Improving the Binding of Electronic Signatures to the Signer by Biometric Authentication

Olaf Henniger, Björn Schneider, Bruno Struif, and Ulrich Waldmann

Fraunhofer Institute for Secure Information Technology,
Rheinstr 75, 64295 Darmstadt, Germany
{henniger, struif, waldmann}@sit.fraunhofer.de

Abstract. Due to the fact that the biometric characteristics of a person are bound to that person, biometric methods deployed for signer authentication have the potential of improving the binding of electronic signatures to persons. If there is evidence that a biometric method was used for signer authentication, and if the level of security of this method is sufficiently high, then the receiver of a signed document can trust that the signature creation was indeed initiated by the legitimate holder of the private signature key. To achieve this goal, an approach to provide evidence of the use of biometric signer authentication has been developed. The approach has been implemented in a prototype electronic signature creation system with fingerprint verification.

1 Motivation

Legal regulations permit biometric methods to be deployed for signer authentication also in products for "qualified" electronic signatures (which have the same legal effects as handwritten signatures on paper), provided that the strength of function of the biometric methods and their resistance against penetration attacks are certified to be sufficiently high. Biometric methods are considered more user-friendly than knowledge-based authentication methods because they free the users from the burden of recalling a PIN or password from memory. Moreover, biometric methods can also increase the binding of electronic signatures to persons since the biometric characteristics of a person are bound to that person and cannot easily be presented by others. Knowledge-based signer authentication on the other hand brings along the risk that the PIN or the password are presented by unauthorized persons.

Since biometric characteristics are not always available (e.g., a fingerprint cannot be presented if the finger is injured), biometric user authentication mechanisms must always be accompanied by knowledge-based fallback mechanisms. In order to increase the binding of electronic signatures to persons by deploying biometric methods, the receivers of signed documents need to be informed in a secure way of the signer authentication method (biometric or knowledge-based) that was used at signature creation time. The signer should neither be able to deny it if a biometric method was used, nor to pretend it if a biometric method was not used. If satisfactory evidence is provided that a biometric method was used for signer authentication, and if the strength of function of the biometric method and its resistance against penetration

D. Zhang and A.K. Jain (Eds.): ICB 2006, LNCS 3832, pp. 523 – 530, 2005.

attacks is sufficiently high, the receiver of a signed document can have high confidence that the signature creation was indeed initiated by the legitimate holder of the private signature key.

This paper presents a solution for providing evidence of the deployed signer authentication method. The solution complies with legal regulations on electronic signatures [1–3] and with commonly used formats for electronically signed documents [4]. It does not impede verifying the electronic signatures with the usual programs.

2 System Architecture

In order to prevent the fraudulent use of a smart card with electronic signature creation function (signature card), the user must be authenticated before the signature creation function can be used. User authentication requires the user to present a secret PIN or biometric characteristics. The comparison of the verification data presented by the user with the stored reference data takes place within the smart card (on-card matching).

The authenticity and integrity of the biometric verification data handed over at the card interface must be protected to ensure that these data are captured anew and not fed in by way of bypass or replay attacks (where an impostor, after having stolen or at least temporarily taken possession of a smart card, sends recorded or otherwise acquired biometric data of the legitimate cardholder to the card, evading the regular data capture equipment. The protection of the authenticity and integrity of the biometric verification data is achieved by mutual authentication of both the signature card and the card terminal, the establishment of cryptographic keys, and subsequent application of cryptographic algorithms to the biometric verification data (secure messaging via a trusted channel) [5, 6]. For this purpose, a security module is integrated into the card terminal [7]. To allow flexible handling of this component, the security module is a smart card in plug-in format. Its functionality could also be completely integrated into a tamper-resistant card terminal. However, the advantage of a plug-in card is that it can be easily replaced, e.g. if a public-key certificate is to be renewed.

