>
<tr>
<td>What was the frequency (number per year, or per month) of using time stamps in your ministry/agency up to now?</td>
<td></td>
</tr>
</tbody>
</table>

### Time Stamp Service Providers

<table>
<thead>
<tr>
<th>Question 7</th>
<th>Answers</th>
</tr>
</thead>
<tbody>
<tr>
<td>The time stamp services of which providers do you use in your ministry/agency?</td>
<td>Name of Time Stamp Service Provider</td>
</tr>
</tbody>
</table>

### Planning of Usage of Time Stamps for the Near Future

<table>
<thead>
<tr>
<th>Question 8</th>
<th>Answers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Are there short-term plans for the usage of time stamps in your ministry/agency?</td>
<td>Yes</td>
</tr>
</tbody>
</table>

### Estimation of Mean-Term Need for Time Stamps

<table>
<thead>
<tr>
<th>Question 9</th>
<th>Strength of Need</th>
<th>Answers</th>
</tr>
</thead>
<tbody>
<tr>
<td>How does your ministry/agency estimate the mean-term trend of the need for using time stamps compared with the current need?</td>
<td></td>
<td>Yes</td>
</tr>
<tr>
<td>9a) decreasing</td>
<td>9b) unchanged</td>
<td>9c) increasing</td>
</tr>
</tbody>
</table>
13.2 Overview of Contacted Ministries and Agencies

The following 8 ministries and agencies that are listed in alphabetical order in Table 2 have been contacted.

Table 2: Ministries and agencies that have been interviewed

<table>
<thead>
<tr>
<th>Ministries/Agencies</th>
<th>Address: Street, City</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bundesministerium der Finanzen</td>
<td>Wilhelmstraße 97</td>
</tr>
<tr>
<td>(Federal Ministry of Finance)</td>
<td>10117 Berlin</td>
</tr>
<tr>
<td>Bundesministerium der Justiz</td>
<td>Mohrenstraße 37</td>
</tr>
<tr>
<td>(Federal Ministry of Justice)</td>
<td>10117 Berlin</td>
</tr>
<tr>
<td>Bundesministerium des Inneren</td>
<td>Alt-Moabit 101 D</td>
</tr>
<tr>
<td>(Federal Ministry of the Interior)</td>
<td>10559 Berlin</td>
</tr>
<tr>
<td>Bundesministerium für Bildung und Forschung</td>
<td>Heinemannstr. 2</td>
</tr>
<tr>
<td>(Federal Ministry of Education and Research)</td>
<td>53175 Bonn</td>
</tr>
<tr>
<td>Bundesministerium für Gesundheit und Soziale</td>
<td>Am Probsthof 78a</td>
</tr>
<tr>
<td>Sicherung (Federal Ministry of Health and</td>
<td>53121 Bonn</td>
</tr>
<tr>
<td>Social Security)</td>
<td></td>
</tr>
<tr>
<td>Bundesministerium für Verkehr, Bau- und</td>
<td>Invalidenstraße 44</td>
</tr>
<tr>
<td>Wohnungswesen (Federal Ministry of Transport,</td>
<td>10115 Berlin</td>
</tr>
<tr>
<td>Building and Housing)</td>
<td></td>
</tr>
<tr>
<td>Bundesministerium für Wirtschaft und Arbeit</td>
<td>Scharnhorststraße 34-37</td>
</tr>
<tr>
<td>(Federal Ministry of Economics and Labor)</td>
<td>10115 Berlin</td>
</tr>
<tr>
<td>Bundesamt für Sicherheit in der Information</td>
<td>Godesberger Allee 185-189</td>
</tr>
<tr>
<td>technik (BSI) (Federal Office for Information</td>
<td>53175 Bonn</td>
</tr>
<tr>
<td>Security BSI)</td>
<td></td>
</tr>
</tbody>
</table>
13.3 Summary and Interpretation of Received Answers

The answers from the interviewed ministries and agencies are collected in Table 3 to Table 11 of this section. The numbers of interview partners in the following tables do not correspond to the alphabetical order of the previous Table 2 for the purpose of anonymity.

In the following tables the abbreviations ‘nfb’ is used for ‘no feedback’ and ‘n.a.’ for ‘not applicable’. ‘m/y’ stands for ‘month/year’.

