**Journal of Theoretical and Applied Electronic Commerce Research**
ISSN 0718–1876 Electronic Version
VOL 4 / ISSUE 3 / DECEMBER 2009 / 72-79
© 2009 Universidad de Talca - Chile

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762009000300007

# Securing Electronic Customer-Signatures in Legally Binding Business Processes: A Case Study from the Insurance Industry

**Vincent Wolff-Marting[1], André Köhler[2], and Volker Gruhn[3]**

University of Leipzig, Chair of Applied Telematics and e-Business, Department of Computer Science
[1] wolff-marting@ebus.informatik.uni-leipzig.de, [2] koehler@ebus.informatik.uni-leipzig.de,
[3] gruhn@ebus.informatik.uni-leipzig.de

Received 12 October 2007; received in revised form 6 October 2009; accepted 30 October 2009

**Abstract**

On the way to a completely electronic workflow, it is necessary to include customer signatures. Legislation in many countries treats electronic signatures similar to handwritten ones. Both are accepted for various purposes such as for finalization of documents, acknowledgement of the document's contents as well as conclusion of agreements. Most important, electronic signatures are accepted as proof of those actions. But customers today often lack knowledge or means to issue them. In this study a business process is described that will produce reliable signatures without the need of previous knowledge or devices on customer side. A threat model for a generic process is described and countermeasures including cryptography, biometric features, tamper-resistant devices, timestamps, signature databases, and others are discussed.

**Key words:** Electronic Signature, Biometrics, Insurance, Case Study, Electronic Workflow

**Journal of Theoretical and Applied Electronic Commerce Research**
ISSN 0718–1876 Electronic Version
VOL 4 / ISSUE 3 / DECEMBER 2009 / 72-79
© 2009 Universidad de Talca - Chile

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762009000300007

# 1 Introduction

Electronic workflows often start with the digitalization of a paper form that has been completed at the point of service. Sometimes the paper forms are generated with the salesman's notebook at the point of service, and are subsequently printed, signed, and mailed to the insurance company only to become digitized again. The original application is destroyed afterwards, while a microfilm or a low-resolution-scan is kept as proof. Depending on the character of the form, the customer's signature might be mandatory by law or desirable to prevent legal proceedings later on. Electronic signatures can substitute handwritten ones [6], [7], [24], [25], but currently most customers lack means such as a cryptographic key or skills to issue appropriate electronic signatures [19].

Some commercial signature pads capture biometric features of handwritten signatures and try to use them instead of cryptographic keys. Biometric features, such as facial human characteristics, fingerprints, or handwritten signatures, are being used for various security-related purposes. It is fairly agreed that such features can provide reliable means for the identification of a human being as long as they are measured directly from the person in question [13], [22]. Trying to enhance security of electronic signatures by the integration of biometric data seems questionable, as these data cannot be considered secret [13]. It is especially difficult to prove that a given digitized handwritten signature belongs to a specific document.

Customer devices, like smart cards or specially prepared mobile phones, are readily available for electronic signing. However, even if potential users are provided with the required equipment, it cannot be taken for granted that they actually adopt it [21]. There still is a cultural predominance of handwritten signatures as well as a special interest that authentication mechanisms based on biometrics receive from business. In this paper, it is described how electronic and handwritten signatures can be combined in a process to ensure a reliable business transaction without the need of previous knowledge or devices on the customer side. A verifiable link between handwritten signature and electronic document will be provided. That process will not reach the same degree of soundness that can be archived with special customer devices, but it will provide a robust solution for cases where such devices are not desirable. To verify the effectiveness of the proposed process, a threat model will be developed. It will be explained in section 4.1 that signatures resulting from the process described meet the requirements for a "reliable" electronic signature as defined in art. 6 of [25] and for an "advanced" electronic signature as defined in art. 2 of [7]. There are – depending on local legislation – some legal transactions which explicitly require further features (e.g., the "qualified signature" in Germany) or exclude electronic signatures at all. However, for any other transaction, these signatures will be suitable.

