



Deployment of 'template protection' in real-life

Michiel van der Veen

CEO - priv-ID B.V., the Netherlands

Michiel Loeff

VP-Sales

Brussels, 18th of January

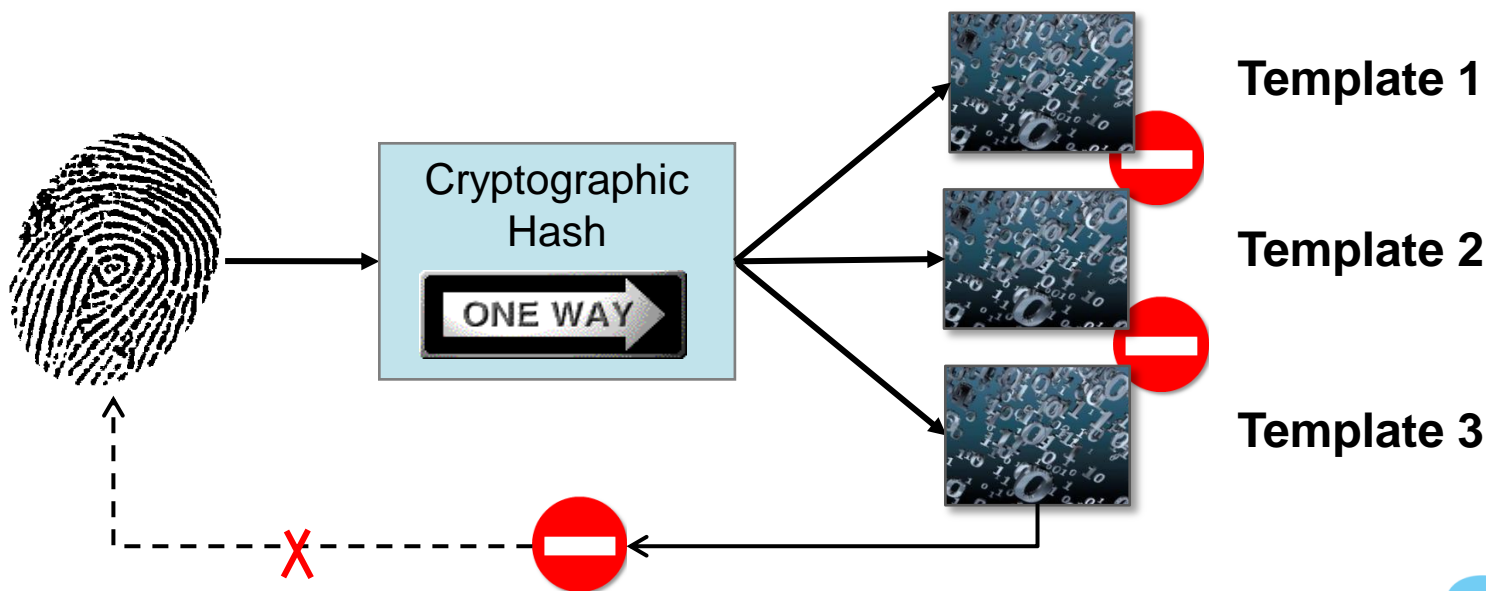
PHILIPS

CryptoBiometrics - BioHASH

Privacy Enhancing Technology

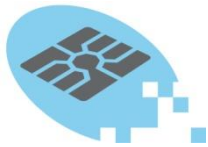


- Irreversible template – no biometrics info stored
- Confidential – anonymous information
- Unlinkable – not traceable over various applications



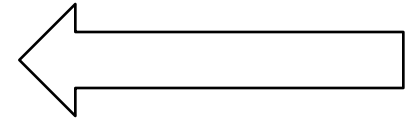
Alternative deployments

In each deployment, privacy is important



Match-on-Card

eID cards
Payment (EMV) cards



Identity Documents

ePassport



Biometric Repositories

Eliminating privacy concerns

MoC (1/2) - Deployment in eID: *Is CryptoBiometrics needed?*



- In eID cards
 - Match-on-Card applied
 - Template does not leave the card
- CryptoBiometrics are easy to implement as MoC
 - Most of the computation takes place on terminal
 - Reduced code size
 - Reduced template size
 - Possibility to deploy in EEPROM



