

Secure Access Control over Wide Area Network

Christoph Busch

Gjøvik University College
<http://www.christoph-busch.de>

ISF julemøte

Oslo - November 18th, 2015



The SWAN Project

SWAN - Secure Access Control over Wide Area Network

- IKTPLUS program
- October 2015 - September 2019
- Funding of 23.055.000 NOK
- Partners from 4 European countries



The SWAN Consortium

Partners:

- Norwegian Biometrics Laboratory (NBL)
@ Gjøvik University College (GUC)
- Department of Informatics @ University of Oslo
- Morpho, France
- Institut de Recherche Idiap, Switzerland
- Association of German Banks, Germany
- Zwipe AS, Oslo



Sponsor: IKTPLUS



Access Control

Authentication can be achieved by:

- Something you **know**:
Password, PIN, other secret
- Something you **own**:
SmartCard, USB-token, key
- Something you **are**:
Body characteristics

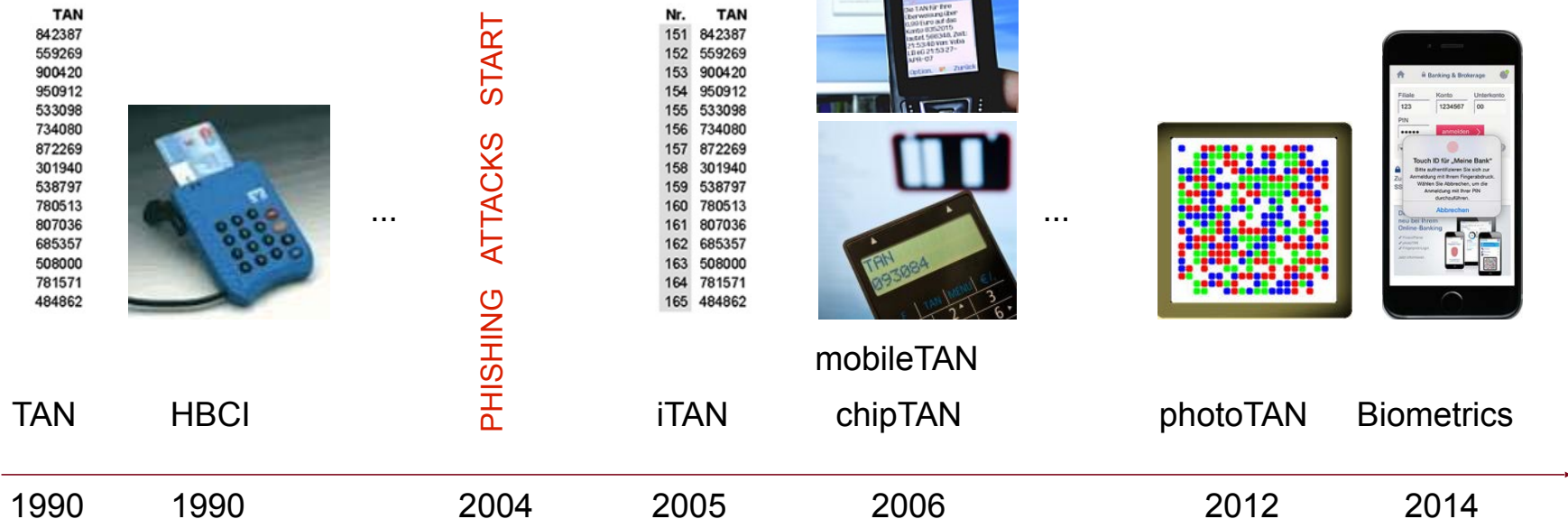


Something you know or own
you may **lose**, **forget** or **forward** to someone else,
with biometrics this is more difficult.