This paper is organized as follows: After an overview of the related work in section 2, a sample business process is presented in section 3. A set of mechanisms to prevent a successful attack is described and analyzed in section 4, and it is specified how individual measures can work together and how they are flanking the process. Eventually, in section 5, the results are summed up.

# 2 Related Work

Signatures are a crucial condition for a large class of business transactions. They can serve different purposes such as finalization of a document and acknowledgement of its content as well as conclusion of an agreement. Furthermore signatures constitute a permanent proof of those actions. Legislation (for example, [6], [7], [24], and [25]) accepts electronic signatures to fulfill those purposes under the certain conditions: There needs to be an unambiguous link between the electronic signature and the signer. The means required to create the signature need to be under the sole control of the signer. Any subsequent alterations to the signature or the signed data need to be detectable [6], [7], [25]. Public-key-encryption [11] can satisfy most requirements, but implementations need to guaranty the "sole control of the signer", which can be described as an authentication requirement [22]. It can be met by different technical approaches and there is an ongoing discussion about how reliable technologies can be tailored for the mass-market. To provide "sole control" of the signer, the approaches either rely on a unique device that has been issued to the signer, or they measure biometric features of the signer. The reminder of this section provides a brief overview over research on the different approaches.

Regarding unique devices, solutions based on smart cards [18] can be considered as mature from a technical point of view. More and more countries are equipping identity cards with smart cards capable of issuing signatures. Fritsch at al. [12] proposed the implementation of signing components to mobile phones to increase the penetration of the market, especially concerning non-technically oriented people. The economic aspects of this idea have been analyzed by Rossnagel and Royer [20]. This idea could certainly solve many challenges discussed in this study. Mobile electronic signatures are offered, for example, by service providers in the Scandinavian and Baltic countries as well as in Turkey (e.g., smarttrust, BITĖ Group, turktrust). Broderick et al. [5] summarized the benefits, expectations, hopes, and fears related to the use of electronic signatures.

Biometric features as natural means of authentication, their transformation to and verification by computer systems have been studied extensively by various researchers. Gasson et al. [13] gave an interesting survey of existing

**Journal of Theoretical and Applied Electronic Commerce Research**
ISSN 0718–1876 Electronic Version
VOL 4 / ISSUE 3 / DECEMBER 2009 / 72-79
© 2009 Universidad de Talca - Chile
This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762009000300007

identification schemes, practical applications, and techniques. They strongly doubt the usefulness of biometric samples as part of electronic signatures. Other works focus on the biometric features of signatures and describe how those features can be sampled by signature pads or scanners: Papers on accelerometry [14], hidden markov models in graphometric features [15], stroke direction coding [16], and graphology [17] provide background information on automated verification of handwritten signatures. Tistarelli et al. [23] as well as Wessels and Omlin [27] have examined further techniques to separate genuine signatures from forgeries.

It can be concluded that with mobile devices and smart cards issued as identity cards two approaches with a growing market share exist, which are capable of rendering handwritten signatures obsolete. Our approach has been developed as an alternative for situations where those techniques are either not available or not accepted by the users. Literature regarding handwritten signatures focuses on techniques to distinguish forgeries from genuine signatures. Our approach also ensures that the signature was given in a certain context and with a specific intention.

# 3 The Case of Insurance Application: A Process Model

The process analyzed in this study is the insurance application process that can be mapped to the individual processes of most insurance companies in continental Europe and countries with an analogous legal tradition. The prevalent semi-electronic process is based on paper forms that are required by legislation or desirable as a proof. Usually the paper forms are digitized or microfilmed and the original copy is destroyed afterwards. The process analyzed here will substitute electronic documents for paper forms. This is supposed to accelerate the application process and compared be conducive to its soundness. The process is generally applicable whenever an application form is filled out by the customer in the presence of a salesperson or representative.

