The legal status of malleable- and functional signatures in light of Regulation (EU) No 910/2014

F.W.J. van Geelkerken,[1,3] H.C. Pöhls,[2]
S. Fischer-Hübner[3]

1. Swedish Institute for legal informatics, Stockholm University, Sweden, Stockholm, Universitetsvägen 10, SE-106 91, franciskus.vangeelkerken@juridicum.su.se

2. Institute for IT-Security and Security Law, Chair of IT-Security, University of Passau, Germany, Innstrasse 43, 94032 Passau, hp@sec.uni-passau.de

3. HumanIT, Karlstad University, Sweden, Karlstad, Universitetsgatan 2, SE-651 88, simone.fischer-huebner@kau.se

Abstract* – *In this article, we analyse the legal status of malleable- and functional signatures in light of 910/2014/EU. Both these forms of signatures possess beneficial properties which already legally acknowledged signatures do not. Namely, they allow subsequent changes by authorised parties to for instance anonymise or remove personal data from signed documents. We conclude that the legal status of both these forms of electronic signatures is – depending on cryptographic properties of the malleable- or functional signature as well as the chosen signature-scheme – similar to that of a qualified electronic signature.

Keywords – electronic signatures, digital signatures, verification, identification, malleable signature, functional signature, electronic identification, regulation no. 910/2014.

I. Introduction

In this article, we provide an overview of two 'classes' of cryptographic signature schemes, and determine their legal position in light of Regulation EU 910/2014 [1] (hereafter eIDAS). In general, the legal status for three different categories of electronic signatures was, from 19 January 2000 until 16 September 2014, regulated through Directive 1999/93/EC [2] (hereafter ESD). As of 1 July 2016 the ESD will become fully repealed by eIDAS.

To determine the legal status – at a European Union level – of more recently emerged cryptographic signatures such as malleable- and functional signatures, we first elaborate in section II on the legal definition and status of different categories of electronic signatures.
Thereafter, in sections III, we go over the technical details of respectively malleable- and functional signatures schemes,[1] to conclude with an overview of the key-differences between the different categories of electronic signatures already (explicitly) regulated and malleable- and functional signatures. Based on these key-differences, in section IV, the legal status of malleable- and functional signatures in light of effectual regulation at a European Union level will be determined.

II. The legal status of electronic signatures

It is possible to distinguish between three different categories of electronic signature (***ES***):

(1) Basic signatures (***BS***);
(2) Advanced signatures (***AS***); and
(3) Qualified signatures (***QS***).

Before expounding on these three categories, though, it is necessary to elaborate on three related terms of high importance. Based on respectively article 3 section 9, section 13, and section 22 eIDAS;

(1) Signatory means a natural person who creates an electronic signature;
(2) Electronic signature-creation data means unique data which is used by the signatory to create an electronic signature; and
(3) Electronic signature-creation device means configured software or hardware used to create an electronic signature.

As said, it is possible to distinguish between the following three different categories of **ES**s. The first, basic signatures (***BS****s*), are defined in Article 3 section 10 eIDAS as data that has to fulfil three requirements;

(1) The data needs to be in electronic form;
(2) The data needs to be attached to, or logically associated with, other electronic data; and
(3) That other electronic data needs to be used by the signatory to sign.

The second category, advanced electronic signatures (***AS****s*), are defined in article 3 section 11 j°. 26 eIDAS. The most notable difference to ***BS****s* is that additional requirements are put on the linking and the data used to create the signature. When combining the different requirements of these articles and the aforementioned definitions, an ***AS*** (in its barest essence) is a ***BS*** which additionally fulfils the following requirements:

(1) The ***BS*** is uniquely linked to signatory;
(2) The ***BS*** is capable of identifying the signatory;
(3) The ***BS*** is created using unique data that the signatory can, use under his sole control; and
(4) The ***BS*** is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable.

