Modular Architecture for Adaptable Signature-Creation Tools

Requirements, Architecture, Implementation and Usability

Vesna Krnjic, Klaus Stranacher, Tobias Kellner, and Andreas Fitzek

Institute for Applied Information Processing and Communications (IAIK),
Graz University of Technology, Graz, Austria
{vesna.krnjic,klaus.stranacher,tobias.kellner,
andreas.fitzek}@iaik.tugraz.at

Abstract. Electronic signatures play an important role in e-Business and e-Government applications. In particular, electronic signatures fulfilling certain security requirements are legally equivalent to handwritten signatures. Nevertheless, existing signature-creation tools have crucial drawbacks with regard to usability and applicability. To solve these problems, we define appropriate requirements for signature-creation tools to be used in e-Government processes. Taking care of these requirements we propose a modular architecture for adaptable signature-creation tools. Following a user-centered design process we present a concrete implementation of the architecture based upon the Austrian Citizen Card. This implementation has been used to prove the applicability of the architecture in real life. Our tool has been successfully tested and has been assessed as usable and intuitive. It has already been officially released and is widely used in productive environments.

Keywords: Electronic Signatures, Qualified Signature, Signature-Creation, Usability, User-Centered Design.

1 Introduction

Electronic services have gained importance in the last years. Compared to conventional services they allow cost reduction and more efficient procedures. An increasing number of electronic services are being provided in all e-Business domains. For security and privacy sensitive services such as e-Government, electronic signatures guarantee authenticity and integrity.

Especially in the e-Government sector the legal aspects of electronic signatures play a major role. In 1999, the European Commission published the EU Signature Directive [1]. The Directive had to be implemented by national laws and defines equivalence between a handwritten signature and an electronic signature fulfilling certain security requirements (‘qualified signature’).

The European Commission Decision 2011/130/EU [2] defines standard signature formats for advanced electronic signatures. In addition, the Digital Agenda for Europe

M.A. Wimmer, M. Janssen, and H.J. Scholl (Eds.): EGOV 2013, LNCS 8074, pp. 274–285, 2013.

[4] and the e-Government action plan [5] aims to create a single digital market for Europe. Obviously, these activities demand for appropriate signature tools.

Currently a variety of signature-creation tools and applications are on the market. Unfortunately most of them lack usability or applicability. Either they do not support 'qualified signatures' or all standard formats, or they are available as online tools only. Nevertheless, many citizens and companies want or have to use an offline tool due to security and privacy obligations. Therefore there is a need for an offline tool creating 'qualified signatures'. In addition, current signature-creation tools do not allow to freely position a visual representation of the signature in the document. To fill this gap our paper presents a modular and adaptable architecture for signature-creation tools. In addition – to validate the applicability of our proposed architecture – we present a concrete and user-oriented implementation of the architecture based on the Austrian Citizen Card. The main reasons for choosing the Austrian Citizen Card as a basis are: (a) electronic signatures are widely used in Austria and thus we expect a high volume of users and (b) the Austrian official signature as introduced by Leitold et al. [12] defines a visual representation of the signature and therefore an adequate positioning of this representation is needed.

The remainder of this paper is structured as follows: Section 2 gives an overview of the legal and technical framework our solution is based on. In Section 3 we elaborate on requirements for adaptable and secure signature-creation tools and applications. Section 4 presents our modular architecture for signature-creation tools. In addition, details about the implementation of this architecture are given. Section 5 describes the user-centered design method we followed to achieve a high grade of usability of our solution. Finally, we draw conclusions and discuss future work.

2 Legal and Technical Framework

2.1 Legal Regulations

The Digital Agenda for Europe aims to "*develop a digital single market in order to generate smart, sustainable and inclusive growth in Europe*" [6]. To achieve this objective, (cross-border) electronic services are one of the key enabling factors. This has been refined in the e-Government action plan for the period 2011-2105 [5]. The action plan objective is to create a new generation of administrative services. However, electronic signatures are necessary to provide secure and reliable electronic services.