For establishing the trusted channel between the SMC and the signature card, a hybrid method is used consisting of both an asymmetric and a symmetric cryptographic algorithm. To make the signature creation system useable for multiple signature cards and to solve the cryptographic key distribution problem, the asymmetric cryptographic algorithm (RSA) is used for establishing the trusted channel. The faster symmetric cryptographic algorithm (Triple DES) is then used to allow a fast calculation and verification of secure-messaging objects. Upon successful completion of the card-to-card authentication both cards have available the symmetric session key for cryptographic checksum calculation and the initial value of the send sequence counter, which is used as initial vector for the calculation of cryptographic checksums. Cryptographic checksums are calculated as retail message authentication code (Retail MAC).

Figure 1 shows an example of a system architecture of a signature creation system consisting of a PC with the signature creation application, a card terminal, and a signature card. A fingerprint sensor, the fingerprint feature extraction component as well as the security module card (SMC) are integrated into the tamper-resistant card

terminal to prevent bypass and replay attacks at their interfaces. Furthermore, the card terminal contains a smart-card interaction component that controls the security protocol running between the SMC and the signature card.

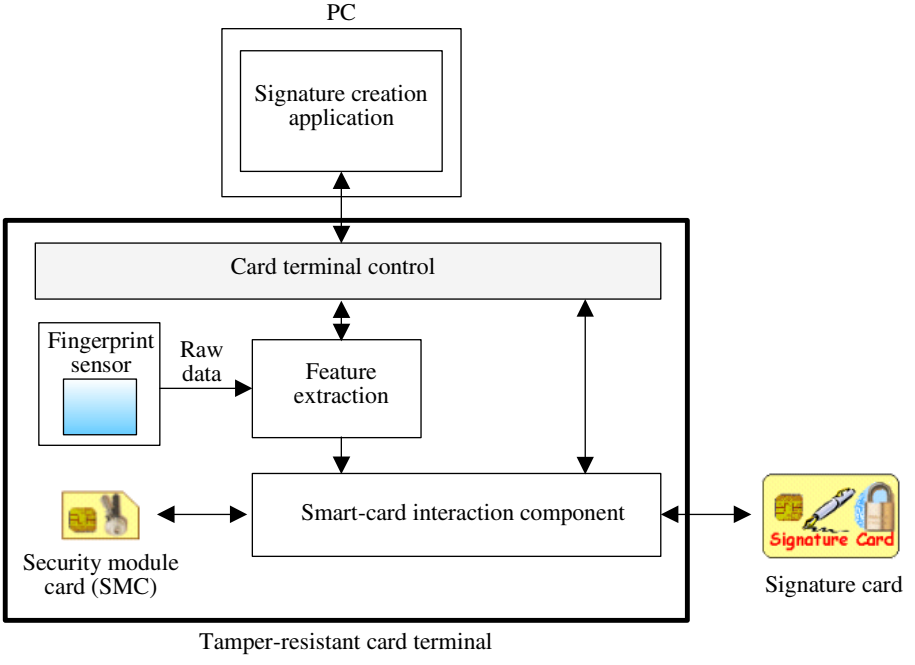

Fig. 1. System architecture of a signature creation system with smart-card interfaces

The signature card is based on a STARCOS SPK 2.4 card of Giesecke & Devrient with a signature creation application certified according to ITSEC E4/high. It has been extended to support minutiae-based fingerprint on-card matching in addition to PIN verification and to provide evidence of the used signer authentication method. The SMC has been implemented on a Java card platform. A prototype of a "Trusted Signature Terminal" [8] serves as a tamper-resistant card terminal.

3 Providing Evidence of the Used Signer Authentication Method

3.1 Different Security Environments for Different Authentication Methods

Each signer authentication method runs in its own security environment on the signature card: The PIN authentication method runs in security environment SE#1, and the fingerprint authentication method in security environment SE#2. The current security environment can be changed by sending a MSE (Manage Security Environment) RESTORE command to the signature card. As soon as the security environment is changed, the local security status, e.g. "Signer authentication successful", is lost.

The applicable signer authentication method depends on the currently selected security environment: It is not possible to carry out biometric authentication in the security environment SE#1 set up for PIN authentication, and it is not possible to carry out PIN authentication in the security environment SE#2 set up for fingerprint authentication.