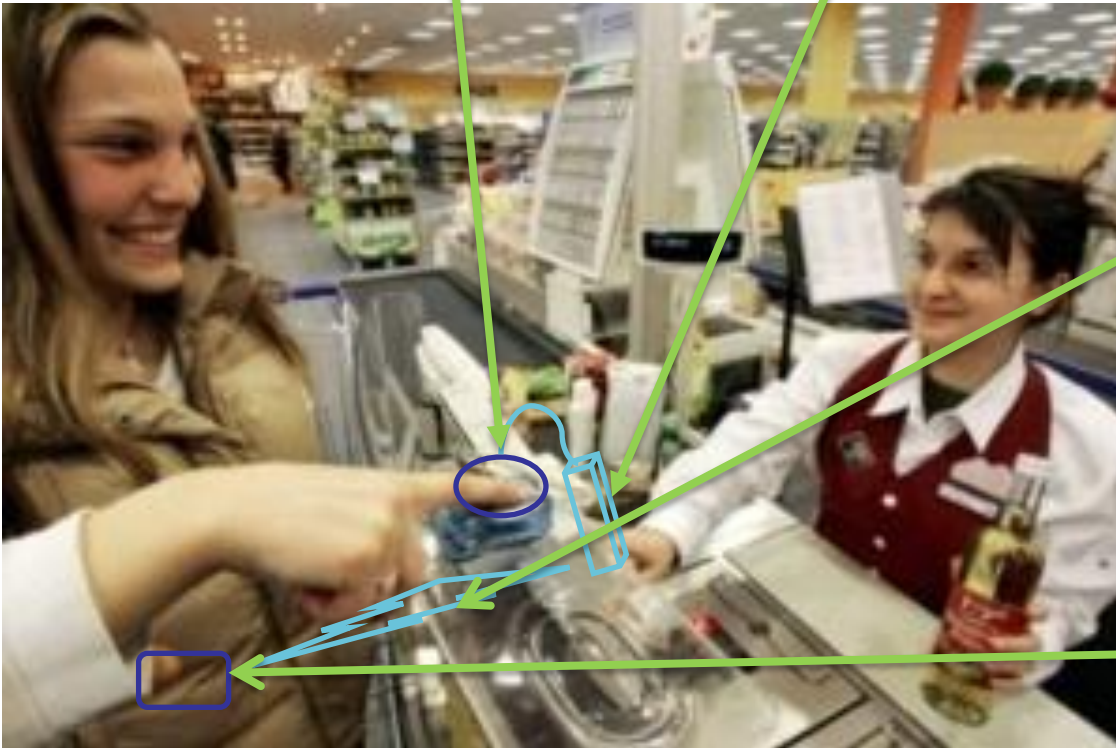
→ But actually “privacy properties are NOT required” !

MoC (1/2) *in payment*



1) To pay, customer is invited to put his finger on the POS

2) POS detects all natural security Contactless system (eg. Smartcard or Mobile Phone ...) around it



3) POS sends the customer biometric data to each authenticated natural Security systems

4) Then natural security system verify biometric data with those embedded & valid the EMV payment transaction

MoC (2/2) - Deployment in payment solutions

Example: biometric payment in EMV environment



Objectives: speed-up transaction,
reduce cash, reduce fraud, reduce
costs.