The third category, Qualified electronic signatures (***QS****s*), are defined in article 3 section 12 eIDAS. Based on this article in conjunction with article 3 sections 10 and 11 eIDAS and article 26 eIDAS, a ***QS*** has to comply with six requirements. The first four are similar to that of an ***AS***, with the addition of the requirements that a ***QS*** is an ***AS*** which is;

(5) created by a qualified electronic signature creation device (***QD***); and
(6) created using electronic signature-creation data based on a qualified certificate for electronic signatures (***QC***).

The requirements for a ***QC*** and ***QD*** are defined in Annex I and Annex II of the eIDAS. Seeing as these requirements are less relevant to the underlying research question, they will be not be elaborated on at this point. It is important to note though that based on article 25 section 1 eIDAS, *all* electronics signatures à priori have legal effect, are admissible in legal proceedings, and that a ***QS*** has the same legal effect as a handwritten signature.

The legal status of two not yet specifically regulated forms of electronic signatures, namely malleable- and functional signatures schemes, will be elaborated on hereafter.

III. Malleable electronic signature scheme

A malleable signature scheme can be defined as;

> *A digital signature scheme with an additional function whereby, on input of message (**m**) and signature (**σ**), it is possible to efficiently compute derived signature (**σ'**) on an altered message (**m'**) for transformation (**T**) that has been allowed with respect to the message (**m**) and the signature (**σ**), i.e.* **(m' = T(m)** *).*[2]

As such, when an ***MS*** is used by the Signer[3] to sign a message, this message can subsequently be altered by the Sanitizer[4] within the scope predefined by the Signer's provided transformation without invalidating the original electronic signature. ***MS****s* are of great use, because cryptographic schemes make it possible to prove that if the transform ***T*** removes or changes information, such that the information – previously contained in ***m*** – is no longer contained in ***m'***, then the information originally in ***m*** cannot be reconstructed from ***m'*** and ***σ'***. For ***MS****s* this property is cryptographically well-known as privacy.[5]

As an ***MS*** is in electronic form, is attached to, or logically associated with, other electronic data (the document to sign), and electronic data (the Signer's key) is used by the signatory to sign, no elaboration is necessary to conclude that a malleable signature is a ***BS*** ex article 3 section 10 eIDAS. Hereafter, ***MS****s* and their characteristics will be analysed to assess whether they (can) fulfil the requirements of – and can be qualified as – an ***AS*** or ***QS***. The reason for this interest is that only the ***QS*** awards some additional legal value following from the statement that a ***QS*** is equivalent to a handwritten signature. Note, that neither eIDAS nor EDS endorse any further legal value of a ***QS***, it is left to member states' individual legal texts to assign these in each specific legal circumstance.

Can an ***MS*** be qualified as an ***AS***?

To be able to conclude that an ***MS*** can be qualified as an ***AS***, an ***MS*** has to fulfil all the requirements the eIDAS prescribes for an ***AS***. As stated, a ***BS*** has to fulfil four requirements to be qualified an ***AS***. The first three requirements can be fulfilled with the aid of asymmetric cryptography, whereby the signature generation key (***sk***) can be kept secret and under sole control and the verification key (***pk***) can be made public. To achieve the linkage and the identification function public key infrastructures (PKI) – that are currently already in place – can be facilitated. This means that whenever an ***MS*** can be instantiated with a signature algorithm for the Signer's signature that is legally established and for which the keys are hence compatible with the already deployed public key certificates,[6] the existing trust infrastructure can be facilitated.[7]

An ***MS*** based on a cryptographic signature algorithm which is legally accepted naturally fulfils the requirement of the Signer's initial signature being created using unique signature creation data.

Next to that, the signatory can keep these unique signature creation data under his sole control, and thus the signature created by the ***MS*** is both uniquely linked to- and capable of identifying the signatory.