- security policy not violated by delegation
- non-repudiation of transactions
„This was initiated by *Igor Popov* misusing my card“

Access Control in the Banking Environment

A European perspective



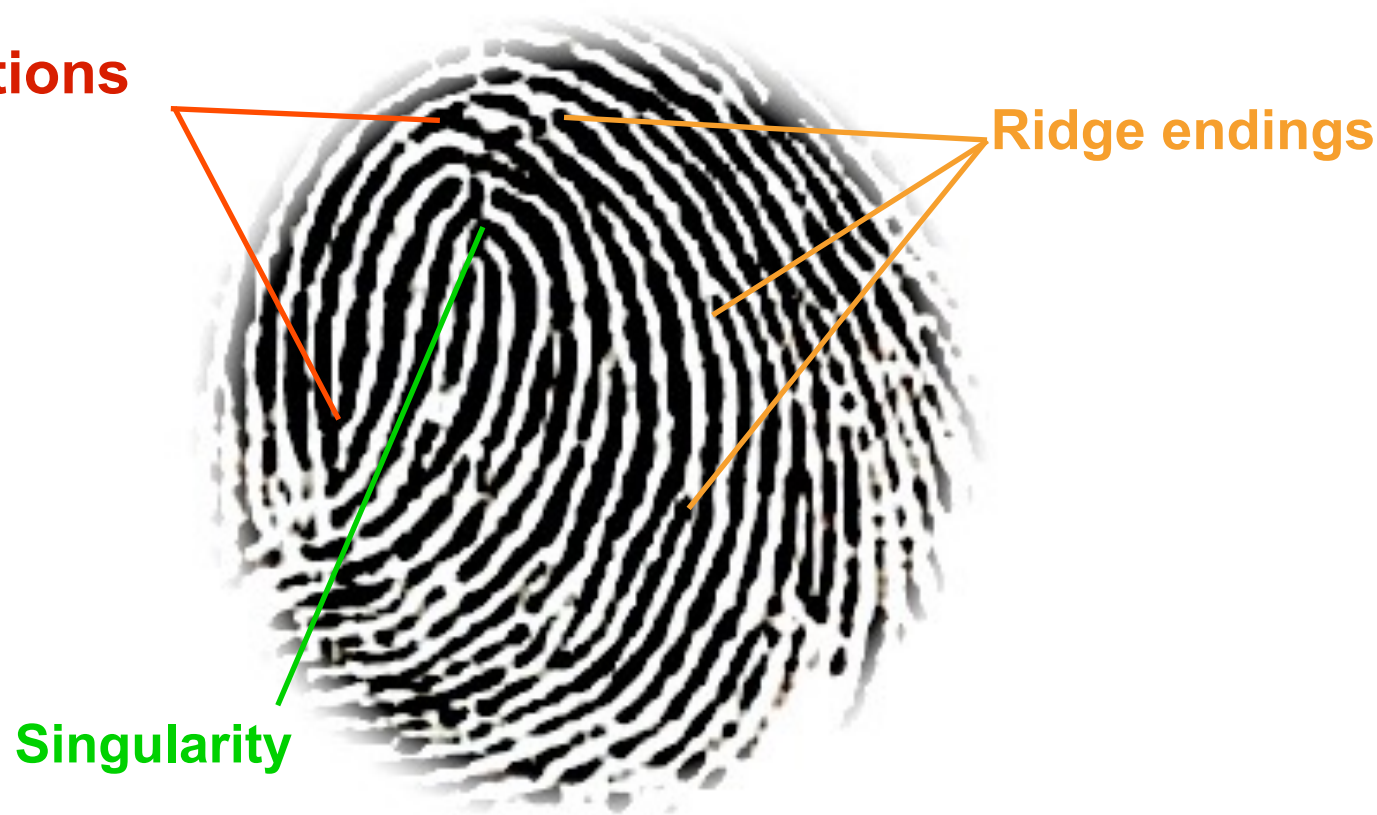
Source: BdB (2015)

Biometrics - Fingerprint Recognition

Analog/digital representation of the finger ridges

- Distinguished points of the fingerprint: **Minutia**

Bifurcations



Biometrics and Access Control

Automated Border Control in Europe

- Automated but supervised border control since 08'2009
- Self-Service to increase throughput



US VISIT

- Visitors with a criminal record are rejected



Source: US Visit

Smartphone Access Control

Foreground authentication (user **interaction**)

