Security and Privacy in Biometric Systems -

The purpose of Biometric Encryption

NIST INTERNATIONAL BIOMETRIC PERFORMANCE CONFERENCE, March 1-5, 2010

Tom Kevenaar

Joint BSI-project with: Ulrike Korte (BSI), Matthias Niesing (secunet), Johannes Merkle (secunet)

Bundesamt
für Sicherheit in der
Informationstechnik

secunet
IT security beyond expectations

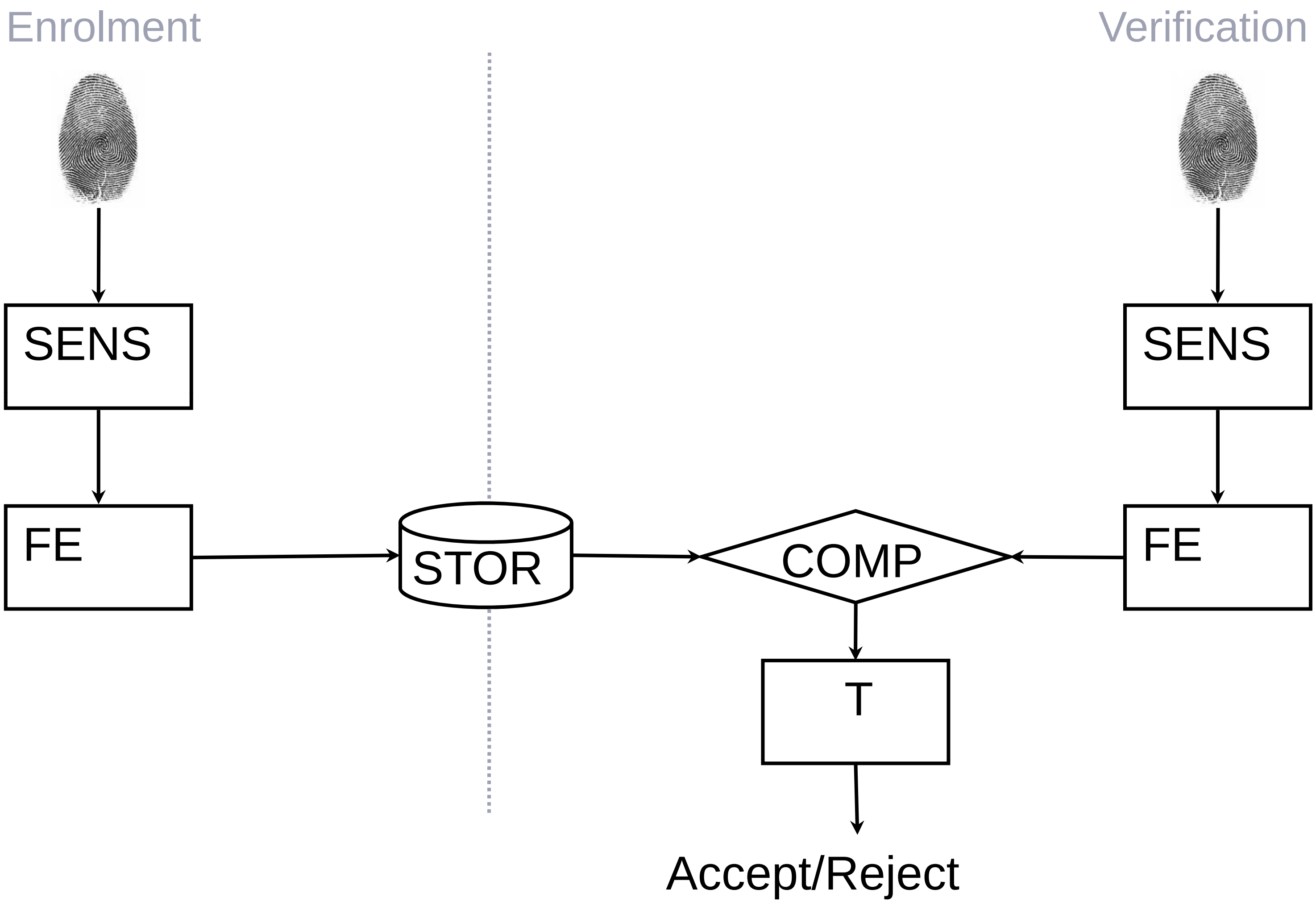
priv-ID

www.priv-id.com

Overview

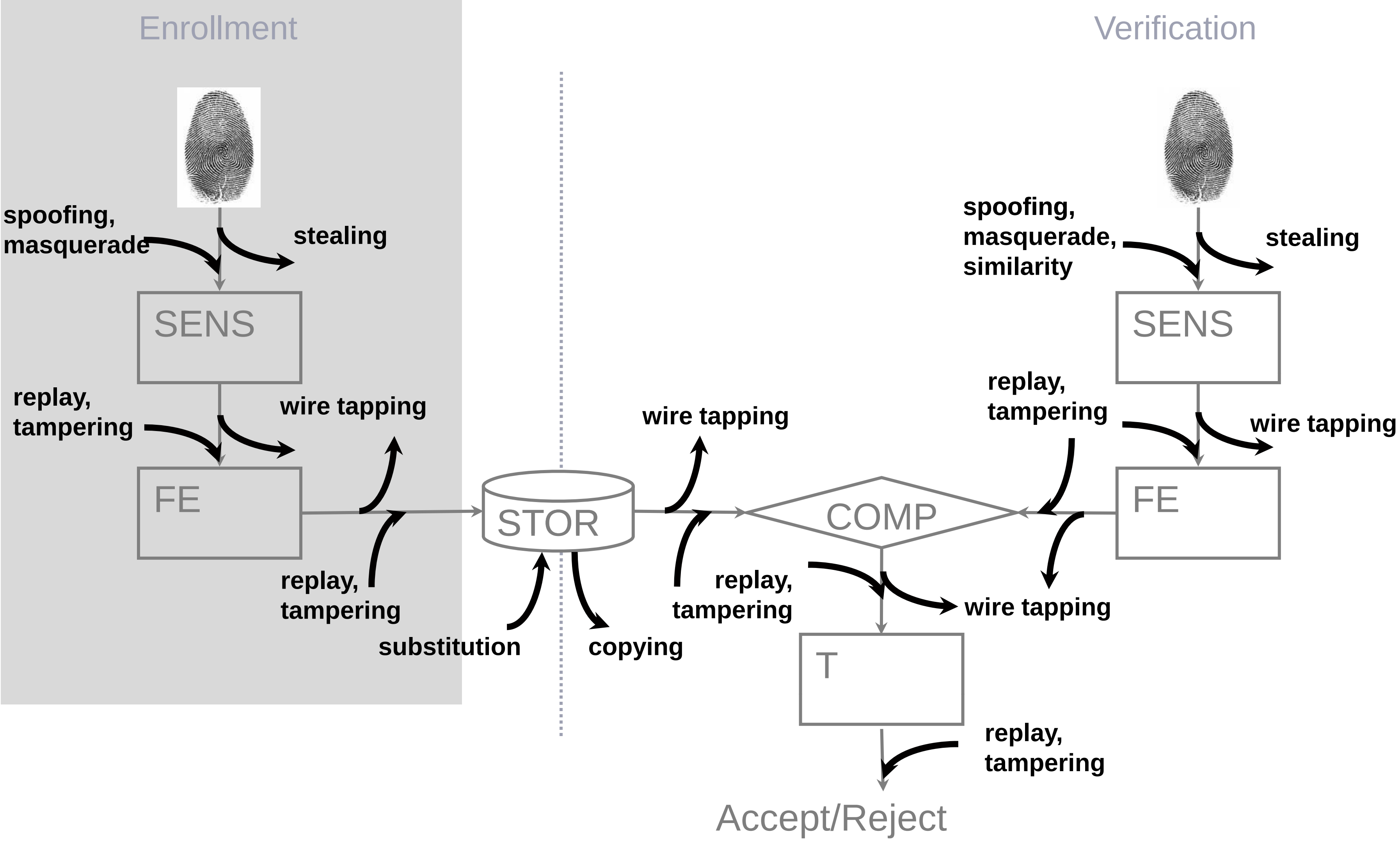
- High level overview of a biometric system
- A perfectly private biometric system
- The purpose of Biometric Encryption