Electronic signatures have been discerned as a key factor for successful e-Government early on. Already in 1999, the European Commission published the Directive on a Community framework for electronic signatures[1] [1]. The Directive defines a basis for legal recognition of electronic signatures. It includes a definition of different characteristics of electronic signatures and defines their legal effect. In

[1] Better known as the EU Signature Directive.

particular, it defines that an advanced electronic signature must meet 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;"* [1]

In addition, Article 5 of the Directive defines that *"advanced electronic signatures which are based on a qualified certificate and which are created by a secure-signature-creation device [...] 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"*[2] [1]. This means that such 'qualified signatures'[3] are legally equivalent to handwritten signatures which is a common precondition for e-Government processes.

2.2 Technical Background

From a technical perspective we concentrate on the Austrian Citizen Card concept [10] as the implementation of our solution is based on it. This concept defines the Citizen Card as a technology neutral instrument that enables to create and verify electronic signatures according to the Austrian e-Government act [8] and e-Signature law [9][4]. That means different forms of Citizen Card tokens can exist. Currently, smart card-based as well as mobile phone-based Citizen Card implementations are available.

To integrate these various tokens a middleware is used. This *Citizen Card Software (CCS)* implements a high level interface[5] that provides diverse functionality such as the creation and verification of electronic signatures. Different types of this citizen card software exist:

- *Online-based CCS*: This smart card-based CCS runs on the server side and provides the desired functionality via a Java applet to the user. Actually, the only available online based CCS is MOCCA Online[6].

[2] The terms 'qualified certificate' and 'secure signature creation' and their requirements are defined in Article 2 of the Signature Directive.

[3] The term 'qualified signature' is not explicitly defined in the Signature Directive. However, this term is usually used in literature.

[4] The Citizen Card offers additional functionality, such as identification of citizens and data encryption. However, these are not needed for our use cases.

[5] The so-called 'Security Layer '

[6] MOCCA Online: `http://joinup.ec.europa.eu/software/mocca/description`

- *Local/Client-based CCS*: This CCS is also smart card-based and has to be installed locally on the client machine. Here, different implementation exists, e.g. MOCCA Local[7], a.sign Client[8] or TrustDesk[9].
- *Mobile phone signature-based CCS*: This CCS which uses a simple mobile phone is available at https://www.handy-signatur.at/. It is based upon a two factor authentication using a password and a TAN (sent via SMS to the mobile phone).

Concerning signature formats, the European Commission, in their Decision 2011/130/EU [2] from 2011, published a set of standard signature formats which must be processable by all competent authorities acting under the EU Services Directive [3]. Namely these formats are the advanced electronic signatures CAdES, XAdES, and PAdES. However, Austria has rolled out a proprietary PDF-based signature format (PDF-AS) several years ago [11,12]. This format is going to be replaced by PAdES, but currently it is still widely used. Therefore, we have chosen this signature format to implement in our signature tool (see Section 4 for details).

3 Requirements

The secure and reliable signature-creation of electronic documents plays a central role in most e-government solutions. Signature-creation tools must meet several requirements to satisfy legal regulations as well as the needs of all user groups. On the one hand, the signature-creation tools must fulfill the requirements for the public sector and organizations. On the other hand, the tools should be intuitive and convenient to use for every single citizen. Considering the needs of all user groups, reliability, usability, adaptability, and modularity are identified as core requirements for signature-creation tools. These requirements are refined as follows:

- **Reliability and Privacy**

Signature-creation tools typically process sensitive personal and business data. Misuse of this data may seriously compromise citizens and businesses. Hence, reliability and trustworthiness of this data is an essential requirement. In addition, the public administration needs certainty about the identity of the citizens or businesses. The same applies for the identity of the public administration. So, reliability of the affected parties must be achieved. Finally, citizens, businesses, and public administration need assurance that the data processing satisfies legal and privacy regulations.

- **Usability**

Usability is another major requirement for signature-creation tools. Signature-creation tools are using cryptographic techniques like public key infrastructure (PKI) or secure signature creation devices (SSCD) such as smart cards as required for generating ‘qualified signatures’. Most likely, users do not have the necessary background

[7] MOCCA Local: `http://joinup.ec.europa.eu/software/mocca/description`

[8] `http://www.a-trust.at/`

[9] `http://www.itsolution.at/digitale-signatur-produkte/desktop/trustDesk.html`

knowledge about complex cryptographic concepts and legal regulations. Plenty of security-sensitive tools are simply too complex for most users. In general, users are not interested in technical details. To improve the usability of signature-creation tools, this complexity must be hidden from the user. Instead, the focus has to be on presenting important information to users. To ensure usability, identified user groups must be involved in the design and development process of such tools.