In the process (as outlined in figure 1), an application form is generated and completed electronically by using the salespersons notebook. It will be signed electronically and additional safety mechanisms that are discussed in the following section are applied. Afterwards it is sent to a sales organization, which extracts relevant data and forwards it to the insurance company. There are many different sales channels for insurance products of which some include one or more intermediate sales organizations while others omit that chain link. In this example, one organization is included, and little changes are required to adjust the model to different distribution types. This study does not cover direct marketing through Internet or other distribution types omitting the sales representative. His contribution is mandatory since he will have to provide hard- and software to the process that the customer cannot be expected to own.

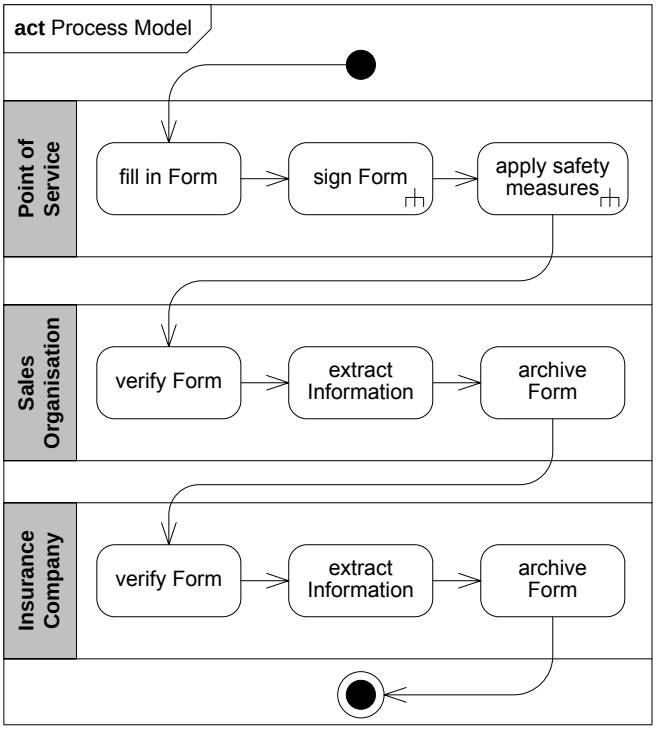


Figure 1: Process Model as an UML Activity Diagram

An insurance application form contains information about the insurant, the property or person insured, and the risks covered by the insurance. The application is expected to bear a signature of the customer. Sometimes there are special clauses, for example, concerning data protection, cancellation, or rescission that have to be signed

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762009000300007

separately. Usually a duplicate of that form will remain with the customer; additional duplicates might remain with the representative and the sales organization.

# 4 Protecting the Electronically Signed Documents against Offences

On the completion of an application form, some kind of finalization is expected. Typically, this is done by a handwritten signature at the end of the document. Electronic signatures can qualify as equivalent in the electronic world, under certain conditions. A generic legal definition of electronic signature is “data in electronic form in, affixed to or logically associated with, a data message, which may be used to identify the signer in relation to the data message and to indicate the signer’s approval of the information contained in the data message” [25]. This leaves a wide space for technical solutions.

## 4.1 Biometrics in Electronic Signatures

From an appropriate substitution for a handwritten signature, most legislation requires additional properties: the link between the signature and the person needs to be unambiguous, the means required to create the signature need to be under the sole control of the signer, and any subsequent alterations to the signature or the signed data need to be detectable [6], [7], [25]. A technical straightforward way to fulfill these requirements is via asymmetric algorithms implemented in smartcards [18]. However, when the customer cannot be expected to own a suitable device, an alternative mechanism will be required. Nevertheless, the alternative solution will be expected to render subsequent changes to the document traceable and to serve the authentication of the customer. Repudiation should be at least as difficult for the signer as it is with handwritten signatures.

The biometric data of the handwritten signature comprise a factor that promises to satisfy these requirements: biometric characteristics are intrinsically tied to an individual human. They can hardly be stolen or eavesdropped, as long as they are verified directly after being sampled from a living person [13]. Nevertheless, if they are sampled, digitized, and transferred, they are no longer reliable. The receiver cannot prove the time or genuine purpose of the measuring [26]. Therefore, the sole attachment of biometric data to a document will not prove much. It is rather important to install further protection techniques.

