Evaluation and Assessment of Editable Signatures for Trusted and Reliable Public Sector Data

Klaus Stranacher[1], Vesna Krnjic[1] and Bernd Zwattendorfer[1] and Thomas Zefferer[2]
[1]E-Government Innovation Center (EGIZ)[1], Graz University of Technology, Austria
[2]Secure Information Technology Center (A-SIT), Austria
Klaus.Stranacher@egiz.gv.at
Vesna.Krnjic@egiz.gv.at
Bernd.Zwattendorfer@egiz.gv.at
Thomas.Zefferer@a-sit.at

Abstract: Due to the increased application of information and communication technologies in the public sector, the amount of data being produced and processed by the public sector has been constantly growing during the past years. As these data can also be useful for the general public and the corporate sector, current initiatives attempt to make these data publicly available. Recent work on this topic has shown that publishing of public sector data potentially raises several issues regarding data integrity and authenticity. These issues render the implementation of solutions based on trusted and reliable public sector data difficult. However, recent work has proposed electronic signatures in general and editable electronic signatures in particular as adequate means to address these issues. While a variety of editable signature schemes has been introduced in literature, their capabilities to assure the integrity and authenticity of published public sector data has not been assessed so far. This renders a concrete implementation of solutions based on editable signatures impossible. To overcome this problem, this paper identifies and discusses legal, organisational, and technical requirements that need to be met by editable signature schemes when applied to public sector data to be published. Afterwards, different existing editable signature schemes are examined and discussed in more detail. Based on the previously identified requirements, the different editable signature schemes are then assessed in detail. The conducted assessment reveals that blank digital signatures, which are a novel approach representing a subset of editable signature schemes, are especially suited to meet the predefined requirements. The results obtained from the conducted survey served as input and basis for the implementation of solutions based on trusted and reliable public sector data.

Keywords: e-government, redactable signatures, editable signatures, blank digital signatures, public sector data

1. Introduction

The public sector produces, collects, processes, and provides large amounts of electronic data. These public sector data can be of interest also for the general public as well as for the corporate sector. In the area of e-Government, two main approaches have evolved to take up the challenge of providing public sector data. The Open Government Data (OGD) initiative bases on the concept of open data and claims that data should be freely available for everyone's use. In addition, the EU Directive on the re-use of public sector information (PSI Directive) defines a legal framework for the provision of public data within the European Union. In June 2013 an amendment of the pre-existing PSI Directive (European Union, 2003) has been published (European Union, 2013). The pre-existing Directive has been published before the emergence of open data. Thus this Directive had a more traditional view on public sector information, which has led to partly different requirements for applications dealing with OGD and PSI related data. This has been consolidated in the updated PSI Directive, which explicitly refers to open (government) data. Nevertheless, security related aspects such as data integrity of authenticity of data are not part of the requirements defined by open data and the updated PSI Directive. To bridge this gap, supplementary security requirements have been defined in literature recently (Stranacher et al., 2013). In this work, the authors have also proposed a concept to meet these additional requirements in practice. The proposed concept employs electronic signatures to allow for the realization of trusted and reliable public sector data. Furthermore, the concept also includes a mechanism to assure the integrity and authenticity of data even if these data need to be redacted. For instance, a redaction can be necessary if the data contain security-sensitive or individual-related information. For such scenarios Stranacher et al. (2013) propose the use of redactable signature schemes, which represent a subset of editable signatures. Editable signatures allow third parties (redactors) to modify signed data without invalidating the original signature. These signature schemes have already proven their usefulness in different fields of application. During the past years, especially the e-Health sector has turned out to be predestinated for an application of editable

[1] EGIZ is a joint initiative of the Austrian Federal Chancellery and the Graz University of Technology

Reference this paper as: Klaus Stranacher et al "Evaluation and Assessment of Editable Signatures for Trusted and Reliable Public Sector Data" *Electronic Journal of e-Government* Volume 11 Issue 1 2013, (pp360 - 372), available online at www.ejeg.com

signature schemes (Bauer et al., 2009) (Slamanig and Rass, 2010). So far, several different editable signature schemes have been proposed and discussed in literature. These schemes differ in various fundamental properties, such as the possibility to explicitly define a designated redactor, or to allow the redacting of predefined data blocks only. Unfortunately, current concepts that propose a use of editable signatures in order to assure authenticity and integrity of public sector data lack on an assessment and definition of appropriate editable signature schemes so far.

In this paper we bridge this gap by assessing existing editable signature schemes and evaluating their capabilities to meet the requirements of public sector data. For this purpose, Section 2 gives the legal and technical status quo on (conventional) electronic signatures and editable signature in particular. In Section 3, we recap the concept of trusted and reliable public sector data. Then Section 4 derives concrete requirements that have to be met by editable signature schemes when being applied to the concept of trusted and reliable public sector data. Potential candidates of editable signature schemes are examined in Section 5. In Section 6, we map the derived requirements to the examined editable signature schemes in order to assess them schemes' capabilities to meet the given requirements. Finally, we summarize the findings and outline the ongoing and scheduled research activities.

2. Electronic signatures status quo

Authentication methods are used to assure authenticity and integrity. Basically two main authentication methods – electronic signatures and challenge-response authentication – exist. Whereas latter methods are mainly used in (low level) protocols, electronic signatures are commonly used in various e-Business applications. Especially the e-Government sector uses electronic signatures as a core technology enabling trusted services.

In general, electronic signatures are used to provide a proof of genuineness for electronic data. They basically assure authenticity, data integrity, and non-repudiation of origin. The receiver of a signed document is able to uniquely identify the creator of the signature (authenticity) and is able to verify that the signed data has not been modified (integrity). At the same time, the creator of an electronic signature cannot deny to have signed the data (non-repudiation). Especially the validation of data integrity becomes important for security critical applications. During the past decades, different forms of electronic signatures with different properties and characteristics have been developed. The following sub-sections briefly discusses

2.1 Conventional signatures

Electronic signatures base on public key cryptography. The creator of an electronic signature holds two keys, a private and a public key. The private key is used to create the signature and is under the creator's sole control. The corresponding public key is used by the verifier of the electronic signature to verify the signature's validity.