It can therefore be concluded that an ***MS*** complies with the first three of the four requirements laid down in article 3 section 11 j°. 26 eIDAS. Compliance with the fourth and last requirement (the ***ES*** is linked to the data to which it relates in such a manner that any subsequent change of the data is detectable) might, however, appear to pose a problem seeing as an ***MS***-scheme is specifically used to make it possible for a Sanitizer to alter the message after it has been signed. In general, this does, however, not mean that such a change would not be detectable. In general verification yields:

Sign ***(m,scope,sk)*** **=** ***σ***	**Sign** ***(m,sk)*** **=** ***σ***
	Sanit ***(m,σ,change)*** **=** ***(m'[scope],σ')***
Verify ***(m,σ,pk)*** **= Valid**	**Verify** ***(m'[scope],σ',pk)*** **= Valid**
Situation 1: Unchanged.	Situation 2: Changed within scope.

The verification of a signature created by an ***MS*** scheme only yields true if the public key ***pk*** corresponds to the secret signature generation key (***sk***) and only in the following two situations; (1) the message ***m*** and its signature ***σ*** remain unaltered; or (2) the message has been altered within the predefined scope into ***m'[scope]***, and a derived signature ***σ'*** has been computed[8]. If the original message is transformed by any third party beyond the scope (altered into ***m'[non-scope]***) no valid signature can be derived and the verification will yield:

Verify ***(m'[non-scope],σ, pk)*** **= False**[9].

In general, an ***MS*** does not differentiate between situation 1 and 2 and returns valid. For legal compliance, however, the detectability of a modification must hold true regardless of the change being authorised or unauthorised, as the eIDAS clearly states "*any subsequent change*".[10] Hence, we need to be able to verify an ***MS*** and get the following three results:

(1) Valid and unmodified (***MS*** created by the Signer),
(2) Valid and modified in authorised way (derived signature correctly computed by Sanitizer), or
(3) Invalid (***MS*** does not verify, indicating malicious or erroneous corruption).

Hence, if there are authorised changes[11] the signature verification must flag the document as containing changes subsequent to signing.[12] This form of triple detectability can be achieved if the ***MS*** scheme offers a cryptographic property called non-interactive public accountability [7].[13] Moreover, it is important to note that in an ***MS*** scheme the derived signature (***σ'***) still verifies under the Signer's public key. As long as the changes after signing (and any subsequent changes) were within the authorised scope the Signer is still identifiable by the Verifier as the signatory for any validly derived message. If the scheme is public non-interactive accountable this can be done in the same manner as a regular ***AS*** signature verification, requiring only the Signer's public key (***pk***).

In summary, a non-interactive public accountable malleable signature that builds on a signature scheme allowing the linking of public signature verification keys to the signatory fulfils all four criteria of article 3 section 11 j°. article 26 eIDAS. This means in light of the eIDAS an ***MS*** is an ***AS***, and the legal position of an ***MS*** is the same as that of an ***AS***.

Can an ***MS*** be qualified as a ***QS***?

To assess whether an ***MS*** can be qualified as a ***QS***, it is necessary to evaluate whether an ***MS*** complies with the aforementioned six requirements of a ***QS***.

Seeing as we concluded in the previous section that an ***MS*** can be qualified as an ***AS***, ***MSs*** comply with the first four requirements of a ***QS***. It is therefore only necessary to assess whether it is possible to create an ***MS*** based on a qualified certificate for electronic signatures (***QC***) using a qualified electronic signature creation device (***QD***).

As follows from Annex I to the eIDAS a ***QC*** has to comply with ten requirements, and none of these requirements pose more of a problem in the case of ***MS***s when compared to other forms of ***ES***s. Especially they pose no problems if the signature scheme used as a basis for the ***MS***, and with it the keys, is equivalent to a legally accepted scheme. It can therefore be concluded it is just as possible to create an ***MS*** based on a ***QC*** as it is to create any other ***ES*** based on a ***QC***.