- Deliberate decision to capture (willful act)
- **Camera**-Sensor
 - ▶ **Fingerprint** recognition
 - Apples iPhone 5S / Samsung Galaxy 5
 - Finger**photo** analysis
 - ▶ Face recognition
 - ▶ Iris recognition
- Touchpad: allows signature recognition



Image Source: Apple 2013

Background authentication (**observation** of the user)

- Microphone
 - ▶ **Speaker** recognition
- Accelerometer
 - ▶ **Gait** recognition
 - ▶ concurrent - unobtrusive



Biometric Speaker Recognition

Offer an **unobtrusive** or **explicit** authentication method

- Use embedded microphone in mobile device to record the voice signal
 - ▶ unobtrusive or
 - ▶ apply willful act for explicit transaction authorization
 - ▶ no extra hardware is needed



Biometric Finger Recognition

Capture process

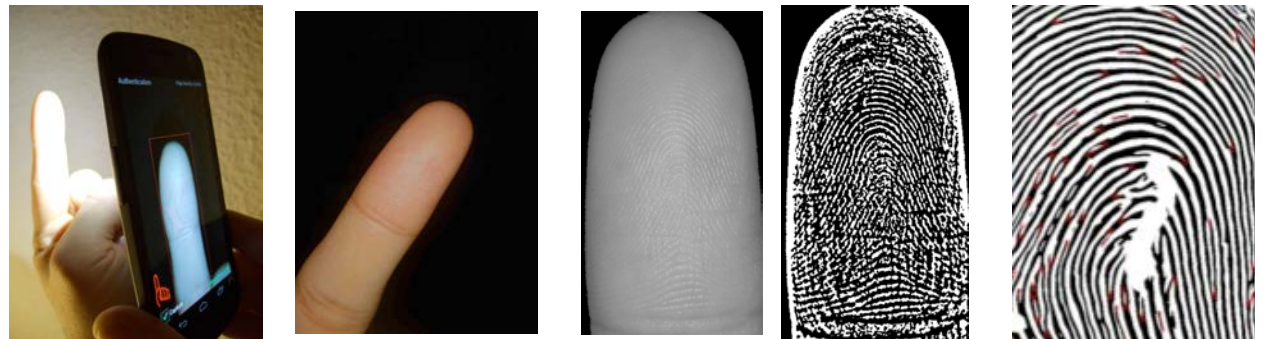
- Camera operating in **macro** modus



Preview image of the camera with LED on (left) and LED off (right)

- LED permanent on

Finger illuminated

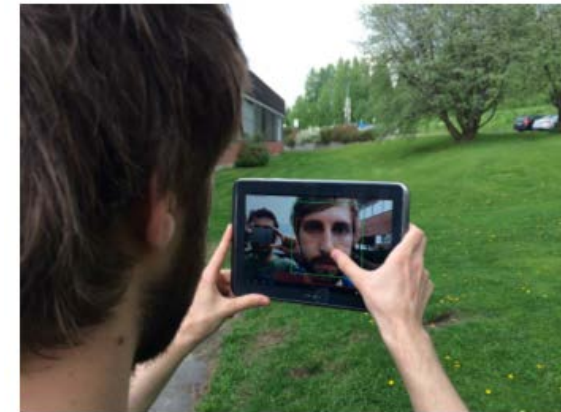


[SNB12] C. Stein, C. Nickel, C. Busch, „Fingerphoto Recognition with Smartphone Cameras“, Proceedings 11th Intern. Conference of the Biometrics Special Interest Group (BIOSIG 2012)

Biometric Eye Recognition

Images captured with either front or back camera

- Challenges
 - ▶ face and eye localization



[RRSB14] K. Raja, R. Raghavendra, Martin Stokkenes, Christoph Busch: „Smartphone Authentication System Using Periocular Biometrics“, (BIOSIG 2014)

Security ?

Operators **will** think:

*„The biometric **sensors** must be robust against fake attacks“*



Gummy Finger Production in 2000 !