A typical signature creation process consists of two steps. At first, the data to be signed is mapped to a fixed length hash value. This mapping is done via a so called hash function[2]. Secondly, this hash value is signed using the creator's private key to create the signature. During the verification of the signature it is verified if the received data corresponds to the originally signed data by comparing the received hash value and the hash value computed out of the received data. If these values differ, the data has been modified. If the data has not been modified, the signature itself is verified by means of the creator's public key.

The legal basis for electronic signatures within the European Union is formed by the Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (European Union, 1999). In particular, the Directive defines three basic types of signatures:

- **Electronic Signature**: Electronic signatures are defined as *"data in electronic form which are attached to or logically associated with other electronic data and which serve as a method of authentication"*.
- **Advanced Electronic Signatures**: The requirements for such a signature are, that the signature is *"uniquely linked to the signatory"*, *"is capable of identifying the signatory"*, *"is created using means that the*

[2] A hash function is a one-way function creating a fixed length data set out of a data set with arbitrary length. Given a hash value, the initial data cannot be determined or re-constructed. The main reason for using a hash function in electronic signature schemes is to reduce the length of the data to be signed, as signing of large data is inefficient and time consuming.

signatory can maintain under his sole control" and *"is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable"*. These requirements are usually fulfilled by conventional signature schemes basing upon a suitable public key infrastructure.

- **Qualified Electronic Signature**: In addition to the requirements for advanced electronic signatures a qualified signature requires to base on a qualified certificate and must be created using a secure signature creation device. The requirements for qualified certificates and secure signature creation devices are also determined in the Signature Directive (Annex I and Annex III). In addition, Article 5 of the Directive defines legal effects of electronic signatures. In particular, it is defined that qualified electronic signatures are legally equivalent to handwritten signatures.

To meet the requirements for advanced electronic signatures, different signature formats have been specified, covering the most wide-spread data formats. These formats are: CAdES[3], XAdES[4] and PAdES[5]. Due to the complexity of these signature formats, which hinders interoperability especially on cross-border level, the European Commission established reference formats for advanced electronic signatures. These reference formats represent appropriate profiles (i.e. subsets) of the mentioned signature formats (European Commission, 2011).

2.2 Editable signatures

Editable signatures provide means to allow (certain) modifications within electronic signatures. Basically editable signatures can be categorized into redactable signatures and blank digital signatures.

2.2.1 Redactable signatures

Redactable signatures have been invented by Johnson et al. (2002) and Steinfeld et al. (2001). In case of conventional signatures, modifications of the signed data are detectable due to an altered hash value. Thus redactable signatures' basic principle bases on retaining the hash value of the original and unmodified data. A main property of these redactable signature schemes is that they only allow blackening out certain message blocks of a signed message. To allow also deletion and replacement of message blocks with other message blocks, Ateniese et al. (2005) introduced the concept of sanitizable signatures, which represent a subset of redactable signatures, but the basic technical concept stays the same.

Figure 1 illustrates this basic principle. First of all, a message m is divided into several message blocks. For illustration, we assume a split into m_1-m_5. For each of these message blocks a hash function H is applied, creating the hash values h_1-h_5. These hash values are concatenated to a total hash value $\text{Hash}_{\text{TOTAL}}$. Finally, this total hash value is signed to create signature S. At this point we still have created a conventional electronic signature.

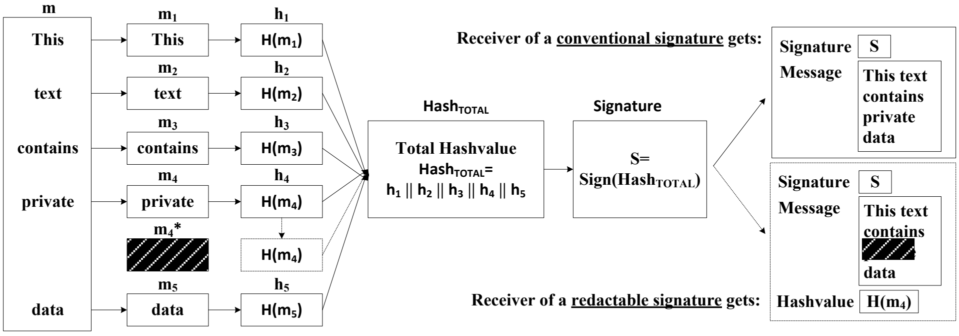

Figure 1: Basic principle of redactable signature schemes

According to the example in Figure 1, the message block "private" (message block m_4*) is redacted. The person, who is allowed to redact message blocks, is usually called redactor. Computing the hash value of the redacted message block will lead to a hash value, which differs from the original hash value and would result in an invalid signature. To avoid this behaviour, the original hash value is retained and used during the signature

[3] CMS Advanced Electronic Signature (ETSI, 2013)

[4] XML Advanced Electronic Signatures (ETSI, 2010a)

[5] PDF Advanced Electronic Signatures (ETSI, 2010b)

verification process[6]. Obviously, the redacted signature must include the original hash value $H(m_4)$. So, the receiver is able to verify the redacted message, but is not able to determine the redacted message block due to the one-way functionality of the hash function. Several redactable signatures schemes do exist, which all base on this basic principle of retaining the original hash values.

2.2.2 Blank digital signatures

Blank digital signatures are a novel scheme invented by Hanser and Slamanig (2013). These signatures have comparable properties to redactable signatures, but the concept behind differs.

