Forensic Implications of Identity Management Systems

dr. Zeno Geradts
dr. Arnout Ruifrok,
Rikkert Zoun, MS
zeno@holmes.nl

AAFS Seattle 2006

Outline

- Introduction
- Biometric systems
- Forensic properties (faking biometrics)
- Biometric Passport
- Future research

Netherlands Forensic Institute

- Digital Evidence Section 40 employees
  - Open Systems (media analysis, crypto, data analysis)
  - Embedded Systems (PDA’s, cell phones, other electronics)
  - Interception
  - Image Analysis and Biometrics
  - Voice and audio

Outline

- Introduction
- Biometric systems
- Forensic properties (faking biometrics)
- Biometric Passport
- Future research

Current activities Biometrics (NFI)

- Photogrammetry
- Facial comparison
- Dutch Biometric Passport (Chip + Biometric)
- Biometrics program Immigration Naturalization Services
  - documents
  - facial recognition at borders
  - verification of people applying for asylum
- FEARID project
- FIDIS www.fidis.org Future of Identification Systems

Future of Identification Systems

- www.fidis.net

European project Network of Excellence with 20 partners

Workpackage 6 : Forensic Implications

Example artefacts :

Media analysis

Mobile phones

Biometric devices

…

In 2006 : profiling - data-analysis of databases

FIDIS Identity definitions

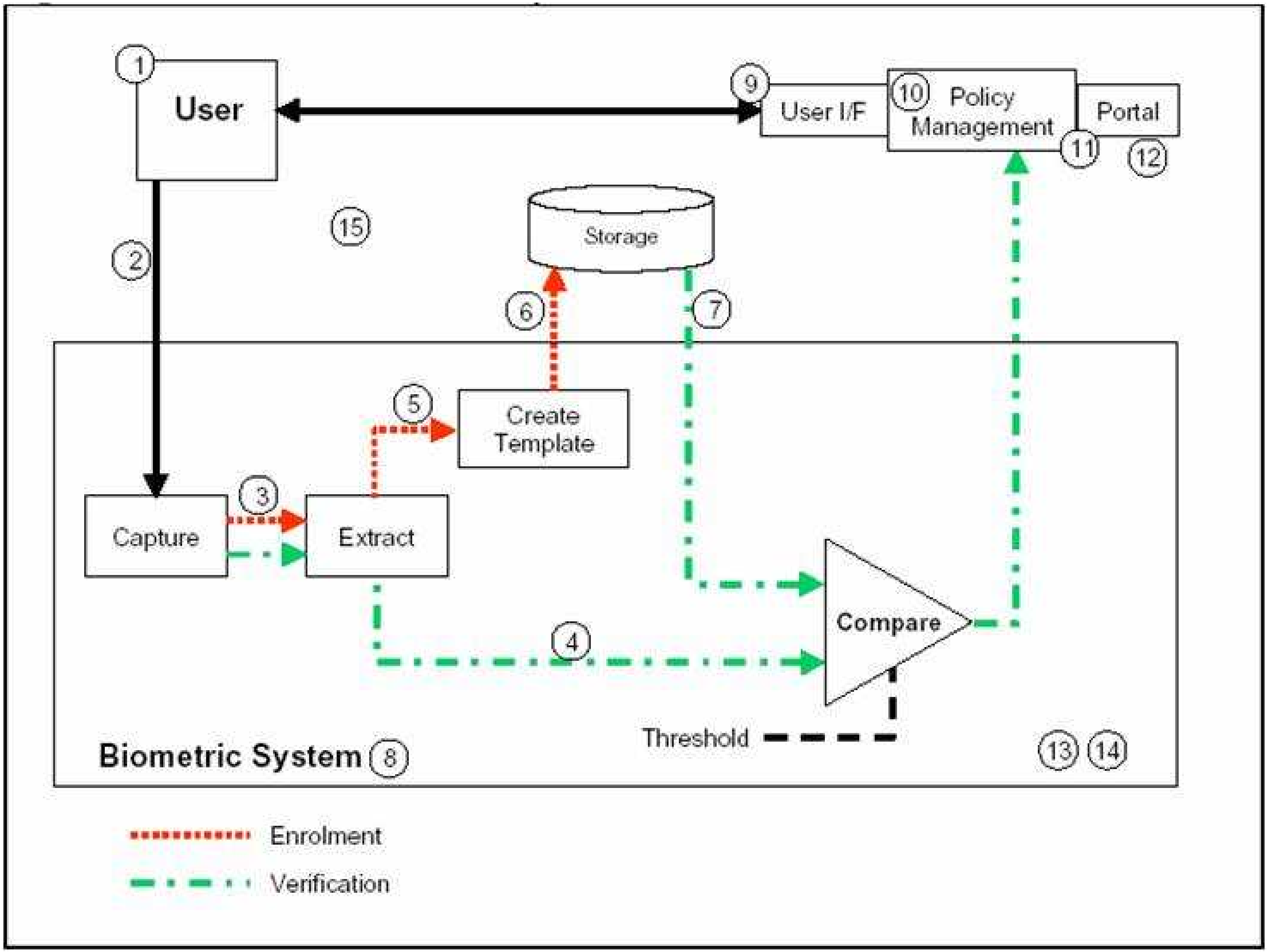
- Artefacts (magstripe, mobiles, biometrics)
- Threat level
- Forensic reliability and other forensic qualities
- Forms of failure
- Verification problems
- Consequences of Failure

Biometrics

Key terms:

- Verification (Authentication): Determination if an identity claim is true (1 to 1 match)
- Identification: Determination if a person already enrolled in a system, and who he/she is (1 to N match)

Schematic Biometric System



Common Methodology for Information Technology Security Evaluation, The Biometric Evaluation Methodology Working Group, 2002

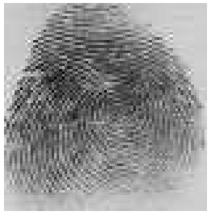
Outline

- Introduction
- Biometric systems
- Forensic properties (faking biometrics)
- Biometric Passport
- Future research

