Information Security
Identification and authentication

Advanced User Authentication I

2016-01-26

Amund Hunstad

Guest Lecturer, amund@foi.se

LiU *expanding reality*

Agenda for this part of the course

Background

Statistics in user authentication

Biometric systems

Tokens

Agenda for lecture I within this part of the course

Background

Statistics in user authentication

Biometric systems

Tokens

Authentication

eID

ePassports

Biometrics in general

Statistics

Fumy, W. and Paeschke, M. Handbook of eID Security

A. Jain, A. Ross and K. Nandakumar, Chapters 1 in "Introduction to Biometrics"

User authentication/identification

Can in an IT system be achieved via

What I know – passwords, PIN

What I have – ID-cards, smart-card, token

What I am/do – biometrics

Identification

Authentication

I AM MORDAC, THE PREVENTER OF INFORMATION SERVICES, AND I BRING YOU MY NEWEST BIOMETRIC SCANNER.

INSTEAD OF A PASSWORD, I PUT THIS ON YOUR HEAD AND SQUEEZE UNTIL YOU SCREAM IN A WAY THAT ONLY YOU CAN SCREAM.

NO, THAT'S NOT YOU.

GAAA! GAAA! GAAA!

© Scott Adams, Inc./Dist. by UFS, Inc.

Human ID identification/authentication: Used when, where and why?

Forensics: Does a suspect match the features of a criminal

Banking/Financial services: Money only to its owners

Computer & IT Security: Access only to those authorised

Healthcare: Correct patient history (and billing)

Immigration: Blocking unwanted residents in spe

Law and Order: Punishing the correct person

Gatekeeper/Door Access Control: Access only if authorised

Telecommunication: Billing, trust base and privacy

Time and Attendance Logging: For future audit

Welfare: Only to valid beneficiaries

Consumer Products: Against unauthorised use, liability etc.

LiU

Biometric examples

SAS – Scandinavian Airline Systems: Fingerprints used to tie the person who checked in luggage to the person who passes the passenger gate.

OMX Group:To enter to most secret part of the company you have to authenticate yourself in an iris scan.

A school in Uddevalla, Sweden: To enter the dining area you needed to identify yourself with your fingerprint.

Disney World, SeaWorld and other amusement parks and entertainment centers: Fingerprints to tie tickets to their users

Fingerprint in third world applications

Authentication requirements

Can be presented only by the correct person

Only the correct person knows the value

Only the correct person can physically present the value

Has enough diversity to be unique enough

Truly unique, can be used for identification

Overlap very unlikely, can be used for authentication

eID: Electronic identity

Then: Manual ID control, e.g. in a bank or post office

Now: Transactions & communication online

Future: Internet of things

eID: Challenges

- New possibilities for criminal activity

  - Public administration, businesses and citizens act within digital networks

- Phishing

- Social engineering

- ID theft, Identity fraud

- Cyber attacks on personal data

- Spoofed websites

- Compromised log-in accounts

eID-threats and risks: Do I have to care?

- 2010: ID fraud survey

  - 5% US population victims of ID theft

  - 13% of ID fraud crimes by someone the victim knew

  - Financial losses

  - Re-establishing attacked ID: On average 21 hours

- Verification & authentication process less transparent than offline

LiU

eID: Necessary qualities

- Trust

- Data control

- Usability

- Interoperability

  - Mutual trust for administrations

  - Provide various security levels for eID services

  - Context sensitive approach

  - Provide private sector participation

eID: Necessary qualities

- ## Role of personal devices

  - ### 2011

    - 6,8 billion inhabitants
    - **4,6 billion mobile phones**
    - 1,7 billion Internet users
    - 1.6 billion TV:s
    - 3,9 billion radios

- ## Privacy protection

  - Pseudonymity & anonymity

- ## Documentless proof of ID?

eID: Challenges

- Need to prove ID on the Internet

- Verify identity of virtual counterpart

  - In eCommerce

  - In eGovernment

- Solution:

  - eID

  - eID management

  - Provide critical infrastructures for electronic businesses and governement & administration

eID: Security measures

Security of the eID document

Cryptography

Security protocols

Biometric techniques

Security of eID chips

"**FIDELITY**: **F**ast and trustworthy **I**dentity **D**elivery and check with **e**Passports **l**everag**i**ng **T**raveler privac**y**"

The ePassport

High efforts to make **travel documents more secure**, especially since September, 11