Figure 2 illustrates the basic principle of blank digital signatures. An originator defines and signs a message template. This template consists of fixed parts of a message and multiple choices of exchangeable parts. Then a redactor[7] is given the permission to create a message instance. In the instantiation process the redactor selects certain choices of the exchangeable message parts. Finally the redactor signs the message instance. This resulting signature can be publicly verified using the originator's and redactor's public keys. If the verification is positive, it is proven that the message has not been altered as well as the message is compliant to the message template.

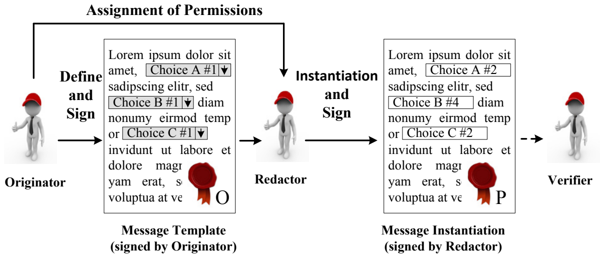
Assignment of Permissions
Define and Sign
Originator
Lorem ipsum dolor sit amet, Choice A #1 sadipscing elitr, sed Choice B #1 diam nonumy eirmod temp or Choice C #1 invidunt ut labore et dolore magr yam erat, s voluptua at ve
O
Message Template (signed by Originator)
Instantiation and Sign
Redactor
Lorem ipsum dolor sit amet, Choice A #2 sadipscing elitr, sed Choice B #4 diam nonumy eirmod temp or Choice C #2 invidunt ut labore et dolore magr yam erat, s voluptua at ve
P
Message Instantiation (signed by Redactor)
Verifier

Figure 2: Basic principle of blank digital signature schemes

3. Trusted and reliable public sector data

This section comprises a brief overview of the findings of Stranacher et al. (2013). Since the re-use of public sector information and the open publishing of governmental data do not define new issues, several requirements for such data provisioning techniques have already emerged over the past years. For instance, the Open Government Working Group (2007) has published eight fundamental principles for open government data. While also the (updated) PSI Directive includes some general and common requirements for providing public sector data, security requirements have not been defined.

[6] That means $H(m_4)$ instead of $H(m_4*)$ is used for calculating $Hash_{TOTAL}$ during signature verification.

[7] The authors use the term proxy for redactor in their proposal.

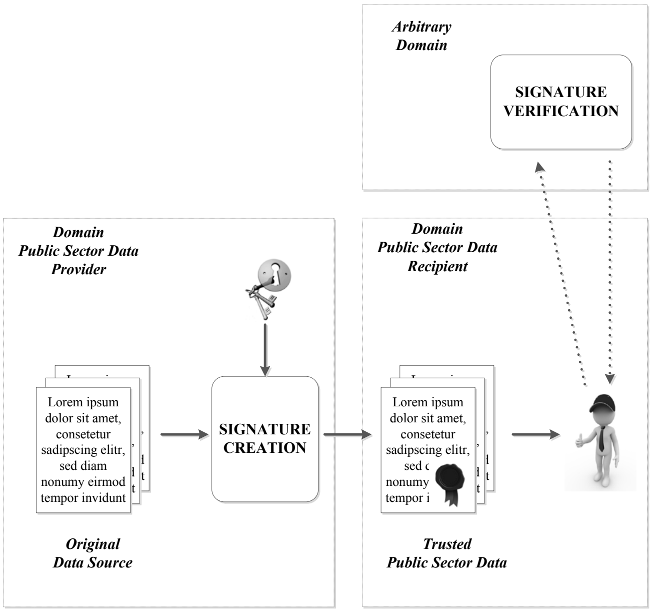
Arbitrary Domain
SIGNATURE VERIFICATION
Domain Public Sector Data Provider
Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt
SIGNATURE CREATION
Original Data Source
Domain Public Sector Data Recipient
Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed c nonumy tempor i
Trusted Public Sector Data

Figure 3: Ensuring authenticity and integrity for public sector data (Stranacher et al., 2013)

Stranacher et al. (2013) define security requirements, namely data integrity and authenticity, when publishing public sector data. Both requirements ensure data consumers that published data have not been altered and are provided by a trustworthy authority. The authors also propose a concept for trusted and reliable public sector data. They distinguish two main use cases. As illustrated in Figure 3, in the first use case public sector data are signed by the data provider before publishing. By using conventional electronic signatures, data integrity and authenticity is ensured.

In the second use case, the public sector data contain personal and private data that need to be anonymized before publishing. Figure 4 illustrates this use case and shows how trusted and reliable anonymization of public sector data without applying a new signature to the modified data is achieved. The original data have been signed by using an editable signature scheme to ensure authenticity and integrity of the entire data set. In case of, these data contain private or personal data, but the remaining data are still useful to publish, the applied editable signature avoids a re-signing process. Avoiding such a re-generation of an electronic signature is useful if the person, who has originally signed the data, is not available anymore for re-signing for some reason.

