Harnessing Electronic Signatures to Improve the Security of SMS-based Services

Thomas Zefferer, Arne Tauber, and Bernd Zwattendorfer

Institute for Applied Information Processing and Communications
Graz University of Technology,
Inffeldgasse 16a, 8010 Graz, Austria
{thomas.zefferer,arne.tauber,bernd.zwattendorfer}@iaik.tugraz.at

Abstract. Powered by the emergence of information and communication technologies, governments and public administrations are nowadays offering online services to facilitate the execution of governmental procedures. Citizens, businesses, and even governments themselves benefit from greater flexibility and cost efficiency of such e-Government services. Recently, the increased mobility of citizens and the growing popularity of mobile communication technologies has raised the need for mobile governmental services. Such services have become known under the term m-Government. Interestingly, most m-Government services still rely on SMS technology. Reasons for that are the simplicity, inexpensiveness and wide support of this technology. Despite these various advantages, a lack of supported security features usually hinders SMS to be used in transactional m-Government services, as these services have higher security requirements. To bypass this issue, we propose a method to enhance SMS-based m-Government services by means of electronic signatures. Our solution allows citizens to generate, electronically sign, and deliver electronic documents by sending well-defined SMS messages. We demonstrate the practical applicability of our approach by means of a prototypical implementation. A detailed discussion of different security aspects of our solution concludes this contribution.

Keywords: SMS, M-Government, Electronic signatures, SMS based services, Austrian Mobile-Phone Signature, Security Analysis

1 Introduction

In order to facilitate administrative procedures, governments and public administrations all over the world have been offering e-Government services for several years. E-Government services incorporate modern information and communication technologies to allow citizens to carry our administrative procedures over the Internet. During the past few years, mobile computing and communication technologies have significantly gained popularity. Governments and public administrations have reacted on this trend and has started to complement e-Government services by mobile communication technologies. These attempts have become commonly known under the terms mobile government and m-Government.

M-Government solutions can be found all over the world in both developing and developed countries. Recent surveys on m-Government [5] [6] have revealed that a majority of current m-Government services still rely on the rather simple SMS (short message service) technology. The popularity of SMS technology has several reasons. First, the sending of SMS messages is often very cheap compared to other more powerful mobile data transmission technologies. Various mobile network operators offer customers special flat rates for sending text messages. Secondly, SMS technology is nowadays supported by virtually every mobile phone and does not require powerful mobile data networks. Thus, SMS based services are not limited to certain end-user devices but can rather be accessed by all users possessing a mobile phone. This is of special relevance in developing countries, in which the market penetration of smartphones in comparison to mobile phones is still low and broadband mobile networks are often not available in rural areas. Another advantage of SMS technology is its simplicity. Even technically inexperienced users are able to send and receive SMS messages. Furthermore, no set-up or configuration is required. SMS technology can be used out of the box similarly to telephony.

The various advantages of SMS technology account for the wide range of SMS based m-Government services. However, there are also drawbacks of SMS based solutions. For instance, due to given technological limitations, SMS based services are usually very simple. In most cases, these services are used to broadcast certain information to citizens or to collect data from citizens. Few SMS based applications actually implement complete transactional services. Depending on the use case, transactional services may have security requirements that can only be met by applying cryptographic methods. This is problematic in the context of SMS based services, for which the capabilities of end-user devices are basically limited to sending and receiving of text based data only.

In this paper we present an application that allows users to securely carry out complete signature-based transactional services by sending SMS messages. The services supported by our application include creation, signing, and delivery of electronic documents. Security requirements such as integrity of digital data and non-repudiation of origin are met by integrating both advanced and qualified electronic signatures.

The remainder of this paper is structured as follows. Section 2 discusses related work on SMS based m-Government services. We introduce basic concepts of electronic signatures in Section 3. In this section, we also introduce a set of approved core components, which our application partly relies on. In Section 4 we discuss architectural and implementation details of our solution and show how it works in practice by means of a concrete case study. Security issues of our approach are discussed in Section 5. Finally, an outlook to future work is given and final conclusions are drawn.

2 Related Work

Although modern smartphones provide users a variety of different communication capabilities, SMS technology is still favoured all over the world [7]. The popularity of SMS technology has led to a plethora of SMS based services. Also the public sector tries to make use of SMS technology's popularity. SMS based m-Government services can already be found in various countries around the world. Comprehensive overviews of existing SMS based projects and initiatives are given in [5] and [6].