Launch of the **ePassport**

specified by **ICAO**

most difficult to forge travel document ever

embedded chip
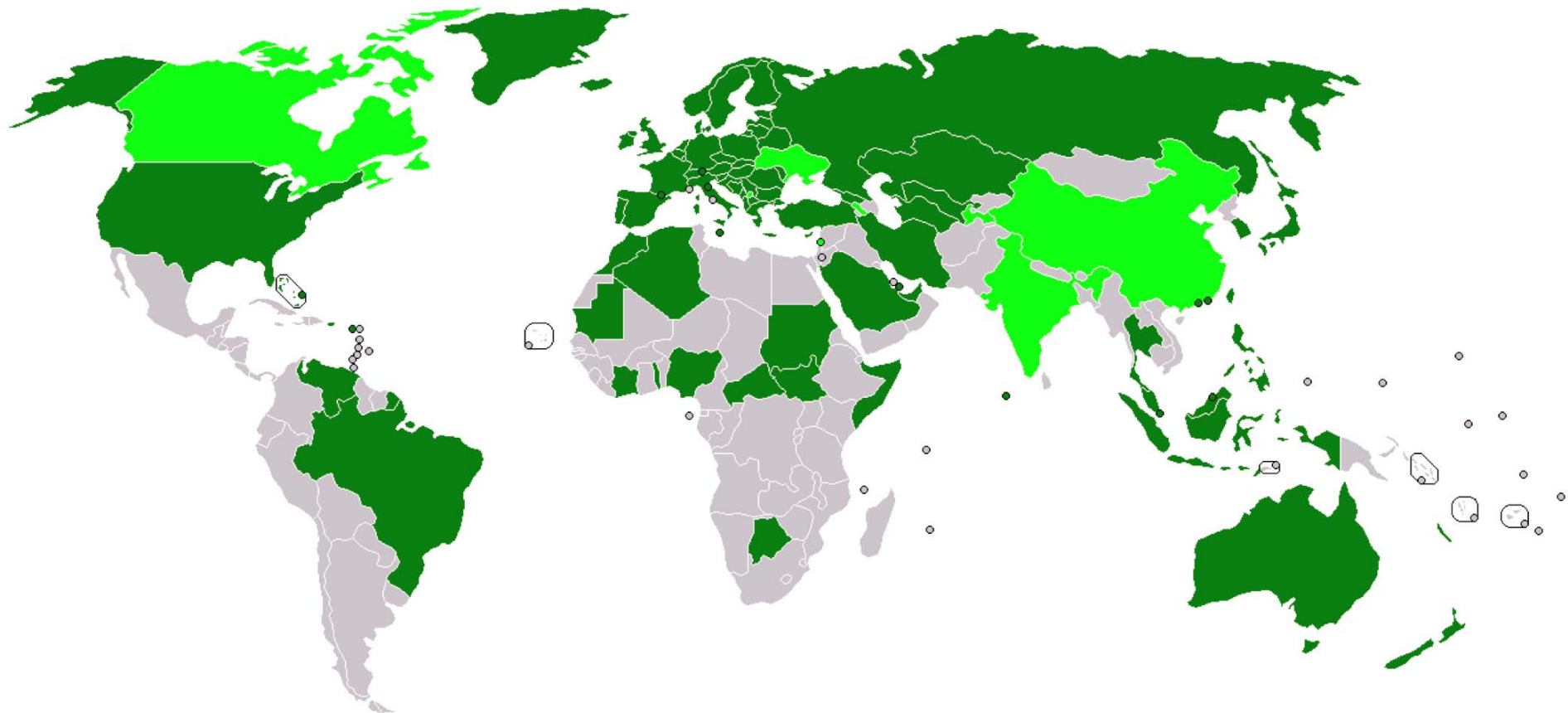
biometry for ID checks
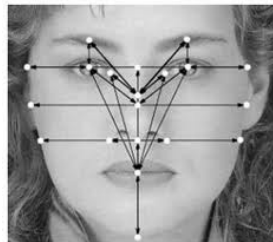
chip features & data

VIS   UV   IR
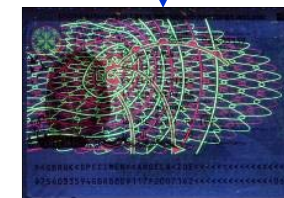
Success in ePassport deployment

345 million ePassports issued by 93 states
(ICAO estimates in July 2011)

Biometric passports available to the general public
Announced future availability of biometric passports

But ...