Table 3: Answers to Question 1

<table>
<thead>
<tr>
<th>Interview Partner</th>
<th>Answers</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>yes</td>
</tr>
<tr>
<td>#</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
</tr>
<tr>
<td>Sum</td>
<td>2</td>
</tr>
</tbody>
</table>
Table 4: Answers to Question 2

<table>
<thead>
<tr>
<th>Interview Partner</th>
<th>2a) Signature Law</th>
<th>2b) Signature Ordinance</th>
<th>2c) Others</th>
<th>Type of Requirement</th>
<th>nfb</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>yes</td>
<td>no/a.</td>
<td>yes</td>
<td>no/a.</td>
<td></td>
</tr>
<tr>
<td>1</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>√</td>
<td>√</td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>√</td>
<td>√</td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td>√</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sum</td>
<td>0</td>
<td>4</td>
<td>0</td>
<td>4</td>
<td>1</td>
</tr>
</tbody>
</table>

Table 5: Answers to Question 3

<table>
<thead>
<tr>
<th>Interview Partner</th>
<th>3a) E-Mail</th>
<th>3b) Long-term archiving of electronic documents</th>
<th>3c) Transformation of documents</th>
<th>3d) Others</th>
<th>Type</th>
<th>nfb</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td>yes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1</td>
<td></td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sum</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>4</td>
</tr>
</tbody>
</table>
### Table 6: Answers to Question 4

<table>
<thead>
<tr>
<th>Interview Partner</th>
<th>4a) Low</th>
<th>4b) Mean</th>
<th>4c) High</th>
<th>nfb</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>2</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>8</td>
<td>√</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Sum</strong></td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>4</td>
</tr>
</tbody>
</table>

### Table 7: Answers to Question 5

<table>
<thead>
<tr>
<th>Interview Partner</th>
<th>yes</th>
<th>no/n.a.</th>
<th>no feedback</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>6</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>8</td>
<td>√</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Sum</strong></td>
<td>1</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>
Table 8: Answers to Question 6

<table>
<thead>
<tr>
<th>Interview Partner</th>
<th>Frequency</th>
<th>Period [m/y]</th>
<th>nfb/n.a.</th>
<th>Frequency Per Year</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>1000</td>
<td>y</td>
<td></td>
<td>1000</td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td></td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td></td>
<td></td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td></td>
<td></td>
<td>√</td>
<td></td>
</tr>
<tr>
<td>Sum</td>
<td>1</td>
<td>7</td>
<td></td>
<td>1000</td>
</tr>
</tbody>
</table>

Table 9: Answers to Question 7

<table>
<thead>
<tr>
<th>Interview Partner</th>
<th>Name</th>
<th>nfb/n.a.</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>2</td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>3</td>
<td>AuthentiDate</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>6</td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>7</td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>8</td>
<td></td>
<td>√</td>
</tr>
<tr>
<td>Sum</td>
<td>1</td>
<td>7</td>
</tr>
</tbody>
</table>
Table 10: Answers to Question 8

<table>
<thead>
<tr>
<th>Interview Partner</th>
<th>Answers</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>yes</td>
<td>no</td>
</tr>
<tr>
<td>1</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>Sum</td>
<td>2</td>
<td>2</td>
</tr>
</tbody>
</table>

Table 11: Answers to Question 9

<table>
<thead>
<tr>
<th>Interview Partner</th>
<th>Answers</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>9a) decreasing</td>
<td>9b) unchanged</td>
<td>9c) increasing</td>
<td>nfb</td>
</tr>
<tr>
<td>1</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Sum</td>
<td>0</td>
<td>1</td>
<td>3</td>
<td>4</td>
</tr>
</tbody>
</table>
The summary and interpretation of the answers got from the interviewed federal ministries and agencies can be characterized as follows:

- Currently there is only a small need for the use of time stamps.
- Statistics on the degree of current time stamp usage do not exist.
- The legal framework including the usage of time stamps exists.
- Many new projects are currently being realized that potentially require the use of time stamps for example in combination with qualified electronic signatures or for signature renewal.
- The interviewed federal ministries and agencies have an increasing need for the mean-term period.
14 Interview of Leading Time Stamp Vendors and Service Providers

Information related to the interview of leading time stamp vendors and service providers is given in the following sections containing

- Questions asked to leading time stamp vendors and service providers
- Overview of contacted time stamp vendors and service providers
- Analysis and discussion of received answers

14.1 Questions Asked to Leading Time Stamp Vendors and Service Providers

The interview of leading time stamp vendors and service providers included the following three questions listed in Table 12.