- **Comprehensive Format Support**

In the next years a significant increase of electronic signature enabled cross-border services is expected (see Digital Agenda for Europe [6] or EU Services Directive [3] for instance). Although the European Commission Decision 2011/130/EU [2] has defined standard signature formats, various other (partly proprietary and nation-wide) formats are still in use. This implies that the support of these signature formats is still required. Hence, the ability to enhance signature-creation tools to support additional signature formats is crucial. Obviously these enhancements should be possible with minimal effort.

- **Cross-Platform Applicability**

Usually, e-Government applications and services must not be limited to specific hardware or software components. Services provided by public authorities must be accessible for all citizens without any restrictions and irrespective of the used environment. Thus, the availability of cross-platform applications is an essential requirement for signature-creation tools.

- **Offline Availability**

In many cases electronic documents contain personal or sensitive data. Therefore document owners are interested in keeping this data undisclosed, either due to privacy regulations, business policies or because of other privacy reasons. Server-based approaches are problematic in this context, because users do not want to upload sensible data to a remote server. Therefore, signature creation tools should offer a client-based implementation for creating electronic signatures.

4 Architectural Design

In this section we elaborate on a modular architecture and design for signature-creation tools satisfying the identified requirements. To verify the applicability of this architecture we have implemented a signature-creation tool for use cases of the Austrian e-Government. Due to the widespread usage of the Austrian signature format PDF-AS we have given this format priority. The following subsections describe the proposed architecture and give details on the implementation.

4.1 Architecture

Fig. 1 illustrates our proposal for a modular and adaptable architecture for signature-creation tools. The architecture supports various document formats, allows for the creation of different signature formats and makes use of different signature-creation devices. This modular approach is achieved by defining a generic signature-creation process. Depending on the current state of the process, specific implementations of the various components are used to create a signature for the current document. All those generic components are adaptable and open for further implementations and extensions to support new document types, signature formats, or signature-creation devices. Subsequently we describe our architecture and the involved components or modules (see Fig. 1):

- **Input**

The input module reads a given document and determines the MIME type[10] for further processing. It generates a document dependent state which is used during the whole signature-creation process. This module can support local files, network files or even streams, and presents this input data in a common form to the other modules. When the input module has finished its task, the state is handed over to the viewer module.

- **Viewer**

The viewer module enables presentation of the document to be signed. It uses document-specific implementations for the presentation. These may be e.g. PDF renderer, MS-Word renderer, XML renderer, HTML renderer, and so on.

Depending on the used signature format, a visual signature representation and a customized signature positioning can be supported. In this case the viewer module provides a Positioning component which presents an overlay to allow the user to position the visual signature representation. The chosen position is then stored in the state of the signature process.

- **Signer**

The signer module is responsible for the delegation between the signature component adapter and the signature creation device component. Depending on the state, the signer component chooses an appropriate signature component for the given document, or uses a preconfigured component for the given document class. It provides the chosen signature component adapter with a specific instance of a matching signature creation device, which again is either chosen on the fly or may be preconfigured.

- **Signature Component Adapter**

This adapter is used to provide a common interface to e.g. a signature library. The signature format implementation generates the signature data and uses an abstract signature-creation device to obtain a valid signature for this signature data. Given the signature and the signer certificate the concrete signature component is able to create a valid digitally signed document. This signed document is again stored in the process state.

[10] The MIME type defines the document format.