After several years of use, some weaknesses became apparent in

ePassport **issuing** process, security of **breeder documents**
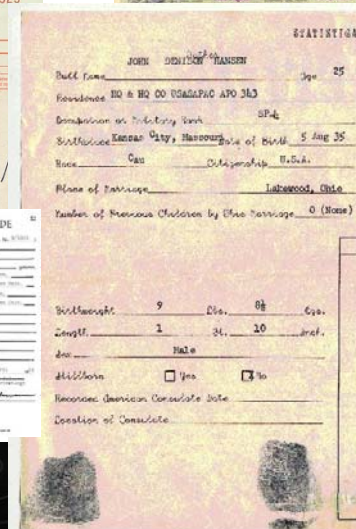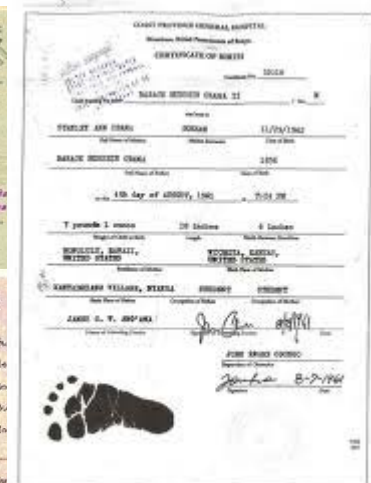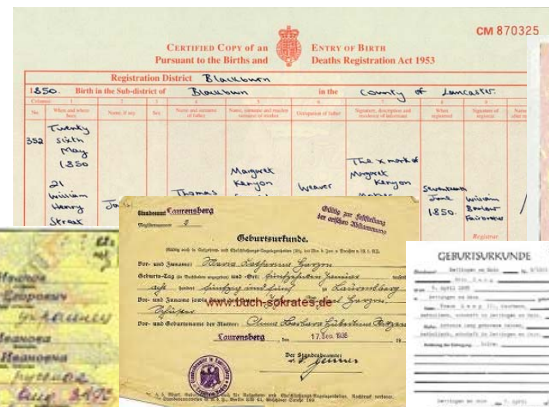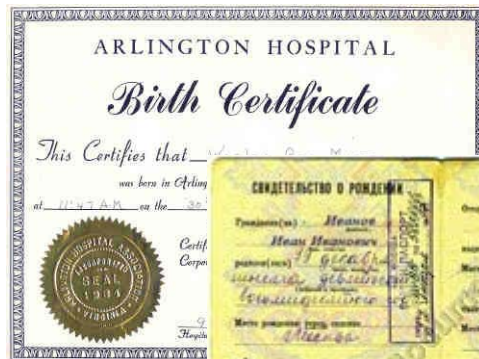
Speed of ID checks at borders

Connections with **remote data bases** (SIS, VIS, Eurodac, PNR, ...)

Certificates management

Personal data protection

Means to check quality of **biometrics** data

Revocation

Frontex study

Reliability of the e-passport issuance

Information exchange

Training (and possibly tool provisioning)

Compile good practices

Common guidelines

Inter-country review

Lookalike fraud with e-passports is a substantial risk for EU/Schengen border control.

Improve the quality of the digital facial image

Usage of fingerprints in border control

Frontex study

The usage of e-passport functionality is limited and not uniform.

Training of border guards

Deployment of e-passport inspection

Harmonisation of the inspection procedure

Collect real-life performance data from Automated Border Control system pilots

Experienced operational difficulties in deploying e-passport inspection infrastructures.

Public key infrastructures

Document signing certificates in the e-passports

"Defect lists" in inspection systems

Frontex study

Cloning of e-passport chips is a serious concern.

Authenticating the chip in all EU e-passports

Security of national identity cards is not standardised, weak link in border control. (C6)

Phasing out the usage of the SHA-1 secure hash function as part of signing e-passport information.

Frontex study

The technical security measures: Increasingly hard to circumvent & standardised to a high degree

Focus of fraudsters is shifting towards the inspection and issuance procedures.
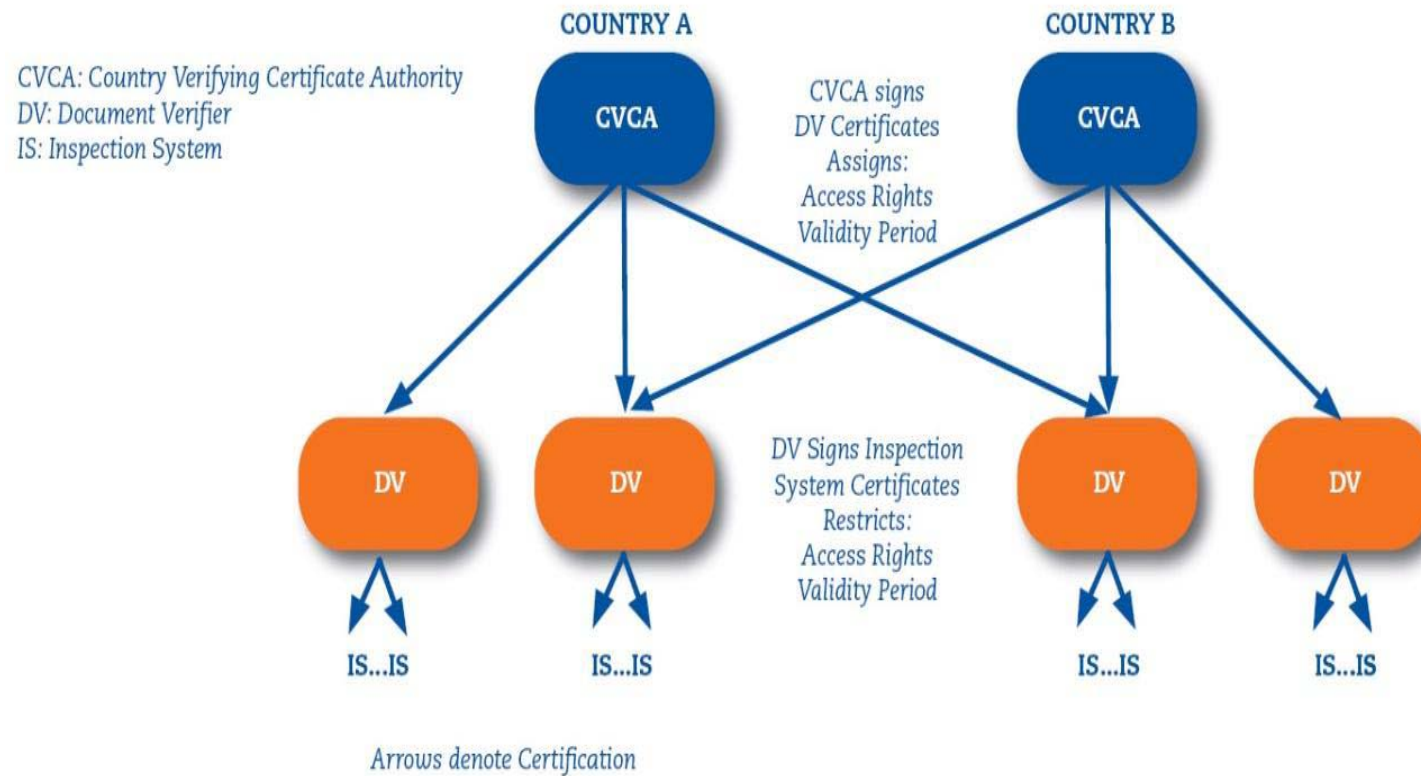
Country Signing Public Key Infrastructure (PKI)