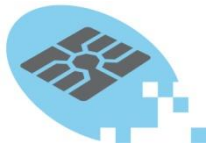
CryptoBiometrics needed for:

- **Revocable** EMV card (similar to current card scheme – Card + PIN)
- Modality independent MoC matcher



Alternative deployments

In each deployment, privacy is important



Match-on-Card

eID cards
Payment (EMV) cards



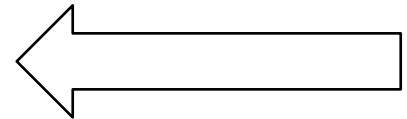
Identity Documents

ePassport



Biometric Repositories

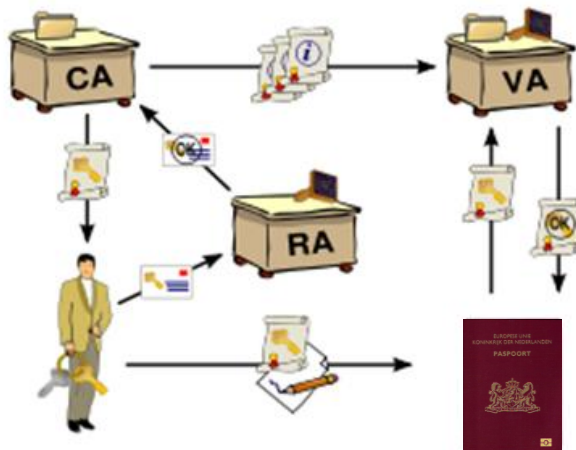
Eliminating privacy concerns



Deployment in MRTD's (1/2) *as an alternative to PKI*



- In most ePassports and eID's fingerprint images are digitally stored in DataGroup 3
- In Europe, DataGroup 3, is protected with Extended Access Control (PKI)
- The strong and complex PKI-based security measures **limits** the practical use of fingerprint verification **in the public** and **private sector**



**Extended Access Control
(PKI) principle**

Public sector example:

- Verification for police force
- Verification for civil service

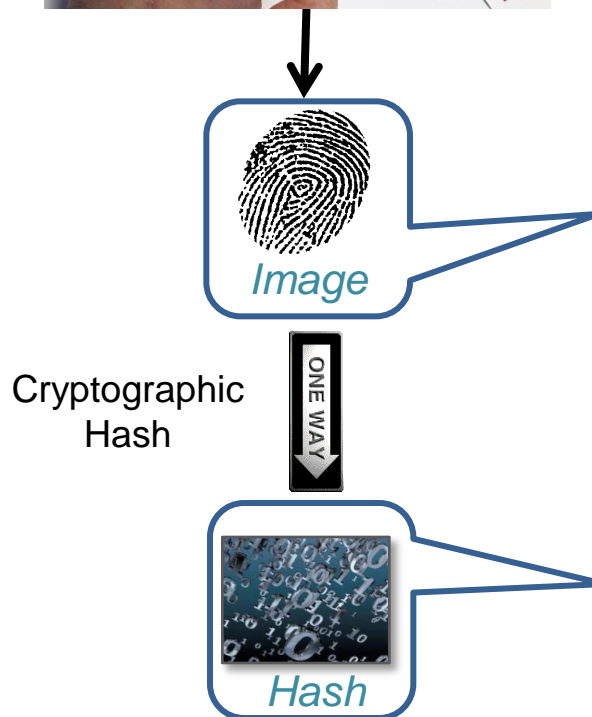
Private sector example:

- Bank branches
- Car rental companies

Deployment in MRTD's (2/2) *as an alternative to PKI*



- Make use of existing enrollment stations to capture fingerprints from the citizens
- Create a BioHASH and store it in DG13 of the ePassport or eID during personalization.



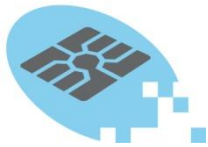
| Logical Data Structure |
|---|
| Data Group 01 – Machine Readable Zone |
| Data Group 02 – Encoded Face |
| Data Group 03 – Encoded Finger |
| Data Group 04 – Encoded Iris |
| Data Group 05 – Displayed Portrait |
| Data Group 06 – Reserved for future use |
| Data Group 07 – Displayed Signature or Usual Mark |
| Data Group 08 – Data Features |
| Data Group 09 – Structure Features |
| Data Group 10 – Substance Features |
| Data Group 11 – Additional Personal Details |
| Data Group 12 – Additional Document Details |
| Data Group 13 – Optional Details |
| Data Group 14 – Security options for Secondary Biometrics |
| Data Group 15 – Active Authentication Public Key Info |
| Data Group 16 – Persons to Notify |

