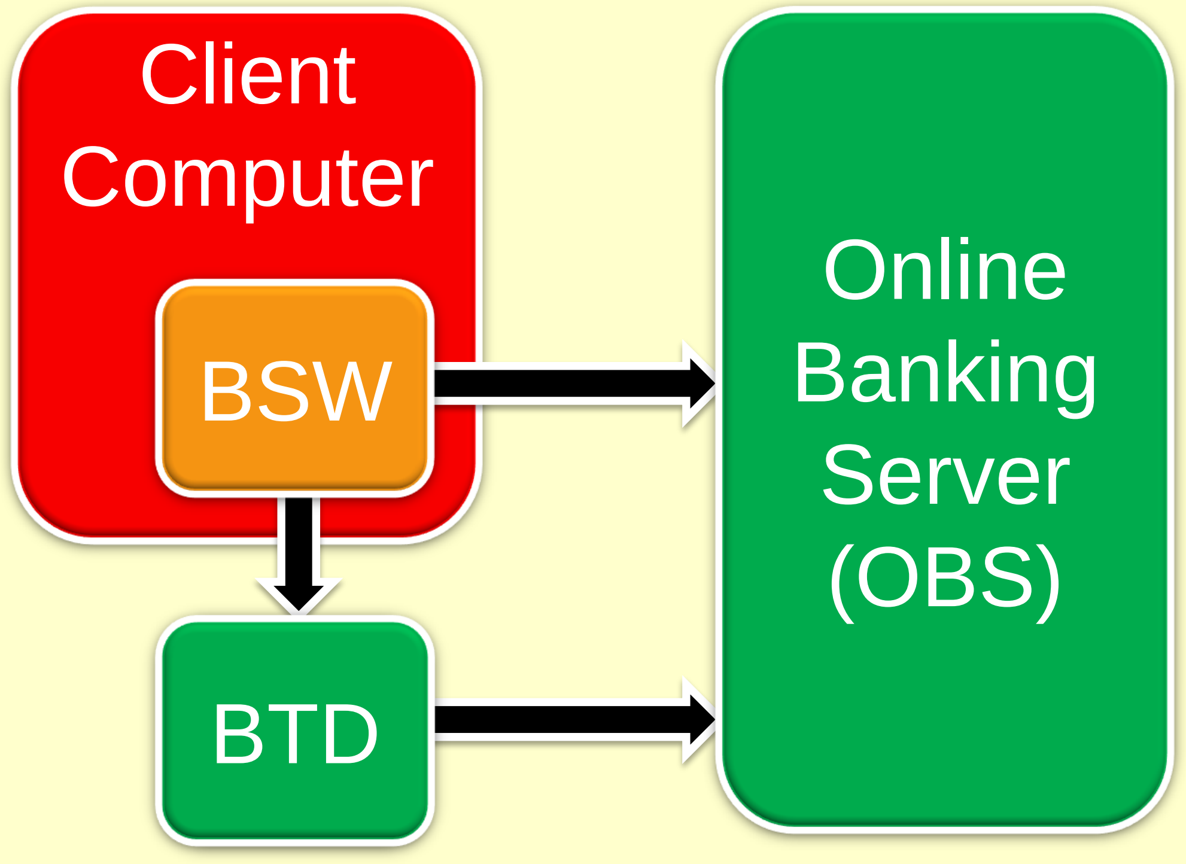
Biometric Transaction Authentication Protocol (BTAP) - Overview

Motivation

- Online-Banking is increasingly targeted by attacks based on malware e.g. on phishing software
- Increase in malware infected clients that can be manipulated
- Online banking is based on PINs, tokens or signatures, which can be delegated

Scenario

- Potentially malware manipulated client computer running banking software (BSW)
- Online banking authentication in the home- or office environment
- Secure banking server communicating with trusted, tamper-proof biometric transaction device (BTD)
- Verification of the transaction receiver and amount by the natural person



