Biometric Authentication Protocols

Verification of Online Banking Transactions

NTNU

Motivation

- Biometric authentication is more convenient and can provide better security than traditional authentication methods
- Smartphones enable low cost rollout of biometric authentication in new areas, like finance applications, to reduce the risk of fraud

Objectives

- Enable biometric authentication for online banking transactions
- Reduce the possibility of misuse in online banking applications
- Provide scalable security depending on transaction values
- Protect all biometric data to preserve user privacy

Approach

- Use smartphones to acquire samples of biometric characteristics (face, eye, finger and voice)
- Local authentication to avoid transmitting biometric data over network and storage in remote location
- Biometric template protection to prevent exploitation of stolen biometric data and protect user privacy
- Biometric fusion to increase biometric accuracy and robustness
- Use a pseudonymous identifier, generated from transaction and biometric data, for verification in remote location

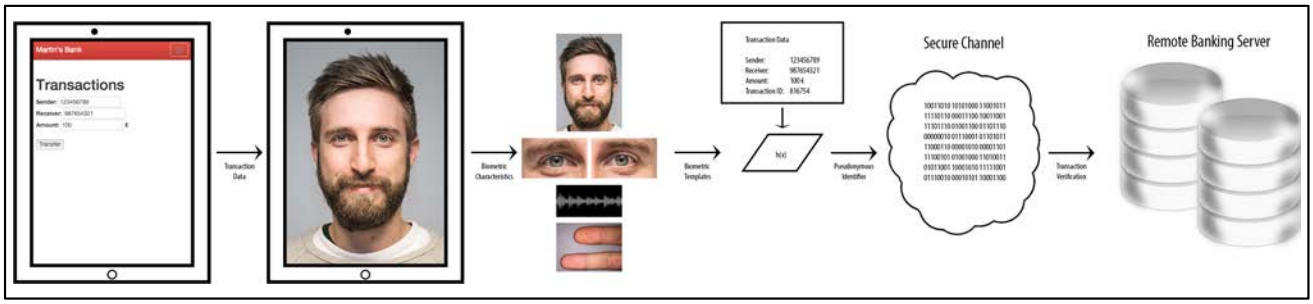

Fig. 1 Banking client is used to initiate a transaction. Smartphone performs biometric authentication, generates a pseudonymous identifier and transmits to remote banking server for verification.

The Research Council of Norway

Martin Stokkenes
martin.stokkenes2@ntnu.no

Dr. Raghavendra Ramachandra
raghavendra.ramachandra@ntnu.no

Prof. Dr. Christoph Busch
christoph.busch@ntnu.no

Norwegian University of Science and Technology – Norwegian Biometrics Lab