Annex II to the eIDAS consists of four articles in relation to ***QD***. Article 1 contains technical requirements a ***QD*** has to comply with, and these should, similar to the requirements a ***QC*** has to comply with, not pose more of a problem in the case of ***MS***s when compared to other forms of ***ES***s; as such this requirement will not be elaborated on. Article 3 states that only a qualified trust service provider may generate or manage electronic signature creation data. Because this provision is irrelevant to the question whether an ***MS*** can be qualified as a ***QS*** this provision will not be elaborated on. Article 4 states that qualified trust service providers may only duplicate the electronic signature creation data for back-up purposes under specific conditions. Because this provision, like article 3, is irrelevant for answering whether an ***MS*** can be qualified as a ***QS*** this provision will not be elaborated on either.

The second article of Annex II eIDAS is highly relevant for the question whether an ***MS*** can be qualified as a ***QS***, and thus what the legal position is of an **MS**, as it reads;

> *[**QD**s] shall not alter the data to be signed or prevent such data from being presented to the signatory prior to signing.*

As such, in essence, a ***QD*** has to fulfil two requirements;

(1) A ***QD*** should not alter the contents of the data to be signed prior to signing;[14] and
(2) A ***QD*** should not make it impossible to show the data to the signatory prior to signing.[15]

In [9] it is stated that the problem of not knowing / showing all possible derivations of a document signed by an ***MS*** would prevent an ***MS*** from being qualified as a ***QS***. After consulting these authors it became clear though that their conclusion is based on a very limited and strict interpretation of German legislative texts that requires electronic signatures to be functionally equivalent to handwritten ones and lists those functions.[16] Under a strict grammatical interpretation the ***MS*** could therefore neither fulfil the *Abschlussfunktion* (conclusory function) nor the *Perpetuierungs- oder Integritäts-funktion* (archiving or integrity function). The argument for their conclusion was that the ***MS*** during signature generation will not be able to present to the signatory all the different versions it might have after subsequent authorised changes.

In forthcoming follow up work of one of the authors the reasoning is, however, less strict by arguing that an ***MS*** can be treated as a blanket statement.[17] It is thus, not a problem that the ***MS*** by its design leaves room for many versions – potentially too many to display – of the signed document. While the technical details may matter for legal questions regarding e.g. liability, technically the ***QD*** does not prohibit the showing of the various iterations.

The last requirement which needs to be fulfilled is that an ***MS*** can be created by a ***QD***. In fact in [10] it was shown that certain ***MS*** (including the non-interactive publicly accountable scheme from [7]) can be executed in such a way that the secret signature generation data never leaves a smartcard, which is technically recognised as a ***QD***. Hence it is possible to generate ***MSs*** using ***QDs***. As long as the modifications by the third party take place within the predefined authorised scope, verification will yield valid:

$$\textbf{Verify } (m'_{[scope]}, \sigma'_{[scope]}, \textbf{pk}) = \textbf{Valid}$$

Once the Signer has created a valid signature using an ***MS***, any authorised alteration or modification of the contents does not need the Signer's secret signature-creation data to generate the σ', which means the (altered) data does not need to be shown to the signatory again nor does it involve the use of the signatories ***QD***. But, if the modification of the contents exceeds the predefined authorised scope, verification will logically yield invalid:

$$\textbf{Verify } (m'_{[scope]}, \sigma'_{[scope]}, \textbf{pk}) = \textbf{False}$$

In case of an invalid signature, i.e. verification yields False, the invalid signature does not increase the legal value of the document.