ICAO compliant

*Only possible
because of
irreversible
template*

Alternative deployments

In each deployment, privacy is important



Match-on-Card

eID cards
Payment (EMV) cards



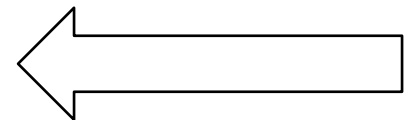
Identity Documents

ePassport



Biometric Repositories

Eliminating privacy concerns



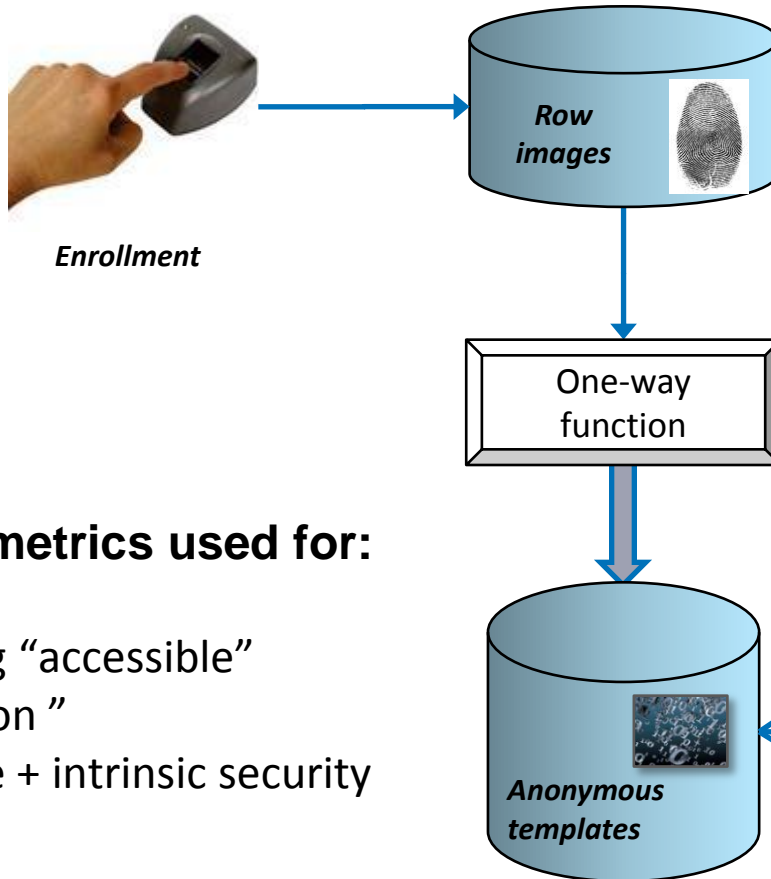
Deployment in database:

Why national biometric repository?



- Primary objectives:
 - Combat identify fraud in application process of Identity Documents (passport, identity card, driving license, etc.)
 - First application are based on birth certificates & other documents (most of them, not standardized)
 - Biometrics is the most effective way for “duplication check”
- Secondary objectives:
 - Identity verification e.g. re-applying for a stolen passport,
 - Identification in exceptional circumstances – check identity in case of calamity
 - Use register for identity verification – (e.g. online services)
- Other possible objectives:
 - Use as a criminal AFIS → **CONTROVERSIAL**

Separation of purpose taking into account various stakeholders



- Strong security on “Raw-images” database (e.g. Offline)
- Create specific legislation concerning usage of the “raw images” database
- No “search” possibility

CryptoBiometrics used for:

- Protecting “accessible” information ”
- Revocable + intrinsic security

Conclusion & outlook



- Turbine contributions
 - Technical developments
 - Standard
- Priv-ID perspective
 - Maturing technology
 - Market demand for privacy
- Example applications
 - MoC
 - MRTD
 - Repositories
- Future
 - Important role for “privacy-tests” (NIST)
 - Privacy Enhancing Technology integral part of the design process of every biometric deployment.





