NTNU

Kunnskap for en bedre verden

Secure and Privacy Preserving Biometrics for Online Authentication

Martin Stokkenes (martin.stokkenes2@ntnu.no)
Norwegian Biometrics Laboratory
Norwegian University of Science and Technology

Supervisor: Prof. Dr. Christoph Busch (christoph.busch@ntnu.no)
Co-Supervisor: Dr. Raghavendra Ramachandra (raghavendra.ramachandra@ntnu.no)

The Research Council of Norway

NTNU

Outline

- Motivation and goals
- Research Questions
- Traditional Biometric Authentication
- eIDAS
- FIDO
- Biometric Transaction Authentication Protocol
- Challenges

Motivation and goals

- The motivation for the project is to enable biometric authentication of users and verification of transactions in online banking.
- Make online banking more convenient for users
- Using smartphones as biometric sensors
- Directive on Payment Services (PSD2) adopted by the European Parliament Oct. 2015. (Directive (EU) 2015/2366)

NTNU

Research Questions

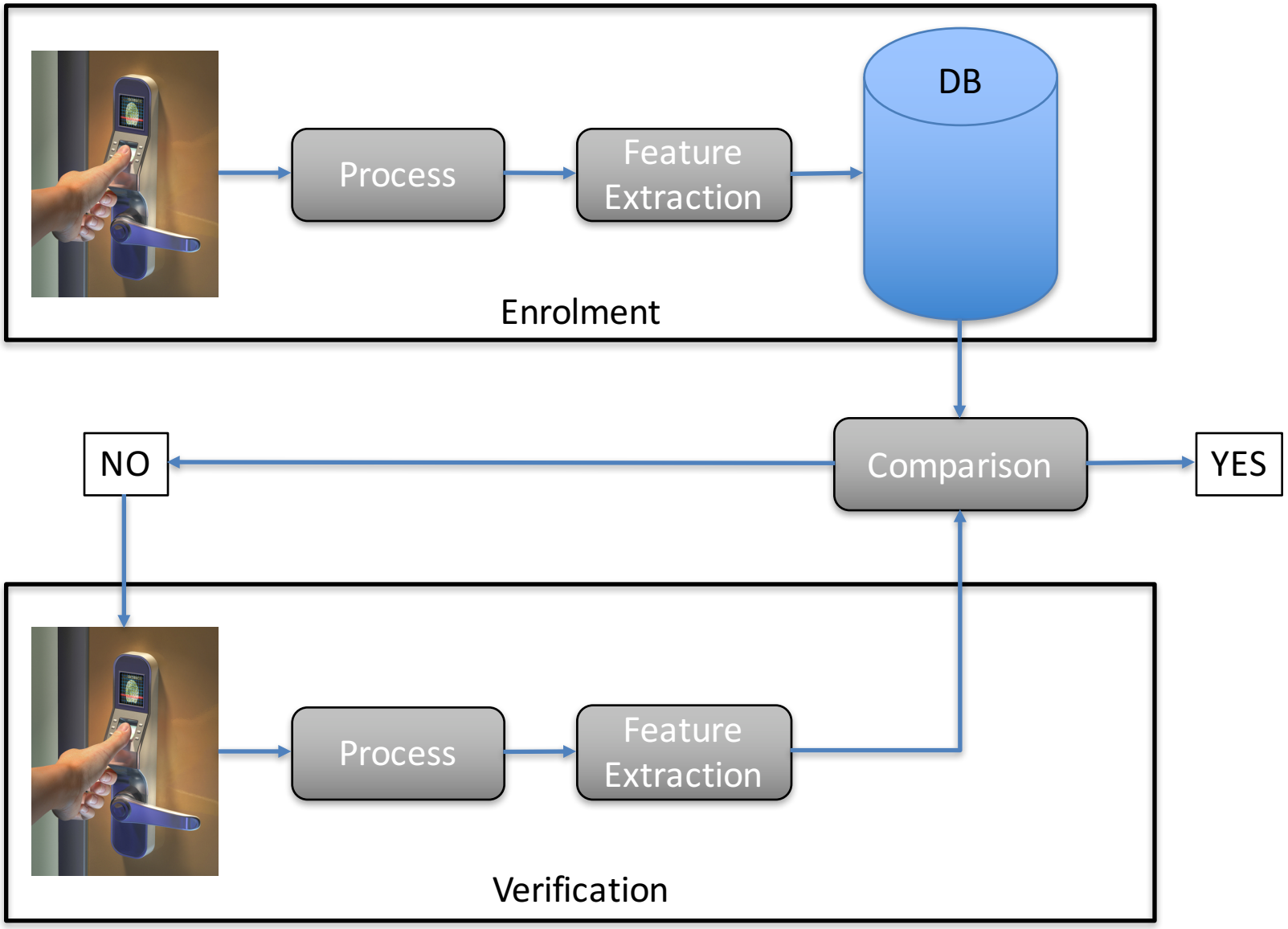
1. What are the challenges with using biometric enabled transaction authentication protocols in online banking and e-services?
2. Can existing biometric transaction authentication protocols be used on smartphones with lower computational capability?
3. What are the challenges posed by privacy preserving biometrics in achieving robust biometric transaction authentication protocols?

