Sebastian Pape

A Survey on Untransferable Anonymous Credentials

Overview

UNIKASSEL VERSITÄT

- Anonymous Credentials
- Approaches to ensure untransferability
- System's Security
- Attacks
- Comparison / Conclusion

Anonymous Credentials

UNIKASSEL VERSITÄT

- Introduced by Chaum
- Consist of cryptographic tokens (ZKP, Blind/Group Signature)
- Allow authentication without identification

- Related to anonymous payment
- But non-transferablity may be wished
  - age verification
  - driving license
  - student ID
  - ...

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

Approaches

UNIKASSEL VERSITÄT

- Two different approaches
  - ⇒ Make the user not wanting to share
    - Embed valuable secrets into the system
  - ⇒ Keep tokens secret from user
    - Use of Biometrics
- Advantages / Disadvantages?

Embedded Secrets

UNIKASSEL VERSITÄT

- Discourage users to share credentials

- Sharing a credential shares a valuable secret
- User's credential is made valuable
  beyond primary intent

- Assumption/Hope: User won't share credentials

- Interactive Protocol for Credential issuing
  - Keeps embedded secret
- May be tough to verify the secret's accuracy

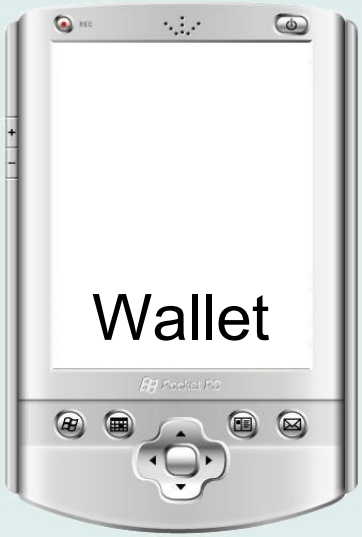
Embedded Secrets

UNIKASSEL VERSITÄT

- Embed secret from outside the system
  - By Lysyanskaya / Rivest / Sahai / Wolf
  - PKI-assured non transferability
  - Valuable Master key
    - To sign legal/financial documents
- Connect all credentials in the system
  - Camenisch / Lysyanskaya
  - All-or-nothing transferability

Hardware (S)

Verifier



- User is able to check information flow
- Observer not needed

AC with Biometrics

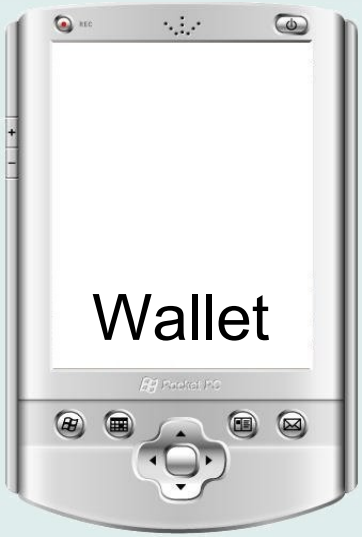
UNIKASSEL VERSITÄT

- Access control by biometrics
- Authentication factor "knowledge" transformed to "possesion"
- Smartcard works as Blackbox for the user
- General biometric problems apply

Wallet-with-Observer

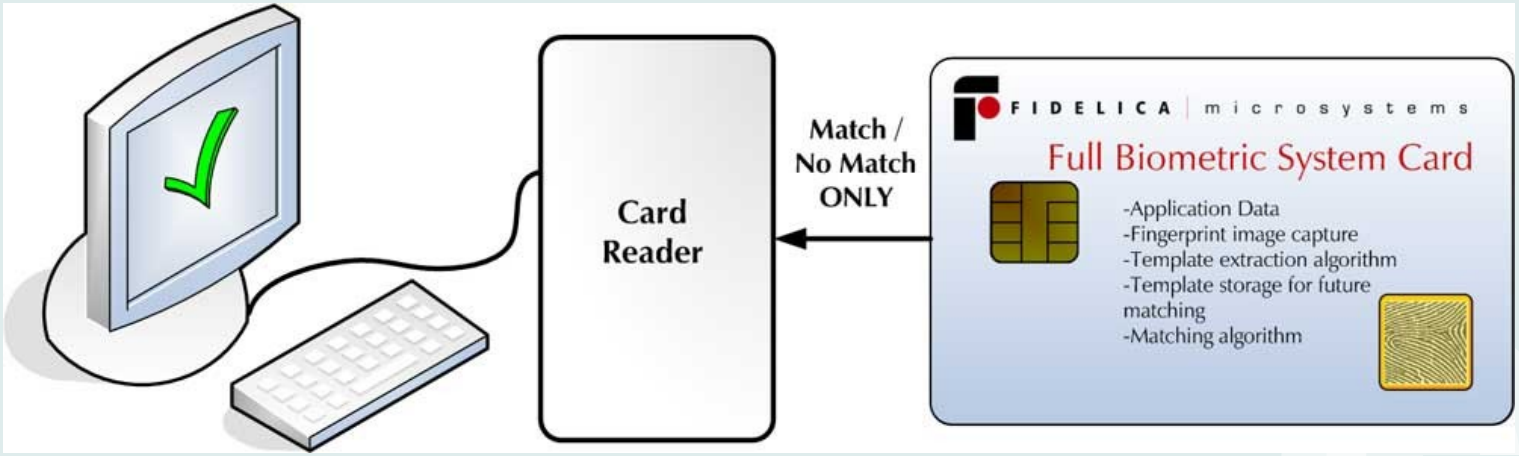
UNIKASSEL VERSITÄT

Verifier



- Suggested by Chaum and Pedersen
- User is able to check information flow
- Organisation has to trust observer