Attack **without** support of an enrolled individual

- Recording of an analog fingerprint from flat surface material
 - ▶ z.B. glass, CD-cover, etc.
with iron powder and tape
- Scanning and post processing:
 - ▶ Correction of scanning errors
 - ▶ Closing of ridge lines (as needed)
 - ▶ Image inversion
- Print on transparent slide
- Photochemical production of a circuit board mold



Privacy Protection ?

Operators **will** think:

*„Biometric systems must be **compliant** to data privacy and data protection principles“*

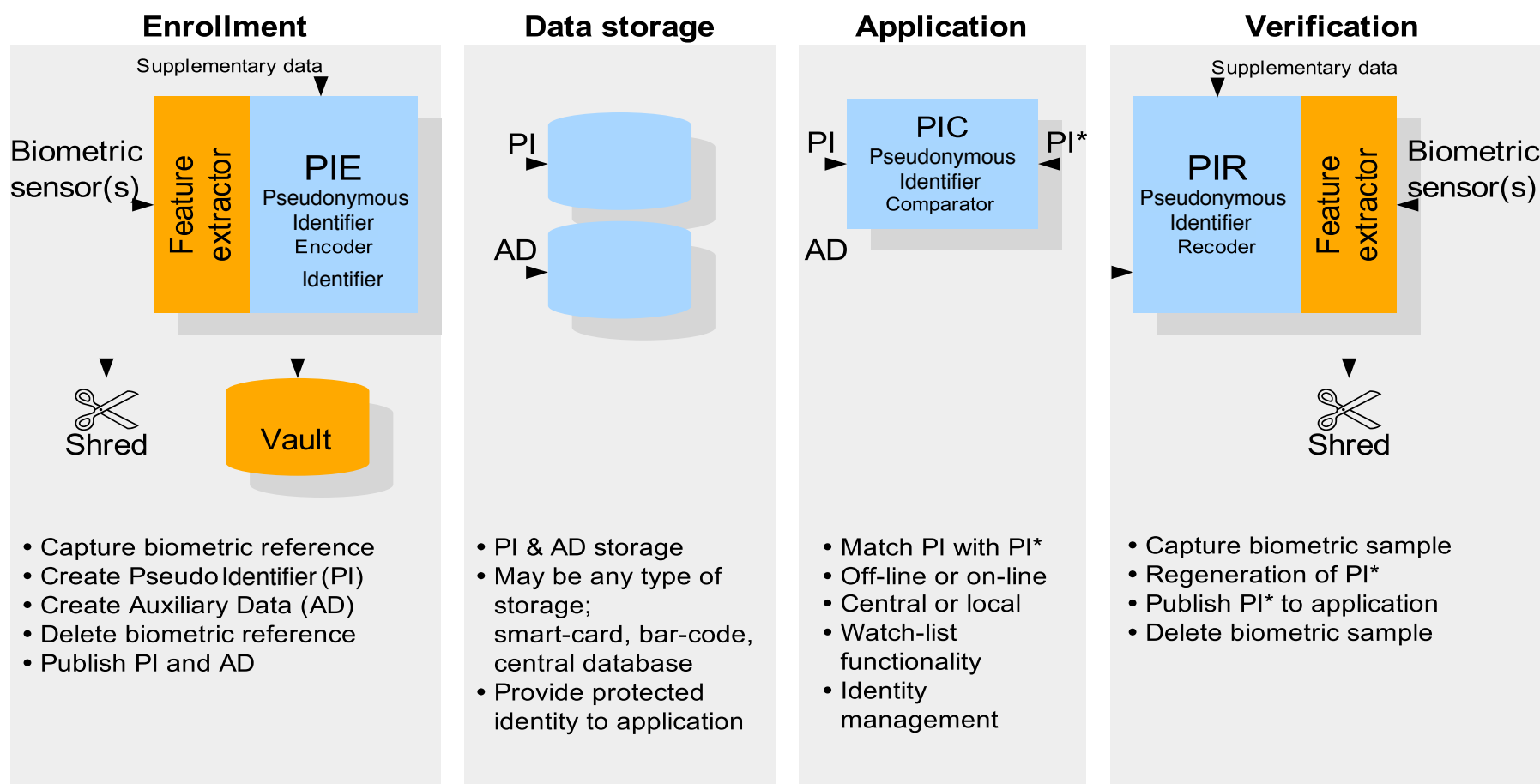


Data Protection Requirements

Technical framework on how to implement requirements for data privacy and data protection