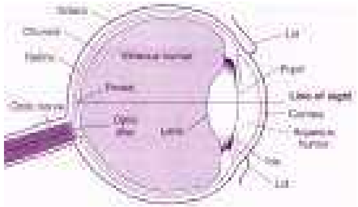
Biometric systems -1

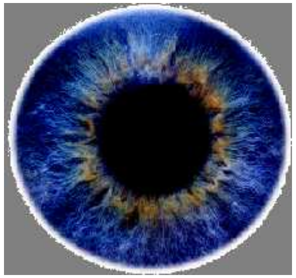
- Facial recognition

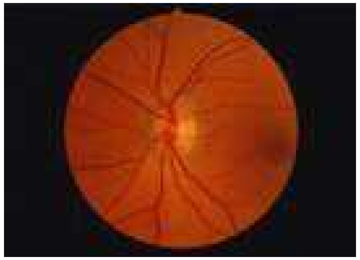
- Fingerprint



- Iris, retina

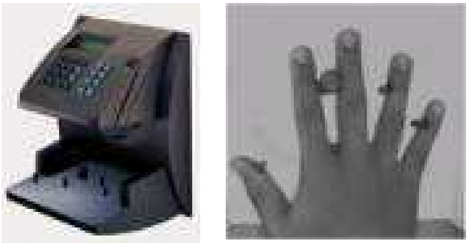






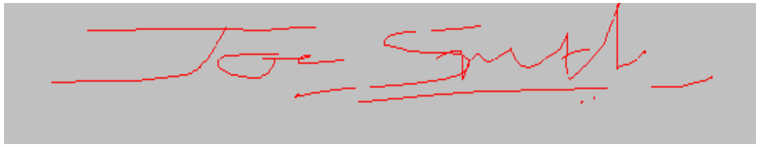
Biometric systems -2

- Hand scan

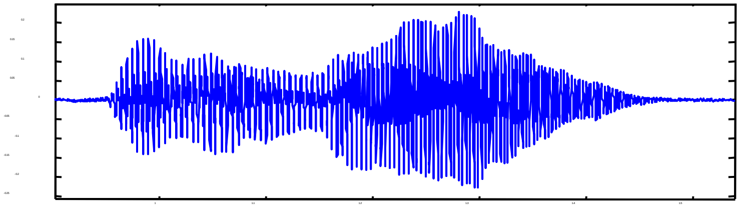


- Vascular patterns

- Signature, writing

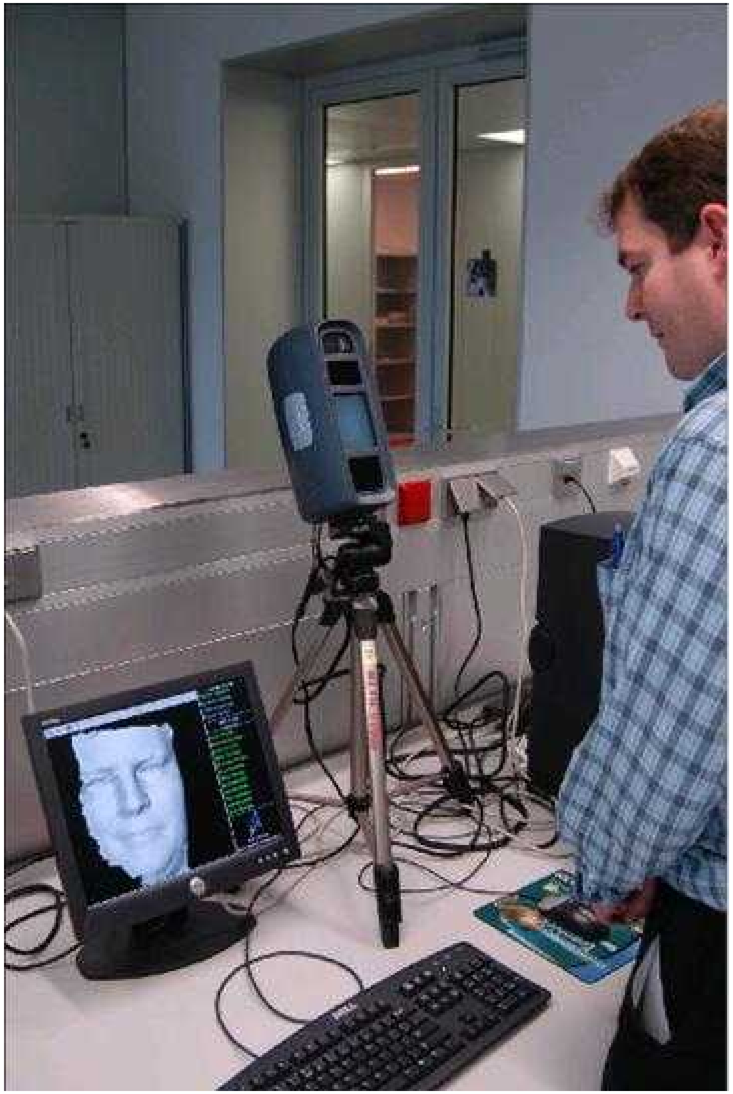


- Speech



- Keystroke

3D facial system

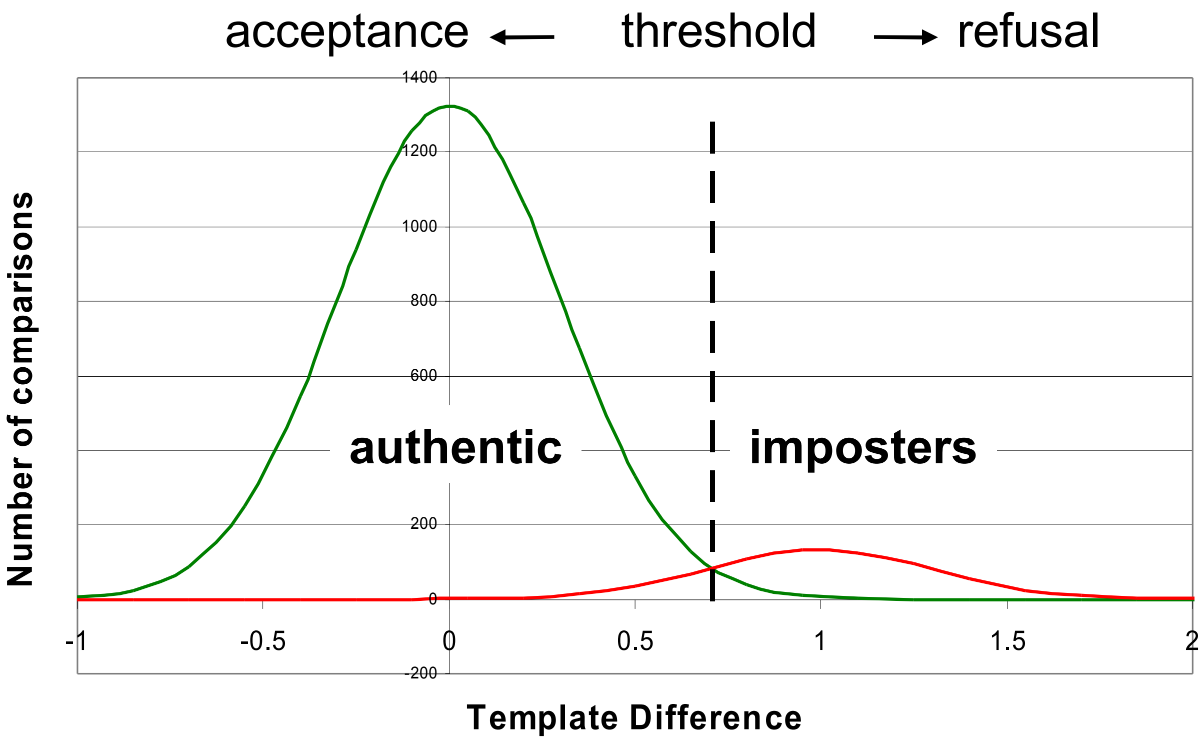


Principles of a biometric system

- Example: facial image
- Enrollment: facial picture taken under controlled circumstances