3.2 Notification of the Used Signer Authentication Method

Only in security environment SE#2, i.e. only after biometric signer authentication, the signature card responds to the command PSO (Perform Security Operation) COMPUTE DS (Digital Signature) with a special signature block that includes, in addition to the signature of the document to be signed, the data objects Control Reference Template (CRT) for Authentication [5] and Biometric Information Template (BIT) [9]. These data objects contain information about the method used for signer authentication.

3.3 Signing the Notification of the Used Signer Authentication Method

The smart-card interaction component in the tamper-resistant card terminal forwards the signature card's PSO COMPUTE DS response within the data field of a PSO VERIFY CC command to the SMC, as it does with any other secure-messaging response from the signature card. Since the SMC receives the information about the method used for signer authentication via the trusted channel, the SMC can trust this information and take on the task of signing the special signature block to confirm it. To achieve this, the functionality of the PSO VERIFY CC command on the SMC is extended as follows:

1. Verify the cryptographic checksum given in the data field.
2. If a signature block with supplementary information about the used signer authentication method is present in the data field, then
   - create a supplementary signature over the signature block by applying the SMC's private key for card authentication PrK.SMC.AUT,
   - store the signature block together with the supplementary signature in a log file.

By signing the supplementary information together with the document signature, the supplementary information is bound to the corresponding signed document. Using the SMC's private key for card authentication PrK.SMC.AUT fulfils the security requirements, as the holder of the signature card cannot control the use of this key. The solution can be considered fraud-resistant because the creation of the supplementary signature is solely under the control of the SMC and cannot be induced from outside. The application range of PrK.SMC.AUT is usually restricted to the INTERNAL AUTHENTICATE command. Its extension to the creation of the supplementary signature must be confirmed by a certification authority responsible for certifying the security of the SMC.

The supplementary signature created by the SMC is appended to the signature block received from the signature card and stored together with it in a log file on the SMC. Afterwards, the smart-card interaction component reads the log file from the

SMC. The log file is selected by a SELECT command and read using READ BINARY commands under the security status "Signature card authentication successful". Then, the signed signature block can be forwarded together with the signed document and the X.509 certificates of both the cardholder's public key for electronic signatures PuK.CH.DS and the SMC's public key for card authentication PuK.SMC.AUT, which are needed for verifying the document signature and the supplementary signature, respectively.

3.4 Format of the Signed Document

The signed document is formatted as a PKCS#7 message [4] of type "signedData" (see Figure 2). This message consists of the signed document ("contentInfo"), the X.509 certificate including the public key of the cardholder for electronic signatures PuK.CH.DS ("certificates"), and the "signerInfo". The "signerInfo" contains

- "authenticatedAttributes": the hash value of the document and the signature creation time,
- "encryptedDigest": the document signature covering the "authenticatedAttributes",
- "unauthenticatedAttributes": optional, informative data that is not signed by the cardholder.

