

# TURBINE architecture and protocols for Trusted ID management

CryptoBiometrics for Enhanced Trusted Identity Management: Dreams & Reality

Hervé Chabanne, Julien Bringer

Morpho

[julien.bringer@morpho.com](mailto:julien.bringer@morpho.com), [herve.chabanne@morpho.com](mailto:herve.chabanne@morpho.com)



2011, January 17th

- 1 Introduction
- 2 A protocol dedicated to remote authentication
- 3 A protocol for access control
- 4 Conclusion

- Secure sketch → presentation by Prof. Gérard Cohen  
(The ones we like the most → presentation by Dr. Vincent Despiegel)
- We do not find secure sketch as secure as we can imagine
- We observe a loss of performance (accuracy) when using them

# What we want? What we get.

- 1 Pseudo-Identity Architecture based on secure sketch aka implementations of secure sketch as they are
- 2 Architectures taking secure sketch's limitations into account
- 3 Generic demo
- 4 Access control
- 5 Remote Authentication

# What we want? What we get.

- 1 Pseudo-Identity Architecture based on secure sketch aka implementations of secure sketch as they are
- 2 Architectures taking secure sketch's limitations into account
- 3 Generic demo
- 4 Access control
- 5 Remote Authentication

Demonstrator application	Protocol	Enhanced functionality	Use case
Application 1	Group Signature (GS)	Anonymous authorization	Pharmacy application.
Application 2	Secure Sketch (or Pseudo Identity - PI)	Authentication	Pharmacy application.
Application 3	Secure Sketch (or Pseudo Identity - PI)	Authentication for access control	Airport access control
Application 4	Secure Access Control (SAC) = local identification	Identification	Airport access control

# Pseudo-Identity Architecture based on secure sketch

- 2 demos:
  - Generic demo: authentication of pharmacists to a Portal which provides access to several web-based services  
(The demonstrator simulates a large pharmacy, where each employee is equipped with one smart card containing the PIs necessary for the applications he or she is authorized to use.)
  - Thessaloniki airport: scenario where security agents in the airport have to have multiple access rights in a secure building
- Development made by TURBINE partners
- Performances (Intel Core 2 Duo CPU E7500 @2.93GHz, 3.25 GB RAM): less than 7 seconds

- 1 Introduction
- 2 A protocol dedicated to remote authentication**
- 3 A protocol for access control
- 4 Conclusion

# A new way to generate cryptographic keys from biometric data

*Use the variability of captures to your own advantage*

# A new way to generate cryptographic keys from biometric data

*Use the variability of captures to your own advantage :  
w taken at the enrollment is treated as confidential.*

# A new way to generate cryptographic keys from biometric data

*Use the variability of captures to your own advantage :  
w taken at the enrollment is treated as confidential.*

- This way biometric keys are easy to obtain and renew.

# A new way to generate cryptographic keys from biometric data

*Use the variability of captures to your own advantage :  
 $w$  taken at the enrollment is treated as confidential.*

- This way biometric keys are easy to obtain and renew.
- In what follows,  $w$  is stored on a card  $\mathcal{C}$ . We have:

Human user $\mathcal{H}$	$\leftrightarrow$	a capture of one of his biometric trait: $w$
	$\leftrightarrow$	his biometric key: $x = H(w)$
	$\leftrightarrow$	his private key in the system: $(x, A)$

# How to deal with the storage of biometric data inside database?

*Suppress database storage and replace it by group authentication*

# How to deal with the storage of biometric data inside database?

*Suppress database storage and replace it by group authentication under the private key  $(x, A)$*

A new entity – the Card Issuer  $\mathcal{I}$  – acts as the group manager.

- 1 A biometric trait is acquired for user  $\mathcal{H}$ :  $w \leftarrow W$ .
- 2 The Card Issuer  $\mathcal{I}$  computes  $A = g_1^{1/(\gamma+x)}$  with the help of  $\gamma$ ,  $x = H(w)$ .
- 3 A card  $\mathcal{C}$  containing  $(w, A)$  is issued by  $\mathcal{I}$  for  $\mathcal{H}$ .