- Calculation of a “template” (series of numbers) for storage on a chipcard or in a database
- Verification: compare with template on a chipcard
- Identification: compare with templates stored in a database

Template matching

- Compare stored template with captured template
- Difference too big: refuse



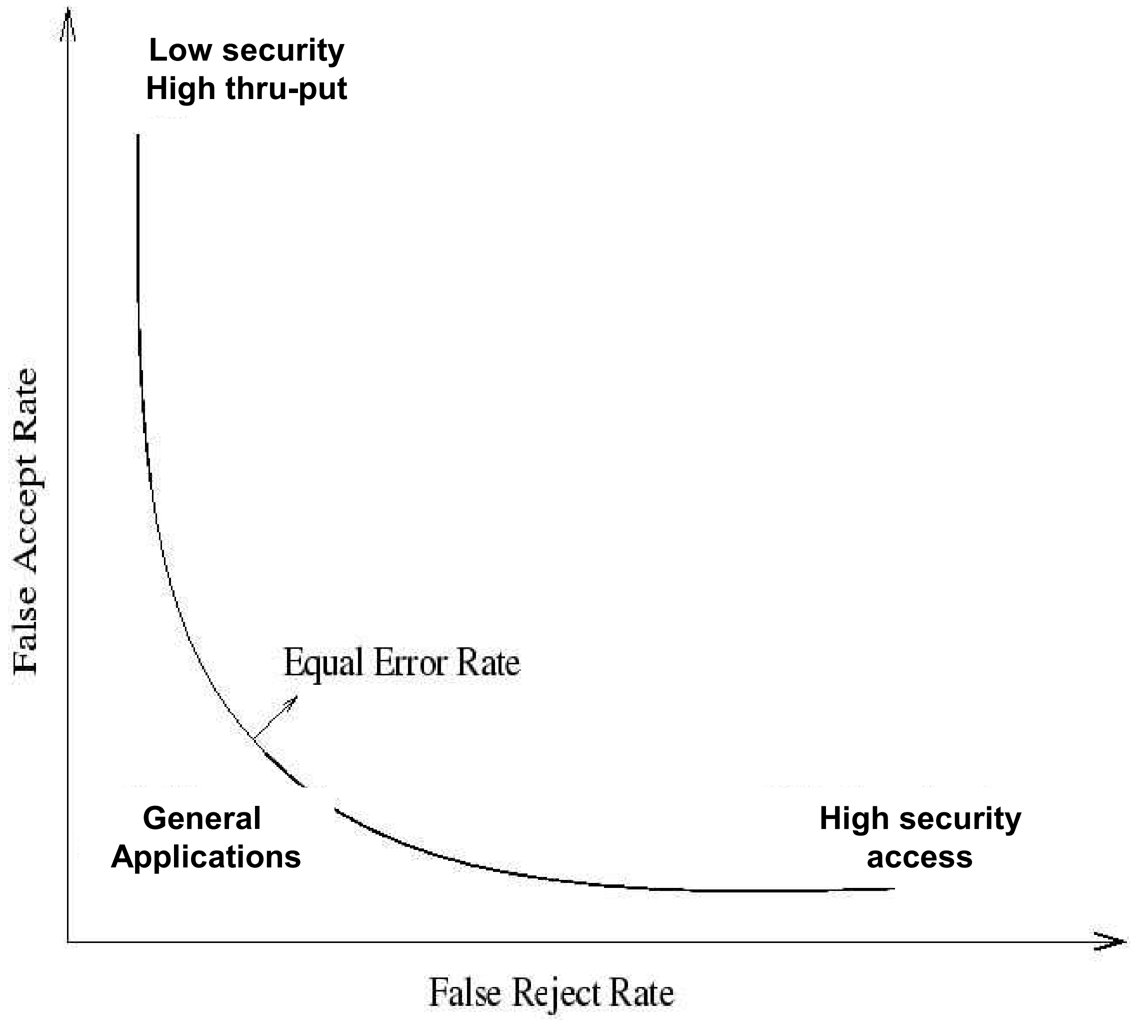
Properties of biometric systems

- FTE, ‘failure to enroll’
  - Probability that a user will be unable to enroll the system

Threshold setting: trade-off between

- FRR, ‘false rejection rate’
  - Probability of unintended refusal
- FAR, ‘false acceptance rate’
  - Probability of unintended acceptance