SMS has played an essential role in developing countries for many years. Especially in rural areas, reliable and powerful fixed-line communication networks are often not available. Contrary, mobile communication networks are often well evolved even in underdeveloped regions. Yet, they are limited to GSM technology most of the time. The consequent restriction to telephony and text messaging has led to the development of various useful SMS based services. For instance, the FrontlineSMS project[1] aims to improve communication capabilities in regions with underdeveloped infrastructures. FrontlineSMS allows data exchange between remote entities (PCs, Laptop, etc.) based on SMS messages. Another example for an SMS based service is Kenya's BloodBank-SMS project[2]. Due to missing reliable fixed-line communication networks, statuses of blood banks are exchanged via an SMS based service between different hospitals.

There are various other SMS based services from the health sector available in developing countries. In South Africa, citizens can request location information on HIV testing centres via SMS. Text to Change[3] is a health education initiative that aims to inform people in developing countries about diseases such as malaria or AIDS using text messaging technologies.

In developed countries, reliable fixed-line communication networks are usually well evolved. Mobile communication networks are thus just one out of multiple communication and information alternatives and mainly used to satisfy demands of the typical western always-on society. Hence, SMS based services in developed regions differ from those of developing countries in various aspects. In fact, most existing SMS based services aim to improve convenience. For instance, in various European cities parking fees can be paid via text messages[4]. In Norway, also tax declarations can be done with the help of SMS messages[5], which has significantly eased the entire tax declaration process for citizens.

Various countries in both developing and developed regions make use of SMS to broadcast relevant information to their citizens. For instance, in Venice, Italy, citizens are supplied with flood warnings per SMS[6]. In London, UK, the Metropolitan police forward bomb alerts and similar security warnings to regis-

[1] http://www.frontlinesms.com/
[2] http://www.media.mit.edu/ventures/EPROM/research.html
[3] http://www.texttochange.org/
[4] http://www.handyparken.at/handyparken/home.seam
[5] http://www.textually.org/textually/archives/2003/04/000349.htm
[6] http://www.textually.org/textually/archives/2008/06/020298.htm

tered citizens via SMS[7]. In Australia, an e-mail and SMS based warning system[8] has been set up, which alerts citizens when forest fire has been detected near their homes.

So far, most SMS based services are rather informational than transactional. This is reasonable since transactional services usually have higher security requirements that are difficult to meet with SMS based approaches. Therefore, transactional services are traditionally provided through web based approaches, which allow an easier integration of cryptographic methods. Unfortunately, there are scenarios in which web access is not available and web based services cannot be accessed. In such scenarios, SMS based transactional services can be useful. The approach introduced in this paper implements transactional services on SMS basis and incorporates electronic signatures to meet security requirements of such services.

3 Background

Electronic signatures are perfectly suitable to meet the requirements for integrity and non-repudiation of transactional e-Government and m-Government services. In this section we discuss basic principles of electronic signatures and related legal aspects. As the application presented in this paper relies on several components of the Austrian e-Government infrastructure, this section also emphasizes the role of electronic signatures in the Austrian e-Government.

3.1 Electronic Signatures

Electronic signatures are an important element of current e-Government infrastructures and services. Electronic signatures rely on asymmetric cryptography and provide integrity of digital data and non-repudiation of origin. To harmonize legal aspects of electronic signatures throughout the European Union, the so-called EU Signature Directive [3] has been enacted in 1999. The EU Signature Directive defines in detail the following two types of electronic signatures.

- **Advanced electronic signature** "means an electronic signature which meets the following requirements:
  - It is uniquely linked to the signatory
  - It is capable of identifying the signatory
  - It is created using means that the signatory can maintain under his sole control; and
  - It is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable"

[7] http://www.emergencysms.org.uk/
[8] http://michael.tyson.id.au/2008/11/13/firewatch-an-email-based-fire-warning-system

– **Qualified electronic signatures** are advanced electronic signatures that are based on qualified certificates and are created by a secure signature creation device. Requirements for qualified certificates and secure signature creation devices are also defined in detail in the annex of this directive.

The EU Signature Directive assures legal equivalence between qualified electronic signatures and handwritten signatures and their mutual recognition throughout the European Union. Enabling citizens to apply legally valid signatures, qualified electronic signatures are an important component of many e-Government services. Citizens typically use smart cards or similar hardware tokens as secure signature creation devices in order to create electronic signatures. However, some countries provide their citizens also alternative approaches. For instance, citizens can use their mobile phones to create qualified electronic signatures in Austria[9] and Estonia[10].