Seeing as neither the requirements for a ***QC*** nor the requirements for a ***QD*** pose a problem in light of an ***MS***-scheme, it is possible to conclude that the legal position of an ***MS*** is the same as that of a ***QS***[18] if the following conditions are met:

(1) The ***MS*** offers non-interactive public accountability,
(2) A legally accepted cryptographic asymmetric digital signature scheme for the Signer's signature is used,
(3) A qualified certificate for the Signer's public key exists, and
(4) The execution of all algorithms involving the Signer's secret signature creation data is computed inside a ***QD.***

IV. Functional electronic signature scheme

Unsurprisingly, a functional electronic signature-scheme relies on the use of a functional signature (***FS***). In short an ***FS***-scheme works based on a key pair consisting of a secret master key (***sk***) to sign messages with and a public key (***pk***) to verify these signed messages. The ***sk*** can be used to sign any message with, and the signatory can derive a separate signing key for a specific task or function (sk_f). This separate signing key (sk_f) the Signer can hand over to any third party so that this party can perform a specific task or function (***f***) on the message (***m***) on behalf of the signatory. With the sk_f the third party can generate a valid signature after transforming the original message. The following overly simplified equation captures that functionality;

$$\textbf{Sign } (f(m), sk_f) \rightarrow \sigma.$$

A valid signature is only created when $\mathbf{sk}_f$ is used to sign a message within the predefined function's image, i.e. the output of ***f***. For a cryptographic overview on ***FS*** see [3]. Therefore, when either ***f(m)*** or ***m*** is verified it yields;

Verify (*m*,σ,*pk*) = True and **Verify (*f*(*m*),σ,*pk*) = True**.

Whereby it is important to note that the latter equation holds true if, and only if, the third party did not exceed the scope, defined by the function ***f*** and the input ***m*** to that function, it was authorised to sign by the signatory. The use of an ***FS***-scheme does not pose too many problems in light of the eIDAS as the term signatory is, as stated before, defined in article 3 section 9 eIDAS as;

A natural person who creates an electronic signature.

In essence this definition states that a signatory is a person who can create any form of electronic signature, i.e. a ***BS***, ***AS***, ***QS***, ***MS***, or ***FS***, either on his own behalf or on behalf of a person or entity he represents.[19] And as an ***FS*** is in electronic form, is attached to, or logically associated with, other electronic data, and is used by the signatory to sign, it can be concluded that a ***FS*** is an ***ES***.

Can an *FS* be qualified as either an *AS* or *QS*?

To determine whether an ***FS*** can be qualified as either an ***AS*** or a ***QS***, it is important to point out that an ***FS*** is, in principle, the same as any other electronic signature, except for the fact that;

(1) instead of using a ***sk*** the signatory (i.e. the third party) uses $\boldsymbol{sk}_f$ to create σ; and
(2) instead of being able to sign any ***m*** the third party is only authorised to sign a predefined function of ***m*** on behalf of the principal.

Because the four requirements an ***ES*** has to comply with to be qualified as an ***AS*** neither contain requirements regarding the signature key, nor contains requirements regarding the scope of the authorisation the signatory has to sign, it can be concluded that an ***FS*** can be qualified as an ***AS***. Regarding the need to know all derivations c.q. iterations of the message at the time of signature creation, the same arguments as for ***MS*****s,** and the same arguments for blanket statements, apply.

Similarly, because the additional two requirements an ***ES*** has to comply with to be qualified as a ***QS*** (next to the first four which make it possible to qualify ***FS*** as an ***AS***) do not contain a requirement regarding either the signature key or the scope of the authorisation the signatory has to sign, it can be concluded that an ***FS*** can be qualified as a ***QS*** if it can be shown to be able to have the signature creation data inside a smartcard or other suitable ***QD***.

Because the third party is always identifiable,[20] if the legal status of the $\boldsymbol{sk}_f$ in relation to the third party is similar to, or the same as, the legal status of a "normal" signature in an ***FS***-scheme with respect to the Signer, it can fulfil the requirements of both an ***AS*** and a ***QS***.

In sum, an ***FS***-scheme complies with all of the six aforementioned requirements for a ***QS*** because the third party to whom the principal provides the $\boldsymbol{sk}_f$ is always identifiable which means the third party is the (mandated) signatory representing the principal.