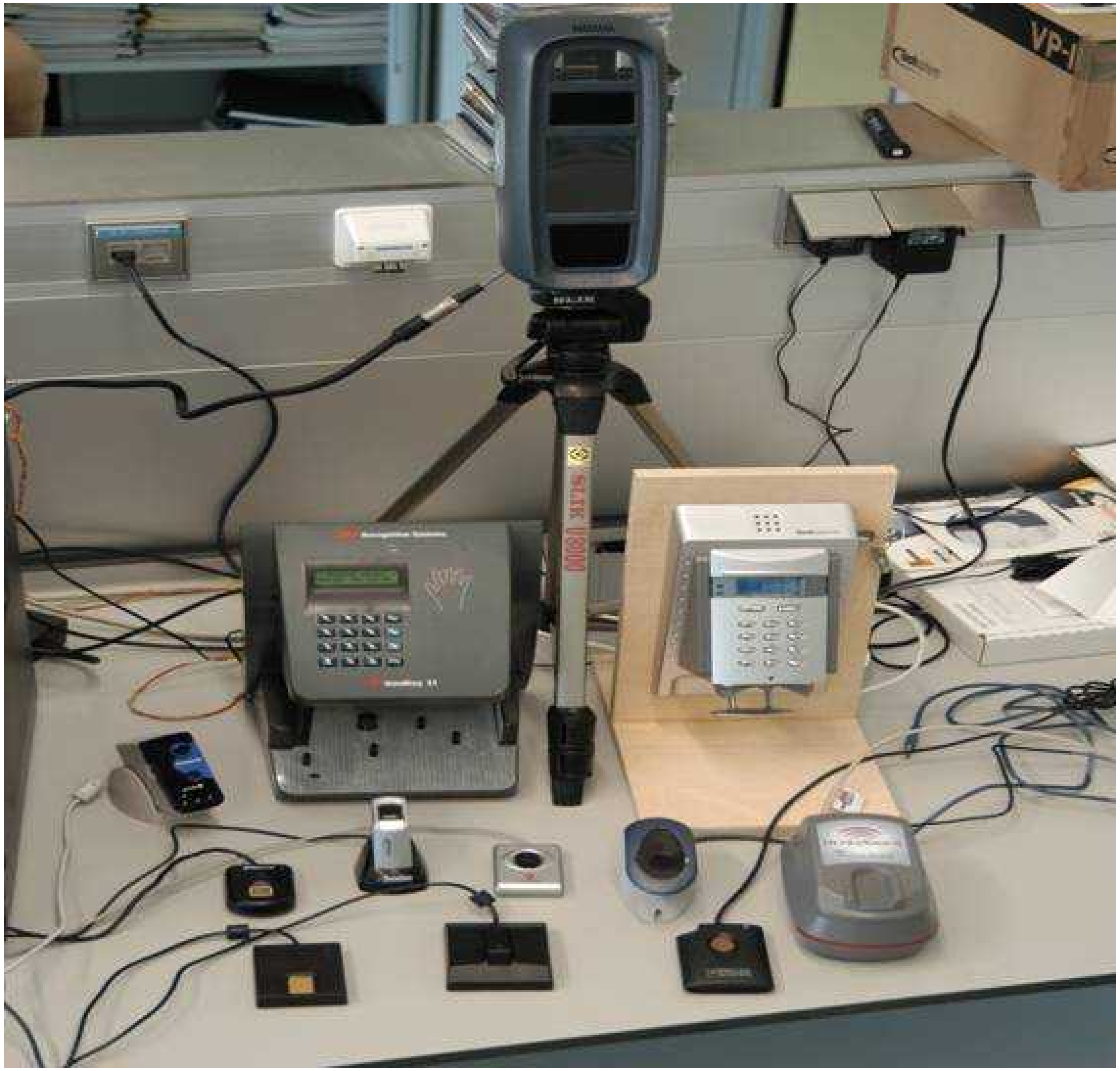
FAR and FRR of different systems



Outline

- Introduction
- Biometric systems
- Forensic properties (faking biometrics)
- Biometric Passport
- Future research

Biometric devices tested

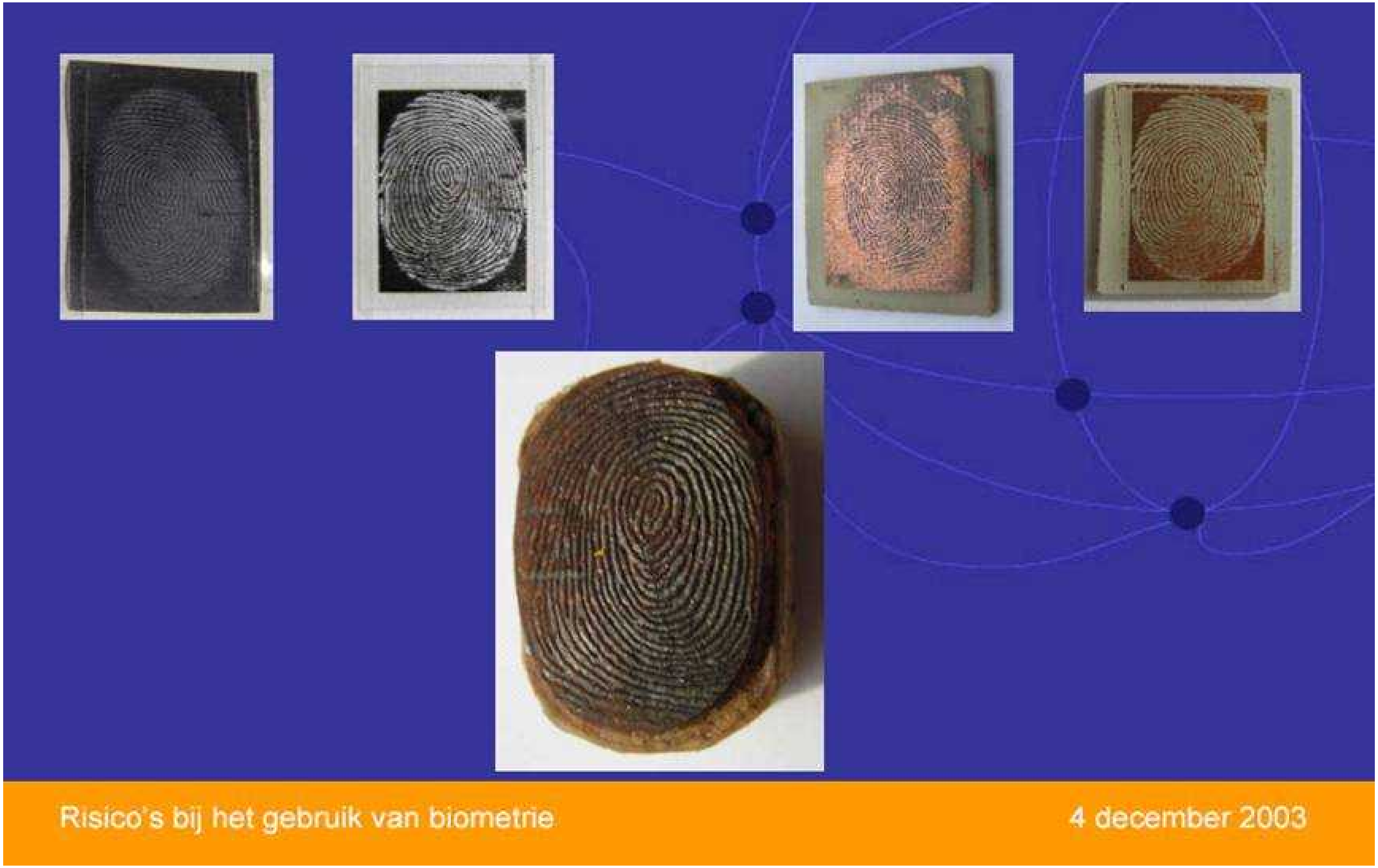


Resistance to fraud

‘Spoofing’ of biometric systems:

- Face – picture or mask
- Fingerprint – silicon/gelatin casting
- Iris – picture with a hole
- Hand - latex model
- Speech - digital or analog recording
- Keystrokes - recording

Vingerafdruk: spoofing



Risico's bij het gebruik van biometrie

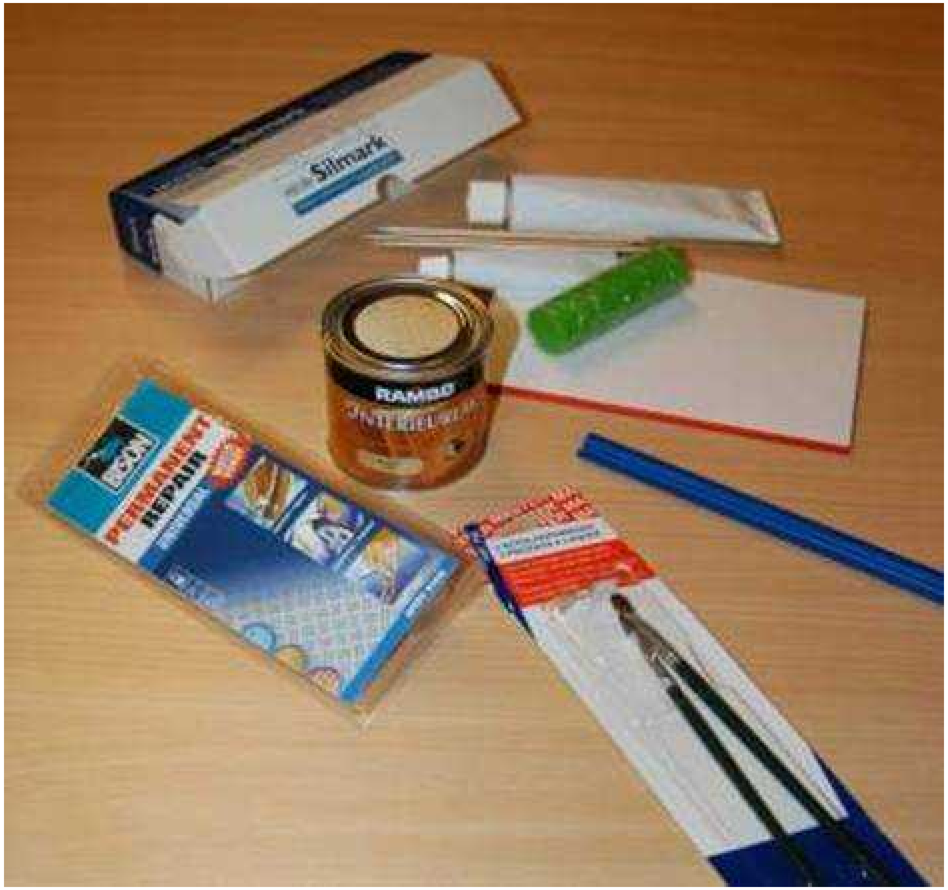
4 december 2003

Justitie Nederlands Forensisch Instituut

Van der Putte, NBF 2003

Fingerprint: spoofing

- Test in house

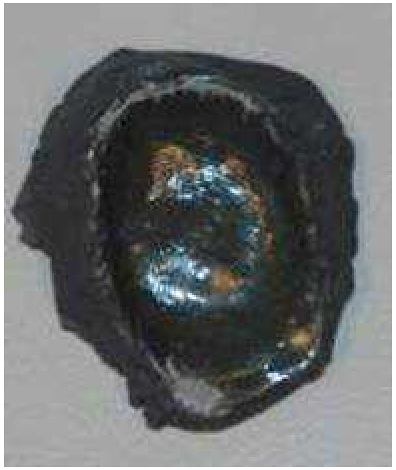


spoofing: epoxy

Negative of epoxy: More details …

- Epoxy not homogeneous

- Acrylate ‘it remains fixed’, a releasing agent



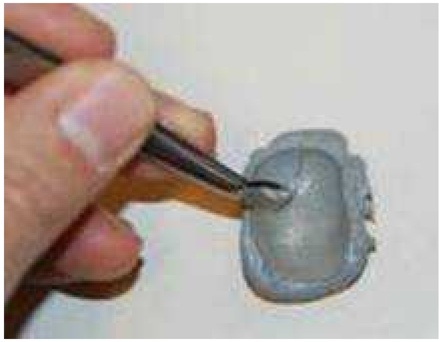
spoofing: silicon

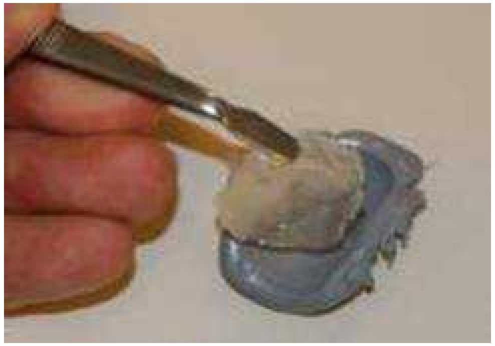
Negatief van silicon (used for toolma

- More details
- Easy to use
- Can be used for with several casts

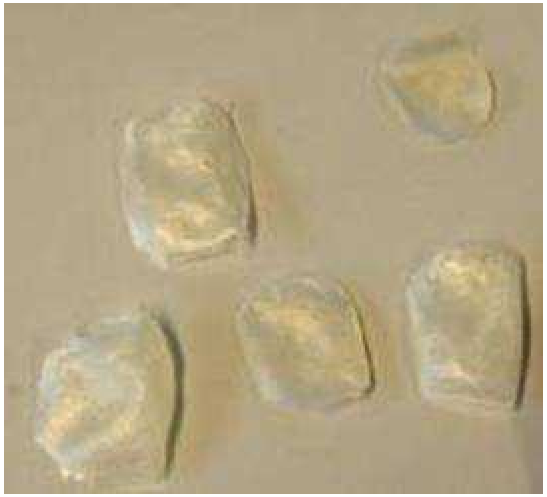
acrylaat ‘fake’