Table 12: Questionnaire for interviewing leading time stamp vendors and service providers

<table>
<thead>
<tr>
<th>Frequency of Usage of Time Stamp Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Question 1</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>What was the frequency (number per year, or per month) with which the time stamp service in your company has been used up to now?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Distribution of Usage of Time Stamp Service to Lines of Business</th>
</tr>
</thead>
<tbody>
<tr>
<td>Question 2</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>How is the usage of the time stamp service in your company distributed to different lines of business?</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
14.2 Overview of Contacted Time Stamp Vendors and Certification Service Providers

We have contacted the following 7 time stamp vendors and certification service providers that are listed in alphabetical order in Table 13.

Table 13: List of Contacted Time Stamp Vendors and Certification Service Providers

<table>
<thead>
<tr>
<th>Company/Organization</th>
<th>Address: Street, City</th>
</tr>
</thead>
<tbody>
<tr>
<td>AuthentiDate International AG</td>
<td>Großenbaumer Weg 6 40472 Düsseldorf</td>
</tr>
<tr>
<td>Bundesnotarkammer (Federal Chamber of Notaries)</td>
<td>Burgmauer 53 50667 Köln (Cologne)</td>
</tr>
<tr>
<td>DATEV eG Zertifizierungsstelle (CA)</td>
<td>Paumgartnerstr. 6 - 14 90429 Nürnberg (Nuremberg)</td>
</tr>
<tr>
<td>Deutsche Post Com GmbH Geschäftsfeld Signtrust</td>
<td>Tulpenfeld 9 53113 Bonn</td>
</tr>
<tr>
<td>D-Trust GmbH</td>
<td>Kommandantenstrasse 15 10969 BERLIN</td>
</tr>
<tr>
<td>T-Systems International GmbH</td>
<td>Untere Industriestr. 20 57250 Netphen</td>
</tr>
<tr>
<td>TC TrustCenter AG</td>
<td>Sonninstraße 24-28 20097 Hamburg</td>
</tr>
</tbody>
</table>
In addition to these service providers the following 17 organizations (chambers of lawyers, and chambers of tax consultants) have been contacted that are using third party services provided by the company DATEV.

- Chambers of Lawyers
  - Hamburg, Bamberg, Berlin, Frankfurt am Main, Koblenz, Munich, and Nuremberg
- Chambers of Tax Consultants
  - Bremen, Berlin, Brandenburg, Free State of Saxony, Munich, Lower Saxony, Nordbaden, Nuremberg, Saarland, and Stuttgart

### 14.3 Summary and Interpretation of Received Answers

The answers from the interviewed leading time stamp vendors and certification service providers are collected in the following three tables of this section. The numbers of interview partners in the following tables do not correspond to the alphabetical order of the previous Table 13 for the purpose of anonymity.

**Table 14: Answers to Question 1**

| Interview Partner | Frequency | Period [m|y] | no answer | Frequency Per Year |
|-------------------|-----------|------------|-----------|--------------------|
| 1                 | 500       | m          |           | 6000               |
| 2                 |           |            | √         |                    |
| 3                 | 35        | y          |           | 35                 |
| 4                 |           |            | √         |                    |
| 5                 | 20        | m          | √         | 240                |
| 6                 |           |            |           |                    |
| 7                 | 0         |            | √         | 0                  |
| Sum               |           |            | 3         | 6275               |
Table 15: Answers to Question 2

<table>
<thead>
<tr>
<th>Answers</th>
<th>Interview Partner</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>Sum</th>
</tr>
</thead>
<tbody>
<tr>
<td>2a) Accountants [%]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>2b) Authorities [%]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>7</td>
</tr>
<tr>
<td>2c) Chambers [%]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>2d) Chancelleries [%]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6</td>
</tr>
<tr>
<td>2e) Enterprises [%]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>2f) Financial institutions [%]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>7</td>
</tr>
<tr>
<td>2g) Hospitals [%]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>2h) Insurances [%]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>7</td>
</tr>
<tr>
<td>2i) Lawyers [%]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>2j) Medical offices [%]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>100</td>
</tr>
<tr>
<td>2k) Notaries [%]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>100</td>
</tr>
<tr>
<td>2l) Pharmacies [%]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>7</td>
</tr>
<tr>
<td>2m) Private sector [%]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
</tr>
<tr>
<td>2n) Public administrations [%]</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>7</td>
</tr>
</tbody>
</table>
### Table 16: Answers to Question 3