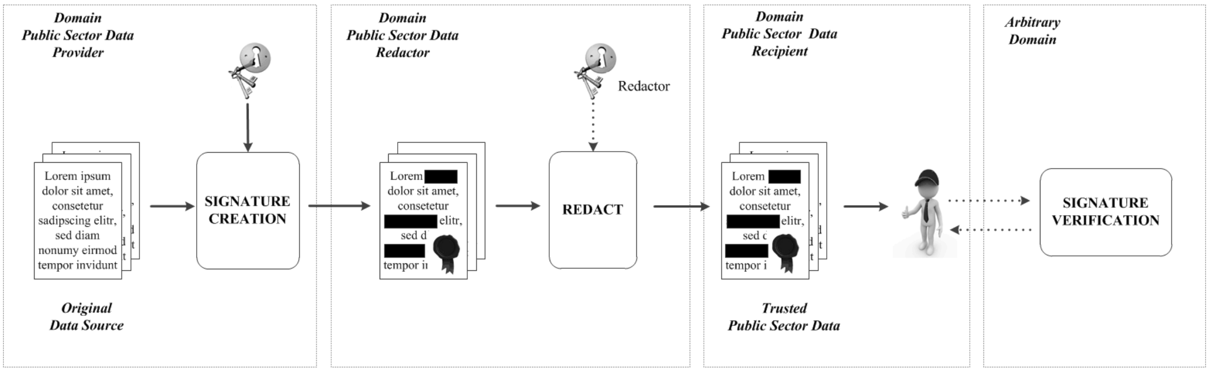
Domain Public Sector Data Provider
Lorem ipsum dolor sit amet, consetetur sadipscing elitr, sed diam nonumy eirmod tempor invidunt
SIGNATURE CREATION
Original Data Source
Domain Public Sector Data Redactor
Redactor
Lorem dolor sit amet, consetetur elitr, sed d tempor ii
REDACT
Domain Public Sector Data Recipient
Lorem dolor sit amet, consetetur elitr, sed c tempor i
Trusted Public Sector Data
Arbitrary Domain
SIGNATURE VERIFICATION

Figure 4: Authenticity and integrity for redacted public sector data (Stranacher et al., 2013)

In the following Section 4 we define concrete requirements for editable signatures applied in this second use case. Additionally we give some more details on different editable signature schemes and their applicability for public sector data in the sections 5 and 6.

4. Requirements for editable signature schemes

The proposed concept of Stranacher et al. (2013) for anonymized public sector data elaborates on the different properties of editable signature schemes, but lacks on defining concrete requirements for editable signature schemes applied to anonymized public sector data. In order to close this gap, this section defines legal, organisational and technical requirements for editable signature schemes.

4.1 General legal requirements

The EU Signature Directive (European Union, 1999) does not differ between conventional signatures, editable signatures or any other signature type. Therefore the regulations and requirements, defined in the Directive, also applies for editable signatures. Therefore, following general legal requirements are defined:

- **Advanced Electronic Signatures**: An editable signature scheme must satisfy the requirements of an advanced electronic signature as defined by Signature Directive. This is a prerequisite for accountability and to identify the original signer.
- **Qualified Electronic Signature**: These additional requirements are not necessarily needed for the public sector data use cases. An editable signature scheme may, optionally, meet also the requirements for qualified electronic signatures as defined by the Signature Directive.
- **Accountability**: In case of a dispute the signatory must be able to prove that certain modifications have been done by a certain redactor. This is of major importance in case of a dispute, being able to give evidence who has signed or redacted specific data (as legal consequences may arise). Accountability can be achieved by technical means (see also technical requirements below).

4.2 General organisational requirements

Beside legal requirements, there exist also some general requirements on organisational level. These requirements concern mainly the role of the redactors and the signatory, i.e. the party, which holds the public sector data. So, following general organisational requirements are defined:

- **Definition and Revocation of Redactors**: Designated redactors should be easily definable by using existing systems (to avoid additional investments) and the signatory should also have the opportunity to revoke redactors.
- **Non-Disclosure Agreement**: Designated redactors must sign an appropriate confidentiality agreement. In particular regarding the data protection as redactors usually have access to private and personal data, which is governed by data protection regulations.
- **Responsibilities:** Responsibilities must be clearly defined both by the signatory and the redactors (e.g. who is allowed to sign/redact, who is responsible in case of a dispute).
- **Service Level Agreement/Security Compliance**: Redactors must ensure to redact data within an appropriate time frame (especially for real time data). In addition, redactors must be compliant to current security regulations as they operate on private and personal data.

4.3 Technical requirements

On a technical level there exists also some requirements, which are tightly bound the particular editable signature schemes. Therefore, we have defined following technical requirements:

- **Designated Redactors**: Designated redactors must be able to be specified by the editable signature scheme. That means that the signatory must be able to determine who is allowed to modify the signed data. Persons except the signatory and the designated redactors must not be able to redact data without breaking the originally signature applied. Any change of the data by unauthorized persons must be recognizable.
- **Privacy**: The redactable data as well as the original signature must not allow revealing the redacted message blocks.
- **Designated Parts**: The signatory must be able to specify which data blocks may be modified. Editing unauthorized data must be recognized and must lead to an invalid signature.

- **Accountability**: See definition in legal requirements.
- **Applicability**: The scheme must be applicable on open and structured data such as XML (W3C Recommendation, 2008)
- **Compatibility:** The signature scheme must be compatible to (at least one of) the reference signature formats defined in European Commission (2011).

5. Examination

In the following, we examine various editable signature schemes. Figure 5 shows an overview on the most relevant[8] editable signature schemes proposed in the last years and their relation to each other. A main requirement for editable signature schemes to be used in e-Business services is to support the definition of designated redactors. Redactable signature schemes, such as Steinfeld et al. (2001) and Johnson et al. (2002)[9], do not offer the definition of designed redactors. Therefore, these schemes have been skipped from a more in-depth analysis. In contrast, sanitizable signature and blank digital signature schemes allow for more complex definitions of modification options and designated redactors. Thus, the following sub-sections examine selected editable signature schemes only. The selected signature schemes, which are marked grey in Figure 5, have been chosen for examination. In addition, following signature schemes have been skipped from the examination:

- Brzuska et al. (2009) proposed a rigorous security model. This model has been incorporated by Canard and Jambert (2010), which is examined below. Therefore we have skipped it from our analysis.
- Brzuska et al. (2010b) proposed an update of Ateniese (2005) which does not permit creating a link between different signatures over the same original message. This functionality is not of interest for the public sector use cases, so we have skipped this scheme.