High level overview of a biometric system



High level overview of a biometric system

Security and privacy vulnerabilities



High level overview of a biometric system
Security and privacy vulnerabilities

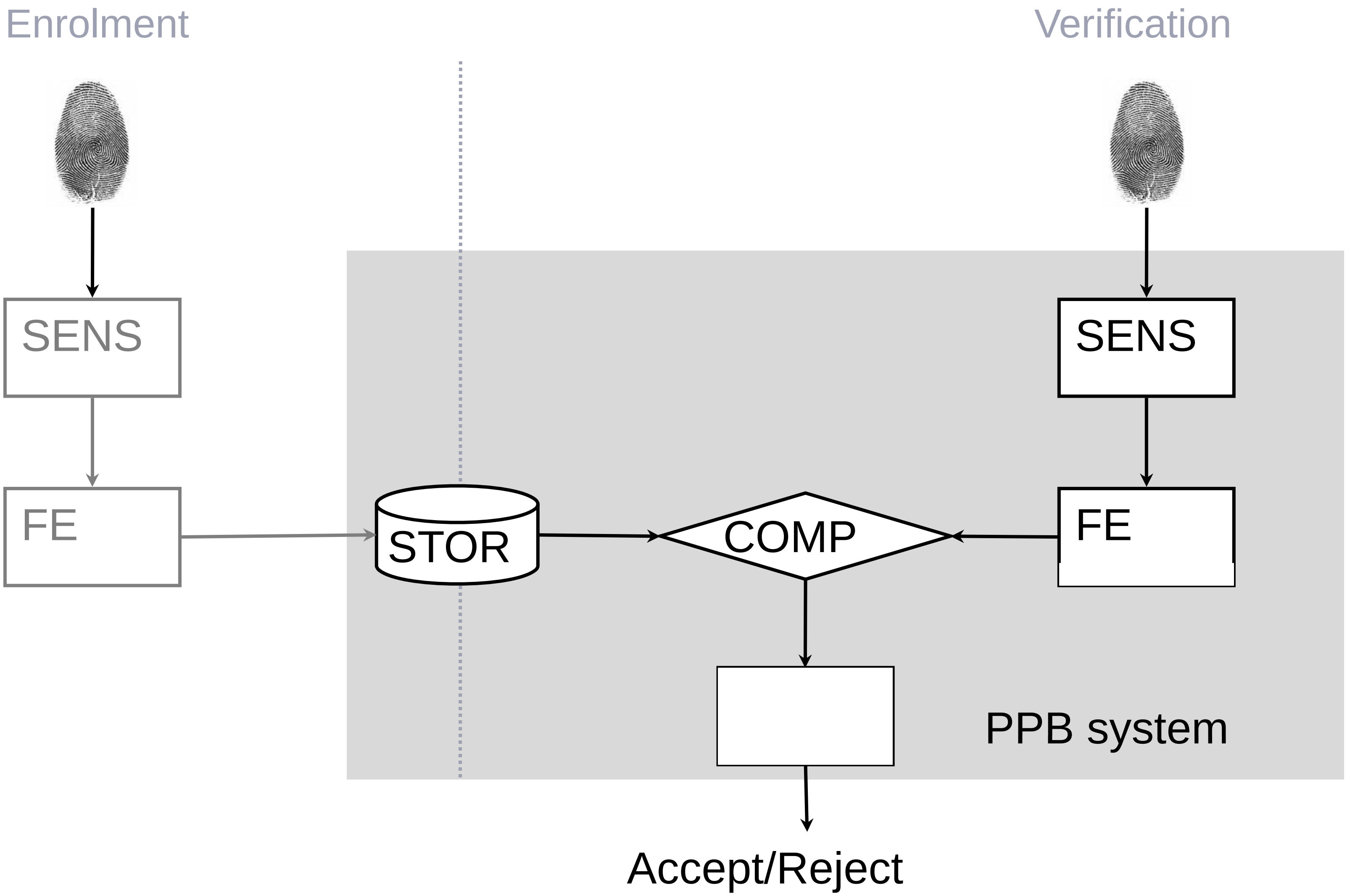
- ***Security*** (ingoing arrows) defines how difficult it is to illegitimately be accepted by the system.
- ***Privacy*** (outgoing arrows) is related to the difficulty to obtain any relevant information from a provided biometric characteristic other than a verification decision.

See also:

•ISO/IEC JTC1 SC27 2ndCD 24745 – Biometric information protection.

•Jeroen Breebaart, Bian Yang, Ileana Buhan-Dulman, Christoph Busch: Biometric template protection, the need for open standards. Datenschutz und Datensicherheit - DuD, Volume 33, No 5, May 2009, Vieweg Verlag, pp299-304.

A Perfectly Private Biometric system



A Perfectly Private Biometric system
A practical implementation

- This PPB system is *perfectly private* in the sense that it outputs the minimal required amount of information in the form of a binary Accept/Reject decision.

- Furthermore, assuming a sensor leaving no latent prints (e.g. a touchless sensor), the system has no eavesdropping vulnerabilities.

- The system is *not perfectly secure* because the comparator COMP will occasionally make a wrong decision.