**How does your company estimate the mean-term trend of the usage of your time stamp services compared with the current degree of usage?**

<table>
<thead>
<tr>
<th>Interview Partner</th>
<th>%</th>
<th>9a) decreasing</th>
<th>9b) unchanged</th>
<th>9c) increasing</th>
<th>9d) strongly increasing</th>
<th>no feed-back</th>
</tr>
</thead>
<tbody>
<tr>
<td>2o) Research institutions</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>2g) Tax consultants</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Universities</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>Others</td>
<td>-</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

Sum: 0 0 4 1 2
The summary and interpretation of the answers got from the interviewed leading time stamp vendors and service providers can be described as follows:

- There has been a very reserved willingness of the interview partners to provide information on their business plans and statistics of service usage.
- Authentidate also explicitly stated that they do not provide such sensible information for the survey.
- They kept their internal business reports and statistics secret.
- There is a strong competition among time stamp vendors and service providers in this market sector.
- The current degree of usage of time stamp service is very low.
- Market sectors in Table 15 that are currently supported are authorities, chambers, lawyers, notaries and tax consultants.
- The interviewed leading time stamp vendors and service providers evaluate the degree of usage of time stamping services as increasing.
15 General Information about AuthentiDate

This chapter contains a collection of information related to time stamping services of the company AuthentiDate that is provided on its web pages. The information provided on the English web page http://www.authenti-date.de/en and on the German web page http://www.authenti-date.de does not show any significant differences. AuthentiDate has grouped its public information into the following main categories:

- Solutions: This entry provides an overview of the solutions that AuthentiDate offers for e-Billing, scanning, archiving, workflow, PKIs, time stamping, signature validation, signature, and electronic postmark.
- Basics: This entry describes the technical and legal foundation for signatures, time stamps and technology on which the solutions of AuthentiDate are based.
- Partners: This entry lists the partners that are using products from AuthentiDate.
- Customers: This entry gives a collection of statements from customers of different branches and national and international projects about the employment of AuthentiDate’s products and solutions.
- News: This entry contains a detailed, and up to date, chronological list of press releases that is related to AuthentiDate’s business activities.

Information related to time-stamping services and products is presented in the following chapters of this document:

- Chapter 16 contains the information related to the time stamp solutions provided by AuthentiDate.
- Chapter 17 summarizes main functions of the eTimestamp Module.

Brief general information about AuthentiDate is provided in the press release, February 21st 2005 which reads as follows:

AuthentiDate (www.authenti-date.de), Düsseldorf, develops and sells open-supplier business process solutions that make a simple and quick integration of digital signatures and time stamps into existing corporate processes possible for the first time. These solutions, which can be used for almost any area such as billing, workflow, archiving, scanning and e-mail communication, for instance, reduce costs and optimize process sequences.

Renowned companies in different industrial sectors have trusted AuthentiDate signature solutions for years on a national and international basis to model legally binding, electronic business processes in accordance with the legal stipulations.
Professional signature solutions are available as products and web services in a modular system through AuthentiDate for the first time and can therefore be used independently or in combination with other solutions. A number of software providers have already integrated the signature products of AuthentiDate as a standard function today. Any company can therefore make use of the benefits of automatic signature processes today.

In addition, AuthentiDate offers certified trust center services in accordance with the German Signature Act and the EU Signature Directive through AuthentiDate International AG. AuthentiDate International AG was accredited by the Regulatory Agency for Telecommunications and Postal Affairs in November of 2001 and operates a trust center especially for time stamp services.

On an international basis, the AuthentiDate Group is also represented in the USA and is the sole supplier today of United States Postal Service Electronic Postmark (USPS EPM), a unique service for secure electronic communication in the USA. AuthentiDate Holding Corp, Inc. (New York) is listed on the NASDAQ (ADAT) and in German over-the-counter market (Security Identification Code 893715).

