How to qualify electronic signatures and time stamps

Detlef Hühnlein

secunet Security Networks AG
Sudetenstraße 16
D-96247 Michelau, Germany
detlef.huehnlein@secunet.com

Abstract. In this work we will show how non-qualified electronic signatures and time stamps can be efficiently enhanced in order to equip them with similar features as qualified ones. In particular we will show how non-qualified electronic signatures can be used in business processes which require the written form. Furthermore we will show how to construct "interval-qualified" (IQ) time stamps which may serve as cost efficient alternative to qualified time stamps issued by a trusted authority. An IQ time stamp issued at time t_i is linked to two qualified time stamps issued at time T_1 and T_2, in a way that one is able to prove that $T_1 < t_i < T_2$.

1 Introduction

Because of national implementations of [EC/1999/93, Article 5 Section 1 (a)], like [BGB, §126a] in Germany for example[1], electronic signatures which are based on a qualified certificate and created using a secure signature creation device, called *qualified electronic signatures* throughout this work, are deemed equivalent to handwritten signatures. This implies that business processes which traditionally require the written form, either need to apply paper or qualified electronic signatures in order to fulfill this formal requirement. As there are legal regulations, like [BGB, §125], which void statements lacking the appropriate form, this formal requirement turns out to be essential. While there are quite a few certification-service-providers in Europe issuing qualified certificates and secure signature creation devices, it is fair to say that Europe is still far away from the omnipresent availability of equipment to produce qualified electronic signatures. Hence there are situations, where the formal need for qualified electronic signatures introduces additional obstacles which may even lead to sticking with paper-based processes. In communities where non-qualified electronic signatures are already used, e.g. for electronic banking or e-mail protection, the formal

[1] We will use the German law to examplify the legal issues related to our proposal. These legal considerations may not translate directly, but would need to be compared to other national laws.

need for *qualified* electronic signatures is even more annoying and it would be desirable to be able to ”enhance the non-qualified electronic signatures in use”, in order to make them equivalent to handwritten signatures.

In a similar fashion there is, due to operational necessities and legal requirements like [SigV, §17], an increasing demand for time stamps issued by a trusted authority. Following [SigG, §2 Nr. 14] we will call such time stamps which are produced in a trustworthy manner *qualified time stamps.* Because of costly requirements, such as the need for sophisticated security concepts, certified products and additional liability issues, it is not surprising that time stamping authorities typically charge relatively high fees per issued time stamp in order to realize a return on their initial investment. If a large number of time stamps is required, such fees may soon become a major cost factor and even jeapardize the business case of an electronic business process. On the other side, one can not simply ignore the costly trust issues and naively use self made time stamps, because they would provide far less evidence. Thus it would also be desirable to be able to ”enhance self made time stamps” in a cost-efficient manner, such that they provide a similar level of evidence as a qualified time stamp.

In this work, we will propose simple solutions for these two problems: We show how to ”qualify electronic signatures and time stamps” in a very cost efficient manner.

First we show how the combination of simple technical and legal measures can be used to enhance non-qualified electronic signatures such that they can be used for business processes which require the written form. As explained in Section 2, this is mainly achieved by having a (in a legal sense) properly authorized central signature server re-signing the non-qualified signatures of the clients using qualified signatures in an automated manner.

Next we show how a few qualified time stamps can be used to enhance an arbitrary number of self made time stamps with moderate computational cost. As explained in Section 3, this is mainly achieved by appropriately linking an arbitrary number of self made time stamps S_i, issued at time t_i, with two qualified time stamps issued at time T_1 and T_2 respectively, in a way that one is able to prove that $T_1 < t_i < T_2$ (see Theorem 1).

2 Qualifying electronic signatures

In this section we will show how a community which uses non-qualified electronic signatures may enhance these signatures, such that the signed documents fulfill the written form in the sense of [EC/1999/93, Article 5, Section 1 (a)].

Let N be a signatory, which is able to produce electronic signatures, denoted by $\sigma(x, N)$. However N is not able to produce qualified electronic signatures, because he does not use a secure signature creation device (SSCD) or he does not use a qualified certificate. Thus N could use software-based PGP-keys without certificates for example.