Used to verify the integrity of the data in the passports chip (has the data not been changed) and their authenticity (does the data originate from an official issuing authority)
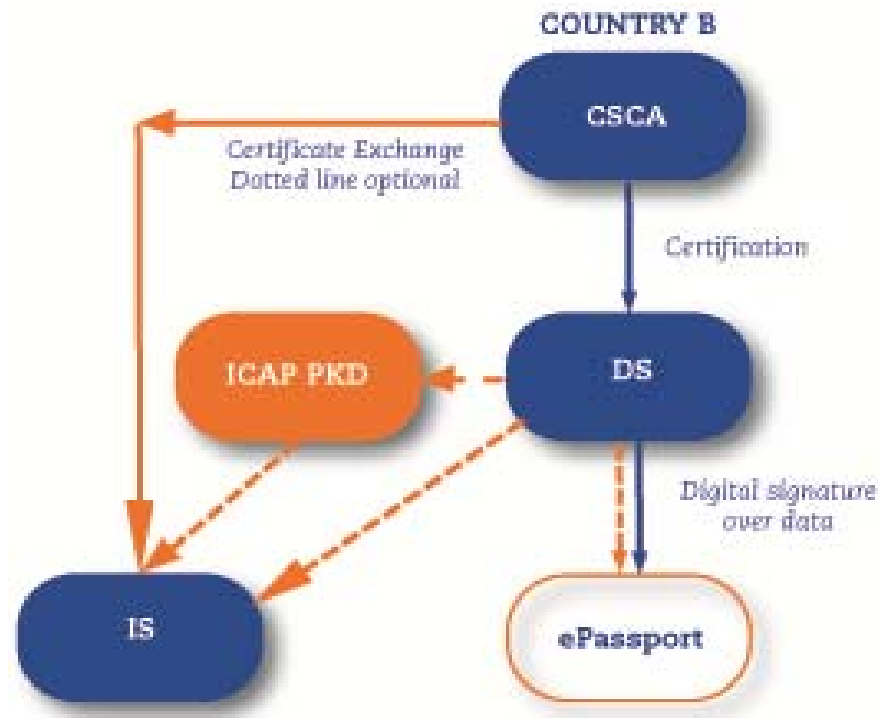
Country Verifying Public Key Infrastructure (PKI)

Authenticates the inspection terminals of automated border control

CVCA: Country Verifying Certificate Authority
DV: Document Verifier
IS: Inspection System

COUNTRY A

COUNTRY B

CVCA

CVCA

CVCA signs
DV Certificates
Assigns:
Access Rights
Validity Period

DV

DV

DV

DV

DV Signs Inspection
System Certificates
Restricts:
Access Rights
Validity Period

IS...IS

IS...IS

IS...IS

IS...IS

Arrows denote Certification

Biometrics, definition

"The automated use of physiological or behavioural characteristics to determine or verify identity"