NTNU

Research Questions

4. Can built-in biometric sensors (e.g. fingerprint sensor in iPhone) be used with biometric transaction authentication protocols?
5. Can we improve the trustworthiness of existing biometric transaction authentication protocol against indirect attacks?

Traditional Biometric Authentication



Traditional Biometric Authentication

- The owner of the system have more control over the different aspects (sensors, enrollment, database)

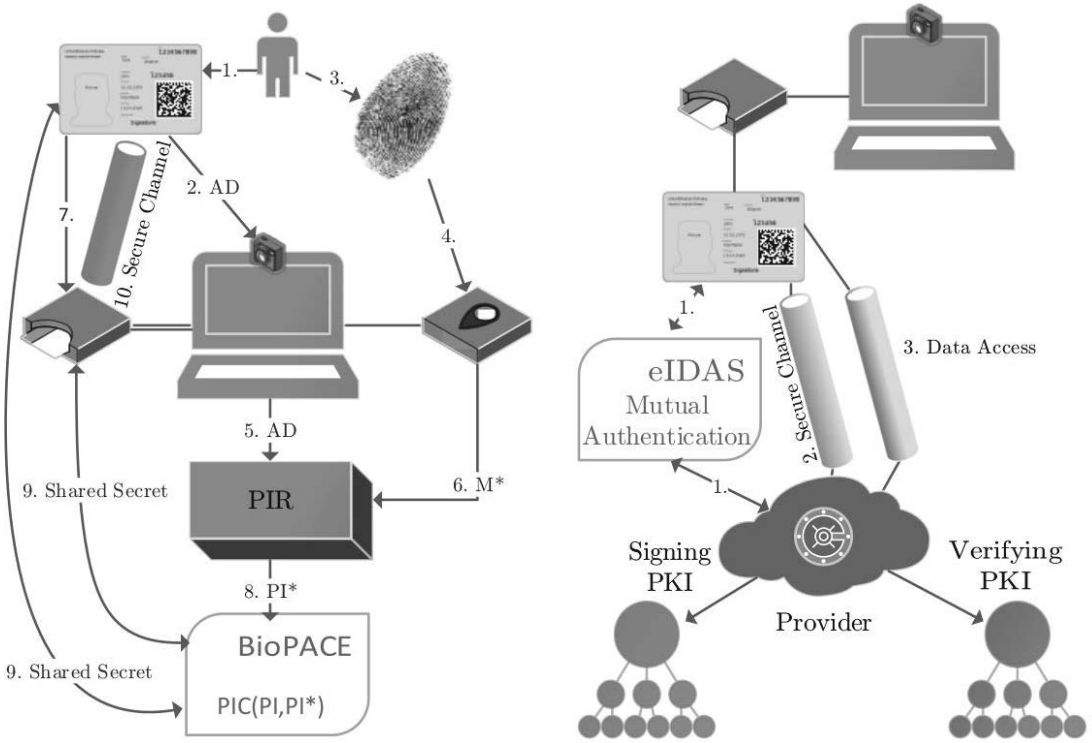
But:

- Need to maintain a centralized database with sensitive biometric information (high value target)
- Biometric data must be transmitted over the network

State-of-the-art

- Biometric authentication performed locally using a smartphones or mobile devices as the biometric sensor
- Pseudonymous identifier (PI) for remote verification
- Biometric template protection to secure biometric data incase of data breaches (one way transformation / key binding)

Biometrics and Electronic Identity (eID)

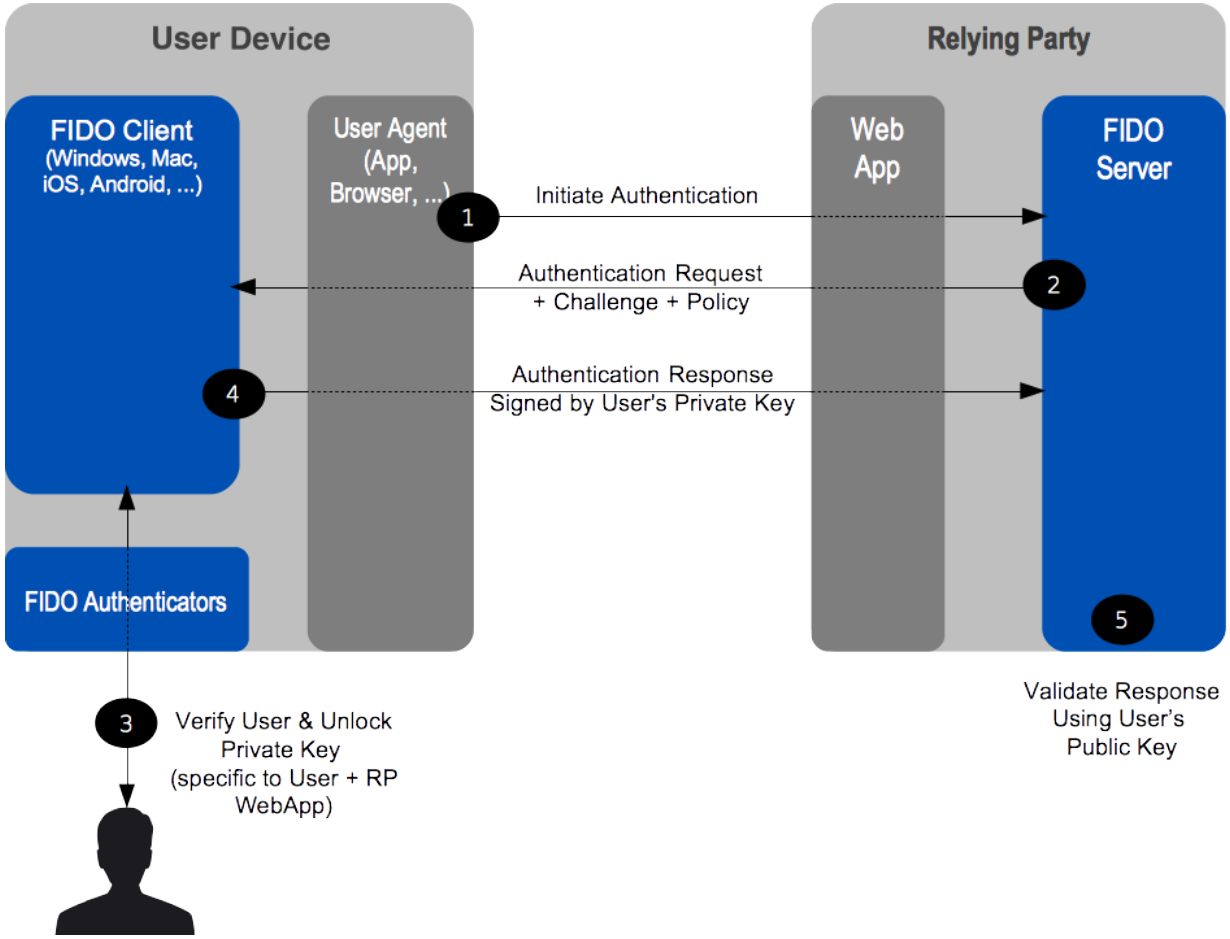


Buchmann, Nicolas, et al. "Towards electronic identification and trusted services for biometric authenticated transactions in the single euro payments area."