Biometrics (Hardware)

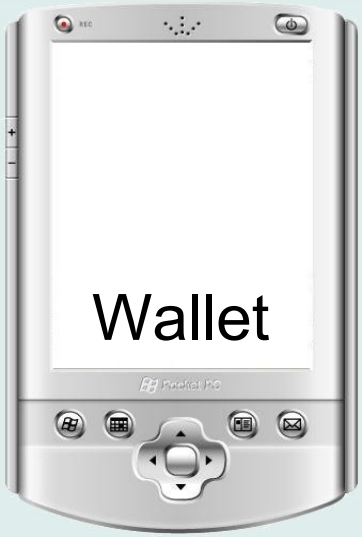


Source: www.fidelica.com

- No template database
- Match-on-card system
- Protected against eavesdropper

Wallet-with-Observer (B)

Verifier



- Extension by Bleumer
- Biometrics to Observer
- User is able to check information flow
- Organisation has to trust observer

System's Security

UNIKASSEL VERSITÄT

(G) Security of the basis credential system

(B) Security of untransferability by biometric access control

(S) Security of untransferability by embedding a valuable secret

System's Security

UNIKASSEL VERSITÄT


(G1) Security of cryptographic functions


(G2) Credentials' secrecy (initialization)


(B1) Quality of tamperproofness


(B2) Difficulty duping biometric sensors


(S1) Value of embedded secret


(S2) Precautions to prevent misuse


(S3) Connection of credential & secret

Scenario

UNIKASSEL VERSITÄT

- Issuer creates credential in regard to biometrics / secret
- Verifier has interest to check credential
  - Discount (student / handicapped ID)
  - Enforcement of laws (tobaco, driving)
- Untransferability is not in the user's interest

Attacker Model

UNIKASSEL VERSITÄT

- Main focus:
  - Comparison regarding untransferability
- Assumptions:
  - No high-security environment
    - Practical view on security
  - 3rd parties have less power than involved p.
  - All parties use trusted hardware
  - Tamperproof device chosen by Issuer/Verifier

Attacker Model

UNIKASSEL VERSITÄT

- Verifier/Issuer wants to gather information
  - Wallet-with-observer architecture holds
- Issuer does not leak/get information
  - e.g. credentials, biometrics, embedded secret
- => User is a possible attacker
  - Untransferability is on the user's part

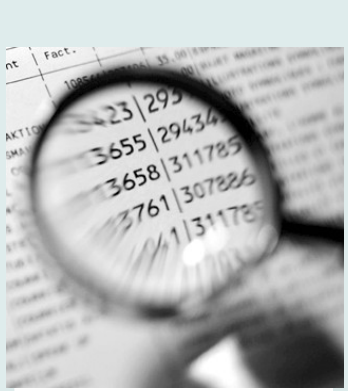
Attacks (G)

UNIKASSEL VERSITÄT

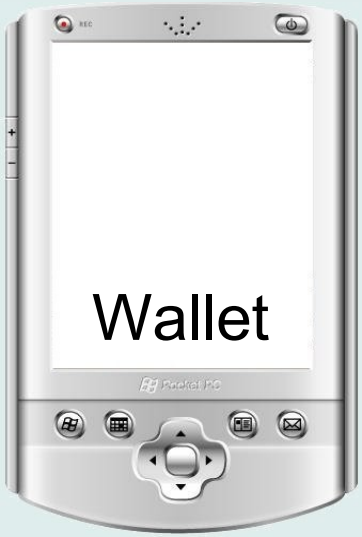
🗝 (G1) Security of cryptographic functions
🗣 (G2) Credentials' secrecy (initialization)

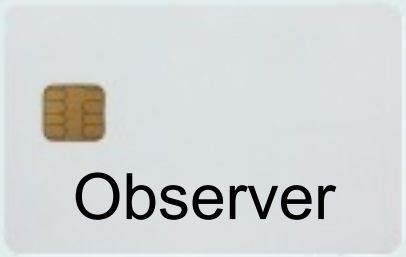
- Apply to both approaches
- Assumed to be safe
- General problem with Wallet-with-Observer

Wallet-with-Observer Architecture



Verifier





- General Problem: Contact to "correct card"?

Attacks (B)

UNIKASSEL VERSITÄT

🛠 (B1) Quality of tamperproofness
👁 (B2) Difficulty duping biometric sensors

- Biometric device embedded in Smartcard
  - Otherwise privacy-risk (cash cards)
- Moderately secure biometric sensor
- Attended or unattended control ?

Attacks (S)

UNIKASSEL VERSITÄT


(S1) Value of embedded secret


(S2) Precautions to prevent misuse


(S3) Connection of credential & secret

- Precautions depend on value of secret
  - User acceptance
- Detaching credentials unfeasible
- Value of secret most important

Attacks (B vs. S)

UNIKASSEL VERSITÄT

(B2) Difficulty duping biometric sensors

- Control depends on (un)attendance
- Expensive, not universal, error-prone?

(S1) Value of embedded secret

- Which secret to use?
- Secret is able to protect lower values
- Raises system's value

Conclusion

UNIKASSEL VERSITÄT

Circumvention	• (un)attended AC	• Secret
Universality	• Biometrics	• Secret
Special device	• Tamperproof + biometric reader	• Not needed
Unint. Sharing	• Unlikely	• May occur
System's Value	• Unchanged	• Raised

Conclusion

UNIKASSEL VERSITÄT

Circumvention	- (un)attended AC	• Secret
Universality	• Biometrics	• Secret
Special device	- Tamperproof + biometric reader	✚ Not needed
Unint. Sharing	✚ Unlikely	- May occur
System's Value	✚ Unchanged	- Raised