Conclusion

The legal standing of malleable signatures (***MS***s) has been analysed in light of Regulation EU 910/2014 (eIDAS), the latest signature legislation at an EU level. We assessed whether they can be qualified as qualified electronic signatures (***QS***). Qualification as a ***QS*** is the highest level of assurance awarded by the eIDAS after meeting six requirements. It gives the document with the ***QS*** the same legal standing as a document signed with a handwritten signature and it cannot be denied legal effect in legal proceedings.

An ***MS*** – in form of the signatory's original signature or in the form of derived signature generated by the authorised third party – can be qualified as a ***QS***, as codified in article 3 section 12 j°. 3 section 11 j°. 26 eIDAS, if the ***MS*** has certain cryptographic properties.

Apart from standard cryptographic security properties, like unforgeability, in particular the cryptographic property of public non-interactive accountability allows the cryptographic verification of an ***MS*** to technically function like existing legally well recognised digital signature algorithms, such as RSA with SHA2, and be based on existing public key certification infrastructures.

The factual value of this malleably signed document is determined by the specific circumstances of the case and the applicable legislation, as well as the evidentiary value attributed to signed documents based on this legislation, of an individual EU Member State.

It should be pointed out that allowing any party to subsequently modify certain well-definable parts of the signed document might aid usability, this does, however, complicate assigning liability to the party who did the subsequent edits (the Sanitizer). Therefore, we advise using ***MS***s which allow identifying the Sanitizer by its derived signature and are designed to comply with the requirements for a ***QS***, as this makes it possible to hold the Sanitizer technically accountable and legally liable for any modifications which might occur subsequent to the signing by the Signer.

The same line of argument is applicable with regard to the legal status of functional signatures (***FS***s). As such, ***FS***s can – if they contain specific cryptographic properties like public non-interactive accountability – be qualified as ***QS***s in the sense of article 3 section 12 j°. 3 section 11 j°. 26 eIDAS.

Acknowledgements

This work was supported by the European Union's 7th Framework Programme (FP7) under grant agreement n°. 609094 (RERUM) and the Horizon 2020 Programme under grant agreement n°. 644962 (PRISMACLOUD). We would like to thank Daniel Slamanig for his willingness to explain and clarify some cryptographic properties and aspects of digital signatures in layman's terms. Next to that we would like to thank Focke Höhne for his participation in the discussion of his previous work.

Notes

1 his article will not go into too many of the cryptographic details; for more technical details and an overview of signatures see [3]; for an in-depth analysis of the legal evidentiary value of malleable signatures see [4].
2 Derived from [5]
3 Hereafter the term Signer is used to refer to the initial signatory mandating a Sanitizer to sign on its behalf.
4 We use the original work's American spelling to stay close to the existing body of technical work, in 2003 the term Sanitizer first occurred [6].
5 Not to be confused with the legal term privacy.
6 Technically the format is also known as X.509
7 For examples of ***MS*** schemes which were designed with this in mind, see [7].
8 The calculation of that derived signature is done by an algorithm denoted usually as ***Sanitize*** or ***Sanit***, whereby it should be noted that the ***Sanitize*** algorithm does not require the Signer's secret signature generation key as input.
9 The same applies for the situation where the signature is altered, but the same (unaltered) message is signed, or for the situation where both the signature and the message are altered, i.e.

Verify (*m, σ'[non-scope], pk*)= False and **Verify (*m'[non-scope], σ'[non-scope], pk*)= False**