First of all, the biometric data has to be protected against unauthorized reading. They might contain personal details about the customer, as his state of health etc. Furthermore, raw (i.e., unencrypted) data might be misused to counterfeit another document. The legitimate use of that data is restricted to the validation of the signers’ identity. Validating biometric data will require at least one valid reference signature and expertise about signatures – be it the artificial knowledge of a software exerciser [17] or the natural knowledge of a forensic appraiser. Such a validation will only be needed in case of dispute. On the other hand, it should be possible to test the consistency, i.e., to detect subsequent changes of the signed document, without decryption of the biometric data since every legitimate holder of a document copy may want to perform that test anytime. Therefore, it might be useful to apply different cryptographic keys or even techniques for the protection of the biometric data and the conservation of the document’s integrity. The private key for the decryption of the biometric data ($K_B^{Private}$) needs to be generated and stored at a protected and trusted site. Depending on local legislation and accepted customs, a civil law notary or someone alike will qualify as trusted third party. The encryption of the biometric data can then be done with the corresponding public key ($K_B^{Public}$), which needs no special protection or treatment.

It seems to be inevitable to keep the biometric data unprotected at the central memory of the computer during the process for at least some time. Whereas this is not the ideal case, it cannot be avoided when using commercially available products.

## 4.2 Countersignature of a Representative

For the reasons stated above, neither the conservation of the electronic document’s integrity nor the link between biometric data and document can be guaranteed by means under the sole control of the customer. With some products, it is tried to solve that dilemma by embedding cryptographic keys within the biometric signature software. It has been demonstrated before that it is hardly possible to protect global secrets in a user device. The DVD copy protection system, Pay-TV-Systems, and some North American local traffic payment systems failed since they relied on global secrets [22], so did more recently the Blu-Ray and HD DVD copy protection system AACS [10].

Alternatively, each sales representative and intermediary can be equipped with a personal, private key ($K_R^{Private}$) used to sign the application form. Thereby, the origin of every form can be tracked. If different versions of an application are circulating containing different content, precisely one person has countersigned each version. He can be interrogated and called to account, if necessary. An (assumed) attacker cannot hide in an anonymous crowd of people who could have done it. Table 1 provides an overview of the keys involved in the whole process.

**Journal of Theoretical and Applied Electronic Commerce Research**
ISSN 0718–1876 Electronic Version
VOL 4 / ISSUE 3 / DECEMBER 2009 / 72-79
© 2009 Universidad de Talca - Chile
This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762009000300007

Table 1: Features of the cryptographic keys

| | Signing/Encryption | Verification/Decryption |
|---|---|---|
| Biometric Data | *public key for encryption:* $K_B^{Public}$ | *private key for decryption:* $K_B^{Private}$ |
| Countersignature | *private key for signing:* $K_R^{Private}$ | *public key for verification:* $K_R^{Public}$ |

Figure 2 illustrates the integration into the process: When the form is signed, the handwritten signature is sampled, and a set of biometric data is derived. That data is encrypted with a public key $K_B^{Public}$, as explained in the previous section. The encrypted cyphertext will then be attached to the document, and both are electronically signed using the representative's private key $k_R^{Private}$. As an option, the signed document can be time stamped afterwards. This measure will be explained in the next section.

The private keys have to be generated and distributed in a way guaranteeing that no one but the legitimate key holder gets a copy [8]. Whoever verifies the integrity of an application form needs the public key of the representative. It can be distributed by a public key infrastructure (PKI) [11]. Concerning public key infrastructures, national as well as international laws and recommendations exist [7], [25]. The infrastructure can be provided by an insurance company, or it can be provided by a third party as well. In some legislation, different compliance levels for a PKI are layed out implicating different legal effects of the resulting signatures. Which level will be suitable for a given company cannot be discussed in this document because of its limited scope, but, generally, the reduced risk of loss due to a fake signature should balance the expense of the infrastructure.