Goals

- Strong binding of natural person and transaction information
- Ensure authenticity and integrity of the transaction data, independent from state of the client
- Data privacy protection

Solution

- Biometric system with spoofing resistant sensor
- Encapsulation of critical functionality on trusted secure environment
- Tamperproof hardware design with minimal provable security features
- Modular system
- Strict compliance with data privacy regulations
- No storage of biometric data on the server side

Related Work

- ISO/IEC 24745: Information technology - Security techniques - Biometric information protection
- Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2009

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

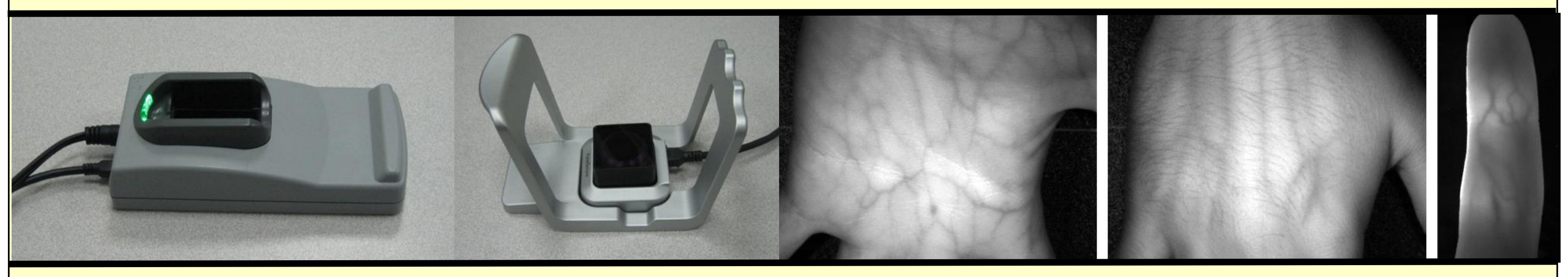
Daniel Hartung
daniel.hartung@hig.no

Gjøvik University College – Norwegian Biometrics Lab

Biometric Transaction Authentication Protocol (BTAP) - Details

Biometric Subsystem

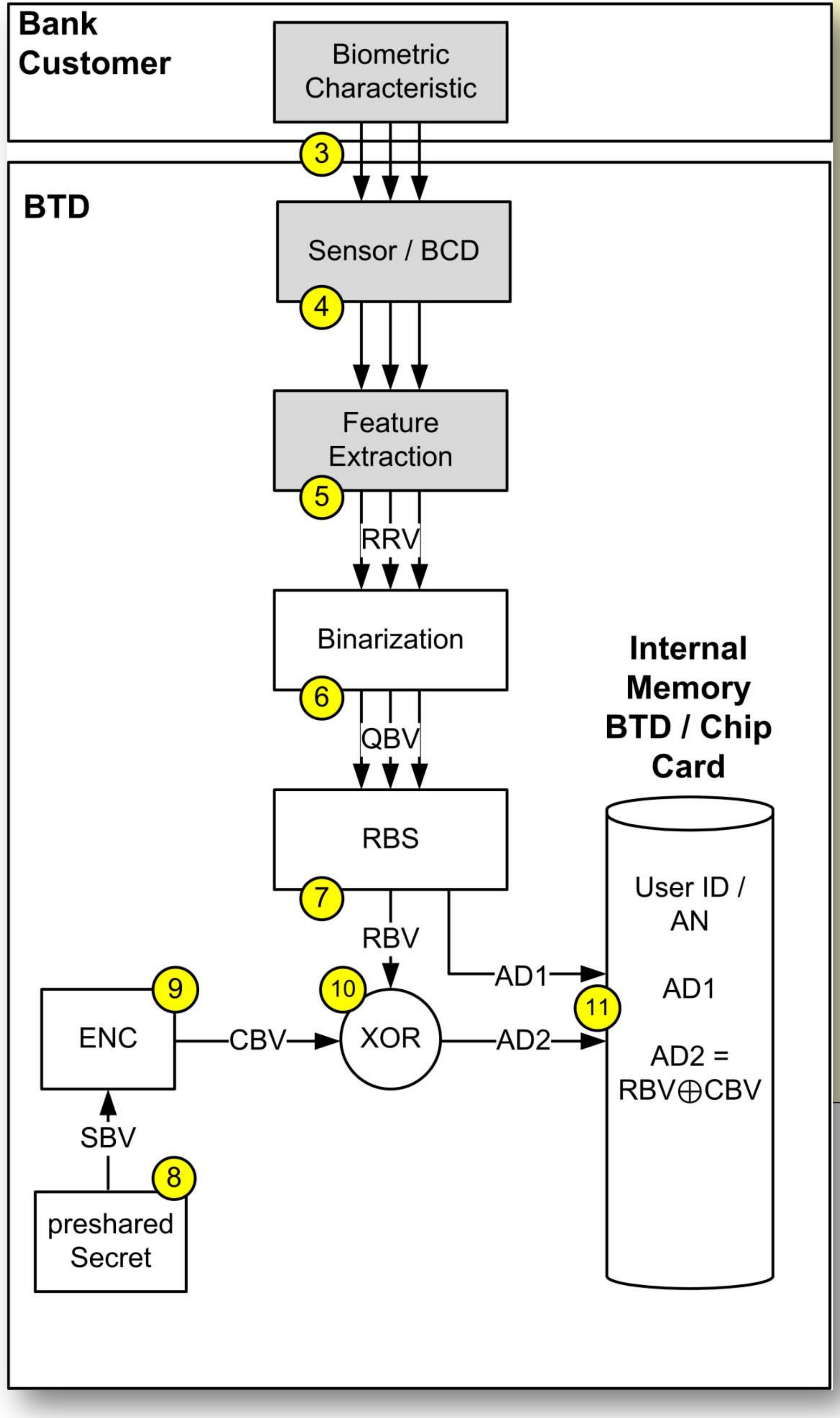
- Spoofing resilient biometric sensor, e.g. based on Vein Pattern Recognition