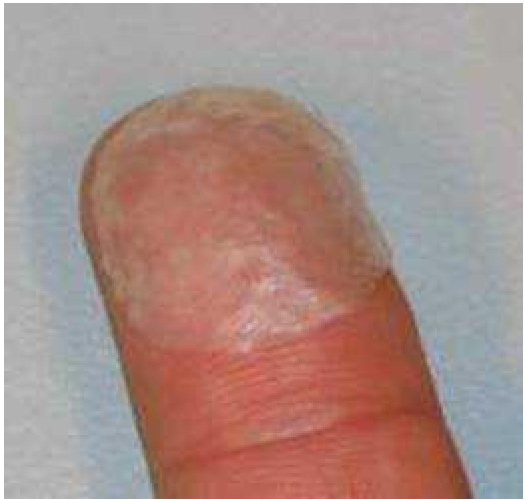
- Easy to remove





- Easy to use

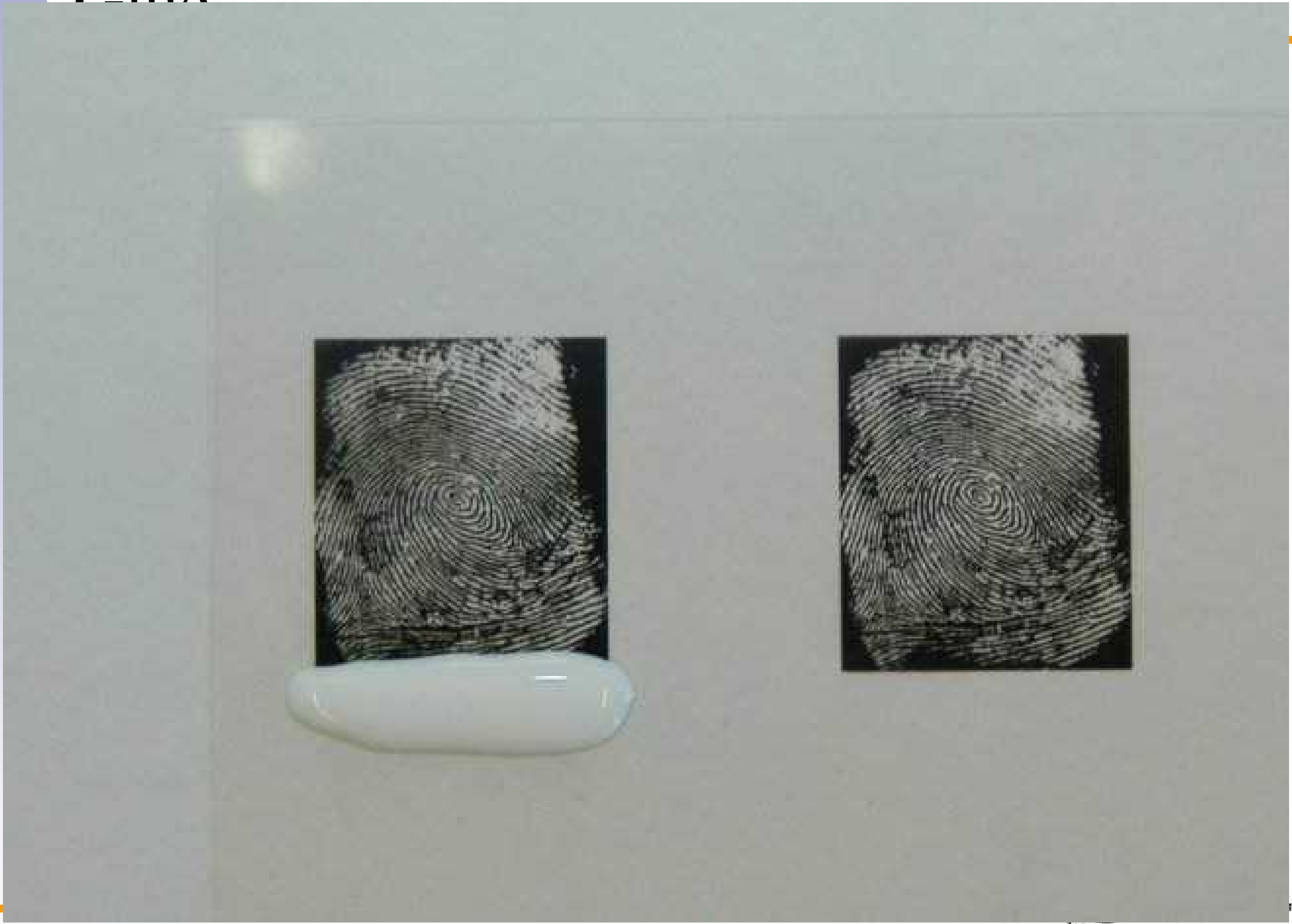


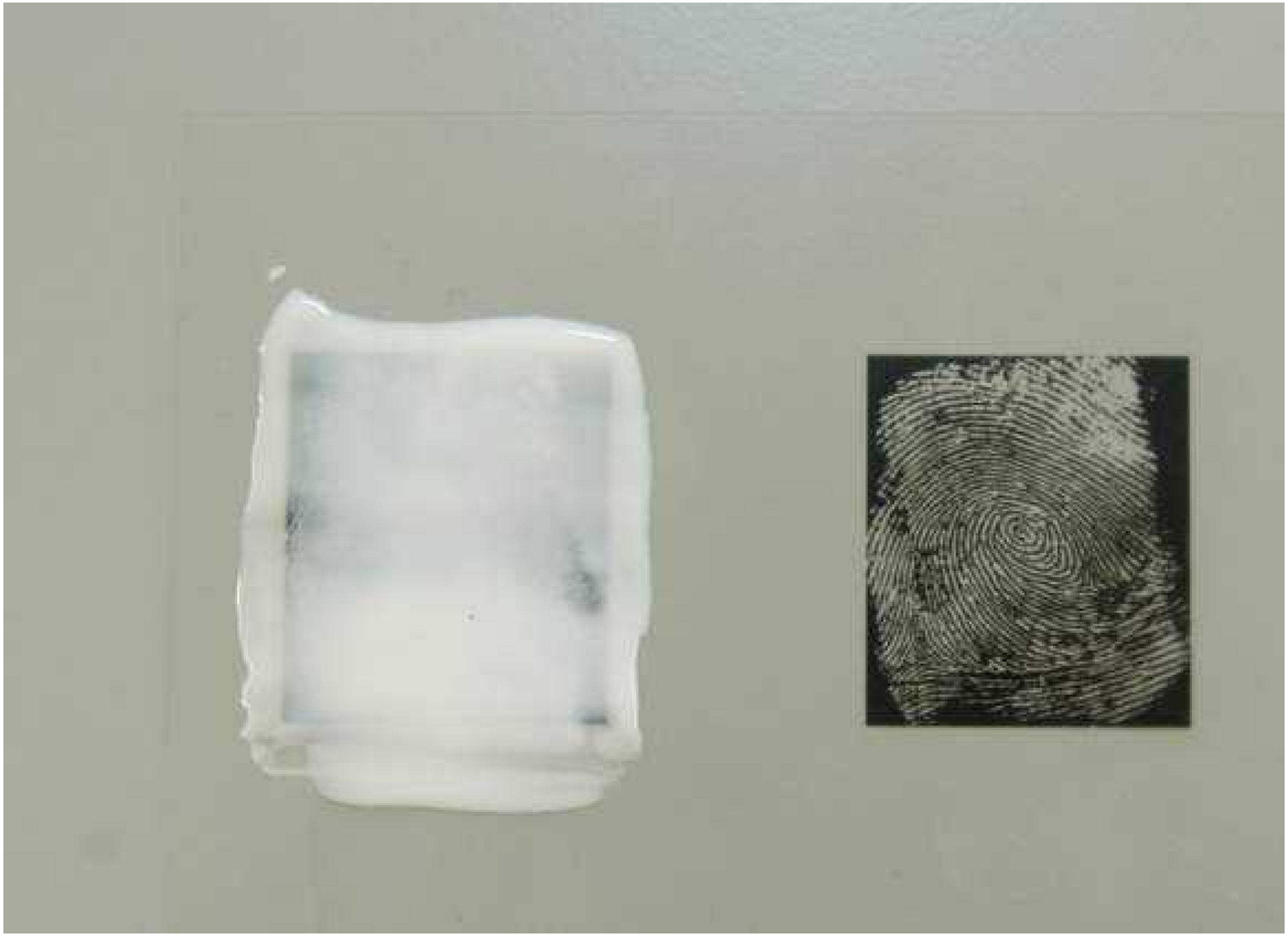