- **exists** ISO/IEC 24745: Biometric Information Protection, (2011)
http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=52946



Mobile Biometric Payment - Biometric Transaction and Authentication Protocol (BTAP)

Biometric Transaction Authentication

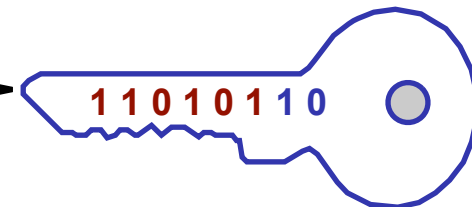
Biometric Transaction Authentication Protocol (BTAP)

1.) Shared **secret**

- received via subscribed letter from the bank
- entered **once** to the smartphone
- ▶ hash over the secret constitutes a **Pseudonymous Identifier (PI)**



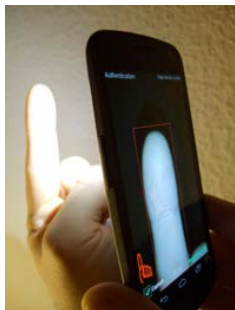
PIN = 4768



CodeBookVector (CBV)

2.) Biometric enrolment

- Biometric samples are captured



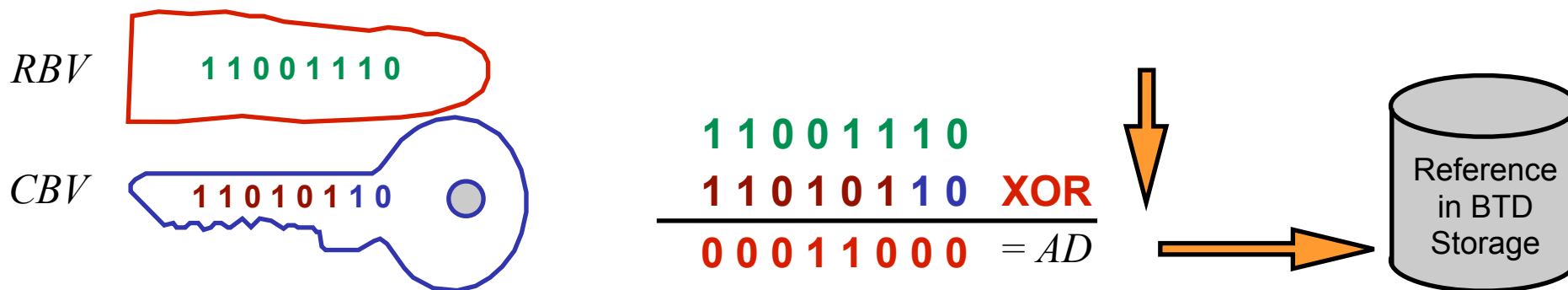
ReferenceBinaryVector (RBV)

Biometric Transaction Authentication

Biometric Transaction Authentication Protocol (BTAP)

3.) Secure storage of **auxilliary data**

- we neither store the confidential secret nor the sensitive biometric data (i.e. feature vector)
- the secret and biometric data are **merged**