5.1 Sanitizable signatures by Ateniese et al. (2005)

The basic principle of sanitizable signatures bases upon commitments[10], which in turn build upon hash-functions. Ateniese et al. (2006) proposed the first scheme for sanitizable signatures, where a designated redactor is able to modify designated parts of a signed message. Here the basic principle bases on chameleon hash-functions instead of conventional hash-functions for conventional signatures. Such chameleon hash-functions are parameterized with the public key of the redactor. Because of the parameterization, the redactor is able to compute collisions. This means the redactor is able to generate messages, which lead to the same hash value as for the data, which is going to be redacted. Based on this mechanism the redactor can replace message blocks with arbitrary message blocks and the verification of the original signature will not fail. In this case it is neither possible to detect if a message has been redacted nor it is possible to detect which message blocks have been modified. Therefore the authors propose to add non-redactable meta information after each redactable message block indicating the restriction for the message to be replaced. Obviously, this is a very inefficient solution.

[8] Relevant in terms of citation rate and author's reputation (mainly based on h-index).

[9] This also applies for Slamanig and Rass (2010), Chang et al. (2009) and Brzuska et al. (2010a), which all base on Johnson et al. [13].

[10] Commitments are often used in cryptographic protocols. They allow a committer to publish a commitment (= a value), which binds the committer to a certain message, but without revealing it. If a verifier wants to check if the message is consistent with the commitment, the committer may open the commitment to reveal the message.

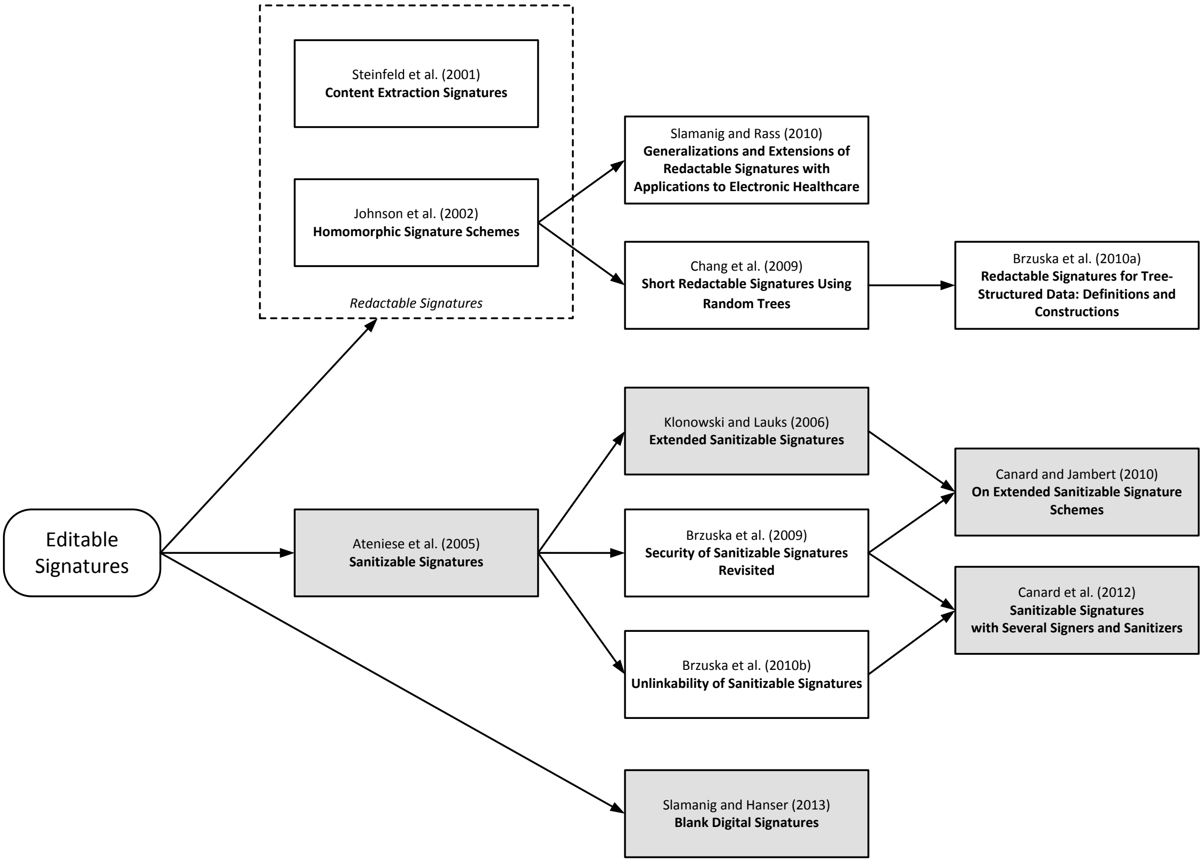
Steinfeld et al. (2001)
Content Extraction Signatures
Johnson et al. (2002)
Homomorphic Signature Schemes
Redactable Signatures
Slamanig and Rass (2010)
Generalizations and Extensions of Redactable Signatures with Applications to Electronic Healthcare
Chang et al. (2009)
Short Redactable Signatures Using Random Trees
Brzuska et al. (2010a)
Redactable Signatures for Tree-Structured Data: Definitions and Constructions
Klonowski and Lauks (2006)
Extended Sanitizable Signatures
Canard and Jambert (2010)
On Extended Sanitizable Signature Schemes
Editable Signatures
Ateniese et al. (2005)
Sanitizable Signatures
Brzuska et al. (2009)
Security of Sanitizable Signatures Revisited
Canard et al. (2012)
Sanitizable Signatures with Several Signers and Sanitizers
Brzuska et al. (2010b)
Unlinkability of Sanitizable Signatures
Slamanig and Hanser (2013)
Blank Digital Signatures

Figure 5: Overview about editable signature schemes

5.2 Extended sanitizable signatures by Klonowski and Lauks (2006)

Klonowski and Lauks (2006) extended the scheme of Ateniese et al (2005). They omitted the added meta information and extended the schema itself to allow the signatory to limit the message blocks which are modifiable by the redactor and to limit the messages which are replaced. This scheme also bases on chameleon hash-functions. For the message replacement restrictions they propose to use accumulators[11] or bloom filters[12].