In the scope of e-Government, electronic signatures are not only used by citizens. Electronic signatures are also an important tool for public administrations to avoid media breaks and to facilitate the processing of administrative procedures. In many countries, administrative rulings are therefore electronically signed before being delivered to citizens. Depending on the underlying technology, different kinds of electronic signatures according to the EU Signature Directive are used for this purpose.

To meet the requirements of different use cases, our solution supports both advanced and qualified electronic signatures. Calling on many years of experience, the Austrian e-Government initiative provides several core components that ease an integration of electronic signatures into e-Government infrastructures. In the following we introduce some of these components, which our application partly relies on.

3.2 Electronic Signatures in Austria

Electronic signatures are a key concept of the Austrian e-Government. The use of electronic signatures within Austrian e-Government processes is facilitated by several core components. Refer to [4] for a comprehensive overview of and introduction to these components.

Citizens use qualified electronic signatures to authenticate at e-Government services, to assure integrity of transmitted data, and to provide written consent in electronic procedures. Public administrations make use of advanced electronic signatures to improve governmental back-office processes and to sign administrative rulings. In the following we discuss core components of the Austrian e-Government initiative dealing with the creation of electronic signatures. Some of these components are used by our SMS-based application.

With the Citizen Card - the national eID - Austrian citizens can create qualified electronic signatures. Although the term Citizen Card suggests the use of

[9] https://www.handy-signatur.at
[10] http://www.id.ee/?id=10995&&langchange=1

smart cards, the Citizen Card concept [1] is actually technology neutral and not limited to a certain signature creation device. Currently, Austrian citizens can use smart cards and mobile phones to create qualified electronic signatures. While smart card based signature creation processes are used in various countries, the mobile phone based approach followed in Austria is novel and especially of interest in the context of our SMS based application.

The Austrian Mobile Phone Signature that has been discussed by Orthacker et al. in [2] follows a centralized approach to carry out mobile phone based signatures. This means that a central hardware security module (HSM) is in charge of creating electronic signatures. The user's mobile phone is solely used to authorize the signature creation process with a mobile transaction number (mTAN). According to this approach, a central service currently hosted by the Austrian certification authority A-Trust[11] represents the core component of the Austrian Mobile Phone Signature. A HSM is an integral part of this central service. For security reasons, all Citizen Card private keys are encrypted with the master key of the HSM and a symmetric encryption key, which is derived from a secure password that is only known to the user.

To start a signature creation process, users have to transmit their mobile phone number and their secure password together with the data to be signed to the central service. This communication takes place through a secured web based interface. With the secure password, the user's personal signing key residing in the central HSM can be decrypted. After successful verification of the secure password and decryption of the user's signing key, a one-time password (TAN) is generated and sent to the user's mobile phone via SMS. To finally initiate the signature creation process, the user returns the obtained TAN through the web based interface to the central service.

The security of the Mobile Phone Signature basically depends on the second, non-web based mobile communication channel that is used to transmit a secure TAN to the user. Similar to smart card based approaches, also the Austrian Mobile Phone Signature relies on a two-factor authentication scheme. The factor *knowledge* is covered by the user's secure signature password. Additionally, the factor *possession* is considered by sending a TAN to the user's mobile phone. This way, the service verifies whether the user is the person she claims to be.

The Mobile Phone Signature facilitates the creation of qualified electronic signatures for Austrian citizens. Public administrations often rely on advanced electronic signatures, which are better suited for automated signature creation. To facilitate signature creation processes for Austrian public administrations, a server-based signature creation module has been developed. This module is called MOA-SS[12] and enables the creation of advanced electronic signatures using preconfigured software keys.

To improve security and reliability, the SMS based m-Government application we are presenting in this paper relies on core signature components, which are provided as open source modules by the Austrian e-Government initiative.

[11] http://www.a-trust.at/
[12] http://egovlabs.gv.at/projects/moa-idspss/

Our solution incorporates both the Mobile Phone Signature and MOA-SS to integrate creation devices for qualified and advanced electronic signatures. This way, our application basically supports two different levels of security, advanced and qualified electronic signatures according to the EU Signature Directive. We will discuss security implications of this approach later in this paper.