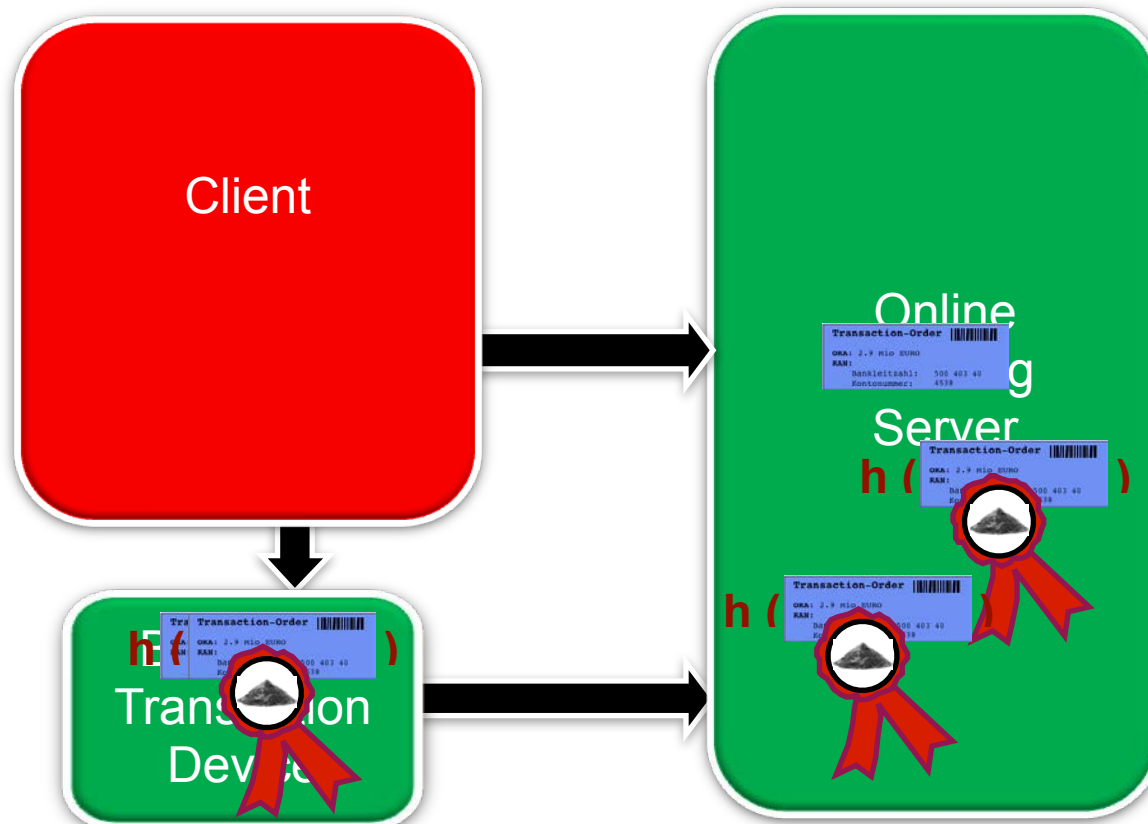


- Auxiliary data (AD) stored in the Smartphone
 - Biometric Transaction Device = FIDO Authenticator

