UNIKASSEL VERSITÄT

Sebastian Pape

Templateless Biometric-Enforced Non-Transferability of Anonymous Credentials

Overview

UNIKASSEL VERSITÄT

- Motivation
- Anonymous Credentials
- Problems with Biometrics
- Wallet-with-Observer Architecture
- Existing Approaches
- Idea
- Example
- Outlook

Motivation

UNIKASSEL VERSITÄT

- Cryptographic primitives are based on secrets
  - Private keys for digital signatures
  - Secrets in Zero-Knowledge-Proofs (ZKP)

- Secret is knowledge and knowledge can be
  - Stolen
  - Transfered to someone

- How can you be sure the secret was used by its regular owner?

Anonymous Credentials

UNIKASSEL VERSITÄT

- Consist of cryptographic tokens
- Allow authentication without identification
  - Based on ZKP

- Non-transferablity may be wished
  - ⇒ Make the user not wanting to share
    - ⇒ Embed valuable secrets into the system
    - ⇒ Share nothing-or-all strategy
      - ✗ Can be circumvented
      - ✗ Raise system's value

  - ⇒ Keep tokens secret from user
    - Use of Biometrics

Problems with Biometrics

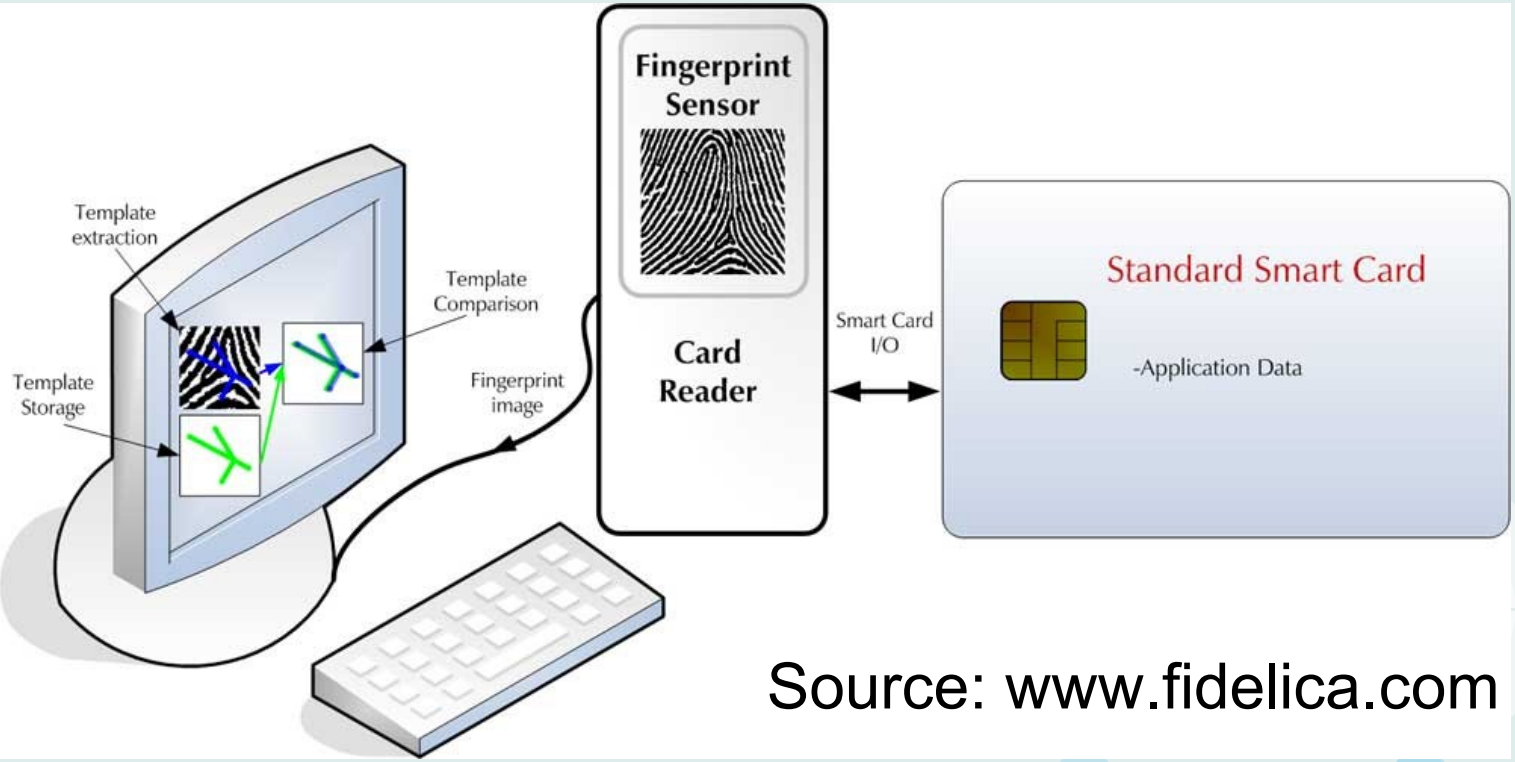
UNIKASSEL VERSITÄT

- Finding good/usable attributes
- Fingerprints
    - Universality
    - Circumvention