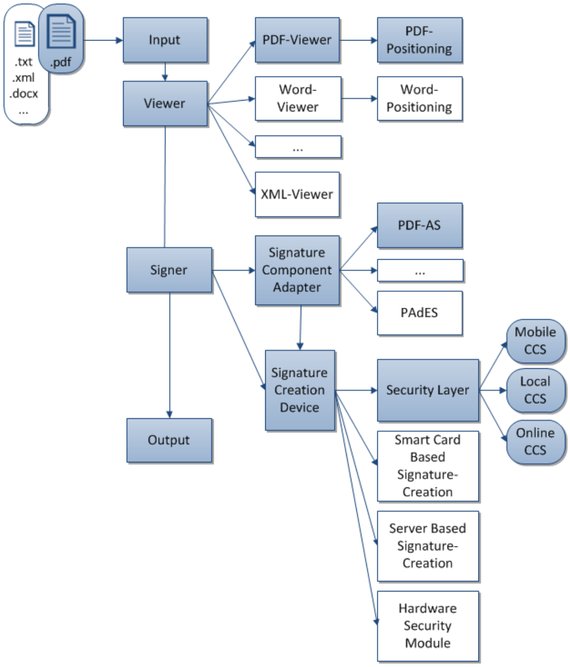


Fig. 1. Modular and adaptable architecture for signature-creation tools

- **Signature Creation Device**

The signature creation device is an abstraction layer for signature-creation. It translates the given requests to implementation specific commands to create a signature. The specific implementations can support any kind of signature-creation device, e.g. smart card [11] -based or server-based signature-creation devices, or hardware security modules. In addition, it supports Austrian citizen card software, which is integrated via the standardized interface ‘Security Layer’. Thus, all citizen card software implementations (online, local and mobile phone-based) are supported.

- **Output**

When a signed document is available within the process state, the output module allows the user to save the signed document, to open it with the default application or to view it again with the appropriate viewer module.

4.2 Implementation

To put the proposed architecture into practice and to verify its applicability, a well-defined subset of this architecture has been implemented: signing of PDF documents with the Austrian PDF-based signature format PDF-AS was chosen. Our implementation is based on Java, thus achieving platform independence. Fig. 1

[11] Using the PC/SC (Personal Computer/Smart Card) interface.

highlights the modules that have been implemented in our application. Namely these main modules are:

- PDF-Viewer module including positioning of the visual signature representation
- Signature Component Adapter PDF-AS
- Signature-Creation Devices based on the Austrian Citizen Card via 'Security Layer'

The process flow starts with the input component, which allows the user to select a PDF document to sign, either via drag and drop, or via an operating system file selection dialog. The viewer displays the PDF document and enables the user to position the visual signature representation. This step can be skipped if the user configured the application for automatic signature positioning. The signer component receives the document to be signed and the desired position of the signature block. With this information, a signature request for the citizen card software is built by the signature component. Here, the user chooses the concrete implementation of the signature creation software (online, local or mobile phone-based implementation). Subsequently, the signature request is signed using the selected citizen card software. Finally, this signature is incorporated into the PDF document by the PDF-AS signature component and the thus signed document is sent to the output component. Within the output component the user is able to save and open the signed PDF document.

The user interface is based on this linear process flow and guides the user through the necessary steps. Fig. 4 shows a screenshot of this interface. Depending on the configuration of the tool, certain process steps can be shortened or entirely skipped for daily use by advanced users. For instance, the document to be signed can be selected by dropping it on the program icon, the signature block can be positioned automatically, the citizen card software can be preselected, or the output filename or folder can be set in advance.

Our tool called *PDF-Over* has been officially launched in Austria[12] and is already widely used[13]. As we followed a user-centered design method for the implementation, the tool has been assessed as easily understandable and usable as well as intuitive. The following section gives detailed insights into this design methodology as applied to PDF-Over.

5 User-Centered Design Method

To fulfill the usability requirements of signature-creation tools discerned above, we followed the user-centered design (UCD) principles [14] in order to implement a security-sensitive application that is effective and usable in practice. UCD is a design methodology that at each stage of the design process focuses on user's needs, goals,

[12] PDF-Over, Version 4.0.0, 15.1.2013, `http://www.buergerkarte.at/pdf-signatur.de.php`

[13] Since the official launch about 2.000 users per month are gained.

preferences, and limitations. It is an iterative design process that requires continuous user feedback and tests. As shown in Fig. 2 the methodology consists of four design stages: analysis, design, implementation and validation. The method enables a complete remodel and rethinking of the design by early testing of conceptual models and design ideas. For the development of PDF-Over we have defined to repeat the entire design process three times[14] before launching an official release. The different stages in the creation of PDF-Over were:

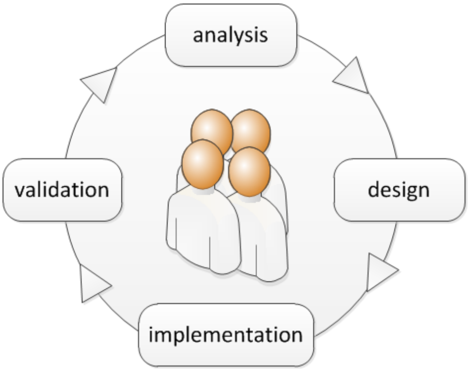


Fig. 2. Four design phases of User-Centered Design Process

- **Analysis**

At the beginning of the process we identified the end-users of PDF-Over. It turned out that the user groups of the signature-creation tool are citizens and authorities. In both groups users can again be divided into standard users and advanced users. After identifying those user groups we posed the question what each user group's main tasks and goals are and what functions are needed to accomplish those. The use case for citizens as standard users is to electronically sign a PDF document. They expect a simple und useable interface without any complexity. The authorities as standard users are interested in applying official signatures. To fulfill the Austrian official signature as introduced by Leitold et al. [12] certain criteria must be met, such as the placement of the visual signature representation. Additionally, advanced users need the possibility to e.g. pre-selected citizen card software, or enable automatic positioning of the visual signature representation. We also analyzed user's need of previous knowledge. In our case the end-user must know what the Austrian Citizen Card is and how to use it.

- **Design**

The second step in the iteration process is the design process. First, paper-based prototypes (see Fig. 3) and the initial architectural design were created. The focus on

[14] This is a common approach for most developments as indicated in `http://www.nngroup.com/articles/iterative-design/`

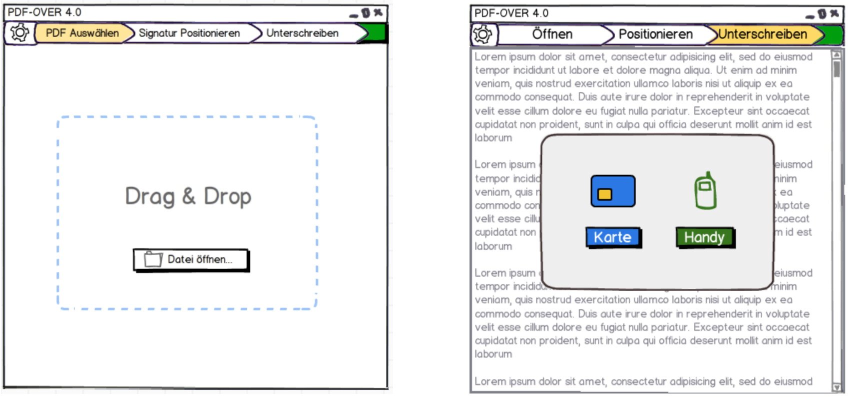


Fig. 3. Design prototypes

the end-users is very important in the early phase of the design. In order to get feedback from the users before writing code or beginning with the development, we performed usability tests with paper mockups.

- **Implementation**

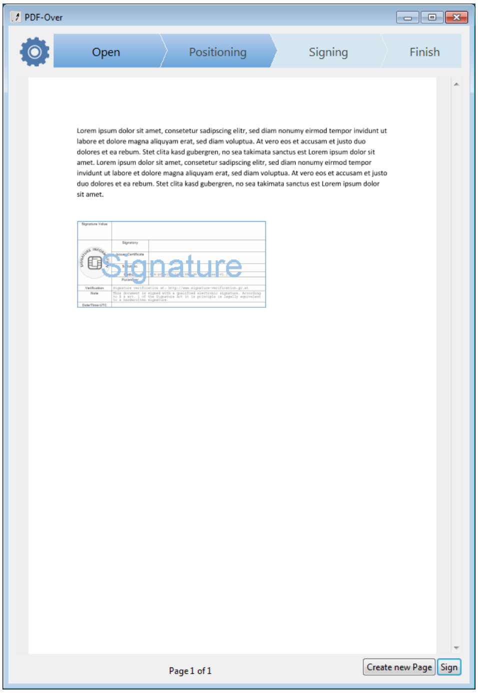
In the implementation stage the detailed design and specifications were implemented and first source code was written. This stage builds upon the results of all prior stages. End-users were not directly involved during the implementation. Fig. 4 illustrates a first implementation of the tool, showing the positioning of the visual signature representation.

- **Validation**

After the implementation phase two approved usability methods have been applied to evaluate PDF-Over. First of all, an expert review was conducted. Here, an evaluator used the tool and assessed its usability against a set of usability principles, the so-called heuristics[15]. The heuristic evaluation provided quick and inexpensive feedback to the design. In the following implementation iteration the results from the heuristic evaluation were implemented.