5.3 On extended sanitizable signature schemes by Canard and Jambert (2010)

Canard and Jambert (2010) presented a second approach to limit the modification of message blocks and the message to be replaced by the scheme itself. As for the other sanitizable signature schemes, the authors base their proposal on chameleon hash-functions. In addition, they use pseudorandom generators and accumulators to implement the message replacement restrictions.

5.4 Sanitizable signatures with several signers and sanitizers by Canard et al. (2012)

Canard et al. (2012) builds upon the findings of Brzuska et al. (2009) and Brzuska et al. (2010b). The proposed scheme allows defining multiple signers and multiple redactors. To support multiple signers and redactors, the authors make use of group signatures[13]. Their scheme also provides group anonymity. That means a signer (resp. redactor) is anonymous for other entities, which are not in the group of signers (resp. redactors).

[11] An accumulator is a one-way hash function which satisfies a quasi-commutative property. See Benaloh and Mare (1994) for details.

[12] Bloom filters are data structures which allow to efficient test whether an element is a member of a certain set or not. See Bloom (1970) for details.

[13] Group signatures give a group of signers signing rights.

5.5 Blank digital signatures by Slamanig and Hanser (2013)

Blank digital signatures, proposed by Hanser and Slamanig (2013), are a new signature scheme, which makes use of elliptic curve pairings[14] and polynomial commitments[15]. In contrast to redactable signatures, blank digital signatures make use of conventional signatures for signing the message template and the message instance. For the definition of the message template polynomials are used. The message instantiation bases upon polynomial commitments. Finally, for the verification of the polynomial commitments pairings are used.
In addition, the authors have published an updated version of this scheme[16]. This update includes a simplified construction of the signatures allowing significantly performance enhancements. Finally, this update incorporates full security proofs.

6. Assessment

6.1 Legal assessment

In this section, we assess editable signature schemes based on legal and organisational requirements. Concerning the legal assessment, the EU Signature Directive defines the legal framework. While this directive primarily considers conventional electronic signatures, the use of sanitizable signatures compliant with this directive has been slightly discussed by Höhne et al. (2012) and Brzuska et al. (2012). The authors examined legal consequences of sanitizable signatures. They especially argue that sanitizable signatures are compliant to advanced electronic signatures but cannot be used for qualified electronic signatures according to the EU Signature Directive. The reason for being not compliant with qualified electronic signatures constitutes missing displaying possibilities for the signatory. According to the Signature Directive, the data to be signed must be viewable by the signatory before the signature creation process. This requirement cannot be fulfilled by sanitizable signatures as modifications of signed data are possible also after signature creation, which the signatory cannot be aware of at the time of the signature creation process regardless the signatory is able to define which message parts are able to be modified and how they can be modified.

Legal considerations for blank digital signatures do not exist yet. Following the argumentation of Höhne et al. (2012) and Brzuska et al. (2012), blank digital signatures are compliant to advanced electronic signatures. The reason for that is mainly based upon the use of public key cryptography. In contrast to sanitizable signatures, blank digital signatures are considered to be compliant with requirements defined for qualified signatures. The reason for being compliant is based upon the usage of conventional signatures for the message template and the message instance signature.
Another legal requirement to be fulfilled by the proposed signature schemes is accountability. Accountability means that redactors, who used her private keys to modify signed data, can be determined. This requirement cannot be met by all described signature schemes (see following Section 6.2).

6.2 Organisational assessment

Equal to legal requirements, several organisational requirements must be met by the proposed signature schemes in order to successfully apply editable signatures to public sector or open government data. In fact, all organisational requirements identified in Section 3.2 are independent of the technical implementation of the proposed signature schemes. While some organisational requirements may be fulfilled using technical means, others require solutions on organisational level. For instance, the requirement on revoking designated redactors can be fulfilled on technical level as all of the proposed schemes rely on a public key infrastructure (PKI) and hence on existing and well-established revocation mechanisms. However, other organisational requirements still require organisational measures. This particularly means that a fulfilment of those requirements requires e.g. some kind of contractual agreements between all involved parties. Within such agreements, especially individual responsibilities, signature validity limitations, or liability questions must be thoroughly elaborated.

[14] Pairings are bilinear mappings as defined by Silverman (1986).

[15] Conventional commitments applied to polynomial functions are called polynomial commitments (see Kate et al. (2010) for details).

[16] https://online.tugraz.at/tug_online/voe_main2.getvolltext?pCurrPk=69904

6.3 Technical assessment

The technical assessment concerning applicability to structured data and the signature format compliance to the European Commission Decision 2011/130/EU can be done for all examined schemes together. Pöhls et al. (2011) have implemented several editable signature schemes based upon XML and the W3C Recommendation on XML signatures (W3C Recommendation, 2008). Hence, they have proven that editable signatures are applicable to structured data, such as XML. Nevertheless, implementations of editable signature schemes fulfilling the requirements for the advanced electronic signatures format XAdES, CAdES or PAdES do not yet exist.

The following sub-sections comprise the further technical assessment of the different editable signature schemes.

6.3.1 Assessment of sanitizable signatures by Ateniese et al. (2005)

Ateniese et al. (2005) states *"[…] as a secure digital signature scheme that allows a semi-trusted censor to modify certain designated portions of the message […]"*[17]. That means the requirement for designated redactor and designated parts is fulfilled. In addition the privacy is also fulfilled as *"[…] the indistinguishhability requirement provides for privacy"*. The author also state that *"accountability follows from the unforgeability requirement"*, but this has been proven by Brzuska et al. (2009) as not true. So the Ateniese sanitizable signature scheme does not provide accountability.

