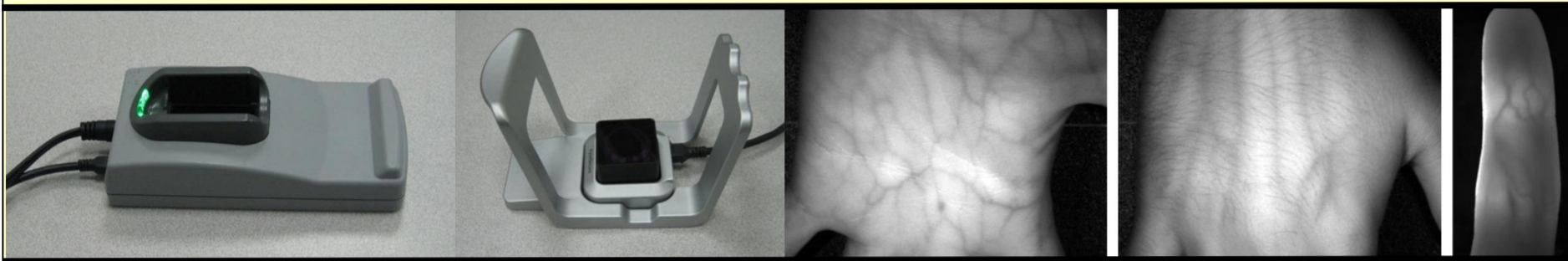


Biometric Transaction Authentication Protocol (BTAP) - Details



Biometric Subsystem

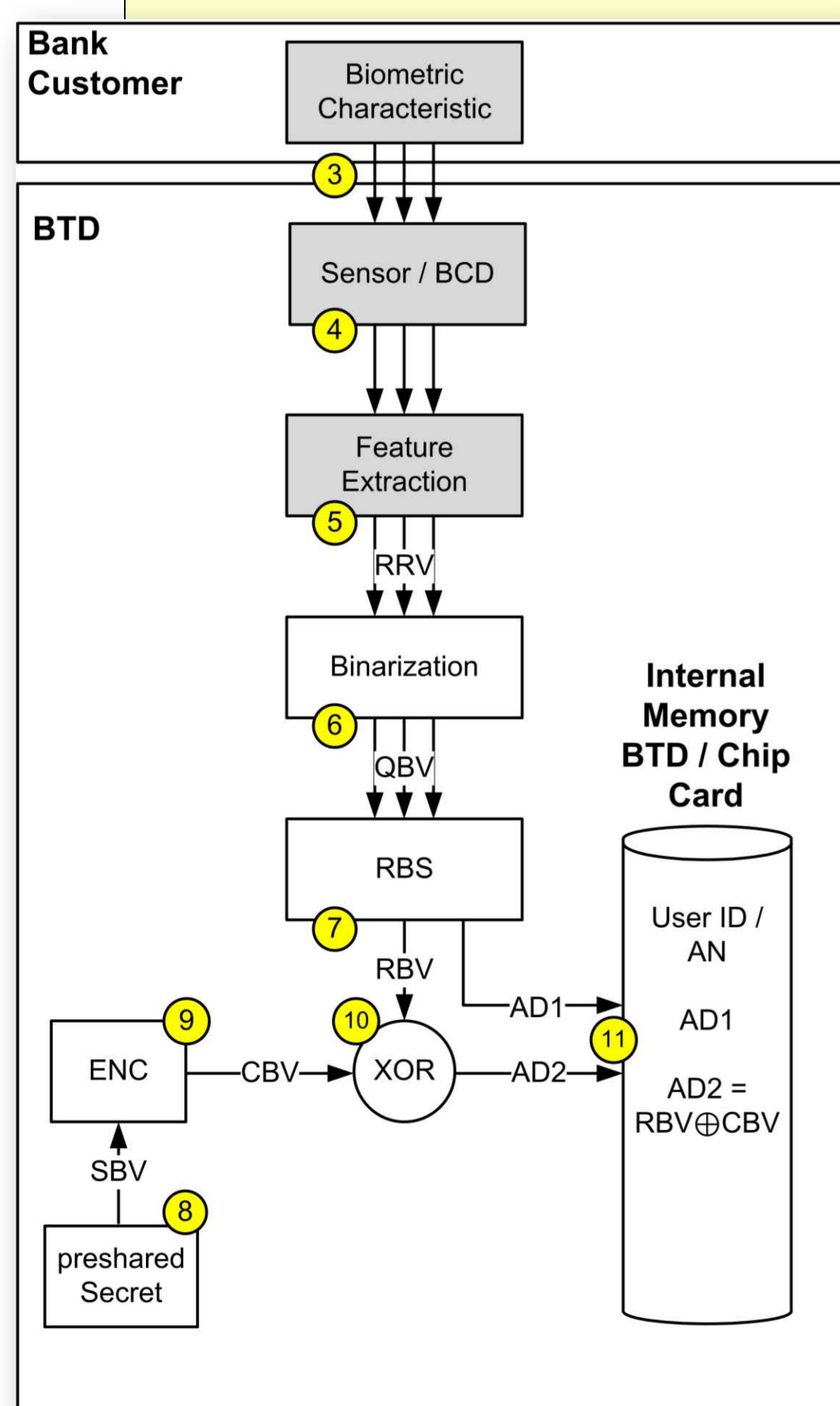
- Spoofing resilient biometric sensor, e.g. based on Vein Pattern Recognition