In the last iteration, we performed a thinking-aloud test with five representative end-users. As indicated by Nielsen [13], five test users are sufficient to find almost all usability problems one would find using many more test participants. Test users have been asked to do representative tasks, while observers, including the developers, watched the test and took notes. The obtained results were analyzed and implemented in the last iteration. With the conducted usability analysis we improved the acceptability and usability of PDF-Over.

[15] http://www.nngroup.com/articles/ten-usability-heuristics/



Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet. Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt ut labore et dolore magna aliquyam erat, sed diam voluptua. At vero eos et accusam et justo duo dolores et ea rebum. Stet clita kasd gubergren, no sea takimata sanctus est Lorem ipsum dolor sit amet.

Signature Value	
Signatory	
Issuer-Certificate	
Serial-No.	
Method	
Parameter	
Verification	Signature verification at: http://www.signature-verification.gv.at
Note	This document is signed with a qualified electronic signature. According to § 4 art. 1 of the Signature Act it in principle is legally equivalent to a handwritten signature.
Date/Time-UTC	

Fig. 4. PDF-Over free positioning of the visual signature representation

6 Conclusions

Signature-creation is essential for many e-Government processes. Especially the creation of ‘qualified signatures’ is of high importance. In this paper we have presented a modular architecture for adaptable signature-creation tools. To prove the practical applicability and flexibility, we have given a concrete implementation of this architecture. To achieve a high impact our solution is based on the Austrian Citizen Card concept. We have followed a user-centered design to achieve a high usability of our tool. This tool has been successfully tested and is ready to accept current and upcoming challenges. The tool has already been officially launched in Austria and is licensed under the European Public Licence EUPL [7]. The current number of downloads amounts to about 2000 per month which confirms the high acceptance and usability of our solution.

Currently, we are integrating additional signature formats. Based upon the European Commission Decision 2011/130/EU we are implementing a PAdES signature component adapter to support PDF advanced electronic signatures. In addition, we are working on the support of batch signatures to allow signing of several documents in one step.

References

1. European Union, Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. Official Journal L 13, 12–20 (January 19, 2000)
2. European Commission Decision, Establishing minimum requirements for the cross-border processing of documents signed electronically by competent authorities under Directive 2006/123/EC of the European Parliament and of the Council on services in the internal market, notified under document C(2011) 1081, 2011/130/EU (February 25, 2011)
3. European Union, Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market. Official Journal L 376, 36–68 (December 27, 2006)
4. European Commission, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A Digital Agenda for Europe, COM/2010/0245 (May 19, 2010)
5. European Commission, The European eGovernment Action Plan 2011-2015 Harnessing ICT to promote smart, sustainable & innovative Government, COM/2010/743 (December 15, 2010)
6. European Union, Digital Agenda for Europe, Summaries of EU Legislation, `http://europa.eu/legislation_summaries/information_society/strategies/si0016_en.htm`
7. European Community, European Union Public Licence, EUPL v.1.1 (2007), `http://joinup.ec.europa.eu/software/page/eupl/licence-eupl`
8. The Austrian E-Government Act: Federal Act on Provisions Facilitating Electronic Communications with Public Bodies. Austrian Federal Law Gazette, part I, Nr. 10/2004; last amended part I, Nr. 111/2010
9. The Austrian Signature Law: Federal Electronic Signature Law. Austrian Federal Law Gazette, part I, Nr. 190/1999; last amended part I, Nr. 75/2010
10. Leitold, H., Hollosi, A., Posch, R.: Security Architecture of the Austrian Citizen Card Concept. In: Proceedings of ACSAC 2002, pp. 391–400 (2002)
11. Leitold, H., Posch, R., Rössler, T.: Reconstruction of electronic signatures from eDocument printouts. Computers and Security 29(5), 523–532 (2010)
12. Leitold, H., Posch, R., Rössler, T.: Media-Break Resistant eSignatures in eGovernment: An Austrian Experience. In: Gritzalis, D., Lopez, J. (eds.) SEC 2009. IFIP AICT, vol. 297, pp. 109–118. Springer, Heidelberg (2009)
13. Hinderer, S.D., Nielsen, J.: How to Recruit Participants for Usability Studies. Nielsen Norman Group (2003), `http://www.nngroup.com/reports/tips/recruiting`
14. International Organization for Standardization, ISO 9241-210:2010, Ergonomics of human-system interaction – Part 210: Human-centred design for interactive systems