Suppose that N wants to declare its intention within a business process, for which the written form according to [BGB, §126] is required. Because of [BGB, §126 (3)], N will be able to use the electronic form according to [BGB, §126a] instead of the written form. In order to fulfill the requirements stipulated there, N would need to use a qualified electronic signature according to [SigG, §2 Nr. 3] to sign a document D. Because N is not able to produce such a signature, it will need to make use of another signatory Q, which is able to produce qualified electronic signatures, denoted by $\sigma_q(x, Q)$. In practice, Q may be a server, which is able to create qualified electronic signatures in an automated manner as explained in [HüKn03].

In this scenario, as depicted in Fig. 1, N will send the electronic document D, which will need to be signed with a qualified electronic signature, together with an appropriate power of attorney P, according to [BGB, §167], to Q. P will contain an appropriate legal statement L_1 and the hash value $h(D)$ of the document D. L_1 states that Q is, for the special purpose necessary to proceed the document D, authorized to act on behalf of N. The power of attorney P will be signed by N with the non-qualified electronic signature $\sigma(P, N)$.

$$\begin{tikzcd}
N \arrow[r, shift left, "{D,\ P=(L_1|h(D)),\ \sigma(P,\ N)}"] & Q \arrow[l, shift left, "{\sigma_q(L_2|D|P|\sigma(P,N),\ Q)}"]
\end{tikzcd}$$

Fig. 1. How to qualify electronic signatures

Thus N will send the triple $D, P = (L_1|h(D)), \sigma(P, N)$ to Q. Q is verifying N's signature and the content of the power of attorney P. If everything is ok, Q will produce the qualified electronic signature $\sigma_q(L_2|D|P|\sigma(P, N), Q)$. Here L_2 states that Q is presently not acting on behalf of its own, but on behalf of N. That Q is allowed to act on N's behalf is shown by the power of attorney P. Note that according to [BGB, §179 (1)] Q can not be liable as long as it is acting within the scope of P. Finally the qualified electronic signature is returned to N.

Now the document D is, together with L_2, P and $\sigma(P, N)$, signed by Q with a qualified electronic signature and hence fulfills the formal requirement of [BGB, §126a]. Because of L_2, it is clear that Q is acting on behalf of N and that it is authorized to do so, because of P and $\sigma(P, N)$. Hence, as stipulated in [BGB,

§164 (1)], the declaration of intention in D is as effective for or against N as it would have signed D itself.

The crucial point that this legal construction is possible, is that, according to [BGB, §167 (2)], the power of attorney P does not need to have the same form as the legal transaction for which it is intended. This implies that even if D requires a qualified electronic signature, it is sufficient that P is only signed with a non-qualified electronic signature.

3 Qualifying time stamps

In this section we will consider a similar scenario, in which N is able to issue time stamps, but N is not able to issue qualified time stamps according to [SigG, §2 Nr. 14], because N is no certification-service-provider (CSP) which fulfills the costly requirements of [SigG, §§4-14 and §17 or §23]. As above, N would like to enhance its self made time stamps, such that they would provide a similar level of evidence as qualified time stamps issued by CSPs. This is realized by constructing "interval-qualified" (IQ) time stamps, which are linked to two qualified time stamps, such that one can prove that they must have been issued between them (see Theorem 1).

The function $h : \{0,1\}^* \rightarrow \{0,1\}^n$ is called a *cryptographic hash function*, if it is infeasible to find some preimage x given $h(x)$ (one-wayness) and that it is infeasible to find a pair x_1, x_2 such that $h(x_1) = h(x_2)$ (collision-resistance).

A *time stamp*, like specified in [RFC3161] for example, is roughly of the form

$$S = \sigma(h(D)|t, TSA), \tag{1}$$

where $h()$ is a cryptographic hash function, D is the data which is to be time stamped, t is the time and σ is a secure electronic signature scheme in the sense that only TSA is able to produce $\sigma(\cdot, TSA)$. A TSA is called *trusted* if it always inserts the present time in the time stamps it issues. A time stamp $QS = \sigma(\cdot, Q)$ is called a *qualified time stamp*[2] if Q is trusted.

The essential value of such a time stamp may be stated as follows.

Proposition 1. *If $QS = \sigma(h(D)|t, Q)$ is a qualified time stamp, then D existed prior to t.*

Proof:. Because Q is trusted, QS proves that $h(D)$ has been existing at time t. Because of the one-wayness of $h()$, it is infeasible to find D given $h(D)$. Hence D must have been used to calculate $h(D)$, which implies that D existed prior to t. □

[2] While the *technical* definition of a qualified time stamp given here, obviously differs from the *legal* definition given in [SigG, §2 Nr. 14], they tend to be "equivalent" in practice in the sense that until today all qualified time stamps, which meet the legal definition also meet the technical definition given here.

Note that D is uniquely specified by $QS = \sigma(h(D)|t, Q)$ because of the collision-resistance of $h()$.

Next we will consider what happens, if one links time stamps as proposed in [HaSt90, Section 5.1] and [BLLV98,Lipm99].

Proposition 2. *Let $QS = \sigma(h(r)|T_1, Q)$ be a qualified time stamp and $S = \sigma(h(QS)|m|\tilde{t}, N)$ be a time stamp, where r and m are arbitrary data. Let t be the creation time of S. Then $t > T_1$.*

Proof: Because Q is trusted, the qualified time stamp QS is produced at time T_1. Because of the one-wayness of $h()$ it is infeasible to find QS given $h(QS)$. Hence QS must have been used to calculate $h(QS)$, which implies that S was created at a later point in time than T_1. □

Note that t might be different from $\tilde{t}$, because N might not be trusted. The other way around is shown analogously.

Proposition 3. *Let $S = \sigma(h(r)|m|\tilde{t}, N)$ be a time stamp and $QS = \sigma(h(S)|T_2, Q)$ be a qualified time stamp, where r and m are arbitrary data. Let t be the creation time of S. Then $t < T_2$.*

Proof:. Because Q is trusted, the qualified time stamp QS is produced at time T_2. Because of the one-wayness of $h()$ it is infeasible to find S given $h(S)$. Hence S must have been used to calculate $h(S)$, which implies that S was created prior to T_2. □

Combining these two simple results, we obtain the following corollary as visualized in Fig. 2.

Corollary 1. *Let $QS_1 = \sigma(h(r)|T_1, Q)$ be a qualified time stamp, $S = \sigma(h(QS_1)$ $|m|\tilde{t}, N)$ be a time stamp and $QS_2 = \sigma(h(S)|T_2, Q)$ be a qualified time stamp again, then $T_1 < t < T_2$, where t is the creation time of S.*

If there is more than one time stamp S_i in between the two qualified time stamps, then one will include QS_1 in every time stamp S_i, $0 < i < n$, and will link all these time stamps in an appropriate manner to the second time stamp QS_2. For this purpose, one may use the batch signature strategy introduced in [PaBo99], which uses Merkle's authentication tree [Merk80] to construct an efficient batch signature scheme.

As shown in Fig. 3, one will construct a binary hash tree from the time stamps S_i and will obtain a qualified time stamp QS_2 for the root of this tree. The relation between S_i and QS_2 can be verified using the S_i-specific reduced hash tree, which consists of data necessary to reconstruct the path from the leave S_i to the root node $R = h(\cdots h(S_i) \cdots)$, as explained in [PaBo99].

By combining the ideas from above, one obtains the IQ time stamps, consisting of the triple (QS_1, S_i, QS_2), as shown in Fig. 4.

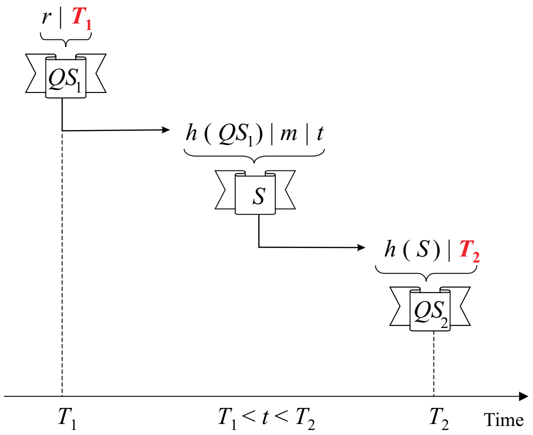

Fig. 2. Relative temporal order induced by $h()$

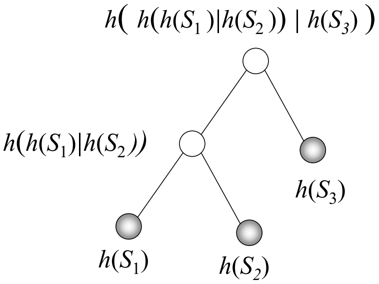

Fig. 3. Hash tree for batch signature with three nodes

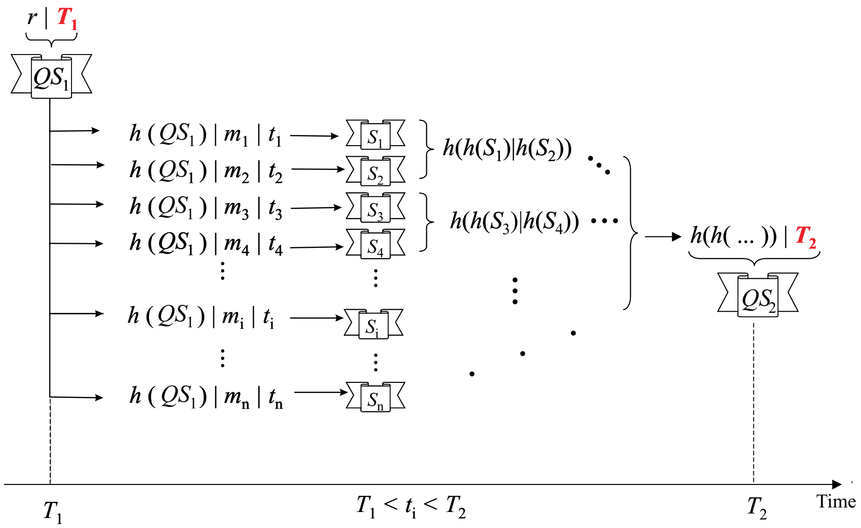

Fig. 4. Construction of interval-qualified time stamps

Theorem 1. *Let $QS_1 = \sigma(h(r)|T_1, Q)$ be a qualified time stamp, $S_i = \sigma(h(QS_1)|m_i|\tilde{t}_i, N)$ be a time stamp and $QS_2 = \sigma(h(\cdots h(S_i)\cdots)|T_2, Q)$ be a qualified time stamp which is constructed as shown in Fig. 4, then $T_1 < t < T_2$, where t is the creation time of S_i.*

Proof: $T_1 < t$ is shown in Proposition 2. That $t < T_2$ can be seen using the same argument for each application of $h()$ in the construction of the hash tree. □

As depicted in Fig. 5, a typical IQ-timestamping system consists of *Clients*, an *Inhouse Timestamping Server* (ITS) and a *Cryptographic Service Provider* (CSP) and operates in the following steps:

1. The ITS requests a qualified time stamp QS_1 from the CSP.
2. The ITS issues an arbitrary number of time stamps S_i to the Clients, where each time stamp S_i includes the hash value of QS_1.
3. Finally the ITS builds a hash tree from the time stamps S_i, as shown in Fig. 4, and obtains a qualified time stamp QS_2 for the root of this hash tree.

4 Conclusion

In this work it was shown that it is possible to equip non-qualified signatures and time stamps with similar features as qualified ones. We believe that there

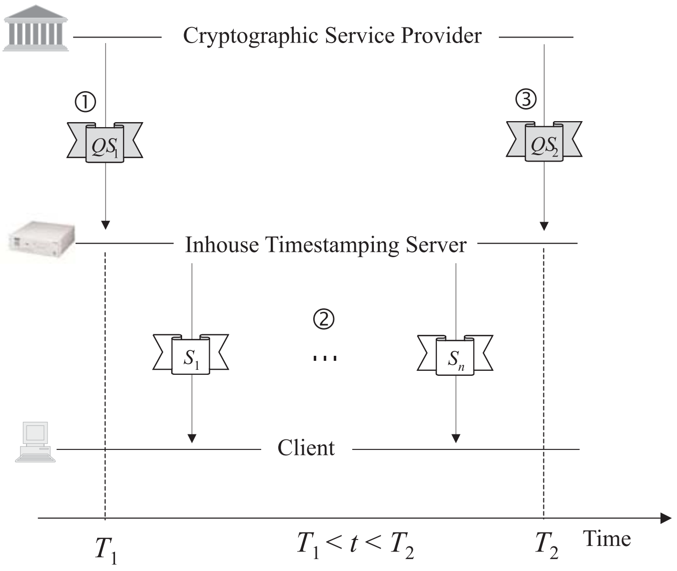

Fig. 5. IQ-timestamping system

are many application scenarios in which costly qualified electronic signatures and time stamps can be replaced by empowered signatures and IQ time stamps without a significant loss in quality. Hence, the simple ideas presented here may lead to more cost efficient solutions for electronic signatures and time stamps.

5 Acknowledgement

I would like to thank Ragna Tern and Volker Zeuner for fruitful discussions and the anonymous referees for valuable suggestions.

References

[BGB] *German Civil Code – Bürgerliches Gesetzbuch*, inofficial translation at http://www.hull.ac.uk/php/lastcb/bgbengl.htm

[BLLV98] Buldas, A.; Laud, P., Lipmaa, H., Villemson, J.: *Time-stamping with Binary Linking Schemes*, in Advances in Cryptology – CRYPTO '98, LNCS 1462, Springer-Verlag, 1998, pages 486-501

[EC/1999/93] *Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures*, via http://europa.eu.int/eur-lex/pri/en/oj/dat/2000/l_013/l_01320000119en00120020.pdf

[HüKn03] Hühnlein, D.; Knosowski, Y.: *Aspects of the automated generation of qualified electronic signatures*, in German, in Proceedings of DACH 2003, IT-Verlag, 2003, ISBN 3-00-010941-2, pages 293-307, via http://www.secunet.de/download/fachartikel/dach2003_aspekte-der-massensignatur.pdf

[HaSt90] Haber, S.; Stornetta, W.S.: *How to time-stamp a digital document*, in A. J. Menezes and S. A. Vanstone, editors, Advances in Cryptology – CRYPTO 90, volume 537 of Lecture Notes in Computer Science, pages 437 - 455. Springer-Verlag, 1991

[Lipm99] Lipmaa, H.: *Secure and efficient time stamping systems*, PhD-thesis at the University of Tartu, Estonia, 1999, via http://www.tcs.hut.fi/-helger/papers/thesis/thesis.pdf

[Merk80] Merkle, R.: *Protocols for Public Key Cryptosystems*, Proceedings of the 1980 IEEE Symposium on Security and Privacy (Oakland, CA, USA, April 1980), pages 122–134

[PaBo99] Pavlovski C.; Boyd C.: *Efficient Batch Signature Generation using Tree Structures*, International Workshop on Cryptographic Techniques and E-Commerce, CrypTEC'99, City University of Hong Kong Press, pages 70–77, via http://sky.fit.qut.edu.au/ boydc/papers/treefinal.ps

[RFC3161] Adams, C.; Cain, P.; Pinkas, D.: *Internet X.509 Public Key Infrastructure - Time Stamp Protocol (TSP)*, RFC 3161, via http://www.ietf.org

[SigG] *Law Governing Framework Conditions for Electronic Signatures and Amending Other Regulations – Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften*, 16.05.2001, BGBl. 2001 Part I Nr. 22, page 876 ff, inofficial translation via http://www.iid.de/iukdg/gesetz/Signaturg_engl.pdf

[SigV] *Digital Signature Ordinance – Verordnung zur elektronischen Signatur*, 16.11.2001 BGBl. 2001 Part I Nr. 59, page 3074 ff, inofficial translation via http://www.iid.de/iukdg/gesetz/SigV161101-engl.pdf