16 Time Stamp Solutions

AuthentiDates solutions comprise technology and products that realize the integration of time stamps produced by trust centers in existing processes or to generate the time stamps by oneself within private applications. The following classes of products are offered:

- OEM time stamp products
- Time stamp server

16.1 OEM Time Stamp Products

AuthentiDate offers OEM time stamp products that are required to use time stamps for data that are processed in archiving or workflow systems. This class of products can be used to generate time stamps for data in the requesting system by the accredited AuthentiDate trust center. The privacy of the data is guaranteed since they never leave the system at any time. The AuthentiDate Product is directly integrated into the archiving workflow system. It generates a legally binding hash value that uniquely represents the concerned data and transmits this hash value to the trust center. The trust center (time stamping authority) produces a qualified time stamp complying with the signature law and sends it back to the requesting system. The archiving respectively the workflow system is now in the possession of the data and the related qualified time stamp. All described procedures are performed automatically via secure connections and with high performance.
16.2 Time Stamp Server

AuthentiDate offers the component “AuthentiDate time stamp server” that allows big companies or public authorities to set-up their own virtual time stamp service. The time stamp server component enables companies or public authorities to generate time stamps within their own infrastructure and to use them for different processes. The time stamp server represents the gateway to the AuthentiDate accredited time stamp service in the trust center.

17 Functionality of the eTimestamp Module

The eTimestamp module can be used to generate qualified time stamps that serve for proving the legally binding time and content of electronic documents. It supports many different application scenarios of time stamps such as:

- Protection of intellectual capitals of an enterprise
- Protection of relevant information under patent law
- Conformant archiving of relevant information under tax law
- Realization of electronic receipt stamps in automatic procurement and call for tenders procedures
- Additional securing of signature times of personal-related signatures
- Resigning of personal-related signatures in cases of changing cryptographic algorithms

Qualified time stamps that have been generated by AuthentiDate’s time stamp service will be archived for a period of 30 years. In addition a copy of each time stamp will be stored in a central data base of the time stamp service.

On demand of an application the eTimestamp module sends a time stamp request to the AuthentiDate time stamp service and passes the received time stamp response to the related application. The eTimestamp module focuses on the automatic and mass-oriented generation and validation of qualified time stamps in electronic processes. The effort for integrating the eTimestamp module into business processes has been minimized by using standardized interface specifications and commercial development environments. The provision of an API in C/C++ and Java enables the integration on the code level.
18 Explanation of the “ArchiSig Project”

ArchiSig (July 2001 until September 2003) was a project funded by a grant from the Federal Ministry of Economics and Labour within the framework of the “VERNET – Secure and reliable transactions in open communication networks” program [ArchiSig]. In the ArchiSig project an interdisciplinary team of representatives from science, industry and users has developed solutions and concepts for the secure and conclusive archiving of electronically signed documents over durations of 30 years and more. The members of the ArchiSig projects have been

- Heidelberg University Medical Center, Department of Medical Informatics
- Fraunhofer Gesellschaft, Institute for Secure Telecooperation (now: Institute for Secure Information Technology)
- University Kassel, Project Group Constitutionally Compatible Technology Development (provet)
- State Office Niedersachsen, Hannover, Public Administration of Archives
- CEYONIQ AG, Bielefeld, (retired since spring 2002)
- IXOS Software AG, Grasbrunn / Munich (partner since 2002)
- SECUDE Sicherheitstechnologie Informationssysteme GmbH, Darmstadt
- PERGIS Systemhaus GmbH, Ludwigshafen (consortium manager)
- DATEV eG, Nürnberg (associated consortium partner since March 2002)

And additional supporting partners

- Fachhochschule Mannheim, University of Applied Sciences, department for Computer Science
- Informatikzentrum Niedersachsen (izn) – Landesbetrieb
- T-Systems Austria GesmbH, Vienna

As one of the conditions of the project the renewal of electronic signatures has to meet the requirements of national legislation. In Germany, these requirements are stated especially in §6 Signatures Law [SigG] and § 17 Signature Ordinance [SigV].