4 Implementation

The basic objective of our application is the implementation of SMS based transactional procedures. In our solution, a procedure defines a process including the generation, signing, and delivery of electronic documents. To meet possible security requirements of such procedures, our solution incorporates electronic signatures. In this section we present the architecture and the general process flow of our solution. To appropriately illustrate our application's functionality, we finally discuss a concrete procedural use case supported by our solution.

4.1 Architecture

The limiting factor of SMS based services defines the end-user's device, which is basically restricted to sending and receiving of SMS messages. Most functionality of our application cannot be modeled via SMS messages and thus has to be outsourced to another component. Therefore, our solution relies on a central web application implementing the main functionality. The central web application makes use of several external components to implement the desired processes.

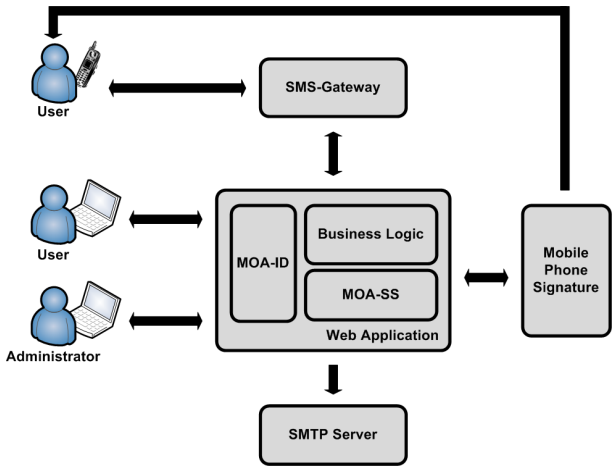

Fig. 1. Architecture and basic building blocks of the presented application.

Figure 1 shows the basic building blocks of our solution. The central web application defines the core component and basically implements all business logic.

Users interact with this web application through an external SMS gateway that translates SMS messages into XML based requests and vice versa. By sending appropriate SMS messages users can electronically create, sign, and deliver documents. All this functionality is basically covered by the web application's business logic.

Our solution supports two alternatives to sign a created document[13]. Qualified electronic signatures can be carried out using the Austrian Mobile Phone Signature. Alternatively, documents can also be signed using a central MOA-SS module being an integral component of the central web application. This approach allows for the creation of advanced electronic signatures.

The web application also features a web based user interface. Through this interface users can review and inspect their documents that have been previously processed via SMS. Additionally, administrators can carry out maintenance tasks through this interface. The web based access to the central web application is protected by a two-factor authentication scheme. Again, we rely on an approved core component of the Austrian e-Government landscape to implement secure user authentication. The open source module MOA-ID[14] encapsulates functionality needed to securely authenticate users by means of a two-factor authentication based on the Austrian Citizen Card concept. Similar to MOA-SS, MOA-ID is an integral component of our central web application.

To facilitate the delivery of signed documents, the web application is also connected to an external SMTP server. However, the generic design of our solution guarantees that also other types of delivery such as registered or certified mail could be used.

4.2 Interfaces and Process Flows

Our application basically provides two different user interfaces. On the one hand, users can communicate with the application by exchanging SMS messages. This interface is mainly used to process procedures. On the other hand, the application can also be accessed through a web based interface. This interface is mainly intended for document inspection and maintenance tasks. The processing of procedures through the application's SMS based interface consists of the following steps:

- **Document creation:** A user starts a procedure by sending a well-defined SMS message. This message contains the unique identifier of the procedure to be processed. A PDF document is created based on a template that is assigned to the selected procedure and on dynamic data defined by the user. This data is transmitted to the application via SMS together with the procedure's unique identifier.
- **Document signing:** The document is signed either by the external Mobile Phone Signature or by the central MOA-SS signature module. Depending

[13] The documents created follow the PDF standard.
[14] http://egovlabs.gv.at/projects/moa-idspss/

on the chosen method either a qualified personal citizen signature or an advanced electronic server signature is created. The user selects the desired signature method by SMS. If the user chooses the Mobile Phone Signature, a TAN is sent to the user's mobile phone during the signature creation process. This TAN has to be forwarded manually to the central application via SMS.
- **Document delivery:** The document is delivered to configured recipients. Different recipients can be defined for each procedure. After successful delivery, the document is stored in a central database for later inspection. The user is notified about the successful processing of the document via SMS and e-mail.