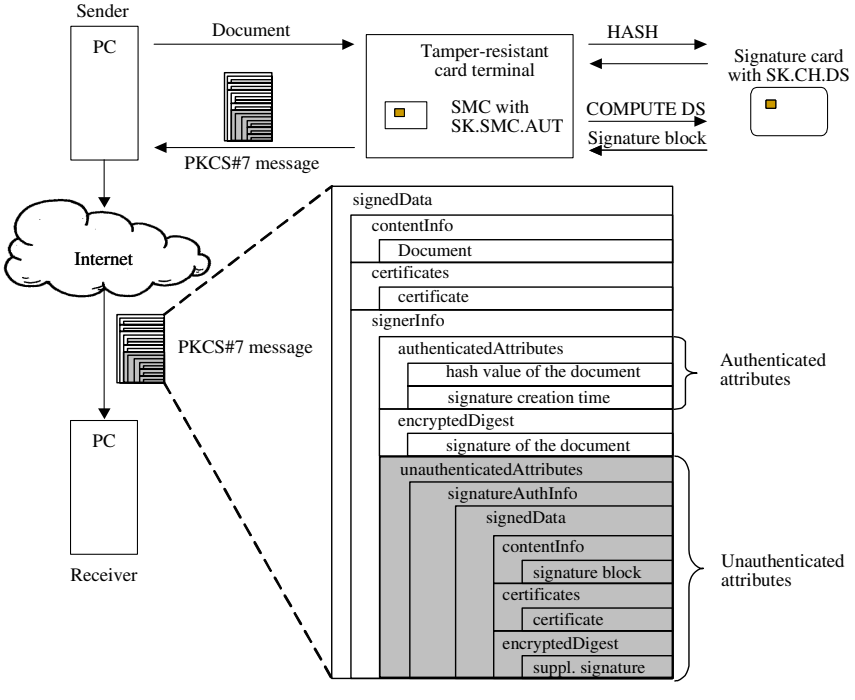

Fig. 2. Informing the document receiver of the signer authentication method

The “unauthenticatedAttributes” include the signature block and the supplementary signature as verifiable evidence that the signer was authenticated by means of a biometric method. The smart-card interaction component formats the notification of the biometric signer authentication mode (“signatureAuthInfo”) like a PKCS#7 message of type “signedData”, consisting of the signature block including the document signature and the supplementary information about the used signer authentication method (“contentInfo”), the X.509 certificate with the SMC’s public key for card authentication PuK.SMC.AUT (“certificates”), and the supplementary signature created using the SMC’s private key for card authentication (“encryptedDigest”). This self-contained and signed PKCS#7 message is integrated into the “unauthenticated-Attributes” block of the original document’s PKCS#7 message.

4 Examining the Evidence of the Signer Authentication Method

Any program that is capable of interpreting PKCS#7 messages, e.g. the e-mail program Outlook under Windows, and that has got the corresponding certificates can verify an electronic signature created as described in the previous sections. However, most signature verification programs offer only a very restricted view of the individual attribute values, actually nothing with regard to the additional attributes. In particular, the programs cannot display the special unauthenticated attributes to indicate the used signer authentication mode. Thus, for interpreting the “unauthenticated-Attributes” an additional program module that provides the following functionality is required:

1. verify the X.509 certificate of PuK.SMC.AUT (for this purpose, the public key of the certification authority signing the certificate, i.e. the CA certificate, is needed),
2. verify the supplementary signature of “encryptedDigest”,
3. in order to prove that the additional information truly belongs to the document, compare the document signature contained in “encryptedDigest” of the overall PKCS#7 message with the document signature of the signature block contained in the “unauthenticatedAttributes”,
4. display the signer authentication mode used by the signer of the document.

After verifying the document signature and the supplementary signature, the receiver of a signed document has to check that the signature attached to the document and the document signature given in the supplementary information about the used signer authentication method are identical. This way, the authenticity and integrity of the document as well as the use of the biometric signer authentication method at signature creation time can be verified.

The additional functionality to indicate the used signer authentication method has been implemented under Windows in form of a plug-in extending the Explorer program. For e-mail files (file extension “.eml”) that contain a PKCS#7 message and therein information about the signer authentication method, this additional information can be retrieved by activating the context menu (right mouse click on the document) and choosing the new menu item “Signer’s authentication info...”. One of two possible notification windows is opened showing information about the signer authentication method used at document signature creation time (see Figure 3). In case a