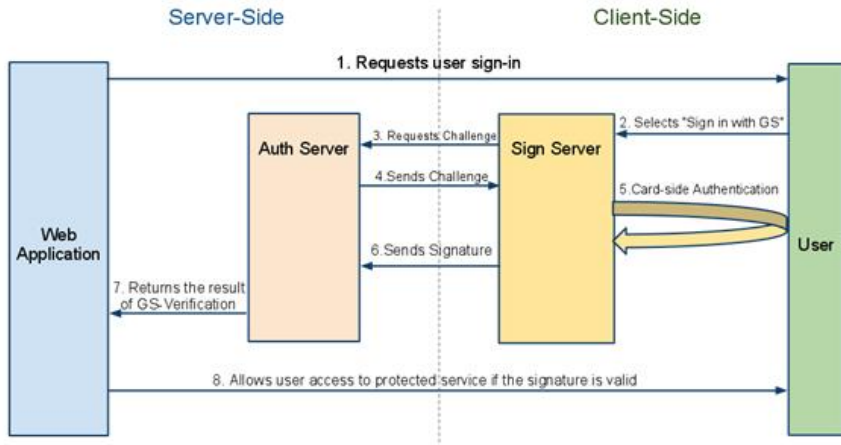
# Verification phase

- 1  $\mathcal{SP}$  sends the challenge  $M$  to sensor  $\mathcal{S}$
- 2  $\mathcal{S}$  gets the “fresh” biometric trait  $w'$  and reads  $(w, A)$  from the card
- 3  $\mathcal{S}$  checks whether  $w' \sim w$ , and in this case computes  $x = H(w)$
- 4  $\mathcal{S}$  computes the signature  $\sigma$  of  $M$  under  $(x, A)$
- 5  $\mathcal{SP}$  verifies the signature  $\sigma$

For details, see:

Julien Bringer, Hervé Chabanne, David Pointcheval, Sébastien Zimmer.  
An Application of the Boneh and Shacham Group Signature Scheme to  
Biometric Authentication. IWSEC, 2008.

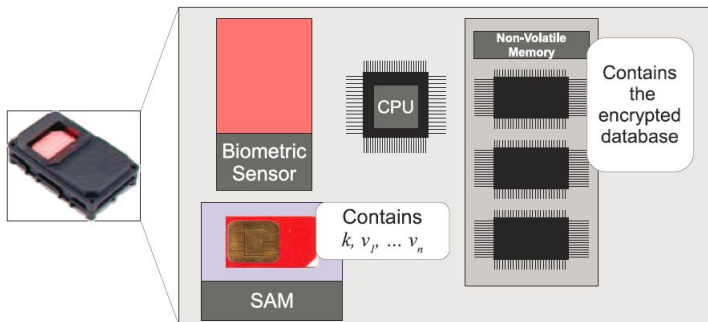
# Generic demo



- Development made by TURBINE partners
- Intel(R) Xeon(R) CPU X3320 @ 2.50GHz, 3 GB RAM
- Elliptic curve with 512-bit-long order and 160-bit-long torsion subgroup (which may provide real world security)
- Revocation list with 50 persons
- Total time: around 3 seconds

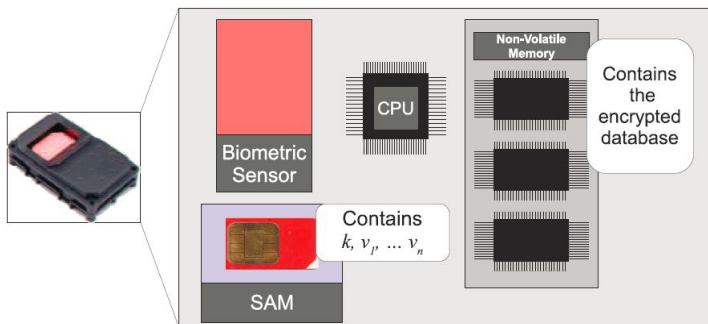
- 1 Introduction
- 2 A protocol dedicated to remote authentication
- 3 A protocol for access control**
- 4 Conclusion