Besides the SMS interface, the application can also be accessed through a web based interface. The set of functionality provided through this web interface actually depends on the user's assigned rights. Standard users can use the application's web interface for the following tasks:

- **Account creation:** In order to use the application, users need to register and create a user profile containing mobile phone number and e-mail address.
- **Register to procedures:** The application allows the dynamic definition of different procedures. Users must register to defined procedures before using them.
- **Inspect documents:** Documents created during the processing of procedures can be inspected and downloaded through the application's web interface.

Users with assigned administrator rights can additionally access the following functions through the application's web interface:

- **Define procedures:** System administrators can define new procedures by choosing an appropriate identifier and a suitable PDF template. Additionally, predefined receivers can be selected to receive newly created and signed documents. Also data that has to be provided by users during the document creation process can be defined.
- **Application maintenance:** Application maintenance involves for instance the activation and deletion of user accounts.

4.3 Case Study: Sick Note

The reporting of absence from work due to sickness is one out of many scenarios that comply with the above mentioned general process flow. In the following we illustrate the functionality of our application by discussing the sick note procedure in more detail. Although this is actually not a typical m-Government procedure, its simplicity makes it perfectly suitable to demonstrate the capabilities of our approach.

Basically, the implemented sick note procedure allows employees to generate, sign, and deliver sick notes to their employer. Using our applications, sick employees can reliably report their absence simply by sending SMS messages but still having the guarantee and non-repudiation property of electronic signatures. The entire procedure requires the following steps to be carried out.

Definition of Procedure Before a procedure can be used, it has to be defined first. Procedures can be defined by users with administrator rights through the application's web based maintenance interface. Once a procedure is defined, users can register to this procedure and use it.

A procedure basically specifies a type of document that may be generated and signed by users during a transaction. Amongst others, a procedure is defined by the following information:

- Unique identifier
- List of key words, which have to be transmitted by the user via SMS, and which are included in the generated document
- List of receivers of completely signed documents

Considering our concrete case study, the procedure that supports the SMS based generation of sick notes comprises the following specifications:

- Unique identifier: SICK
- List of key words: FROM
- List of receivers: DEPARTMENT HEAD, PERSONNEL OFFICE

Figure 2 shows the web interface that can be used to define new procedures. Amongst others, this interface allows the assignment of receivers and key words. Receivers and key words can by defined via similar web based interfaces.

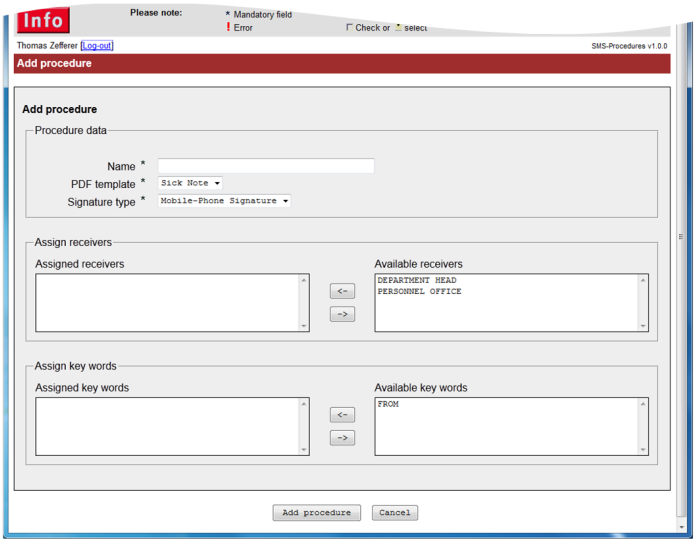

Fig. 2. Web based interface for the definition of new procedures.

Registration Users must register through the web application's web interface in order to gain access to the application. Therefore, users are securely authenticated using a two-factor authentication scheme based on the Austrian Citizen Card concept.

During the registration process, a user account is created, which contains required user related data such as user name and mobile phone number. To avoid misuse, newly created user accounts must be organisationally verified and manually activated by system administrators.

As soon as the user's account is activated, she may register to procedures that have been previously defined by system administrators. This registration takes place through the web interface shown in Figure 3. The registration for procedures is only required once. After successful registration no further web based interaction with the application is required.