Bio from Greek life

Metric from Greek measurement

In this case we measure
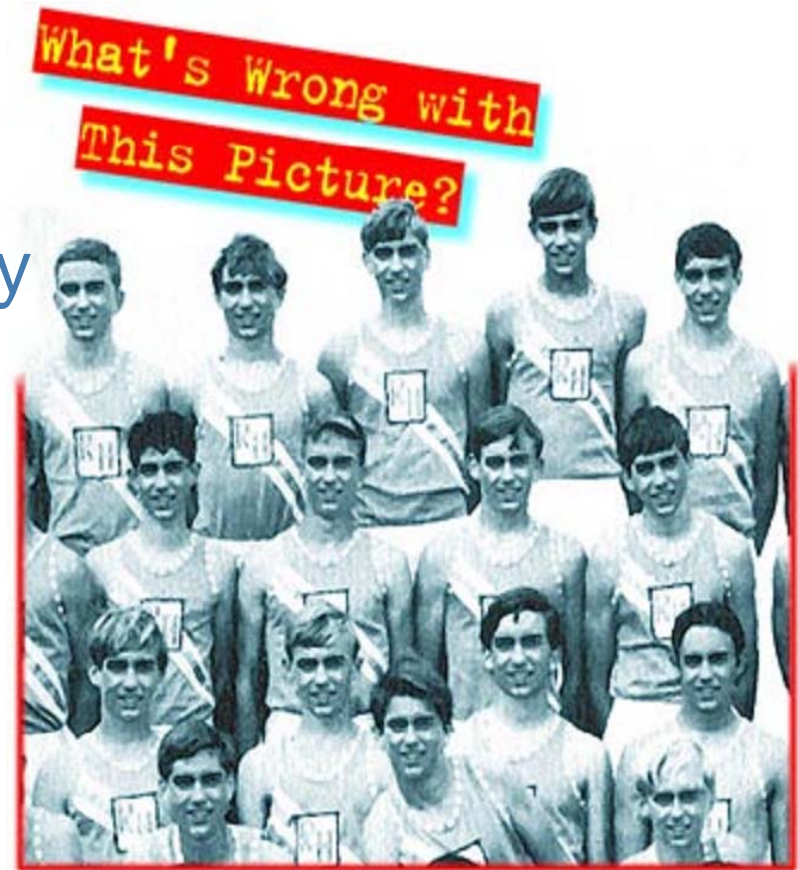
Physical properties of the user's body

Behaviour properties of the user

Biometrics

One of the remarkable abilities of humans and most animals is to identify other individuals

Humans do it primarily through face and voice.

Body proportions, movements etc. are also important

What's Wrong with This Picture?

Using the anthropometry for biometrics is not a new idea...

Alphonse Bertillon 1853-1914

Identification through a system that involved around eleven measurements of the human anatomy

Paris, 1882

"Portrait parlé"

About an identification process that enables finding the name of a repeat offender based on his description only, and that can be used in the context of a classification of photographies in the police headquarters, in the national security office, at the ministry of justice, etc.

Alphonse Bertillon, 1881.

body measurements

iris coloration

photography

individual
particularities
(including
fingerprints)

Anthropometry

Biometrics, examples

Written signature

Retinal scan

DNA

Vein pattern

Thermal pattern of the face

Keystroke dynamics

Finger prints

Face geometry

Hand geometry

Iris pattern

Voice

Ear shape

Body motion patterns

Fingerprint	Face	Iris	Retina	Ear
Palm print	Hand geometry	Periocular	Conjunctival vasculature	Key stroke dynamics
Anthropometry	Signature	Facial thermogram	Hand thermogram	Gait