The ArchiSig concept for long-term conservation of provability of electronically signed documents is a centralized approach based on a central archiving system, which can also be designed as a service. It generates renewed electronic signatures for transferred data in the form of so called “ArchiSig-ArchivTimeStamps” and secures them on a long-term basis.

The basis of the ArchiSig-ArchivTimeStamp is the principle of the hash-tree described by Merkle [Merkle].
The leaves of the shown tree represent the hash values of any kind of data objects, e.g. documents. A time stamp is requested only for the root hash of the tree. To guarantee maximum security, the use of time stamps generated by accredited certification providers is recommended. An initial ArchiSig-ArchivTimeStamp should be generated preferably at the moment when a document is included in the archiving system but at the latest before the extinction of the security suitability of the used cryptographic algorithm. In the case of time-stamp-renewal only the time stamp part of an ArchiSig-ArchivTimeStamp has to be hashed and time stamped afresh. In case of hash-tree-renewal not only the ArchiSig-ArchivTimeStamp but also the referred data objects have to be hashed and time stamped again.

The concept of the ArchiSig-ArchivTimeStamp method is described in more detail in the proceedings of ISSE 2002 [LTCons].

Subsequent to the ArchiSig project the Fraunhofer Institute SIT has developed the complete software package ArchiSoft as the practical implementation of the ArchiSig concept.

A proof of the ArchiSig concept and implementation was carried out in two pilot projects, one within the university clinics at Heidelberg and another in the public administration of the state of Lower Saxony.
With the aid of the ArchiSig project standardization of the integration of verification data into signatures and signature renewal for long-term conservation purposes was tackled. On the one hand within the scope of the national standardization initiative ISIS-MTT [ISIS_MTT_LT] and on the other hand in the context of the international standardization activities of the Internet Engineering Task Force (IETF) Working Group “Long Term Archiving and Notary Services” (LTANS) [IETF_LTANS].

In the context of the ISIS-MTT standardization initiative a legal opinion was commissioned that proves that the proposal “Long-Term Conservation of Electronic Signatures” complies with the German Signature Law. Both documents are published on the ISIS-MTT website [ISIS_MTT_LT].

In succession of ArchiSig the project TransiDoc has been started. The project is described in the Final Report “Electronic Signature Laws and PKI Projects in European Union and Germany”, chapter 5.5.2, “TransiDoc”.
### Abbreviations and Acronyms

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ETSI</td>
<td>European Telecommunications Standard Institute</td>
</tr>
<tr>
<td>IETF</td>
<td>Internet Engineering Task Force</td>
</tr>
<tr>
<td>OID</td>
<td>Object Identifier</td>
</tr>
<tr>
<td>PKIX</td>
<td>Public-Key Infrastructure X.509</td>
</tr>
<tr>
<td>QC</td>
<td>Qualified Certificate</td>
</tr>
<tr>
<td>RDN</td>
<td>Relative Distinguished Name</td>
</tr>
<tr>
<td>SAGA</td>
<td>Standards and Architectures for eGovernment Applications</td>
</tr>
<tr>
<td>SigBü</td>
<td>Signature Alliance (Signaturbündnis)</td>
</tr>
<tr>
<td>SigG</td>
<td>German Signatures Law (Signaturgesetz)</td>
</tr>
<tr>
<td>SigG*</td>
<td>First German Signatures Amendment Law</td>
</tr>
<tr>
<td>§</td>
<td>Symbol used in German legislation for paragraph or article</td>
</tr>
<tr>
<td>TS</td>
<td>Technical Specification</td>
</tr>
<tr>
<td>URI</td>
<td>Universal Resource Identifier</td>
</tr>
</tbody>
</table>
References


[ISIS-MTT] T7&TeleTrusT Specification: Common ISIS-MailTrusT Specifications for Interoperable PKI Applications
   — Part 1: Certificate and CRL Profiles,
   — Optional Profile: SigG Profile, and
   — Optional Profile: Optional Enhancements to the SigG Profile, March 2004.


[SigG]\* Bundesgesetzblatt (Federal Law Gazette) No. 1, p 2: First Law Amending the Signature Law, (Entwurf eines Ersten Gesetztes zur Änderung des Signaturgesetzes 1. SigÄndG), please note that currently an English version of this amendment law is not available, January 2005

[SigBü] Signature Alliance: Specification of the Application Programming Interface to the Signature Card, October 2004