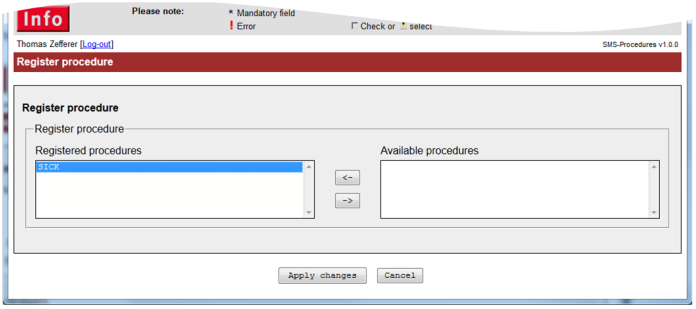

Fig. 3. Web based interface allowing users to register to available procedures.

Document Processing The processing of procedures represents the main use case of our application and is completely carried out via the application's SMS interface. To start the process flow (i.e. to create a sick note), users send an SMS to the web application. The SMS contains the unique identifier of the corresponding procedure (i.e. 'SICK') and a list of key words (i.e. 'FROM') with associated key values (e.g. '2011-11-01') that have to be provided for this procedure.

As the application supports two signature creation alternatives, the user's preferred signature method must also be included in the SMS message. If the user desires to sign the document to be generated by the Server Signature Module MOA-SS, the key word 'server' has to be appended to the SMS message. If the user prefers the Mobile Phone Signature approach, the user's Mobile Phone Signature password has to be appended instead.

Reconsidering the sick note example, a user could send the following text message to start the process flow and sign the document using the Server Sig-

nature Module:

*SICK*FROM:2011-11-01*server*

To generate the same document (sick note) but sign it with the Mobile Phone Signature, the following SMS message has to be sent:

*SICK*FROM:2011-11-01*<password>*

In this example, '<password>' denotes the user's personal password for the Mobile Phone Signature service. In this scenario, a signature creation request is sent to the Mobile Phone Signature. The user receives a mobile TAN during the signature creation process. This TAN has to be forwarded to the web application via SMS. In order to complete the signing process, the central web application forwards the TAN to the Mobile Phone Signature for verification.

Irrespective of the chosen signing method, the signed document is finally delivered to all configured receivers of the procedure. According to the definition of the Sick Note procedure, the created and signed sick note is sent to the department head and to the personnel office. The user is notified about the success of the document processing by SMS and e-mail.

Figure 4 illustrate the SMS based user interaction from the user point of view. In the shown example, the user requests the creation of a sick note indicating a sick leave that starts on 2011/11/21. Furthermore, the user selects the MOA-SS based signature creation method by adding the key word 'server'. The application notifies the user via SMS after having created, signed, and delivered the sick note.

Fig. 4. SMS message exchange during processing of procedure.

Document Inspection The whole process of document and signature creation is basically carried out by the central web application. Since users communicate with the web application via SMS only, created and signed documents cannot be accessed immediately. To guarantee an appropriate degree of transparency, the application stores the signed document in an internal database for later inspection. Previously generated and signed documents can be accessed via the application's web interface. Again, access to this interface and to own documents is protected by a secure two-factor authentication scheme.

Figure 5 shows the web based user interface. The left area contains a list of available documents. Details of the selected document are displayed in the main area. Details include document related data and the document's processing log. Available PDF files can be downloaded by clicking the displayed PDF icons.

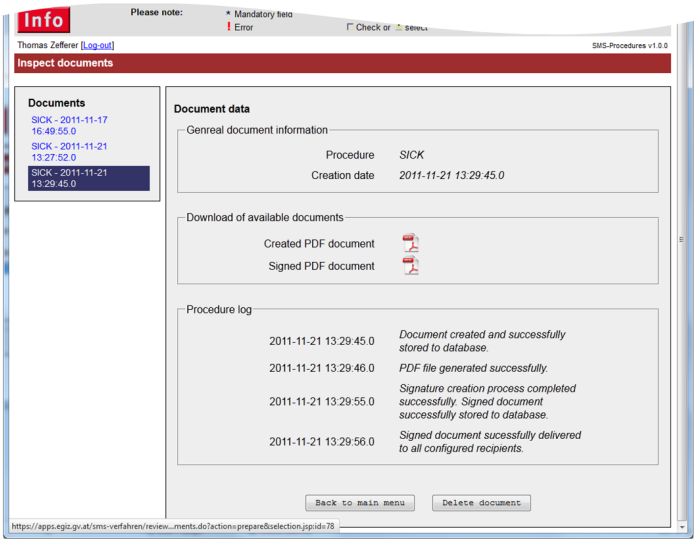

Fig. 5. Web based interface allowing users to inspect documents.

5 Security Analysis

This section discusses aspects, which may have an impact on the security level of SMS-based procedures. Security considerations have been made during the conceptual design of the main architecture and also during the prototypical implementation.