Face

Voice

Iris

Signature

Fingerprint

Gait

Hand geometry

Palmprint

Enrollment
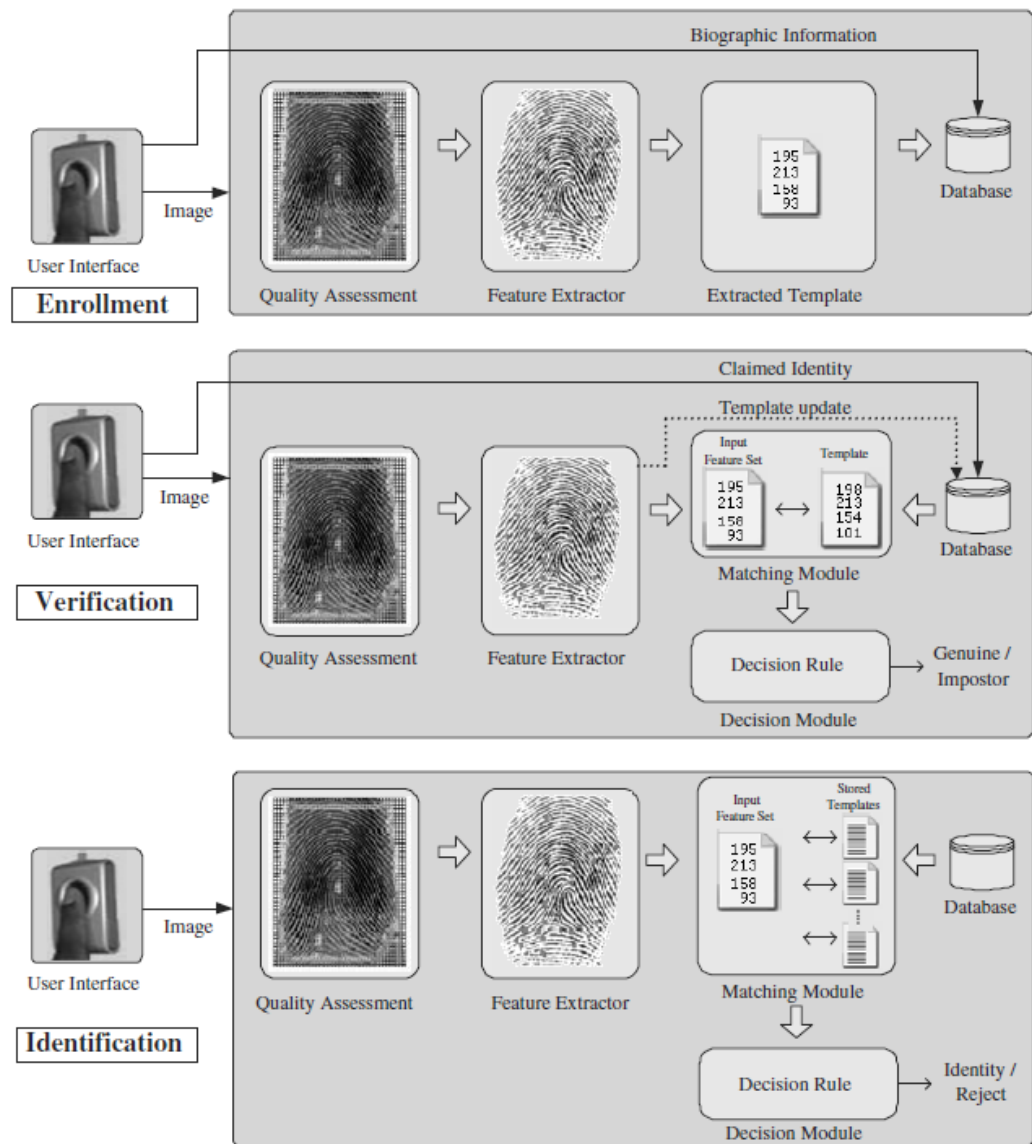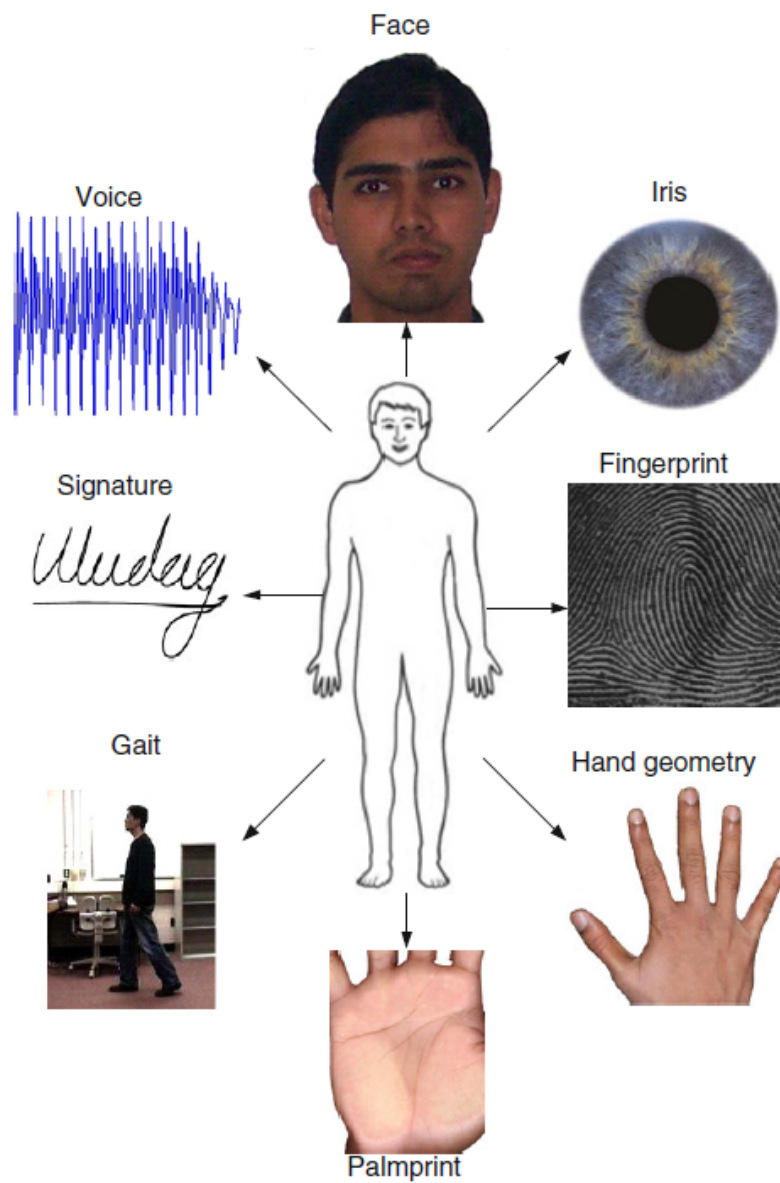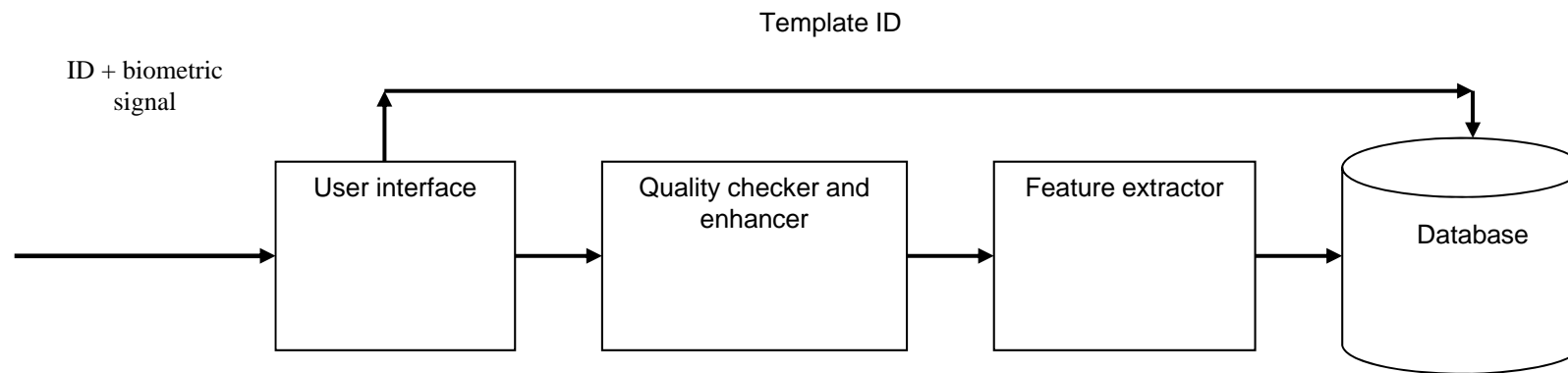User Interface | Image | Quality Assessment | Feature Extractor | Extracted Template | Biographic Information | Database
195 213 158 93