10 There are differences in the level of detectability in technical algorithms, as well as in technical definitions of the protection goal of Integrity, for more see [4] and also [8].
11 Or technically only if the signature was derived by ***Sanit***, to keep the cryptographic property of privacy as argued for in [4], [7], and [8].
12 This is one of the central results obtained by Henrich C. Pöhls in his PhD. thesis, see [4].
13 An ***MS*** satisfies non-interactive public accountability, if and only if, given a valid message and a signature over the message, a third party can correctly decide whether the message-signature pair originates from the Signer or from the Sanitizer without interacting with the Signer or Sanitizer, i.e. just from using public knowledge of the message, the signature and the Signer's (or the Sanitizer's) public signature verification key.[4]
14 A qualified electronic signature creation device can in that sense be likened to an automated postage meter or franking machine, the application of postage or franking to an envelope does not alter the contents of the envelope.
15 As such, based on the previously used analogy, the signatory can verify that the contents of the envelope were not altered by the application of postage or franking.
16 See for example *Deutscher Bundestag*. Drucksache 14/4987, Dec. 2000 (German only).
17 Blanket statements are underspecified statements, similar to blank cheques. Legally, you are allowed to leave certain fields underspecified or empty, allowing them to be filled with information later. From [4]: In German law it is found that if a blanket statement is done in a consented way, any specific information filled in later is attributed to the original signatory of the blanket statement, see BGH 11 July 1963 – VII ZR 120/62, 1963 (German only).
18 This conclusion – an ***MS*** can be qualified as a ***QS*** – is not affected if one can identify the Sanitizer and hold the Sanitizer accountable as an individual party. See [3] and [4] for different classes of malleable signature schemes: redactable signature schemes (RSS) allowing for public subsequent erasure of signed data, and sanitizable signature schemes (SSS) allowing for subsequent changes but only by specified Sanitizers. See also very recent work on accountable RSS [11].
19 Despite the rephrasing of the definition in the eIDAS, similar to the (old) article 2 section 3 ESD, under the eIDAS a signatory can act either on his own behalf or on behalf of a person he represents.
20 Seeing as the principal derives **sk*f*** from **sk** for a specific task or function and for a specific party, this party is always identifiable. If the third party hands over the **sk*f*** to another party who signs any message with it, the third party is considered the signatory and the third party will be liable for any damages which might arise from an alteration of the message beyond the predefined scope.

References

[1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[2] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures (OJ 2000, L 013/12-20)

[3] D. Slamanig & D. Derler (eds.), *PRISMACLOUD D4.4: Overview of Functional and Malleable Signature Schemes*, 31 July 2015.

[4] H. C. Pöhls, *Increasing the Legal Evidentiary Value of Private Malleable Signatures (diss.)*, Passau, Germany: University of Passau (forthcoming), 2016.

[5] M. Chase M., M. Kohlweiss, A. Lysyanskaya, and S. Meiklejohn, *Malleable Signatures: Complex Unary Transformations and Delegatable Anonymous Credentials*, Cryptology ePrint Archive, report 2013/179, 2013, p. 1.

[6] K. Miyazaki and S. Susaki and M. Iwamura and T. Matsumoto and R. Sasaki and H. Yoshiura, *Digital documents sanitising problem*, Techreport at IEICE, ISEC2003-20, 2003.

[7] H. Pöhls, K. Samelin, and C. Brzuska, 'Non-Interactive Public Accountability for Sanitizable Signatures', in *Proceedings of the 9th European PKI Workshop: Research and Applications (EuroPKI)*, Springer, p. 178, 2012.

[8] H. de Meer, H. C. Pöhls, J. Posegga, and K. Samelin, 'Scope of security properties of sanitizable signatures revisited', in *Proceedings of the 10th Intl. Conference on Availability, Reliability and Security* (ARES), IEEE, pages 188–197, 2013.

[9] F. Höhne, H. Pöhls, and K. Samelin, 'Rechtsfolgen editierbarer Signaturen' in *Datenschutz und Datensicherheit* 2012 (7), p. 485-491. (German only)

[10] H. C. Pöhls, S. Peters, K. Samelin, J. Posegga and H. de Meer, 'Malleable Signatures for Resource Constrained Platforms', in *Proceedings of Information Security Theory and Practice (WISTP)*, pages 18-33, Springer-Verlag, 2013.

[11] H. C. Pöhls and K. Samelin, 'Accountable Redactable Signatures' in *Proc. of the 10th International Conference on Availability, Reliability and Security* (ARES 2015), IEEE, 2015.