- All vulnerabilities can be solved using standard encryption techniques *without the need for long-term secrets* ***except*** *the protection of stored biometric information*

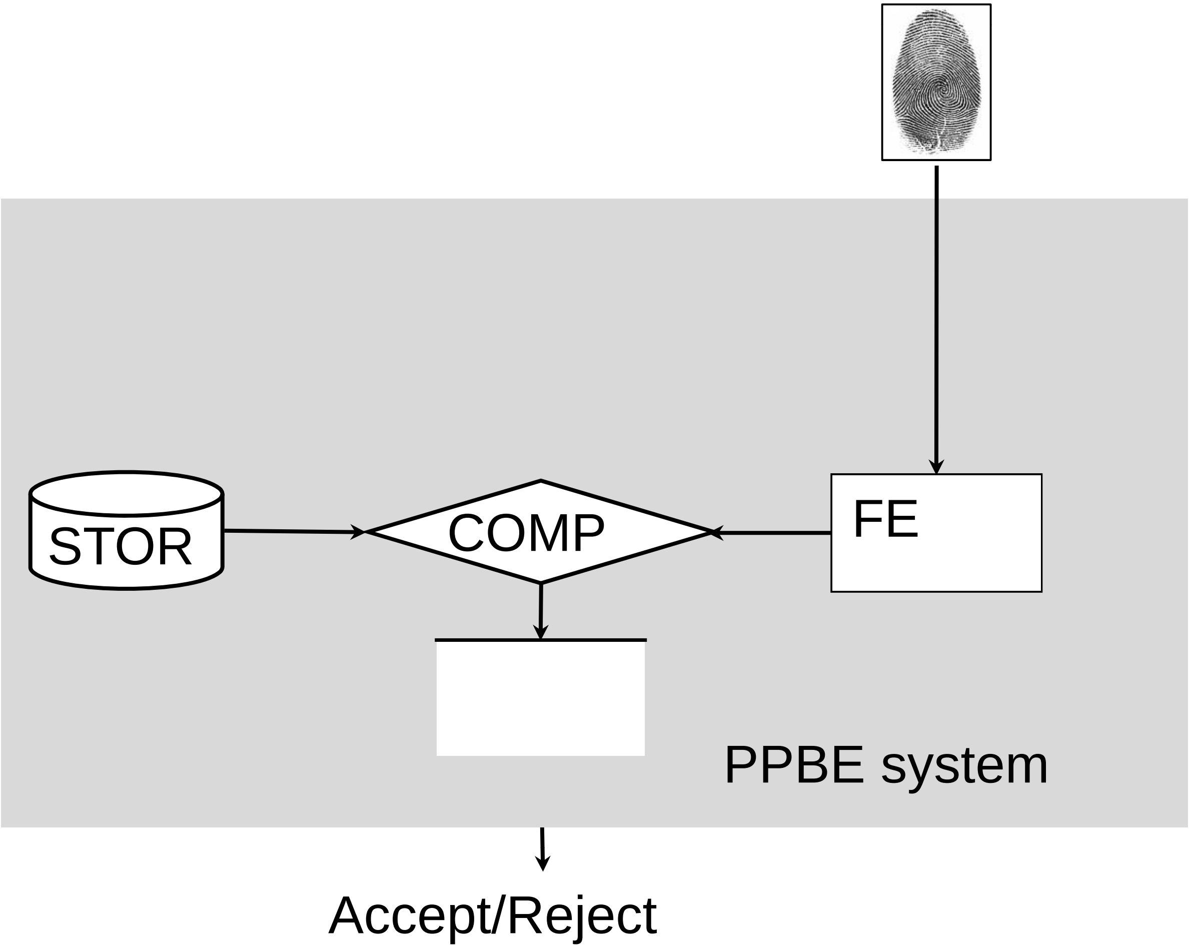
A Perfectly Private Biometric system
A practical implementation

Long-term secrets to protect stored biometric information

- access to the secrets means access to the biometric information
- secrets must be protected
  - by the system owner (which assumes that the owner can be trusted)
  - by the user (secret is password, passphrase, stored on token etc.). No duplicate check possible

The purpose of Biometric Encryption

A Perfectly Private Biometric Encryption system



The purpose of Biometric Encryption

- The purpose of Biometric Encryption is to implement a PPBE system, or,

The goal of Biometric Encryption technology is to prevent relevant biometric information to be obtained from storage facilities in biometric systems without the need for long-term secrets.

Conclusion

- All vulnerabilities of a biometric system can be solved using standard cryptographic techniques without long-term secrets
- The only exception is protecting stored biometric information which requires long-term secrets
- The goal of Biometric Encryption technology is to prevent relevant biometric information to be obtained from storage facilities in biometric systems without the need for long-term secrets.

Bundesamt
für Sicherheit in der
Informationstechnik

secunet
IT security beyond expectations

priv-ID
www.priv-id.com