Verification
User Interface | Image | Quality Assessment | Feature Extractor | Claimed Identity | Template update | Input Feature Set | Template | Database
195 213 158 93 | 198 213 154 101
Matching Module
Decision Rule → Genuine / Impostor
Decision Module

Identification
User Interface | Image | Quality Assessment | Feature Extractor | Input Feature Set | Stored Templates | Database
195 213 158 93
Matching Module
Decision Rule → Identity / Reject
Decision Module

Enrollment

Creating a user template

Template ID

ID + biometric
signal

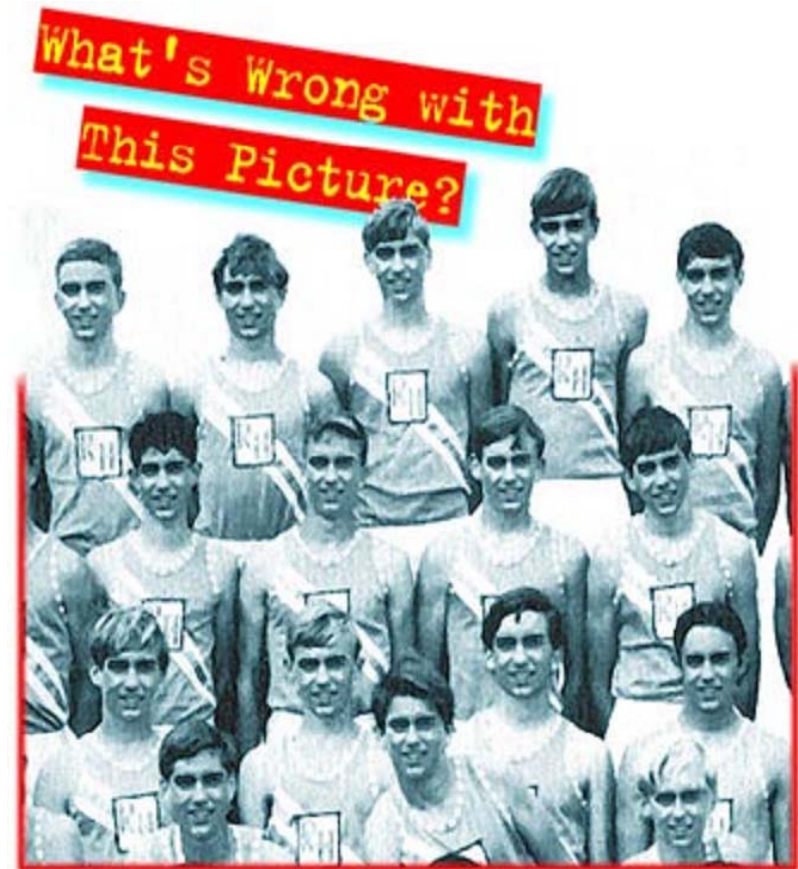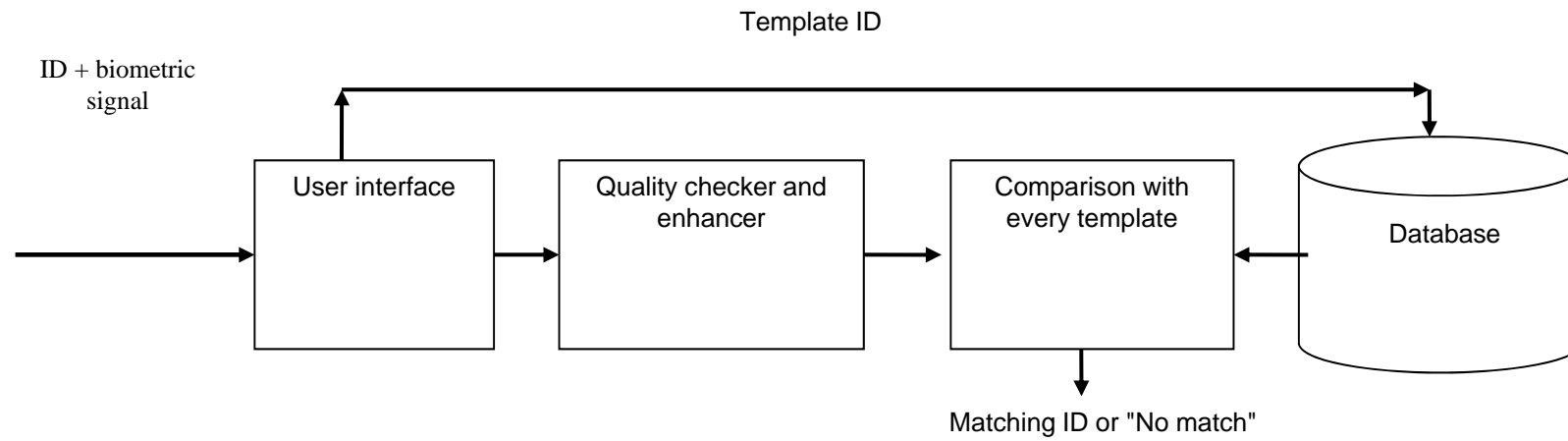| User interface | Quality checker and enhancer | Feature extractor | Database |