- Helper Data Schema for the protection of the biometric templates

Enrolment

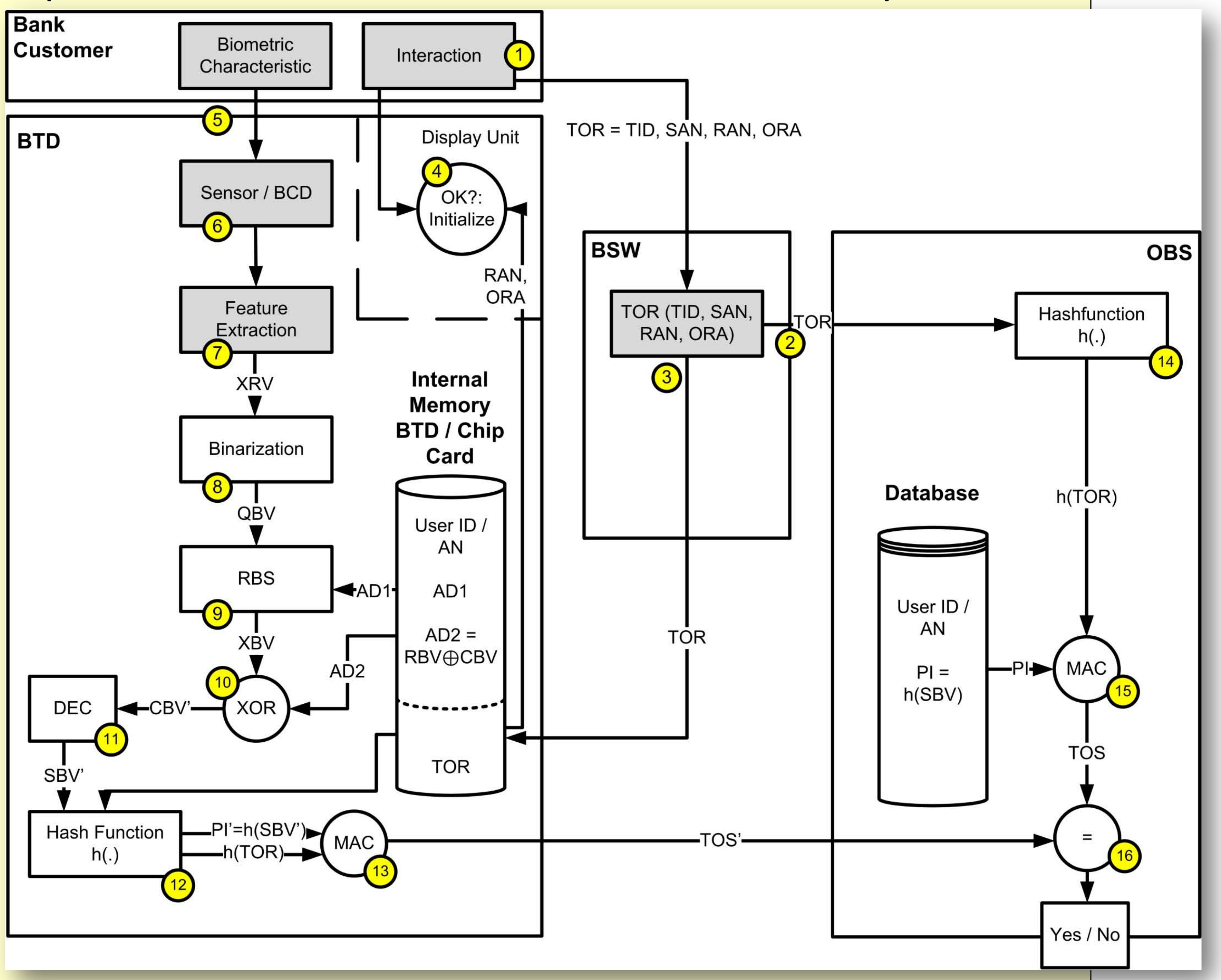
- Biometric samples of the customer are captured, a binarized feature vector QBV and helper data AD1 (information about the reliability of the vector elements) are derived from it, resulting in a binary reference feautre vector RBV – the reliable information from QBV
- Customer enters secret SBV, which was created by the online banking server OBS and send e.g. via regular post



- An error correction encoder creates a codebook vector CBV from SBV
- CBV and RBV are fused using the XOR operation resulting in helper data AD2
- Enrolment in the OBS: create bank account AN and pseudo-identifier PI = hash (SBV), send SBV to customer

Transaction Authentication

- Customer creates Transaction order record TOR with banking software BSW, BSW sends TOR to OBS and to the biometric trusted device BTD
- Relevant information from TOR is displayed on BTD: e.g. Receiver-Account-Number (RAN) and Ordered Amount (ORA)
- For the transaction authentication the customer has to present his/her biometric trait to the BTD, a sample is taken



- Helper data AD1 is released to compute the reliable probe vector XBV from the binarized probe sample
- Codebook vector CBV’ is reconstructed from helper data AD2 and XBV, (CBV‘=XBV xor AD2)
- Error correction code is applied to compute secret SBV’ from CBV’, the hash of CBV‘ results in the pseudo identifier PI’
- The transaction order seal TOS’, which constitutes a MAC from hash(TOR) and reconstructed PI’ the transaction data with the natural person
- OBS receives TOR from the unsecure banking software BSW and TOS’ from BTD. Has the original PI for the customer and reconstructs TOS independently
- Compares reconstructed TOS with the TOS‘ send by BTD: If TOS == TOS’, transaction data is authentic and verified by the enrolled customer

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

Daniel Hartung
daniel.hartung@hig.no