5.1 Omission of Communication Channel

The traditional Austrian Mobile Phone Signature uses a two-factor authentication mechanism based on two communication channels. This means that on

the one hand mobile phone number and signature password entered in a web form ensure knowledge and on the other hand the correct TAN sent by SMS ensures proof of possession. Hence, if the phone is stolen, without knowing the signature password a signature creation process cannot be initiated. In contrast, the purely SMS based procedures proposed in this paper have just one communication channel, the mobile phone. Even if a pure SMS based solution may increase usability, a single communication channel inevitably decreases the security level. If the used mobile end device is infected with malware, the use of a single communication channel may become critical as both signature password and TAN are transferred via the same device. This issue is discussed in more detail in Section 5.5.

5.2 Security of Intermediary Components

In case of the Austrian Mobile Phone Signature, the TAN is directly exchanged between the user and the Mobile Phone Signature service. Several intermediary components are involved in case of SMS based procedures. It is necessary that all these components fulfil certain security requirements to protect the TAN from disclosure. The security of the whole system is just as strong as the weakest link. This does not only concern the components itself, but the inter-component communication as well. For example, an intermediary component using GSM may threaten the security of the whole system due to known vulnerabilities of GSM [9].

5.3 Signature Password Handling

When using the Austrian Mobile Phone Signature in SMS based procedures, the application requires the user's password to create the signature. The only possible way is to transmit the password within an SMS from the user to the application. This approach has two drawbacks. First, it requires full trust in the application and intermediary components. A malicious SMS gateway could intercept signature passwords and exploit them in an abusive way. A second problem is the sending of the user's signature password over the same channel as the TAN. This is a heightened security risk because if the channel is compromised, also the signature process might be compromised. Users are also advised to delete their sent SMS messages from their mobile phones frequently. Otherwise, the secure signature password may appear in locally stored communication histories and get compromised if the device gets lost or stolen.

5.4 Display of Signature Data

According to the Austrian Signature Act, involved technical components must ensure that the signed data can be displayed to the signatory upon request. When using the Austrian Mobile Phone Signature in the user's web browser, this functionality is provided. Support of this feature is more difficult with our SMS

based approach as only text based data can be displayed by SMS technology. However, this does not render application of our approach impossible, since our solution relies on the Austrian PDF signature standard PDF-AS [8]. PDF-AS allows the text based signing of PDF documents, i.e. only the extracted text is signed. This text could also be displayed in one or more SMS messages. This feature is not yet supported in our prototype implementation, but can be added easily if required.

5.5 Malware

Traditional mobile phones with limited functionality can usually be considered as secure. This assumption does not apply to smartphones. Since smartphones can be extended and equipped with arbitrary additional software called *Apps*, they are more vulnerable to different kinds of malware. Apps may get rights to access various parts of the phone's functionality, e.g. including SMS capabilities. This way, an App may intercept unnoticedly incoming or outgoing SMS messages. This is the reason why it can be problematic to enter the signature password on a smartphone. Having caught the password and being able to unnoticedly intercept incoming SMS messages, malware could theoretically create qualified electronic signatures with legal value on behalf of the user.

5.6 Identity Spoofing

Another critical security target is spoofing of the user's identity. SMS spoofing[15] is a common and legitimate technique offered by phone providers so that SMS messages appear to originate from a particular company (name) or a particular phone number. However, the technique can illicitly be used to impersonate another person or company. This way, an attacker may trigger SMS based procedures on behalf of the user. The issue becomes critical if the procedure does not use any confirmation TAN, for example if the user initially triggers the procedure via SMS and the remaining part is processed on the server side (including the generation of the signature).

6 Future Work

The conducted security analysis revealed several security issues that have to be considered in future work. One key issue that has been identified is the vulnerability of the exchanged SMS messages and the integrity and confidentiality of the data contained within these messages. Hence, in a first step we attempt to identify and test different approaches to overcome this issue.

The weakness of the encryption schemes used by the GSM protocol has already been shown by Barkan et al. in [9]. The identification of weaknesses in the GSM protocol has raised the demand for appropriate mechanisms to guarantee

[15] http://www.smsspoofing.com/

secure GSM based communications. Various approaches to satisfy this demand have already been introduced. A comprehensive overview of current approaches to enhance the security of SMS is given by Medani et al. in [13]. Most known approaches make use of cryptographic methods to assure confidentiality and integrity of exchanged SMS messages. For instance, Lisonek and Drahansk [10] enhanced the security of SMS messages by using asymmetric cryptography. Another method relying on both symmetric and asymmetric encryption schemes has been proposed by Anuar et al. [11]. In [12] a hybrid cryptographic scheme has been introduced to meet given security requirements.