For more info, please contact:

Name: Michiel Loeff

Email: Michiel.loeff@priv-ID.com

Tel: +31627066185

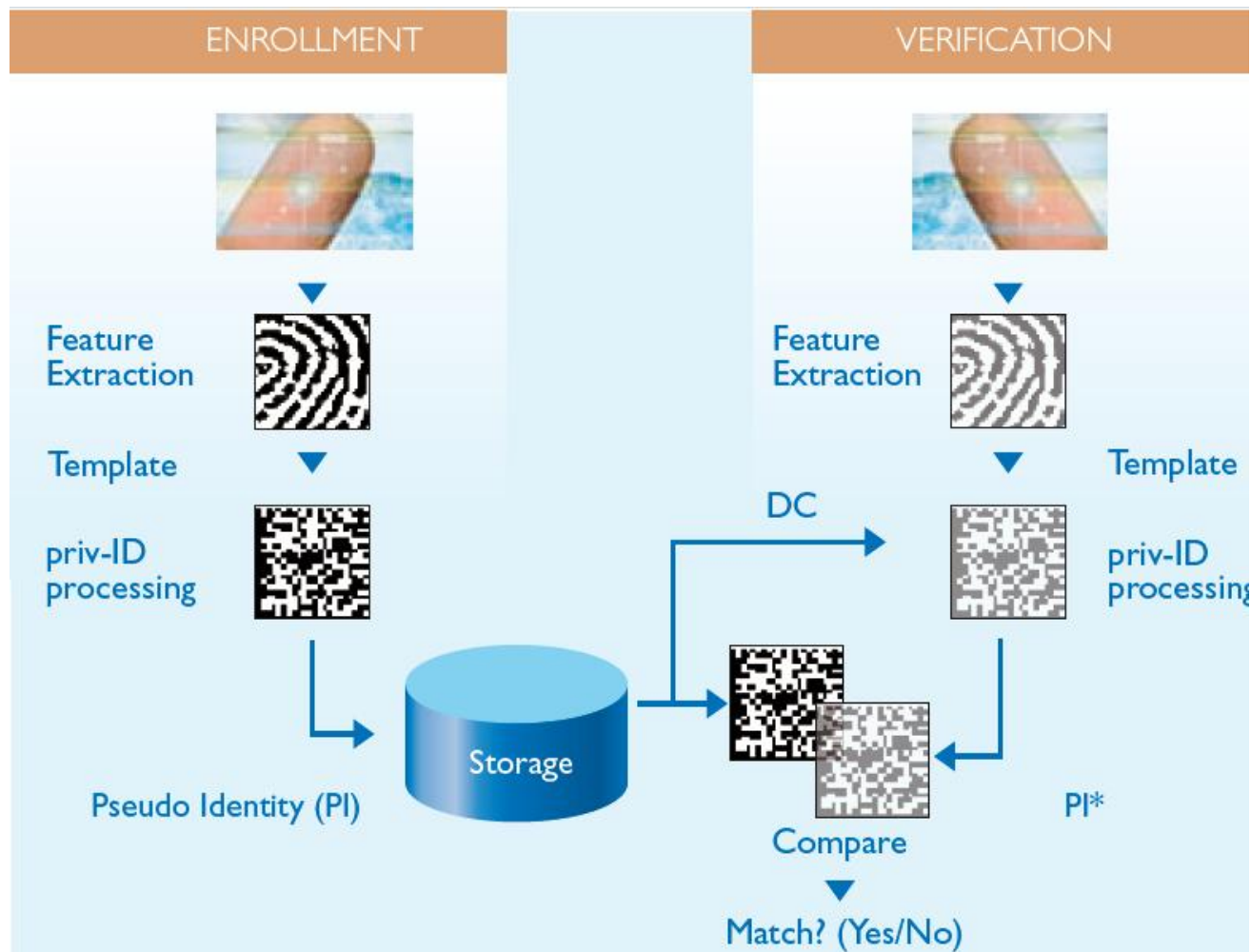
Web: www.priv-id.com

Email: info@priv-id.com



BioHASH Deployment Procedure

Same enrollment and verification procedure as traditional biometrics



BioHASH Technology

Protect biometric by means of a Cryptographic Hash function