Biometrics and Electronic Identity

- Electronic identification and trust services for electronic transactions in the internal market
- Biometric Authenticated Connection Establishment (BioPACE)
- Replace password with PI generated from biometric

Fast IDentity Online Alliance (FIDO)



https://fidoalliance.org/

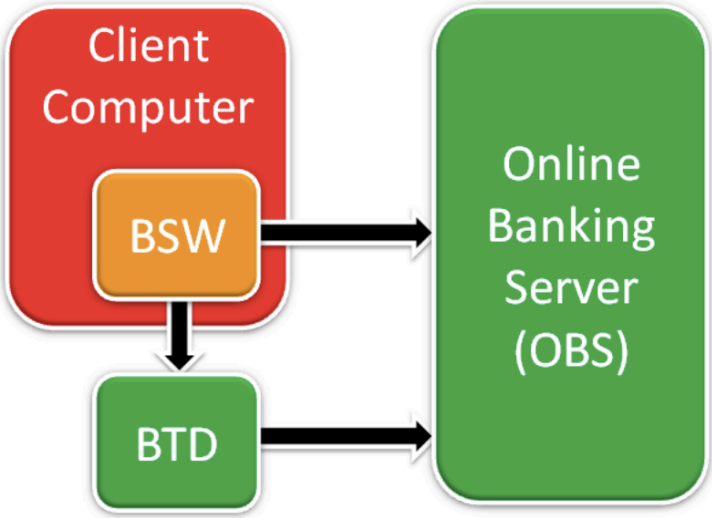
NTNU

Biometric Transaction Authentication Protocol (BTAP)

- Add biometric factor to the transaction
- Similar security to token based systems
- Enables non-repudiation
- Biometric template protection

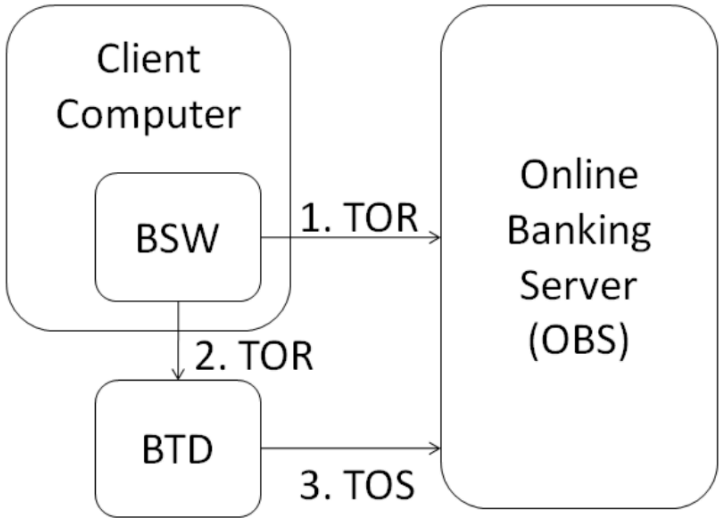
BTAP entities

- Banking software on client computer
  - Potentially vulnerable
- Biometric transaction device
  - Assumed to be secure
- Online Banking Server
  - Communicates with client and BTD



Transaction Authentication protocol

- Transaction order record (TOR)
  1. Transaction id
  2. Sender id
  3. Receiver id
  4. Amount
- Transaction order seal (TOS)
  - Message Authentication Code
- TOS recreated on server



NTNU

Banking Server

- Enrolment protocol:
  1. Generate unique secret
  2. Communicated to BTD
  3. Secret stored as hash value