6.3.2 Assessment of extended sanitizable signatures by Klonowski and Lauks (2006)

The extended sanitizable signature scheme of Klonowski and Lauks (2006) provides a designated redactor and designated parts as stated by the authors: *"[…] in this scheme the designated censor can change the content of designated (so called mutable) parts of a signed message […]"*. They also state that privacy is fulfilled due to the basement of their extended scheme on Ateniese et al. (2005). Concerning accountability we have to distinguish between the two characteristics of this scheme. The accumulator technique provides accountability whereas bloom filter does not. Nevertheless, the authors miss a concrete security model and proofs for their proposed schema. This implies an unpredictable security risk, which disqualifies this scheme.

6.3.3 Assessment of extended sanitizable signature schemes by Canard and Jambert (2010)

As this scheme strongly bases on Ateniese et al. (2005), it provides designated redactors as needed by our defined requirements. In addition, Canard and Jambert (2010) state that *"[…] to force some admissible blocks of a signed message to be modified only into a predefined set of sub-messages."*[18] and *"[…] privacy is also included by transparency in the extended model."*. Thus, the scheme fulfils the requirements for designated parts and privacy. In addition, the authors prove that *"Unforgeability (and thus accountability) is reached thanks to the computation of a new tag per message."*. This is one of the major extensions of Ateniese et al. (2005).

6.3.4 Assessment of sanitizable signatures with several signers and sanitizers by Canard et al. (2012)

The scheme of Canard et al. (2012) supports the definition of designated redactors as the authors state that *"[…] a model where one signer (among n) can choose a set of sanitizers (among m)"*. Furthermore the scheme also provides to define designated blocks due to *"Given a message m of length l and divided into t blocks […], which will be modifiable by the sanitizer"*. As this scheme strongly bases on Brzuska et al. (2009) and Brzuska et al. (2010b), the requirement privacy is supported as well. Finally the authors also proofs that their scheme is accountable.

6.3.5 Assessment of blank digital signatures by Slamanig and Hanser (2013)

The proposed template mechanism by Hanser and Slamanig (2013) fulfils the requirement for designated parts, as the originator defines the message template, i.e. only the exchangeable parts, defined by the originator, are modifiable. In addition, the designated redactor requirement is fulfilled as *"Immutability guarantees that no malicious proxy can compute message templates or templates instantiations not intended*

[17] They used the name censor for the redactor.

[18] Message parts which can be modified by a redactor are often called admissible blocks.

by the signer". They even prove that their scheme supports the privacy requirement. Finally, the scheme fulfils the accountability requirement, as the redactor signs the message template instance with a conventional signature (which provides accountability in any case).

6.4 Assessment summary

Table 1 summarizes the results of the legal and technical assessment. It shows that Ateniese et al. (2005) lacks on the requirement on accountability. Furthermore Klonowski and Lauks (2006) miss a security model and proofs for the proposed scheme. Therefore these two schemes are assessed to be not suitable for the public sector data use cases.

In contrast, the sanitizable signature schemes of Canard and Jambert (2010) and Canard et al. (2012) as well as blank digital signatures of Slamanig and Hanser (2013) meet all technical requirements. Hence these schemes are appropriate to the use cases of redacted public sector data as defined in Stranacher et al. (2013). In addition, blank digital signatures fulfil the nice-to-have requirement on qualified electronic signature.

Nevertheless, obstacles hindering an application of these schemes in public sector data applications exist. Concrete implementations for these signature schemes do not exist yet or are not compliant to the standard advanced signature formats defined by the European Commission Decision 2011/130/EU.

Table 1: Assessment summary (legal and technical) of examined editable signature schemes

Signature Scheme	**Legal Requirements**			**Technical Requirements**				
	Account-ability	***Advanced Signature***	***Qualified Signature***	***Designated Redactor***	***Designated Parts***	***Privacy***	***Applicab. Structured Data***	***Compliance 2011/130/ EU***
Ateniese et al. (2005)	No	Yes	No	Yes	Yes	Yes	Yes	Partly
Canard and Jambert (2010)	Yes[19]	Yes	No	Yes	Yes	Yes	Yes	Partly
Canard et al. (2012)	Yes	Yes	No	Yes	Yes	Yes	Yes	Partly
Klonowski and Lauks (2006)	Yes	Yes	No	Yes	Yes	Yes	Yes	Partly
Slamanig and Hanser (2013)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Partly

7. Conclusions

The emerging trend to make public sector data available to the general public and to the corporate sector raises the demand for innovative techniques to meet arising security requirements. Electronic signatures in general and editable electronic signature schemes in particular have recently been proposed as adequate enabler for such security preserving techniques.

In this paper we have made the next step towards a concrete implementation of these techniques by evaluating different proposed schemes for editable signatures and by assessing their capabilities to enhance the security of publishing (anonymized) public sector data. The assessment has been based on a set of legal, organisational, and technical requirements, which have previously been defined and discussed. The conducted assessment of existing editable signature schemes has revealed that especially blank digital signatures by Slamanig and Hanser (2013) are well suited to enhance the security of published public sector data.

[19] This scheme supports accountability only for the version where accumulators are used. In case the bloom filter is used accountability is no achievable.

The results that have been obtained from the conducted assessment pave the way for several future activities in this field. The blank digital signature scheme that has been identified by the conducted assessment has been implemented on a prototype basis and allows for creation of XAdES-based signatures. Currently, this implementation serves as basis for the development of solutions based on trusted and reliable public sector data.

References

Ateniese, G., Chou, D. H., de Medeiros, B., Tsudik, G. (2005), *Sanitizable Signatures*, in European Symposium on Research in Computer Security ESORICS 2005, LNSC, vol. 3679, pp. 159-177, Springer.