All these methods are basically able to enhance the security of data being exchanged via SMS. However, all these solutions also add a certain amount of complexity and require the incorporation of additional components. For our prototypical implementation we have therefore omitted all security enhancing features. A detailed evaluation of existing security enhancing approaches and their integration into our solution is therefore regarded as future work.

Besides the general weaknesses of the GSM protocol, malware running on mobile end devices has been identified as second key issue regarding the security of our solution. Due to their comprehensive software management facilities, especially modern smartphones are known to be prone to malware. We are currently working on the development of practical means and methods to detect malware on smartphones in order to ensure a secure and trustworthy execution environment for security sensitive mobile applications. We plan to integrate outcomes of these attempts into the SMS based document processing solution presented in this paper in order to enhance its overall security.

7 Conclusions

In this paper we have presented an SMS based application that makes use of advanced and qualified electronic signatures to meet security requirements of transactional m-Government services. Our application allows users to dynamically create, electronically sign, and deliver PDF documents on a pure SMS basis. Tests have shown that our solution allows documents to be created, singed, and deliverd within a few seconds.

Although being fully functional, the presented application is still in a prototypical state. The basic goal of this prototypical implementation was to evaluate whether an integration of electronic signatures into SMS based services is technically feasible. Definitely, our application shows that this is basically possible.

The security of the presented approach has been continuously assessed during design, implementation, and practical evaluation. Malware running on mobile end devices and general weaknesses of the GSM protocol have been identified as key issues regarding the overall security of our solution. The identified challenges need to be faced and overcome, before the presented solution can finally be set into productive operation. The development of appropriate counter measures to the identified threats is an ongoing activity. The integration of the outcomes of this activity into our solution is regarded as future work.

References

1. Leitold, H., Hollosi, A., Posch, R.: Security Architecture of the Austrian Citizen Card Concept. In: Proceedings of the 18th Annual Computer Security Applications Conference (ACSAC '02), IEEE Computer Society (2002)
2. Orthacker, C., Centner, M., Kittl, C.: Qualified Mobile Server Signature. In: Proceedings of the 25th TC 11 International Information Security Conference (2010)
3. 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. In: Official Journal of the European Communities (1999)
4. Posch, K.-C., Posch, R., Tauber, A., Zefferer, T., Zwattendorfer, B.: Secure and Provacy-preserving eGovernment - Best Practice Austria. In: Rainbow of Computer Science, Springer (2011)
5. Mobi Solutions Ltd: Mobile Government: 2010 and Beyond. (2010)
6. Thomas Zefferer: Mobile Government - E-Government for Mobile Societies. http://www.a-sit.at/pdfs/Technologiebeobachtung/mobile_government_1.0.pdf (2011)
7. MBAONLINE: Planet Text - How SMS Messaging is Changing the World. http://www.mbaonline.com/planet-text/ (2011)
8. EGov-Labs: PDF-AS.http://egovlabs.gv.at/projects/pdf-as/ (2012)
9. Barkan, E., Biham, E., Keller, N.: Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication. In: J. Cryptol., vol. 21, pp. 392-429 Springer (2008)
10. Lisonek, D., Drahansk, M.: SMS Encryption for Mobile Communication. In: International Conference on Security Technology, pp. 198–201 IEEE Computer Society (2008)
11. Anuar, N. B., Kuen, L. N., Zakaria, O., Gani, A., Wahab, A. W. A.: GSM mobile SMS/MMS using public key infrastructure: m-PKI. In: W. Trans. on Comp., vol. 7, pp. 1219–1229, WSEAS (2008)
12. Al-bakri, S., Kiah, M.: A novel peer-to-peer SMS security solution using a hybrid technique of NTRU and AES-Rijndael. In: Scientific Research and Essays, vol. 5(22), pp. 3455-3466, Academic Journals (2010)
13. Medani, A., Gani, A., Zakaria, O., Zaidan, A. A., Zaidan, B. B.: Review of mobile short message service security issues and techniques towards the solution. In: Scientific Research and Essays, vol. 6(6), pp. 1147-1165, Academic Journals (2011)