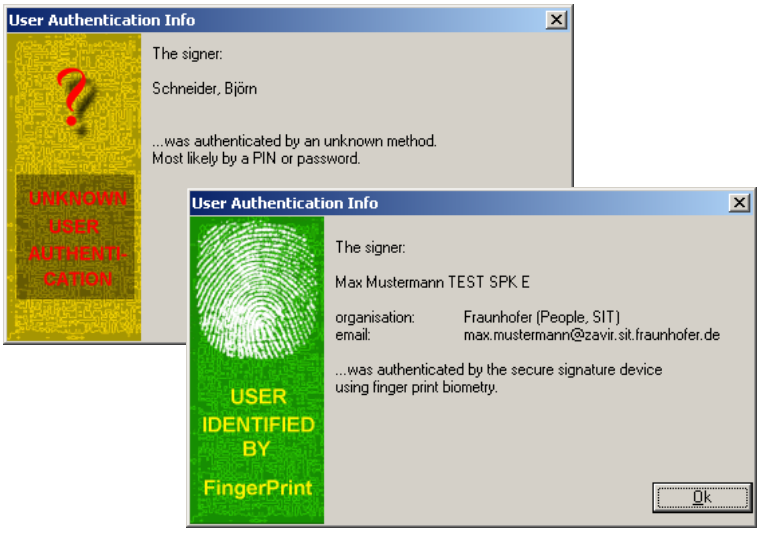

Fig. 3. Pop-up windows "User Authentication Info"

PKCS#7 message is received without supplementary information about the used signer authentication method, knowledge-based signer authentication is assumed by default. In addition to the signer authentication mode some standard information about the signer's certificate is displayed.

5 Summary and Outlook

Since biometric characteristics are bound to a certain person, the binding of electronic signatures to persons can be improved by the deployment of biometric methods for signer authentication. If it is satisfactorily shown that a biometric method was used for signer authentication, and this method's strength of function and resistance against penetration attacks is sufficiently high, then the receiver of a signed document can have high confidence that the electronic signature creation was indeed initiated by the legitimate holder of the signature key.

In this paper, a solution has been presented, which fulfills these requirements in compliance with standardized signature formats. Furthermore, the solution does not interfere with the regular signature verification. Based on the STARCOS SPK 2.4 signature card of Giesecke & Devrient, a prototype of a signature card with finger-print on-card matching as alternative to PIN verification has been developed. The response to signature creation commands indicates whether or not the biometric signer authentication method was used. In order to protect the authenticity of this information, the signature block is signed again. This supplementary signature is created by the SMC, which is integrated into the tamper-resistant terminal. In order that the notification of the signer authentication mode can be attributed to a certain document, the supplementary signature covers also the corresponding document

signature. The SMC has been implemented based on a Java card. The functionality of the card terminal has been implemented in a prototype of a "Trusted Signature Terminal" [8].

The outlined solution offers the chance to make electronic signatures applicable also for high-value business processes by improving the binding of electronic signatures to persons. The approach should be enhanced in the direction that the signature card by itself creates a fraud-resistant information about the used signer authentication method without the SMC being involved. However, such an extension would require substantial changes within the operating system of already existing and certified signature cards.

Acknowledgements

This research was supported by the German Federal Ministry of Education and Research. The authors are grateful to the other members of the project team, in particular to Gisela Meister and Florian Gawlas of Giesecke & Devrient, for fruitful discussions.

References

[1] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for Electronic Signatures
[2] German Signature Act, Fed. Law Gaz. 2001, Part I no. 22, May 2001
[3] German Signature Ordinance, Fed. Law Gaz. 2001, Part I no. 59, Nov. 2001
[4] Public-Key Cryptography Standards (PKCS) #7, Cryptographic Message Syntax Standard v1.5, RSA Laboratories, Bedford, Maine, USA, Nov. 1993
[5] Information technology – Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange. Internat. Standard ISO/IEC 7816-4, 2005
[6] Application Interface for Smart Cards used as Secure Signature Creation Devices, Part 1 – Basic requirements, Version 1 Release 10, CWA 14890-1, March 2004
[7] D. Scheuermann, U. Waldmann: Protected Transmission of Biometric User Authentication Data for On-card Matching. In *Proc. of the ACM Symposium on Applied Computing*, Nikosia, Cyprus, March 2004
[8] O. Henniger, B. Struif, K. Franke, R. Ulrich: Trusted Signature Terminal – A trustworthy signature creation environment. In P. Horster (ed.): *Proc. of the D-A-CH Security Workshop*, Erfurt, Germany, 2003. – In German
[9] Information Technology – Identification Cards – Integrated Circuit Cards – Part 11: Personal Verification through Biometric Methods. Internat. Standard ISO/IEC 7816-11, 2004