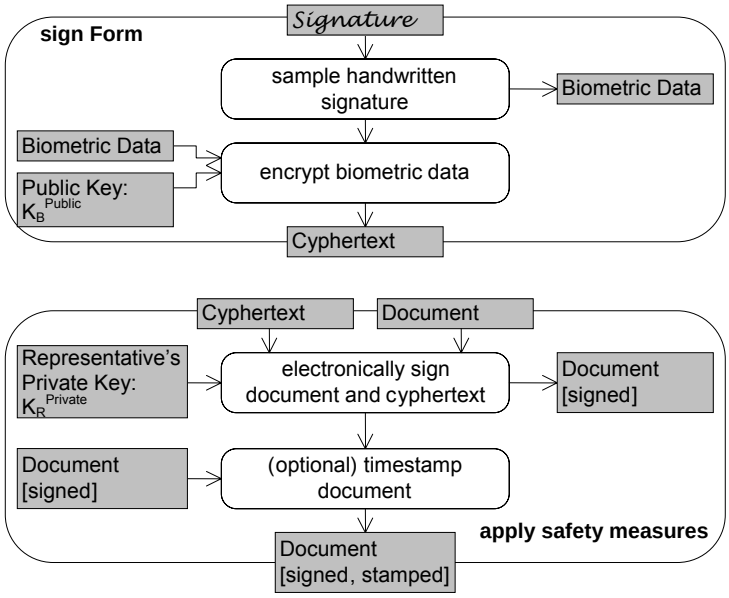


Figure 2: Refinements of the Steps "sign Form" and "apply safety measures"

Disadvantageous of the countersignature is that the liability is passed on to the representative [3]. If fake signatures appear, he will be suspected first. To minimize that risk, state-of-the-art technology (i.e., what qualifies as "secure-signature-creation device" according to the community framework for electronic signatures [7], as, for example, smartcards with a secure smart card reader) should be used, and the implementations have to be reviewed diligently.

The actual signing of the application and the biometric data should be conducted in the protected environment of the tamper-resistant device. The representative has to authenticate himself first. If he fails to (e.g., if he enters a wrong PIN three consecutive times), the device can disable itself permanently or for a fixed time span, and the process will be cancelled. Such a restrictive approach might be deprecated by some representatives, as they might lose a lucrative customer in case they fail to authenticate by accident. They might improve tactics to circumvent that danger – eventually by writing their PIN on the device – and thereby ruin the effort to secure the process [11]. To prevent annoyance of customer and representative, the form might instead be signed using a temporary key. In this case, the representative would have to approve the form with a valid signature later. The tamper-resistant device can verify the integrity of the temporary signature before appending the new one. This way the delayed signature does not comprise additional threat to the process.

**Journal of Theoretical and Applied Electronic Commerce Research**
ISSN 0718–1876 Electronic Version
VOL 4 / ISSUE 3 / DECEMBER 2009 / 72-79
© 2009 Universidad de Talca - Chile
This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762009000300007

### 4.3 Timestamp

Some products claim to gain security by embedding timestamps into the signatures. This section shall explain the mode of operation and impact of that feature. A timestamp is a string of the current time and date appended to an electronic document. It is important whenever the chronological sequence of a process shall be traceable.

There are different ways of timestamping an application form. The least secure way is to use the internal clock of a computer. Any attacker can change it at will [11]. A timestamp from the sampling device would be more secure. This timestamp is regularly encrypted together with the biometric data, but it should rather be appended as plain text to the yet unsigned application form. Thereby, it stays readable to whom it may concern while being protected by the signature. Since this has to be done by the computer, there is some risk of intervention by an attacker. The most secure way would be a timestamp issued by the tamper-resistant device, but commercially available products do not support this option yet. Finally, an external timestamp service provider could act as a trusted third party. A communication link from the point of service to the provider is required for this solution adding an additional point of failure.