- Cannot be changed
- False nonmatch rate vs. False match rate

- Privacy Issues

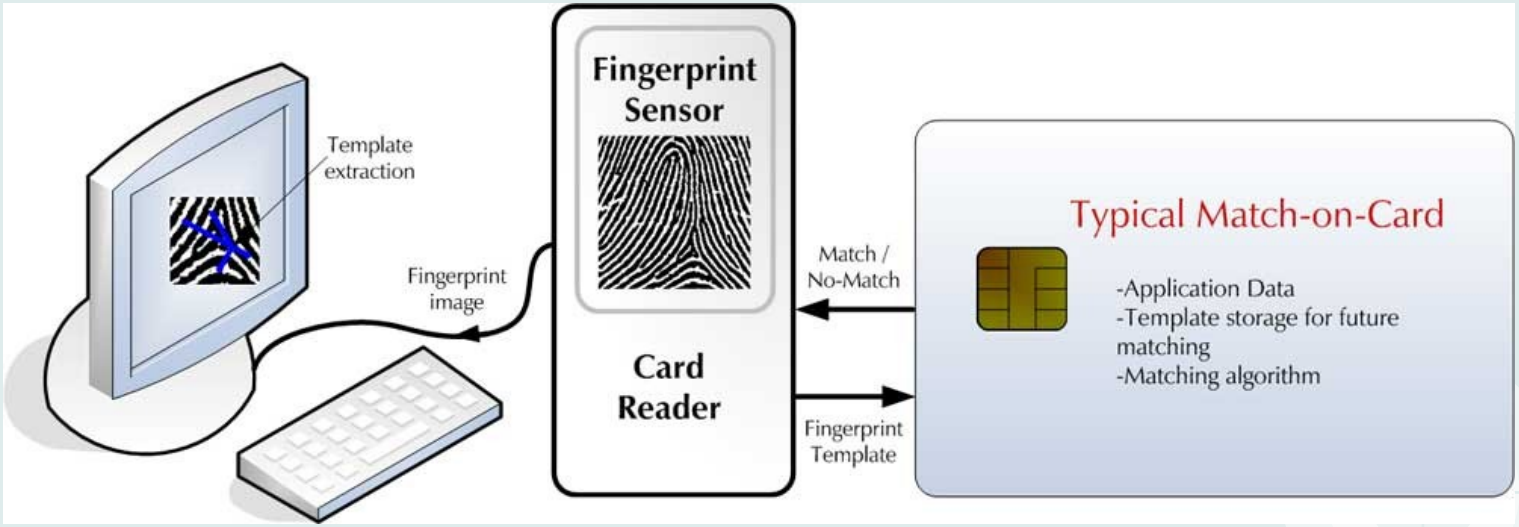
Hardware (outdated)



Source: www.fidelica.com

- Privacy problem: Template database

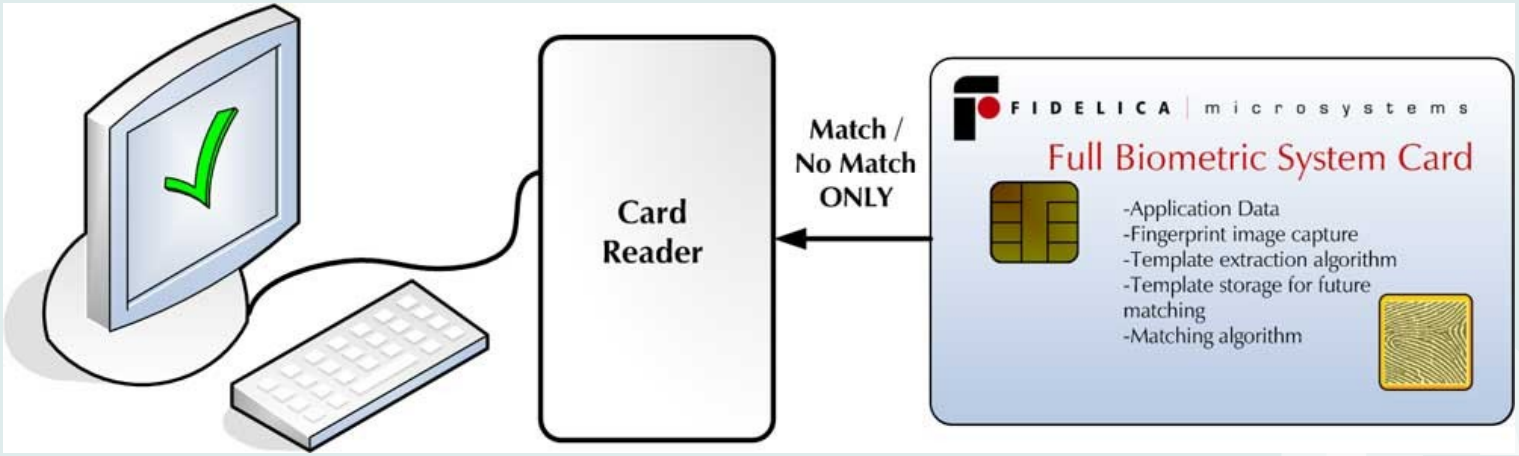
Hardware (match-on-card)