- Helper Data Schema for the protection of the biometric templates

Enrolment

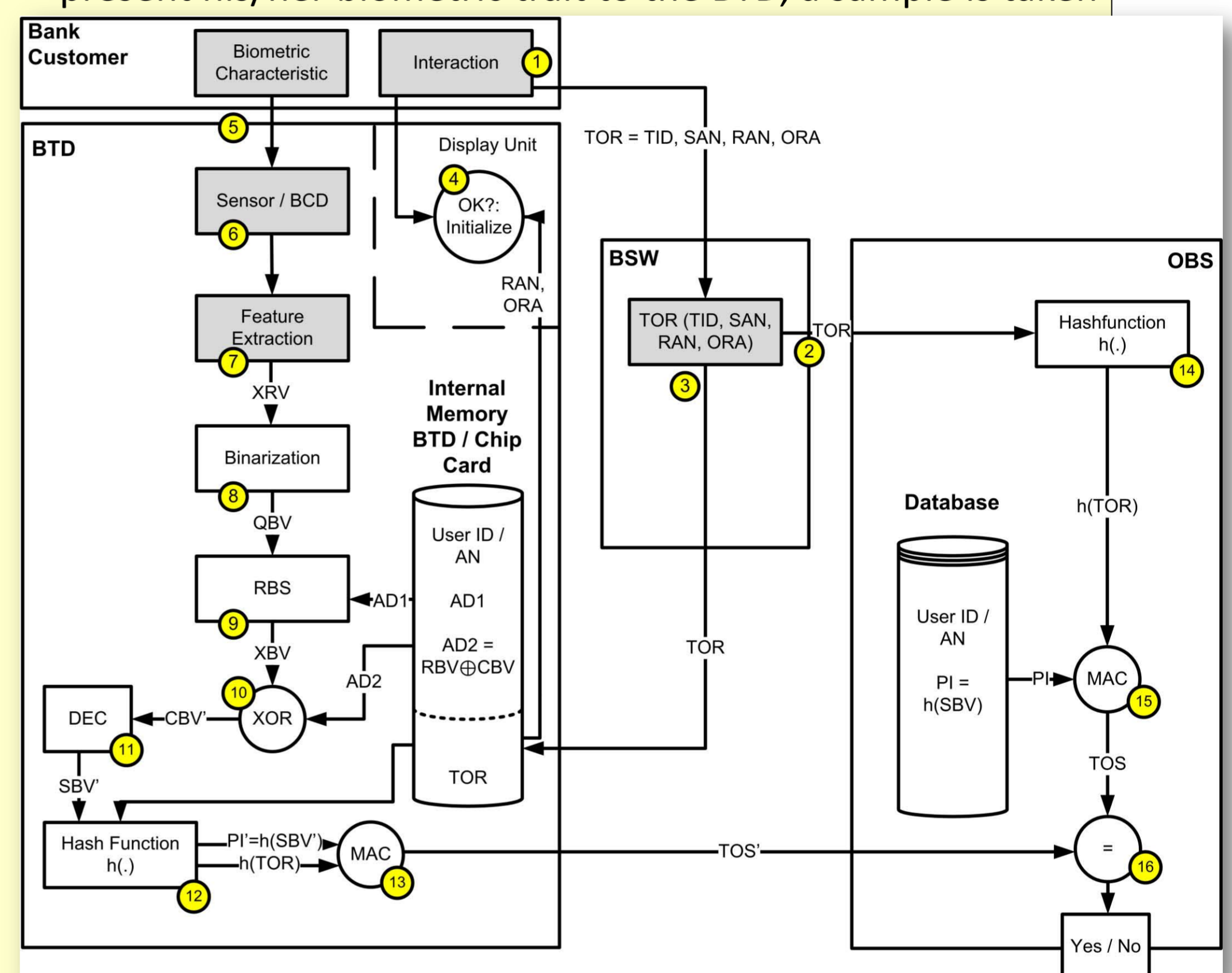
- Biometric samples of the customer are captured, a binarized feature vector QBV and helper data AD1 (information about the reliability of the vector elements) are derived from it, resulting in a binary reference feature vector RBV – the reliable information from QBV
- Customer enters secret SBV, which 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 $PI = \text{hash}(SBV)$, 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 XB from the binarized probe sample
- Codebook vector CBV' is reconstructed from helper data AD2 and XB, ($CBV' = XB \text{ xor } AD2$)
- 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 $\text{hash}(TOR)$ 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