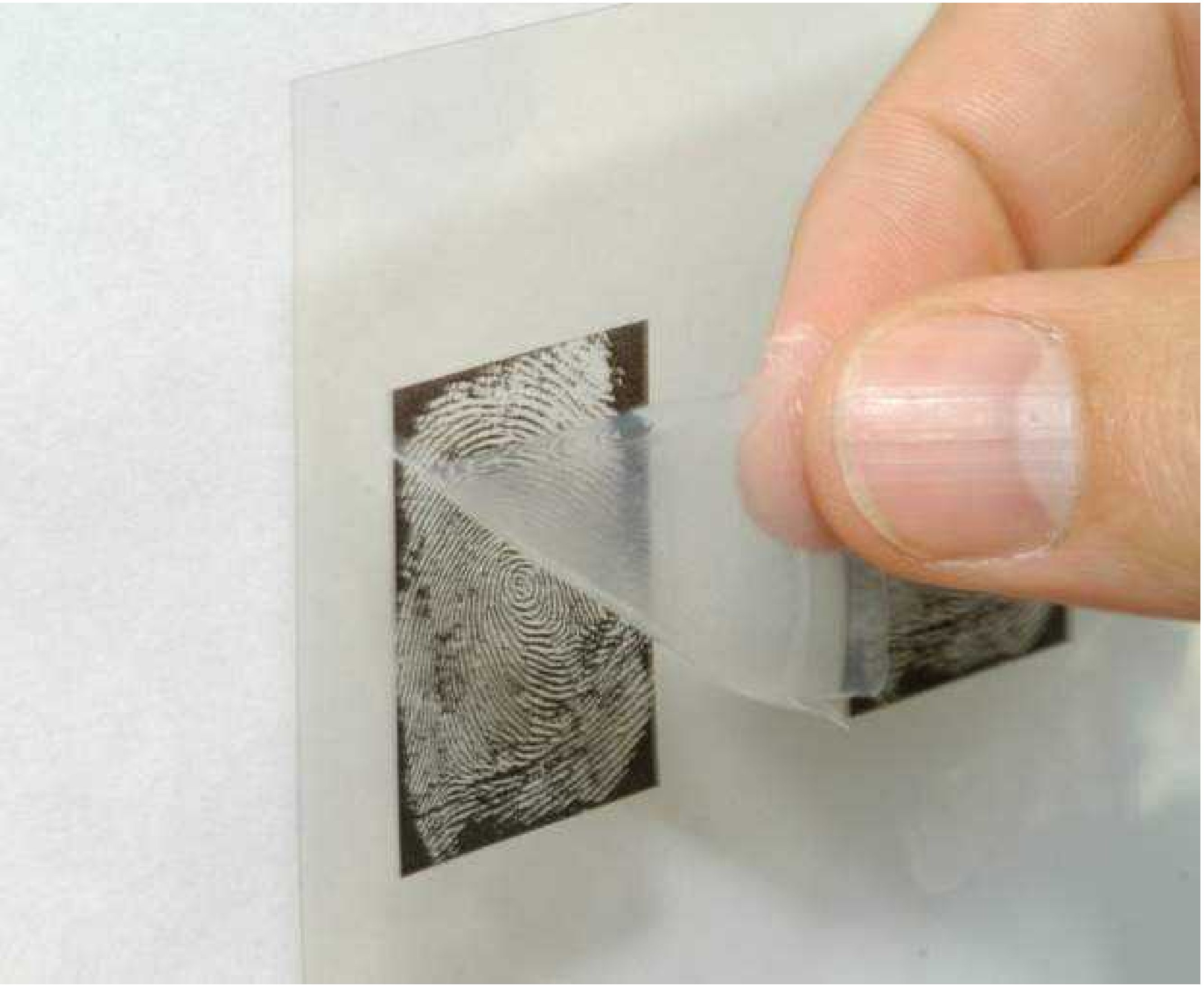
Other tested methods

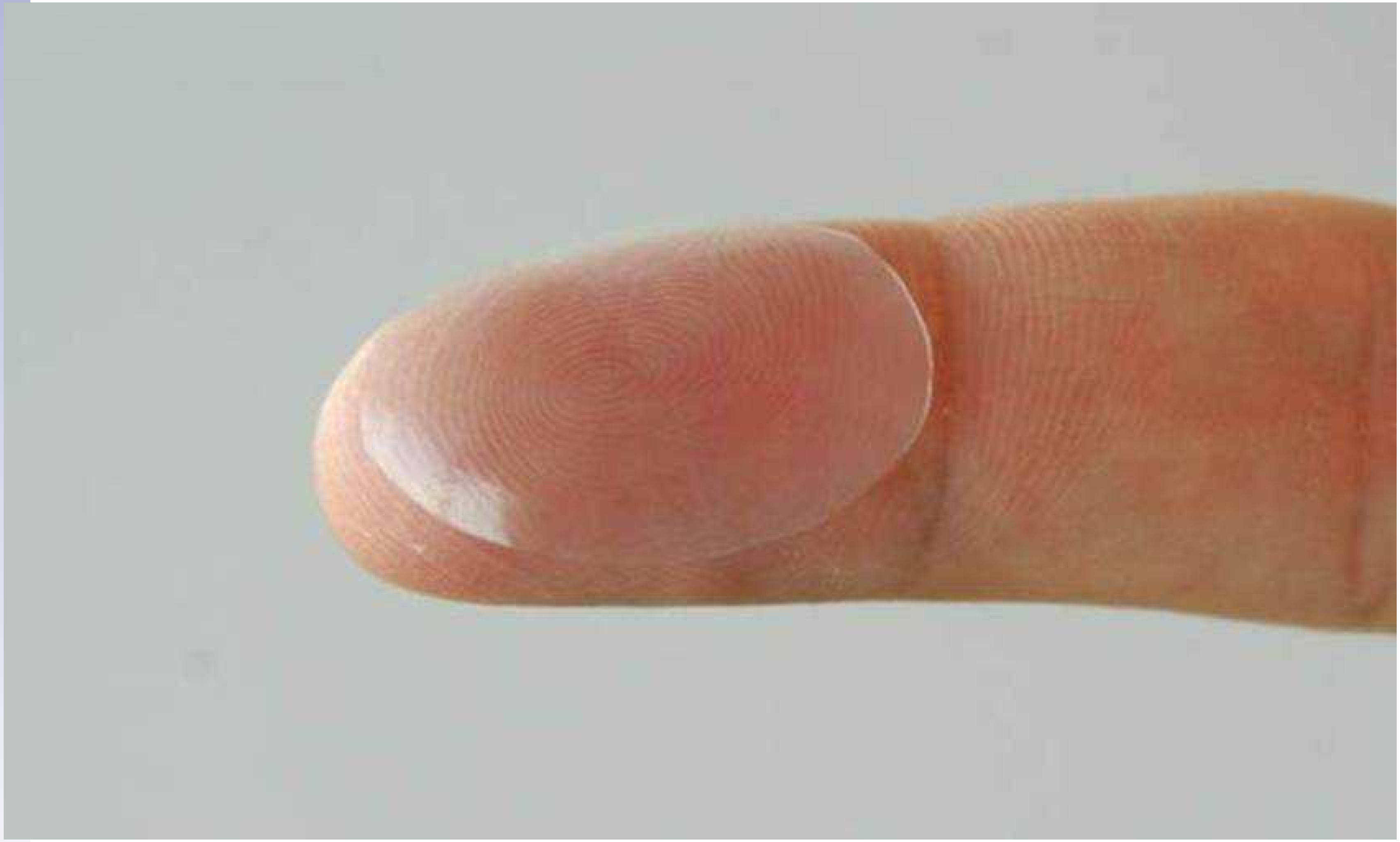