Source: www.fidelica.com

- No template database
- Privacy problem: Eavesdropper

Hardware (embedded)



Source: www.fidelica.com

- No template database
- Protected against eavesdropper

Some Problems of Biometrics

UNIKASSEL VERSITÄT

- Finding good/usable attributes
- Fingerprints
    - Universality
    - Circumvention

- Cannot be changed
- False nonmatch rate vs. False match rate

- Privacy Issues
- Trust to system

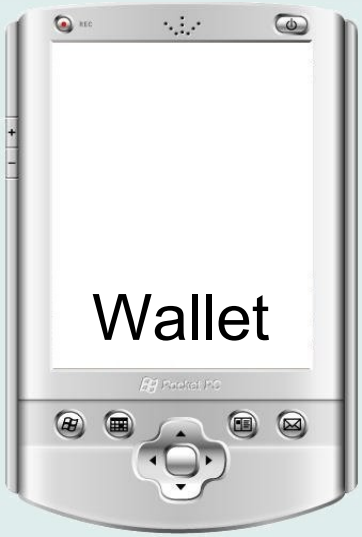
Wallet-with-Observer Architecture

- General Problem: Contact to "correct card"?

Wallet-with-Observer Architecture + Biometrics

UNIKASSEL VERSITÄT

Verifier



Wallet

Observer

- Biometrics to Observer

Existing Approaches

UNIKASSEL VERSITÄT

- Current approaches compare biometrics to templates
  - ✔ Underlying system needs no change
  - ✗ Stored Templates
- Fuzzy extractors provide same output to "close" input
  - "error correcting hash"
  - Private keys can be derived from Biometrics

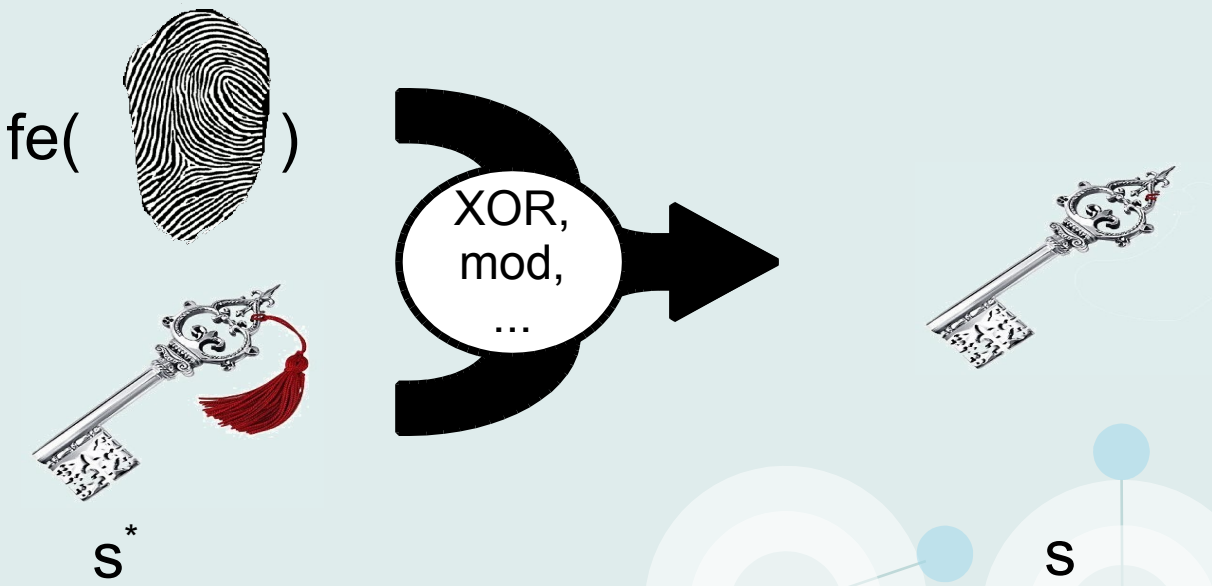
fe()  s 

  - ✗ Derived keys need to suit to underlying system
  - ✔ No templates/storage needed