Bauer, D., Blough, D., Mohan, A. (2009), *Redactable Signatures on Data with Dependencies and their Application to Personal Health Records*. In: Proc. of the 8th ACM Workshop on Privacy in the Electronic Society, WPES ’09, pp. 91–100. ACM Press, New York

Benaloh, J., Mare, M., (1994), *One-Way Accumulators: A Decentralized Alternative to Digital Signatures*, in Advances in Cryptology — EUROCRYPT 1993, LNCS, vol. 765, pp. 274-285, Springer.

Bloom, B. (1970), *Space/time trade-offs in hash coding with allowable errors*, in Communication of ACM, vol. 13, no. 7, pp. 422-426

Brzuska, C., Fischlin, M., Freudenreich, T., Lehmann, A., Page, M., Schelbert, J., Schröder, D., Volk, F. (2009), *Security of sanitizable signatures revisited*, in Jarecki, S., Tsudik, G. (eds.) PKC 2009. LNCS, vol. 5443, pp. 317–336. Springer.

Brzuska, C., Busch, H., et al. (2010a), *Redactable Signatures for Tree-Structured Data: Definitions and Constructions*, in Applied Cryptography and Network Security 2010, LNCS, vol. 6123, pp. 87-104, Springer.

Brzuska, C., Fischlin, M., Lehmann, A., Schröder, D. (2010b), *Unlinkability of Sanitizable Signatures*, in Public Key Cryptography – PKC 2010, LNCS, vol. 6056, pp. 444-461, Springer

Brzuska, C. Pöhls, H., Samelin, K. (2012), Non-Interactive Public Accountability for Sanitizable Signatures, in Proceedings of the 9th European PKI Workshop: Research and Applications (EuroPKI 2012), Springer, Note: to appear.

Canard, S., Jambert, A. (2010), *On Extended Sanitizable Signature Schemes*, in Topics in Cryptology - CT-RSA2010, LNCS, vol. 5985, pp. 179-194, Springer.

Canard, S., Jambert, A., Lescuyer, R. (2012), Sanitizable Signatures with Several Signers and Sanitizers, AFRICACRYPT'12 Proceedings of the 5th international conference on Cryptology in Africa, pp. 35-52, Springer.

Chang, E., Lim, C., Xu, J. (2009), *Short Redactable Signatures Using Random Trees*, in Topics in Cryptology – CT-RSA 2009, LNCS, vol. 5473, pp. 133-147, Springer.

ETSI (2010a), *Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XAdES)*, V1.4.2.

ETSI (2010b), *Electronic Signatures and Infrastructures (ESI);PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles*, V1.2.1.

ETSI (2013), *Electronic Signatures and Infrastructures (ESI);CMS Advanced Electronic Signatures (CAdES)*, V2.2.1.

European Commission (2011), 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, 25.02.2011.

European Union (1999), *Directive 1999/93/EC on a Community framework for electronic signatures*.

European Union (2003), *Directive 2003/98/EC of the European Parliament and the Council of 17 November 2003 on the re-use of public sector information*

European Union (2013), *Directive 2013/98/EC of the European Parliament and the Council of 26 June 2013 on the re-use of public sector information*

Höhne, F., Pöhls, H., Samelin, K. (2012), Rechtsfolgen editierbarer Signaturen, in Datenschutz und Datenrecht (DuD), vol. 36(6), pp. 485-491

Johnson, R., Molnar, D., Song, D. X., Wagner, D. (2002), *Homomorphic Signature Schemes*, in Topics in Cryptology CT-RSA 2002, LNCS 2271, pp. 244-262, Springer.

Kate, A., Zaverucha, G. M., Goldberg I. (2010), *Constant-size commitments to polynomials and their applications*. In Advances in Cryptology - ASIACRYPT 2010, pp. 177-194, 2010

Klonowski, M., Lauks, A. (2006), *Extended sanitizable signatures*, in: Rhee, M.S., Lee, B. (eds.) ICISC 2006. LNCS, vol. 4296, pp. 343–355. Springer.

Open Government Working Group (2007), *8 Principles of Open Government Data*, http://www.opengovdata.org/home/8principles.

Pöhls, H., Samelin, K., Posegga, J. (2011), *Sanitizable Signatures in XML Signature — Performance, Mixing Properties, and Revisiting the Property of Transparency*, in Applied Cryptography and Network Security, LNCS, vol. 6715, pp. 166-182, Springer.

Silverman, J. (1986),*The Arithmetic of Elliptic Curves*, volume 106 of Graduate Texts in Mathematics, 1986, Springer.

Slamanig, D., Hanser, C. (2013), *Blank Digital Signatures*, in Proceedings of 8th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2013), pp. 95-106, ACM.

Slamanig D., Rass, S. (2010), *Generalizations and Extensions of Redactable Signatures with Applications to Electronic Healthcare*, in Communications and Multimedia Security 2010, LNCS, vol. 6109, pp. 201-213. Springer.

Steinfeld R., Bull, L., Zheng, Y, (2001), *Content Extraction Signatures*, in Kim, K.-c. (ed.) ICISC 2001. LNCS, vol. 2288, pp. 285–304. Springer.

Stranacher, K., Krnjic, V., Zefferer, T. (2012), Vertrauenswürdiges Open Government Data, in 1.OGD D-A-CH-LI Konferenz, pp. 27-39.

Stranacher, K., Krnjic, V., Zefferer, T. (2013), Trust and Reliability for Public Sector Data, Proceedings of International Conference on e-Business and e-Government, pp. 124-132.

W3C Recommendation (2008), *XML-Signature Syntax and Processing (Second Edition)*, http://www.w3.org/TR/xmldsig-core/

Yuen, T., Susilo, W., Liu, J., Mu, Y. (2008), *Sanitizable Signatures Revisited*, in Cryptology and Network Security, LNCS, vol. 5339, pp. 80-97, Springer.