Supplemental Biometric User Authentication for Digital-Signature Smart Cards

Olaf Henniger, Ulrich Waldmann

Fraunhofer Institute for Secure Information Technology
Rheinstr. 75
D-64295 Darmstadt, Germany
olaf.henniger@sit.fraunhofer.de
ulrich.waldmann@sit.fraunhofer.de

Abstract: This paper specifies how biometric verification methods can be applied in addition to PIN verification on digital-signature smart cards in compliance with established smart-card standards. After successful PIN verification, multiple digital signatures can be created; each signature creation, however, is preceded by biometric verification.

1 Motivation

Tamper-resistant, personal smart cards are used for the secure storage of private signature keys and as protected environment for the creation of digital signatures [DIN V 66291-1, Pie08, EN 14890-1]. For checking the access rights on the protected functions of a digital-signature smart card, also biometric features of the cardholder can be used in addition, or as alternative, to a secret PIN (personal identification number). The strengths of biometric methods lie in their relative ease of use. If sufficiently resistant against direct and indirect attacks, biometric user authentication methods can strengthen the binding of digital signatures to the legitimate signature-key owner since biometric characteristics are bound to a certain person. For user authentication prior to digital-signature creation, handwritten signatures show particular promise as they have found acceptance for a long time and are regarded as evidence of a deliberate decision of the signer.

In order that a successful verification cannot be feigned to the smart card whose signature-creation function is to be protected, the biometric features should be compared inside the smart card itself. On-card comparison offers the additional advantage that the biometric reference data of the legitimate cardholder never leave the smart card and remain protected against misuse in case the card is tampered with. It would be best if all steps of biometric verification – from biometric data capture over pre-processing, the extraction and comparison of features up to the accept/reject decision – were carried out within the protected smart card. Though prototypes of smart cards with an integrated biometric sensor already exist, we consider only the case that the sensor is off-card and biometric feature data is sent to the smart card for on-card comparison.

In case that a biometric user authentication method shows only a moderate attack resistance, it should be used only in addition (and not as an alternative) to PIN verification [SigV01]. We focus on this case. [TR-03115] suggests that the users must authenticate themselves once by entering their PIN and that afterwards multiple digital signatures can be created, before each of which the users must authenticate themselves by presenting their biometric characteristics. This paper specifies how to realise this in compliance with pertinent smart-card standards [ISO/IEC 7816-4]. This is new ground, not covered yet in digital-signature card specifications [DIN V 66291-1, Pie08, EN 14890-1].

Other aspects, such as how to convey the required format of the biometric probe to the off-card application [ISO/IEC 7816-11] and how to ensure that the biometric probe data handed over at the card interface are captured anew and not fed in by way of bypass or replay attacks [EN 14890-1], are out of scope of this paper because specified elsewhere.

2 Specification of user authentication procedure

2.1 Data objects

The on-card signature-creation application holds the private key needed for the creation of digital signatures. The private key is called PrK.

For user authentication prior to digital-signature creation, the application shall use a PIN consisting of at least six digits [EN 14890-1] and may, in addition to the PIN, also use a biometric reference (BR). PIN and BR are each associated with

- a retry counter indicating the number of remaining allowed verification attempts and
- a security status evaluation counter indicating how often the security status achieved after successful user authentication may be used until re-verification is required.

The initial values of the retry counters $\mathrm{PIN.RC_{start}}$ and $\mathrm{BR.RC_{start}}$ indicate the supported maximum number of verification attempts. $\mathrm{PIN.RC_{start}}$ should typically be 3 [EN 14890-1]. $\mathrm{BR.RC_{start}}$ depends on the chosen biometric method. The initial values of the security status evaluation counters $\mathrm{PIN.SSEC_{start}}$ and $\mathrm{BR.SSEC_{start}}$ should both be 0. Their maximum values $\mathrm{PIN.SSEC_{max}}$ and $\mathrm{BR.SSEC_{max}}$ indicate the supported maximum number of uses of the security status after successful verification. $\mathrm{PIN.SSEC_{max}}$ should be n with $n \geq 1$ or represent "infinity". $\mathrm{BR.SSEC_{max}}$ should be m with $1 \leq m \leq n$.

2.2 Access rules

Each access rule for data objects on the card consists of two parts: an access mode that indicates specific card commands and a security condition that is required to be met in order to get access to the object using that access mode. A security condition is expressed in terms of security statuses that may result from completion of authentication procedures. When trying to access a protected object, the card operating system checks whether the security condition is satisfied. If not, access to the object is denied, and an appropriate error message such as "Security status not satisfied" is returned.