- Transaction Authentication Protocol
  1. Receives TOR from client
  2. Receives TOS from BTD
  3. Recreates TOS using TOR and hashed secret
  4. Transaction verified if and only if both TOS are equal

Biometric Transaction device

- Enrolment protocol
  1. Receives secret from banking server
  2. Acquire biometric data from user
  3. Calculate auxiliary data from secret and biometric data
  4. Non sensitive auxiliary data stored on the device

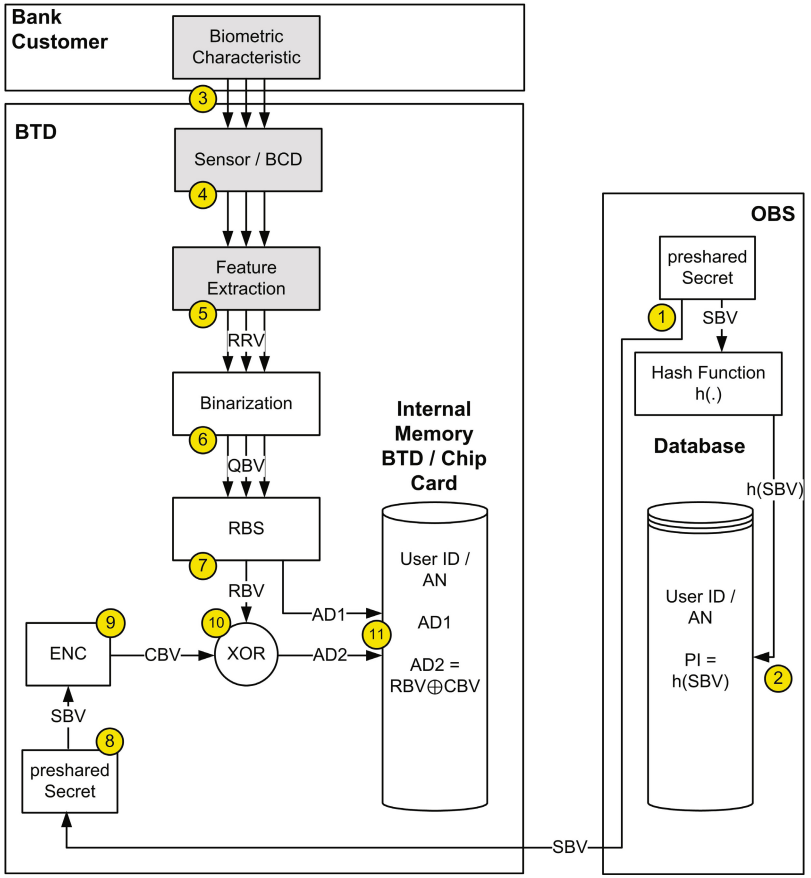
Biometric Transaction Device

- Transaction Authentication Protocol
  1. Receive TOR from banking software
  2. Recapture biometric data from user
  3. Recreate secret key from biometric data and stored auxiliary data
  4. Use hashed secret key to seal TOR
  5. Communicate TOS to online banking server

Biometric transaction authentication protocol (BTAP)

Transaction data communicated from client to biometric transaction device And banking server

Transaction verified on server using pseudonymous identifier



Hartung, Daniel, and Christoph Busch. "Biometric transaction authentication protocol: Formal model verification and “Four-eyes” principle extension."

Practical Implementation

Challenges

- How was the user enrolled in the system?
- Acquire samples conveniently with good quality
- Securing the biometric data to protect the privacy of the users without loss of accuracy
- Communicating the result of biometric authentication result remote location

NTNU

Thanks for your attention!

Questions?

Citations

1. Buchmann, Nicolas, et al. "Towards electronic identification and trusted services for biometric authenticated transactions in the single euro payments area." *Privacy Technologies and Policy*. Springer International Publishing, 2014. 172-190.
2. Hartung, Daniel, and Christoph Busch. "Biometric transaction authentication protocol: Formal model verification and “Four-eyes” principle extension." *Financial Cryptography and Data Security*. Springer Berlin Heidelberg, 2011. 88-103.