Idea

UNIKASSEL VERSITÄT

- Combine Advantages
  - ⇒ No Templates stored
  - ⇒ No change of underlying system



Example (Setup) based on Feige-Fiat-Shamir Id.-Protocol

UNIKASSEL VERSITÄT

Authority

chooses two large prime integers p,q
calculates n= p * q
generates $s_1, \ldots, s_k$ with $\gcd(s_i,n) = 1$
computes $v_i \equiv s_i^2 \pmod n$

Public (known by verifier and prover): n, v_i

Secret (kept inside the smartcard): s_i

Secret (kept by authority): p, q

Card initialization:
s_i is overwritten by $s^*_i \equiv s_i - fe(fp_u) \pmod n$

Example (Prove) based on Feige-Fiat-Shamir Id.-Protocol

UNIKASSEL VERSITÄT

Smartcard:

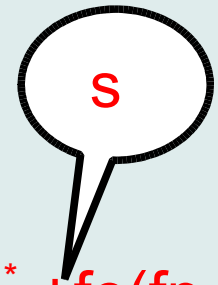
chooses a random integer r,

a random sign $\sigma \in \{-1,1\}$

computes $\sigma\, x \equiv r^2 \pmod n$ ↗ V

Verifier:

chooses numbers $a_i \in \{0,1\}$ ↗ S



Smartcard:

reads fingerprint fp_u

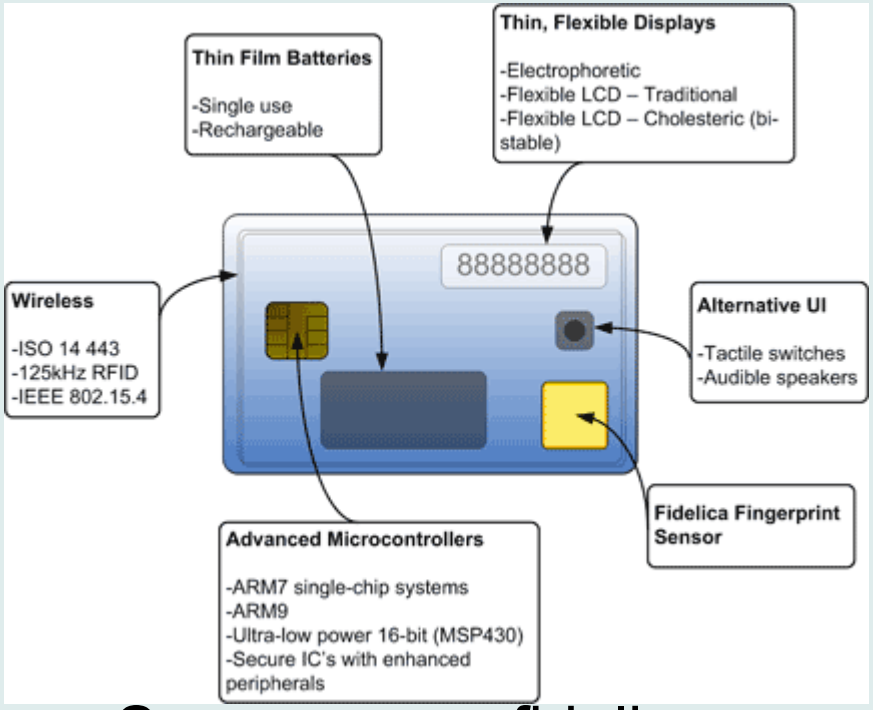
computes $y \equiv r(s^*_1+fe(fp_u))^{a_1} * \ldots * (s^*_k+fe(fp_u))^{a_k} \pmod n$ ↗ V

Verifier:

checks if $y^2 \equiv \pm x\, v_1^{a_1} * \ldots * v_k^{a_k} \pmod n$

decides if the prover has passed authorisation.

Outlook



Source: www.fidelica.com

Connection to proper smartcard?

User interleaved

Use of flexible display

e.g. for r^2

Unlimited number of uses

base on n-time anonym. authentification

Concrete implementation