Transaction-Verification

Key features of BTAP

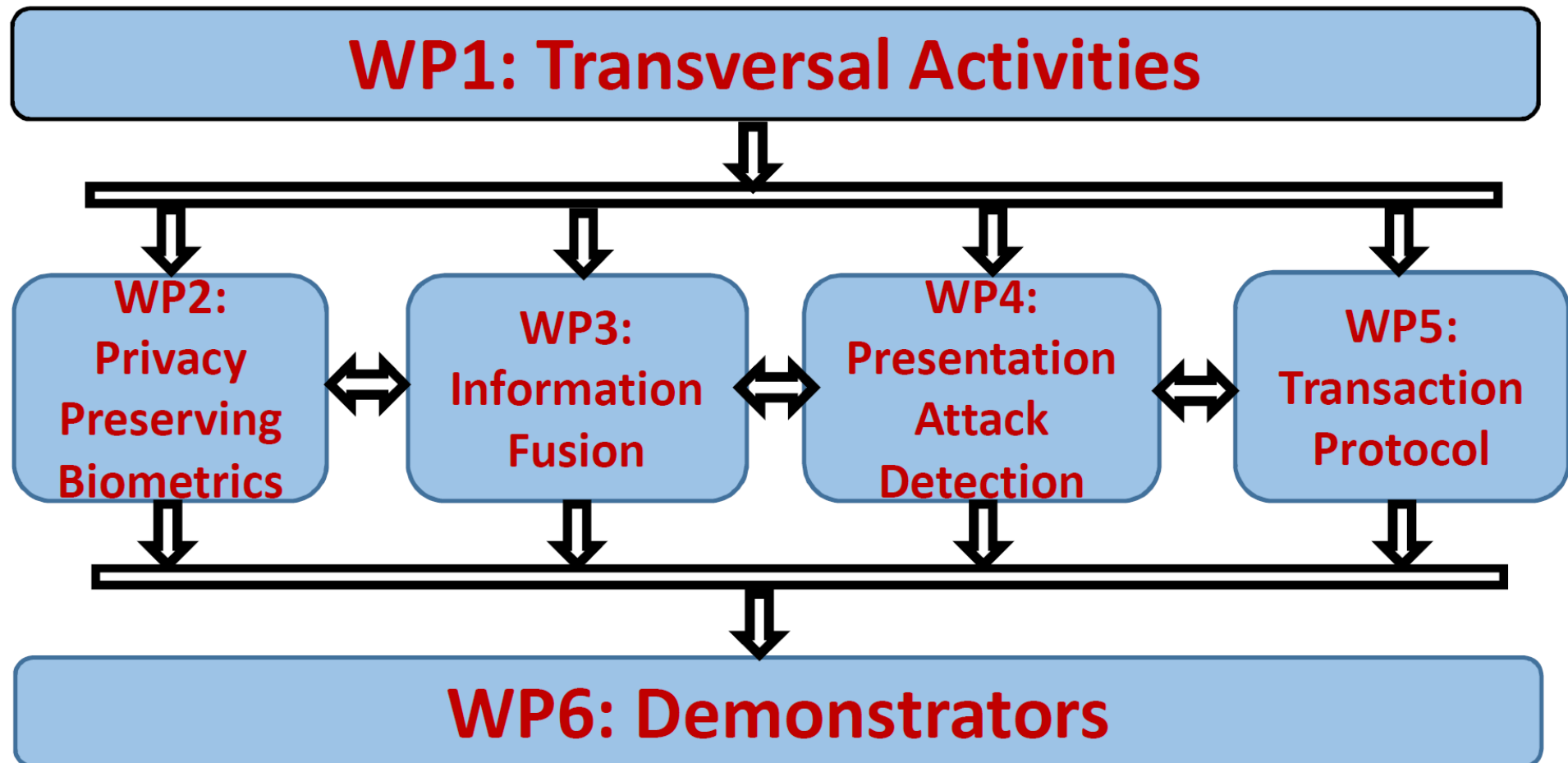
- independent **two channel** verification
- **reconstruction** of shared secret
- the Pseudonymous Identifier (PI) constitutes a seal
- **seal operation** over the TOR to authenticate the transaction



Objectives

- To develop and demonstrate **biometric** solutions that are fast, trustworthy and secure for real-time authentication of individuals at banking transactions.
- To enable privacy-preserving bank transaction authentication protocols over wide area network with a **privacy-by-design** approach.
- To study vulnerabilities and limitations of the biometric **modalities** such as a 2D face, fingerprint, eye, and voice
- To develop **transaction authentication** protocols using biometrics that can overcome the need for centralized storage of biometric data.

Work Structure



Invitation

SWAN-project end-user group is meeting

- February 24th in Gjøvik
- Banking representatives are invited

Annual Workshop of the
Norwegian Biometrics Laboratory (NBL)

- February 25th in Gjøvik
- You are welcome to visit the NBL on that occasion



Conclusion

Biometrics is possible with today's smartphones

- a **multi-biometric** authentication scheme with **scaling factors** is a good choice with respect to security threats

Biometric **standards** are **available**

- financial transaction schemes should follow **privacy** standards

BTAP follows the two channel concept

- is based on international ISO/IEC **standards**
- is **privacy friendly** as no biometric reference is stored on a banking server

More and detailed information on SWAN and BTAP at:

http://nislalab.no/biometrics_lab/swan

<http://www.christoph-busch.de/projects-btap.html>

Contact

Contact:

