Klaus Stranacher, Vesna Krnjic, Bernd Zwattendorfer, Thomas Zefferer - "Assessment of Redactable Signature Schemes for Trusted and Reliable Public Sector Data" - Proceedings of the 13th European Conference on e-Government, 2013, pp. 508-516

# Assessment of Redactable Signature Schemes for Trusted and Reliable Public Sector Data

Klaus Stranacher, Vesna Krnjic, Bernd Zwattendorfer
E-Government Innovation Center (EGIZ)[1], Graz University of Technology, Austria
Klaus.Stranacher@egiz.gv.at, Vesna.Krnjic@egiz.gv.at, Bernd.Zwattendorfer@egiz.gv.at

Thomas Zefferer
Secure Information Technology Center (A-SIT), Austria
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 redactable electronic signatures in particular as adequate means to address these issues. While a variety of redactable 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 redactable signatures impossible.

To overcome this problem, this paper first identifies and discusses legal, organisational, and technical requirements that need to be met by redactable signature schemes when applied to public sector data to be published. Afterwards, different existing redactable signature schemes are examined and discussed in more detail. Based on the previously identified requirements, the different redactable signature schemes are then assessed in detail. The conducted assessment reveals that sanitizable signature schemes, which represent a subset of redactable signature schemes, are especially suited to meet the predefined requirements. Among the wide set of existing sanitizable signature schemes, the conducted survey has revealed two concrete schemes to be best suited to assure the integrity and authenticity of public sector data to be published. The results obtained from the conducted survey will serve as input and basis for the implementation of solutions based on trusted and reliable public sector data.

**Keywords:** eGovernment, Redactable Signatures, Sanitizable 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) (European Union, 2003) defines a legal framework for the provision of public data within the European Union.

Both approaches define partly different requirements for applications dealing with OGD and PSI related data. Surprisingly, security related aspects such as data integrity of authenticity of data are not part of these requirements. 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 proposed 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 allow third parties (redactors) to modify signed data without invalidating the original signature.

Redactable 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

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

for an application of redactable signature schemes (Bauer et al., 2009) (Slamanig and Rass, 2010). So far, several different redactable 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 redactable signatures in order to assure authenticity and integrity of public sector data lack on an assessment and definition of appropriate redactable signature schemes so far.

In this paper we bridge this gap by assessing existing redactable signature schemes and evaluating their capabilities to meet the requirements of public sector data. For this purpose, we first recap the concept of trusted and reliable public sector data in Section 2. In Section 3, we then derive concrete requirements that have to be met by redactable signature schemes when being applied to the concept of trusted and reliable public sector data. Potential candidates of redactable signature schemes are examined in Section 4. In Section 5, we map the derived requirements to the examined redactable signature schemes in order to assess them schemes' capabilities to meet the given requirements.

## 2. 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 PSI Directive includes some general and common requirements for providing public sector data, security requirements have not been defined.

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. In the first use case public sector data are published as it is. To ensure data integrity and authenticity, conventional electronic signatures are applied to these data. In the second use case, the public sector data contain personal and private data that need to be anonymized before publishing. Redactable signatures are used in this case. Figure 1 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. Avoiding the re-generation of electronic signatures e.g. might be useful if the person, who has originally signed the data, is not available anymore for re-signing for some reason.

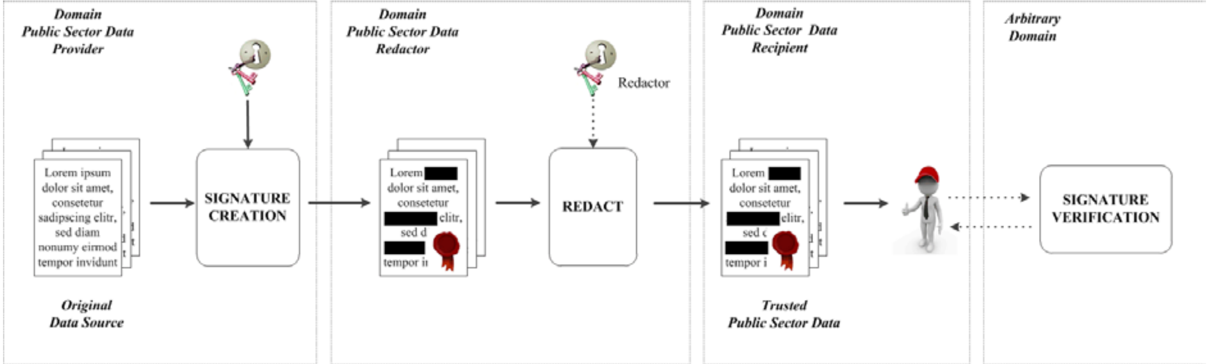

**Figure 1:** Authenticity and integrity for redacted public sector data (Stranacher et al., 2013)

In the following Section 3 we define concrete requirements redactable signatures for this use case. Additionally we give some more details on different redactable signature schemes and their applicability for public sector data in the sections 4 and 5.

## 3. Requirements for Redactable Signature Schemes

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

### 3.1. General Legal Requirements

The concept of trusted and reliable public sector data bases on electronic signatures. The legal basis for electronic signatures 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 addition, the national regulatory authorities are responsible for implementation of the Signature Directive on the national level. Therefore, following general legal requirements are defined:

- **Advanced Electronic Signatures**: Such a signature defines, among other things, that the signature is *"uniquely linked to the signatory"* and *"is capable of identifying the signatory"*. There a redactable signature scheme must satisfy the requirements of an advanced electronic signature as defined by European Union (1999). This is a prerequisite for accountability and to identify the original signer.
- **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. These additional requirements are not necessarily needed for the public sector data use cases. Nevertheless a redactable signature scheme may, optionally, meet also the requirements for qualified electronic signatures as defined by European Union (1999).
- **Accountability**: In case of a dispute the signatory must be able to prove that certain modifications have been done by a certain redactor. Accountability can be achieved by technical means (see also technical requirements below).

### 3.2. 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.

### 3.3. Technical Requirements

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

- **Designated Redactors**: Designated redactors must be able to be specified by the redactable 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 structured data such as XML (W3C Recommendation, 2008).
- **Compatibility:** The signature scheme should be compatible with existing signature standards, such as XMLDSIG (W3C Recommendation, 2008) or XAdES (ETSI, 2010).

## 4. Examination

Redactable Signatures provide a cryptographic mechanism to allow redactors to apply modifications to signed messages without invalidating the original signature and have been introduced by Steinfeld et al. (2001) and Johnson et al. (2002). This mechanism has many applications in electronic healthcare as shown by Slamanig and Rass (2010) and several other areas presented in Ateniese et al. (2005). A main property of redactable signatures is that they only allow blacking certain parts of the signed data. To remove or replaced designated parts of the signed messages with an arbitrary string, Ateniese et al. (2005) proposed Sanitizable Signatures. Sanitizable signatures can be seen as a small subset of redactable signatures, as they are basically redactable signatures where the replacement part is permanently exchanged.

Figure 1 shows an overview of about the most relevant redactable and sanitizable signature schemes proposed in the last years and their relation to each other. There exist also other schemes (not shown in Figure 1), but either they have been the basis for one of the mentioned schemes or they have been proven as insecure or not applicable. For instance, the authors of Yuen et al. (2008) lacks on accountability of the proposed schema or Pöhls et al. (2011) contains only minor updates on the property transparency (which is not of special interest for our use cases).

For our following examination we have looked initially on the redactable signature schemes proposed by Steinfeld et al. (2001), Johnson et al. (2002), Slamanig and Rass (2010), Chang et al. (2009) and Brzuska et al (2010a). Right at the beginning of the examination we have figured out that all of these schemes do not support the specification of designated redactors. As this is one of the main requirements for the public sector data use cases, all of these schemes are not applicable for these scenarios. Therefore we omitted an in-depth analysis of these schemes and concentrated on sanitizable signature schemes instead.

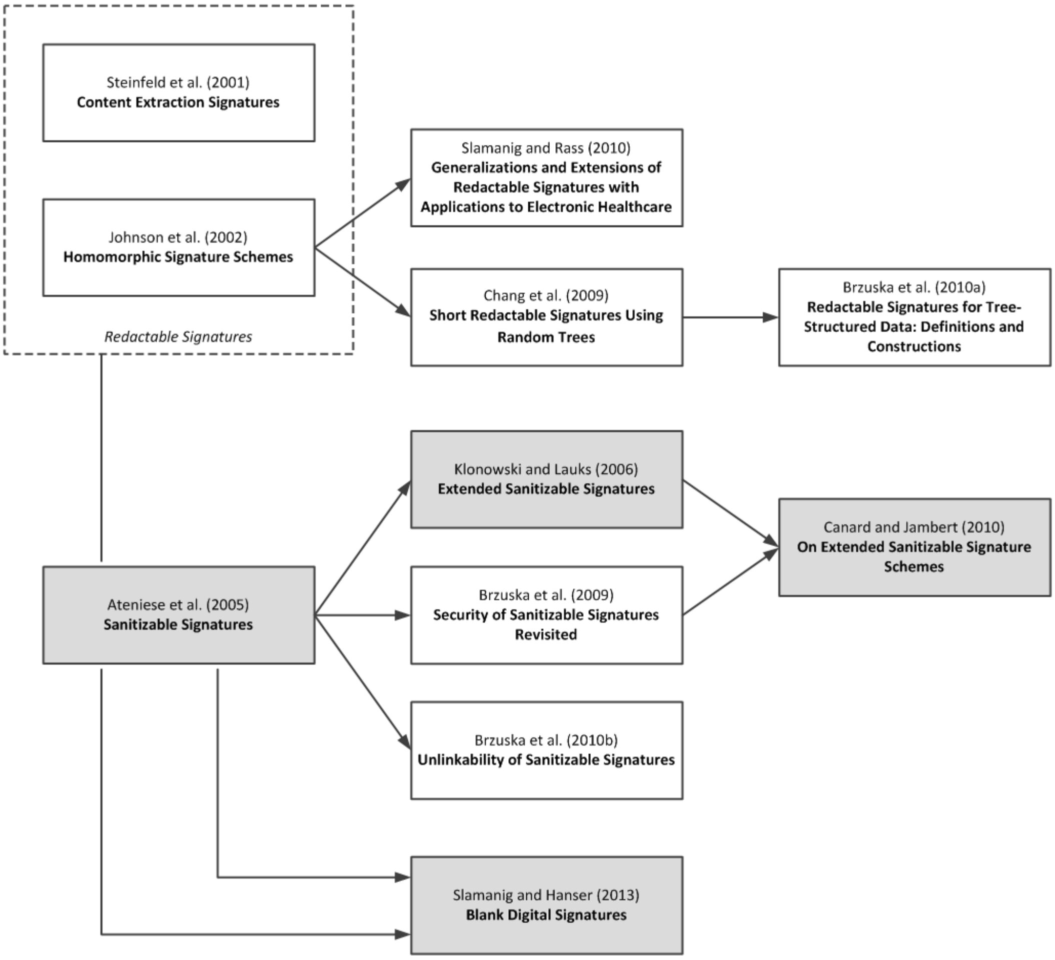
Steinfeld et al. (2001)
Content Extraction Signatures
Johnson et al. (2002)
Homomorphic Signature Schemes
Redactable Signatures
Slamanig and Rass (2010)
Generalizations and Extensions of Redactable Signatures with Applications to Electronic Healthcare
Chang et al. (2009)
Short Redactable Signatures Using 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
Ateniese et al. (2005)
Sanitizable Signatures
Brzuska et al. (2009)
Security of Sanitizable Signatures Revisited
Brzuska et al. (2010b)
Unlinkability of Sanitizable Signatures
Slamanig and Hanser (2013)
Blank Digital Signatures

**Figure 2:** Overview about redactable and sanitizable signature schemes

Figure 2 shows the sanitizable signature schemes we have chosen for our examination (highlighted in grey). A few sanitizable signature schemes we have skipped from our examination due to following reasons:

- 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.

Following sub-sections give the examination of the chosen sanitizable signature schemes. In addition, we examine on the proposal of Slamanig and Hanser (2013) on Blank Digital Signature, which incorporates the findings of redactable and sanitizable signatures.

### 4.1. Sanitizable Signatures by Ateniese et al. (2005)

The basic principle of redactable signatures bases upon commitments[2], which in turn build upon hash-functions. This principle basis upon retaining the original hash values for redacted message blocks and to use them during the signature verification process (instead of calculating a new hash value over the redacted data). This process is described in Stranacher et al. (2013) and in more detail in Johnson et al. (2002) and Steinfeld et al. (2001).

[2] 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.

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.

### 4.2. 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[3] or bloom filters[4].

### 4.3. 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.

### 4.4. Blank Digital Signatures by Slamanig and Hanser (2013)

Slamanig and Hanser (2013) proposed a new signature scheme, which bases on redactable and sanitizable signatures. They specified a message template, which is defined by an originator and describe a message containing fixed message blocks and multiple choices of message blocks, which are exchangeable. This template is signed by the originator. A proxy[5] is then able to sign an instantiation of this template, i.e. selecting concrete message blocks of the defined choices. Finally, the resulting message can be verified by a third party using the originator's and proxy's verification keys. Their proposal builds upon conventional signature schemes, elliptic curve cryptography and polynomial commitments[6].

## 5. Assessment

### 5.1. Legal and Organisational Assessment

In this section, we evaluate redactable and sanitizable signature schemes based on legal and organisational requirements. In order to use redactable and sanitizable signatures for ensuring trusted

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

[4] 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.

[5] For the public sector use cases the proxy can be seen as the redactor.

[6] Polynomial commitments are conventional commitments applied to polynomial functions.

and reliable public sector data, all defined requirements must and can be fulfilled by the proposed signature schemes.

The European Union has published the EU Signature Directive (European Union, 1999) to define how electronic documents can achieve statutory trust within its Member States. While this directive primarily considers conventional electronic signatures, the use of redactable and sanitizable signatures compliant with this directive has been only slightly discussed so far. Höhne et al. (2012) and Brzuska et al. (2012), for instance, examine legal consequences of redactable and sanitizable signatures. They especially argue that redactable and 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 redactable and 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. 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 5.2).

Equal to legal requirements, several organisational requirements must be met by the proposed signature schemes in order to successfully apply redactable and sanitizable 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.

## 5.2 Technical Assessment

This sub-section comprises the technical assessment of the examined sanitizable signature schemes according to the defined requirements in Section 3. In the following, the schemes are assessed in detail and Section 5.2.5 summarizes the findings of this technical assessment.

### 5.2.1 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 […]"[7]. 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.

### 5.2.2 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).

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

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.

### 5.2.3 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."*[8] 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).

### 5.2.4. Assessment of Blank Digital Signatures by Slamanig and Hanser (2013)

Slamanig and Hanser (2013) state that *"Immutability guarantees that no malicious proxy can compute message templates or templates instantiations not intended by the signer."* and *"[…] is called private, if for any polynomial-time algorithm A the probability of winning Game 2 is negligible as a function of security parameter k."* It follows that the proposed scheme provides a designated redactor and privacy. The requirement, that designated parts must definable, is fulfilled because of the proposed template mechanism, where the signatory defines a message template. Additionally accountability is also fulfilled as the proxy signs the template instantiations with a conventional signature, which provides accountability.

### 5.2.5. Technical Assessment Summary

The requirements for applicability to structured data and compatibility with existing signature standards can be assessed together for all examined schemes. Pöhls et al. (2011) have shown several implementations of sanitizable signatures based upon XML and the W3C Recommendation (2008) on XML-Signature Syntax and Processing (XMLDSIG). The authors have proven that sanitizable signatures are applicable to structured data and fit into XMLDSIG without invalidating the recommendation. In addition, the findings of Pöhls et al. (2011) may be applied to the examined schemes with slight changes.

Table 1 summarizes the results of the 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 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).

**Table 1:** Technical assessment of examined sanitizable signature schemes

| **Signature Scheme** | **Design. Redactor** | **Privacy** | **Design. Parts** | **Account-ability** | **Applicable to Structured Data** | **Compatibility** | **Comment** |
|---|---|---|---|---|---|---|---|
| Ateniese et al. (2005) | Yes | Yes | Yes | No | Yes | Yes | |
| Canard and Jambert (2010) | Yes | Yes | Yes | Yes | Yes | Yes | |

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

|  |  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|
| Klonowski and Lauks (2006) | Yes | Yes | Yes | Yes[9] | Yes | Yes | No security model and no proofs are given |
| Slamanig and Hanser (2013) | Yes | Yes | Yes | Yes | Yes | Yes |  |

## 6. 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 redactable 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 redactable 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 redactable signature schemes has revealed that especially sanitizable signature schemes, which represent a subset of redactable signatures schemes, are well suited to enhance the security of published public sector data. Among the set of evaluated sanitizable signature schemes, especially two schemes proposed by Canard and Jambert (2010) and by Slamanig and Hanser (2013) have turned out to be able to meet given legal, organisational, and technical requirements.

The results that have been obtained from the conducted assessment pave the way for several future activities in this field. In a next step, the two most promising schemes that have been identified by the conducted assessment will be implemented and integrated into approved electronic signature schemes such as XMLDSIG. This implementation will then serve 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-RSA 2010, LNCS, vol. 5985, pp. 179-194, 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.

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

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

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*

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.

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.

Slamanig, D., Hanser, C. (2013), *Blank Digital Signatures*, in Proceedings of 8th ACM Symposium on Information, Computer and Communications Security (ASIACCS 2013), Note: to appear.

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, Note: to appear.

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.