# Extending Match-On-Card to Local Biometric Identification

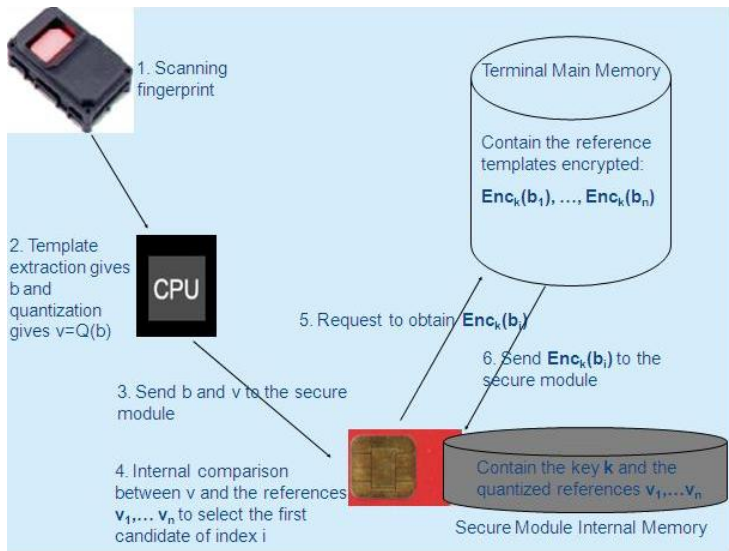


# Extending Match-On-Card to Local Biometric Identification

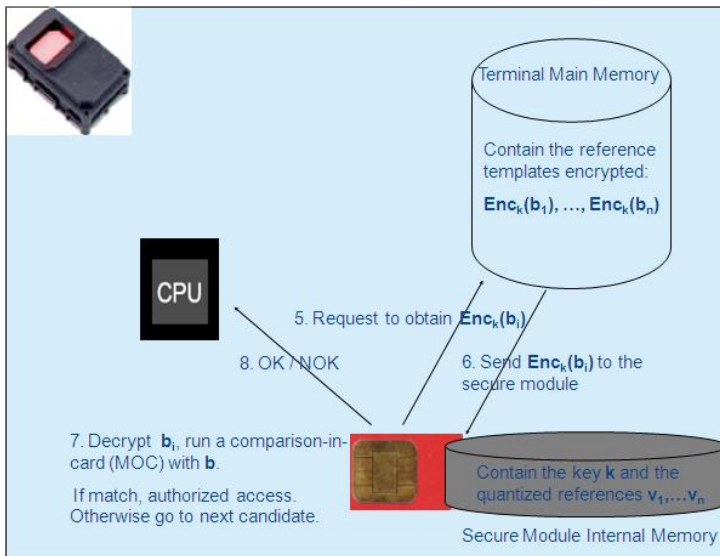
- Secure sketch are used to minimize the number of MOC operations
- Secure sketch are considered confidential and stored inside a tamper-resistant chip (called Secure Access Module - SAM)
- This chip can also performed the MOC
- Biometric data are stored outside the SAM encrypted by a key  $k$



# How does it work?



# How does it work?



## For further details

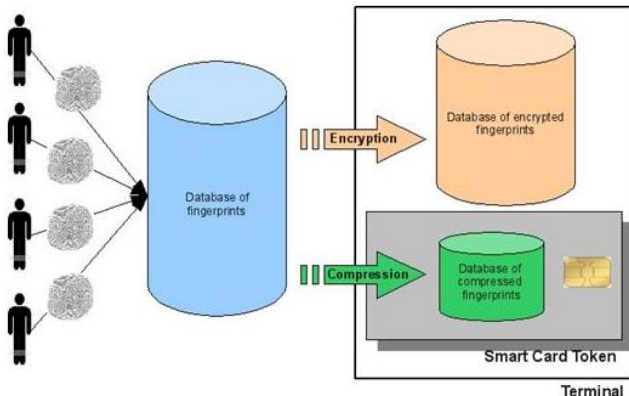
- Julien Bringer, Hervé Chabanne, Tom Kevenaar, Bruno Kindarji: Extending Match-On-Card to Local Biometric Identification. BiID MultiComm 09
- Julien Bringer, Hervé Chabanne, Koen Simoens: Blackbox Security of Biometrics. IIH MSP 10

# Demo at the airport

- Olympic Airways Cargo building
- Development made by TURBINE partners
- Access control granted in around 8 seconds

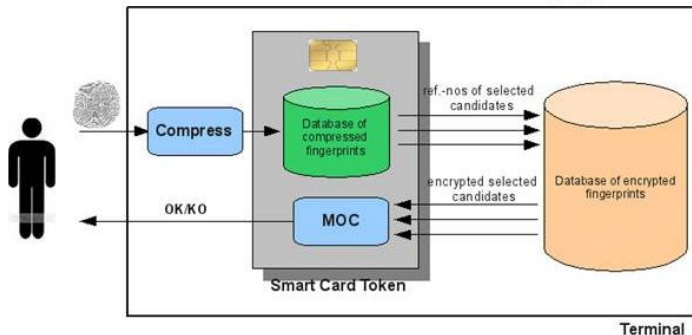
# Demo at the airport

- Olympic Airways Cargo building
- Development made by TURBINE partners
- Access control granted in around 8 seconds



# Demo at the airport

- Olympic Airways Cargo building
- Development made by TURBINE partners
- Access control granted in around 8 seconds



- 1 Introduction
- 2 A protocol dedicated to remote authentication
- 3 A protocol for access control
- 4 Conclusion**

- Different solutions exist today
- It's time for their evaluation ...
  - Koen Simoens' presentation
  - Analysis of Biometric Authentication Protocols in the Blackbox Model  
by Koen Simoens, Julien Bringer, Hervé Chabanne, Stefaan Seys,  
submitted (available on arXiv.org server  
<http://arxiv.org/abs/1101.2569>)
- ... and to deploy them.

Thanks! Any questions?