The access rules for PIN, BR, and PrK should be set as described in Table 1 through Table 3. The tables also list actions to be executed when accessing PIN, BR, and PrK.

Table 1 Access rules for PIN

Access mode	Security condition	Actions to be executed
CHANGE REFERENCE DATA or RESET RETRY COUNTER	Application-specific/out of scope (e.g. successful master PIN verification)	− Change PIN and/or − PIN.RC := $PIN.RC_{start}$
VERIFY	ALWAYS	If PIN.RC > 0, then − Decrement PIN.RC − If the value from the command data field matches the PIN, then • PIN verification successful • PIN.RC := $PIN.RC_{start}$ • PIN.SSEC := $PIN.SSEC_{max}$
Other	NEVER	None

Table 2 Access rules for BR

Access mode	Security condition	Actions to be executed
CHANGE REFERENCE DATA	Application-specific/out of scope (e.g. successful master PIN verification)	Change BR
VERIFY	PIN.SSEC > 0 (PIN verification successful)	If BR.RC > 0, then − Decrement BR.RC − If the probe from the command data field matches BR, then • Biometric verification successful • BR.RC := $BR.RC_{start}$ • BR.SSEC := $BR.SSEC_{max}$
Other	NEVER	None

Table 3 Access rules for PrK

Access mode	Security condition	Actions to be executed
PSO: COMPUTE DIGITAL SIGNATURE	(PIN.SSEC > 0) AND (BR.SSEC > 0) (PIN verification and biometric verification successful)	− Decrement PIN.SSEC − Decrement BR.SSEC − Compute digital signature
Other	NEVER	None

2.3 User authentication procedure

[ISO/IEC 7816-4] describes how to specify conjunctions and disjunctions of security conditions, but not how to specify the temporal ordering of security conditions. Still, a two-stage user authentication procedure can be realised as follows: Security condition for accessing PrK is successful PIN verification and successful biometric verification, while security condition for biometric verification is successful PIN verification. This enforces that biometric verification is preceded by successful PIN verification.

The security status achieved after successfully verifying PIN or BR remains valid up to a reset of the card, the selection of a different on-card application, or until the associated security status evaluation counter (SSEC) reaches 0. The security status achieved after successful biometric verification should be reset after each PSO: COMPUTE DIGITAL SIGNATURE command. The security status achieved after successful PIN verification may remain valid for multiple subsequent commands.

2.4 Special cases

If the initial value of BR.SSEC (before any verification attempt) represents "infinity", then the biometric user authentication is skipped. The PIN verification is skipped if the initial value of PIN.SSEC is set to represent "infinity". In case that the attack resistance of the biometric user authentication method is assessed as "high", the PIN verification could be switched off without damage.

3 Outlook

The proposed solution for applying biometric user authentication methods in addition to PIN verification is being implemented in prototype OpenPGP cards with biometric on-card comparison. In OpenPGP cards, which do not aim at "qualified" electronic signatures (which have the same legal effects as handwritten signatures on paper), the biometric user authentication may even replace the PIN verification for convenience.

In spite of their ease of use and their strong binding to persons, biometric methods are barely used in products for creating qualified electronic signatures. One reason is that, as yet, no biometric product has attained a sufficient security certificate. This is not only because the security of biometric products may still need to be improved, but also because the IT security evaluation methodology needs to be adjusted to biometric products.

References

[DIN V 66291-1] Pre-standard DIN V 66291-1:2000. Chip cards with digital signature application/function according to SigG and SigV – Part 1: Application interface

[EN 14890-1] European Standard EN 14890-1:2008, Application interface for smart cards used as secure signature creation devices – Part 1: Basic services

[ISO/IEC 7816-4] International Standard ISO/IEC 7816-4:2005, Information technology – Identification cards – Integrated circuit cards – Part 4: Organization, security and commands for interchange

[ISO/IEC 7816-11] International Standard ISO/IEC 7816-11:2004, Information technology – Identification cards – Integrated circuit cards – Part 11: Personal verification through biometric methods

[Pie08] A. Pietig: Functional specification of the OpenPGP application on ISO smart card operating systems. Vers. 2.0, 2008

[SigV01] Verordnung zur elektronischen Signatur (Signaturverordnung – SigV). 2001

[TR-03115] Bundesamt für Sicherheit in der Informationstechnik: Komfortsignatur mit dem Heilberufsausweis. Technische Richtlinie TR-03115, Vers. 2.0, 2007