Identification

"Who am I?"

Comparisons are made with every template in the database

The result is an identity (name or user ID) or "NO MATCH"

What's Wrong with This Picture?

Identification

Template ID

ID + biometric signal

User interface → Quality checker and enhancer → Comparison with every template ← Database

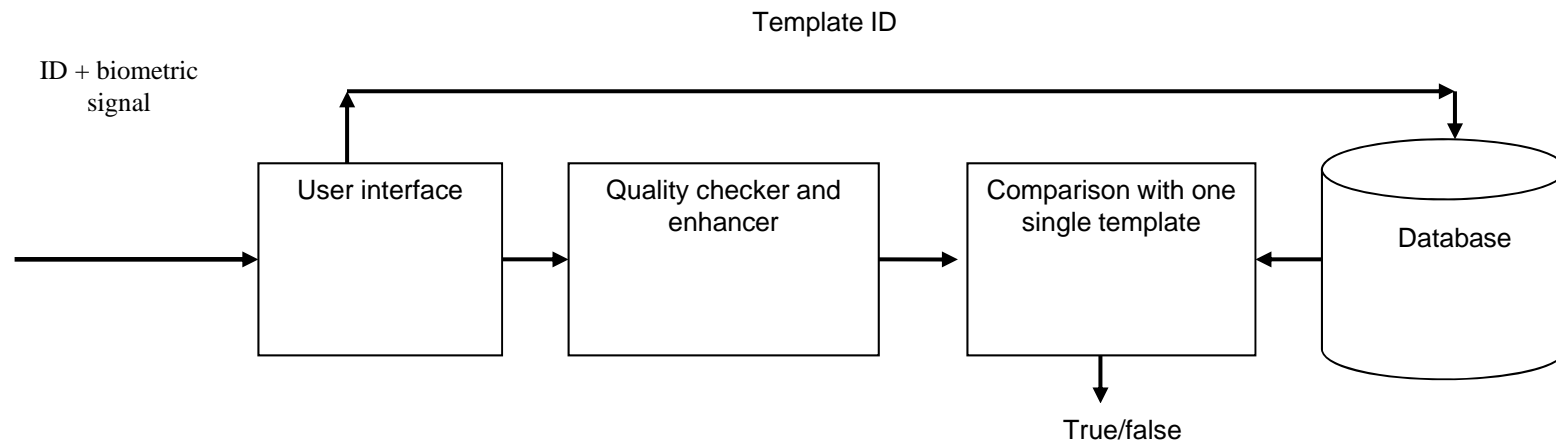Matching ID or "No match"

Identity verification = Authentication

"Am I the person who I claim I am?"

The user claims to have a certain identity (e.g. by specifying a user name)

Comparisons are made only with one template.

The result is TRUE/FALSE

Identity verification

Template ID

ID + biometric
signal

```
User interface  →  Quality checker and  →  Comparison with one  ←  Database
                   enhancer                single template
                                                │
                                            True/false
```

Agenda for lecture I within this part of the course

Background

Statistics in user authentication

Biometric systems

Tokens

Authentication✓

eID✓

ePassports✓

Biometrics in general✓

Statistics

Fumy, W. and Paeschke, M. Handbook of eID Security

A. Jain, A. Ross and K. Nandakumar, Chapters 1 in "Introduction to Biometrics"

Linköping University

expanding reality