A timestamp set during signature-creation renders additional plausibility checks possible. A timestamp reveals application forms antedated with the intent to defraud. Antedating insurance applications has been a way to obtain insurance surreptitiously for damages that have already occurred. Such a defraud will become less promising as the processing time of an electronic form is significantly faster compared to a paper form. Therefore, an application form out of date will be suspicious with or without valid timestamps. External timestamps and timestamps from tamper-resistant sampling devices also strengthen the link between a document and the biometric data. A considerable old timestamp can be a sign of a reused signature from an older application form. In such a case, the timestamp can help identify the original application bearing the misused signature. If many signatures are generated within a very short period of time or if they are dated at unusual times, they are possibly set by the representative without knowledge and consent of the potential customer, and further investigation might be useful. If multiple signatures are set at exactly the same time, then it either is a huge technical fault or defraud. It depends on process-specific factors whether plausibility checks like these are appropriate; therefore, it has been marked as optional in figure 2.

### 4.4 Verification of the Document

Upon receipt, the sales organization will verify the signature with the public key of the representative. It should be confirmed that all required signatures are in place. The authenticity of biometric features cannot be verified at this point. The biometric data can only be verified against another sample of that data from the same person. If biometrics is used for frequent authentication of a relatively closed user group, then reference samples are usually stored in a database. Use cases like banks inspecting signatures on cheques and remittance slips or access control systems need to rely on such databases. Insurance companies, on the contrary, do not get new documents signed by existing customers on a regular base. It has to be assumed that the forms are signed by applicants whose signature is unknown to the company. Even if the applicant is a regular customer, existing signatures can be several years old. Natural variances of the signature increase the risk of false rejection.

In section 4.1, the risk adherent to the verification of biometric data has been shown: The data have to be available unencrypted or as a verification-template and can, at least theoretically, be misused. In this context, a signature database bears a risk. The risk can be minimized by restrictive access control, detailed documentation of database requests, and similar mechanisms. Nevertheless, as long as the database can be used for few applications with a high false rejection rate, it does not seem efficient to invest into either database or safety mechanisms.

Only in case of controversy about the insurance application, the biometric data need to be verified. The required keys $K_B^{Private}$ should be under the sole control of a trusted party, as described in section 4.1. Neither insurance company nor sales organization should have direct access to that key. Any contested signature has to be decrypted by the third party and forwarded to a forensic appraiser or a software exerciser.

Most of the time, a verification of the countersignature and – if provided – timestamps will be sufficient. The public keys of the representatives are usually provided by a central server (see section 4.2). This server might be part of the insurance company; it might be operated by the sales organization or an independent third party as well. Even multiple servers at different locations can be an option.

In case a signature cannot be verified, the reason for the failure needs to be investigated. Possible reasons are transmission errors, accidental transmission of an unfinished application, or an attempt to defraud. Depending on the assumed reason, appropriate actions must be taken, for example, asking the customer to sign the application again or proposing a contract based on the invalid application.

### 4.5 Information Extraction

If the application is signed validly, then the sales organization can extract all data needed for further processing. It has to be emphasized that the organization thereby relies only on signed and verified data; no unsigned secondary

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762009000300007

data stream shall exist. To simplify the integration into existing workflows, some products do not use the signed document but an unsigned data stream for further processing. The data to be signed is captured with a special printer driver, somehow being an image of the real document. The signed data is not structured, which means that it can be difficult to extract a certain piece of information from such a document. Structured documents in contrast follow a defined layout and provide easy access to the content.

It should be avoided to route the same information over two parallel streams, because it bears the danger of inconsistency. As the signed but unstructured stream cannot be analyzed automatically, any discrepancy can remain hidden for a long time. To prevent that problem, solely signed data should be used throughout the process. In principle, any electronic data format can be used, since signature algorithms can process any bit string regardless of its meaning. Some formats, as the Portable Document Format (PDF) [1] or the Extensible Markup Language (XML) [4], are designed to hold structured data and electronic signatures and even biometric data [2].

With structured documents, it is possible to define which part of the document is covered by a signature [1]. This is especially useful for documents containing more than one signature. Later, it can be analyzed automatically whether the required signatures are present at the right place. With non-structured documents, automated processes can only verify if there are signatures at all. Not even an optical review can verify that everything is in place, since it might be deceived by a picture of a valid signature.

# 5 Remaining Issues and Conclusions

The process described addresses most threats associated with the insurance application process. Especially the countersignature of the representative minimizes the possibilities to issue manipulated application forms. All kinds of changes to the form need to be finalized through a signature of the representative. The representative most likely will not consciously sign a counterfeited document. Counterfeiting the representative's signature will be almost impossible as long as the underlying cryptographic algorithms are reliable and soundly implemented. Pictures used to feign signatures will be detected as each signature within the structured document will be explicitly verified.

It is worth mentioning that the use of a signature database as it is mandatory in the banking business will not at all improve the security in this context. On the contrary, the data in such a database might be misused. Therefore, it has to be advised against it. The biggest gain in protection is provided by the countersignature of the representative. That measure is still advantageous, even if the representative himself is an adversary, because it simplifies penalization.

Attacks utilizing real biometric data cannot be eliminated; customers can always sample their own handwritten signature, and it might be possible to obtain handwritten signatures in blank by some confidence trick. For example, it will be possible for an attacker to tell the victim that he needs to sign a receipt (e. g. for a parcel) while actually the signature is sampled for a contract. Such confidence tricks are not much different from what is possible with the traditional paper based process. These attacks are beyond the control of the insurance company and cannot be prohibited completely. However as the company will eventually send an insurance policy to the victim, the chance that altered or completely fabricated application forms will stay unnoticed are considerably low. Consequently, a malicious representative bears a high risk of getting caught.

Purposeful or accidental malfunctions of the verification system remain a challenge. The threat by malicious soft- or hardware suppliers, however, is not limited to signature verification systems. Recent research on aspects of this challenge has been made by Wheeler [28], for example. Certification (such as Common Criteria [9]) might add some creditability to a verification system. Fidelity bonds can cover remaining dangers.

Altogether, it seems realistic to set up a process that generates documents electronically signed by customers who need no special devices or knowledge. Compared to conventional semi-electronic processes that destroy the paper forms after archiving a digitized copy, the process provides a noticeable increase in security. The process can be set up using commercially available components. Admittedly, they have to be configured carefully. The example focuses on the insurance application process. The results can probably be transferred to other scenarios as well, as long as some representative or salesperson is involved at the point of service. It has been explained in this paper that the signing process is compatible to the legal requirements of the European Parliament [7] and UNCITRAL [25]. It has also been reviewed and found compatible with German legislation. It remains to be determined whether the process described here meets the demands of a given local legislation regarding signatures.

This paper is available online at
www.jtaer.com
DOI: 10.4067/S0718-18762009000300007

# References

[1] Adobe Systems Incorporated. (2007, November) PDF reference version 1.6, Fifth Edition. [Online]. Available: http://partners.adobe.com/public/developer/en/pdf/PDFReference16.pdf.
[2] T. Aichelen. (2003, August) XML common biometric format. [Online]. Available: http://www.oasis-open.org/specs/index.php.
[3] N. Bohm, I. Brown, and B. Gladman, Electronic commerce: Who carries the risk of fraud, Journal of Information Law and Technology, vol. 2000, no. 3, 2000.
[4] T. Bray, J. Paoli, C. M. Sperberg-McQueen, E. Maler, F. Yergeau, and J. Cowan. (2006, September) Extensible Markup Language (XML) 1.1, second edition. [Online]. Available: http://www.w3.org/TR/xml11/.
[5] M. A. Broderick, V. R. Gibson, and P. Tarasewich, Electronic signatures: They're legal, now what? Internet research: Electronic networking applications and policy, vol. 11, no. 5, pp. 423–434, 2001.
[6] 106th United States Congress. (2000, June) Electronic signatures in global and national commerce act. [Online]. Available: http://www.gpo.gov/fdsys/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf.
[7] The European Parliament and the Council of the European Union, Directive 1999/93/EC of the european parliament and of the council of 13 December 1999 on a community framework for electronic signatures, Official Journal of the European Communities, vol. L 12, pp. 12–20, 2000.
[8] Federal Office for Information Security (Ed.): IT Baseline Protection Manual, Cologne: Bundesanzeiger Verlag, 2004.
[9] Federal Office for Information Security and TÜV Informationstechnik (Eds.): Common Criteria Protection Profile for Biometric Verification Mechanisms, Bonn, Essen, December 2004.
[10] E. Felten. (2007, January) AACS decryption code release. [Online]. Available: http://www.freedom-to-tinker.com/?p=1104.
[11] N. Ferguson, and B. Schneier, Practical Cryptography. Indianapolis: Wiley Publishing, 2003.
[12] L. Fritsch, J. Ranke, and H. Rossnagel, Qualified mobile electronic signatures: Possible, but worth a try?, in Information Security Solutions Europe (ISSE) Conference, Vienna, 2003.
[13] M. Gasson, M. Meints, and K. Warwick. (Eds.) (2005, July) A Study on PKI and biometrics, [Online]. Available: http://www.fidis.net/fileadmin/fidis/deliverables/fidis-wp3-del3.2.study_on_PKI_and_biometrics.pdf.
[14] N. M. Herbst, and C.-N Liu, Automatic signature verification based on accelerometry, IBM Journal of Research and Development, vol. 21, no. 3, pp. 245–253, 1977.
[15] E. J. R. Justino, A. E. Yacoubi, F. Bortolozzi, and R. Sabourin, An off-line signature verification system using HMM and graphometric features, in Fourth IAPR International Workshop on Document Analysis Systems (DAS), Rio de Janeiro, 2000, pp. 211–222.
[16] R. S. Kashi, W. Turin, and W. L. Nelson, On-line handwritten signature verification using stroke direction coding, Optical Engineering, vol. 35, pp. 2526–2533, Sep. 1996.
[17] L. Oliveira, E. J. R. Justino, Cinthia Freitas, and R. sabourin, The graphology applied to signature verification, in 12th Conference of the International Graphonomics Society (IGS), Salerno, 2005, pp. 178–182.
[18] W. Rankl, and W. Effing, Smart Card Handbook, 3rd. ed., Chichester: Wiley & Sons, 2004.
[19] H. Rossnagel, and D. Royer, Investing in security solutions - Can qualified electronic signatures be profitable for mobile operators?, in Proceedings of the Eleventh Americas Conference on Information Systems (AMCIS), Omaha, Nebraska, 2005.
[20] H. Rossnagel, and D. Royer, Profitability of mobile qualified electronic signatures, in The Ninth Pacific Asia Conference on Information Systems, Bangkok, 2005.
[21] H. Roßnagel, On diffusion and confusion – Why electronic signatures have failed, in Trust and Privacy in Digital Business, LNCS 4083 (S. Fischer-Hübner et al., Eds.), Heidelberg: Springer, 2006, pp. 71–80.
[22] B. Schneier, Secrets and Lies: Digital Security in a Networked World. New York: John Wiley & Sons, 2004.
[23] M. Tistarelli, J. Bigun, and E. Grosso, Advanced Studies in Biometrics, ser. Lecture Notes in Computer Science. Berlin, Heidelberg: Springer Verlag, no. 3161, 2005.
[24] UNCITRAL, Ed., Model Law on Electronic Commerce with Guide to Enactment. New York: United Nations Publication, 1999.
[25] UNCITRAL, Ed., Model Law on Electronic Signatures. New York, Wien: United Nations Publication, 2002.
[26] U. Waldmann, D. Scheuermann, and C. Eckert, Protected transmission of biometric user authentication data for OncardMatching, in SAC '04: Proceedings of the 2004 ACMSymposium on Applied Computing, New York: ACM Press, 2004, pp. 425–430.
[27] T. Wessels, and C. Omlin, A hybrid system for signature verification, in IEEE-INNS-ENNS International Joint Conference on Neural Networks (IJCNN), vol. 5, 2000, p. 5509, 2000.
[28] D. A. Wheeler, Countering trusting trust through diverse double-compiling, in 21st Annual Computer Security Applications Conference, Tucson, Arizona, 2005.