- Printing a stamp of a fingerprint and using that
- Printing on paper and using glue for copying a fingerprint

Glue



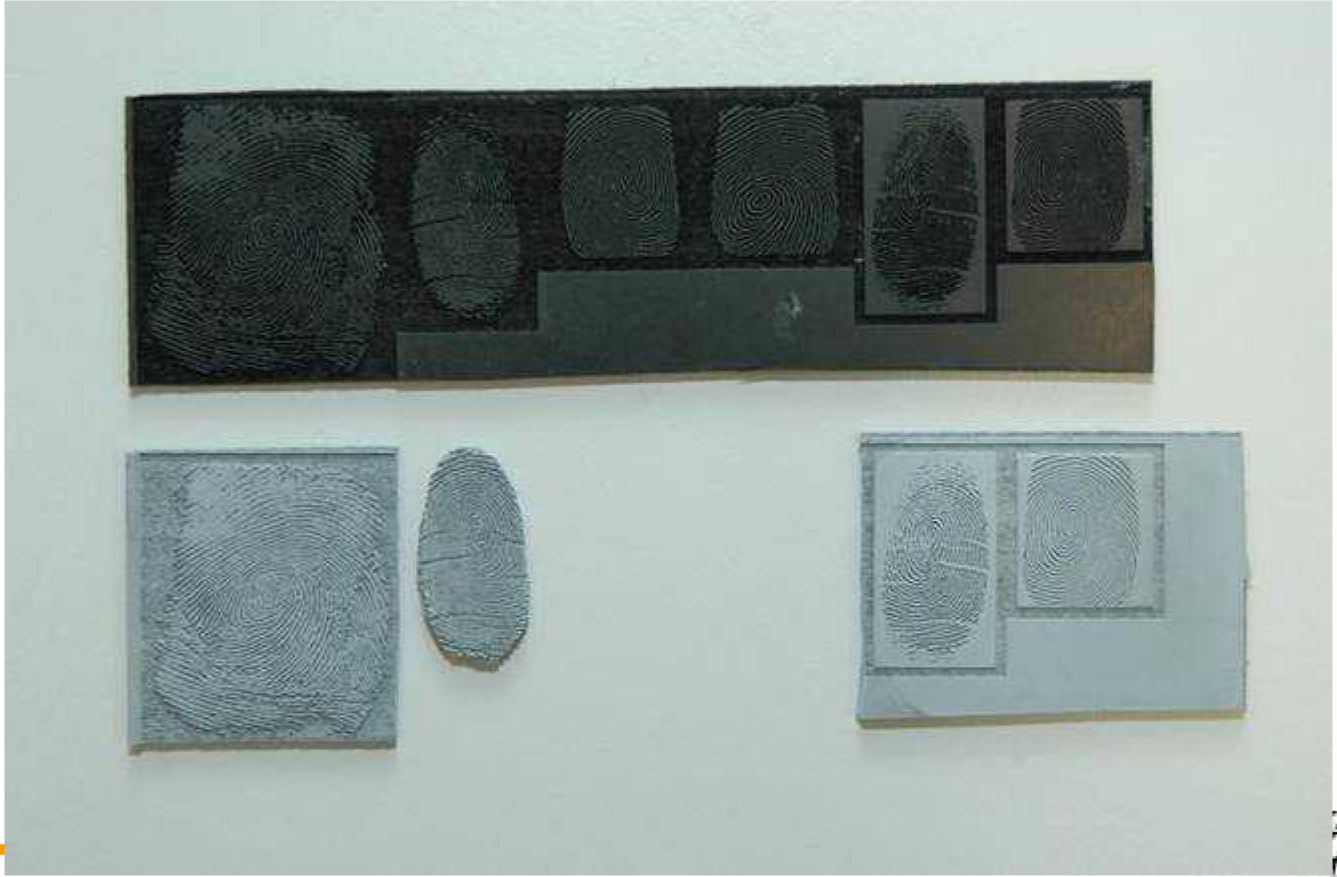




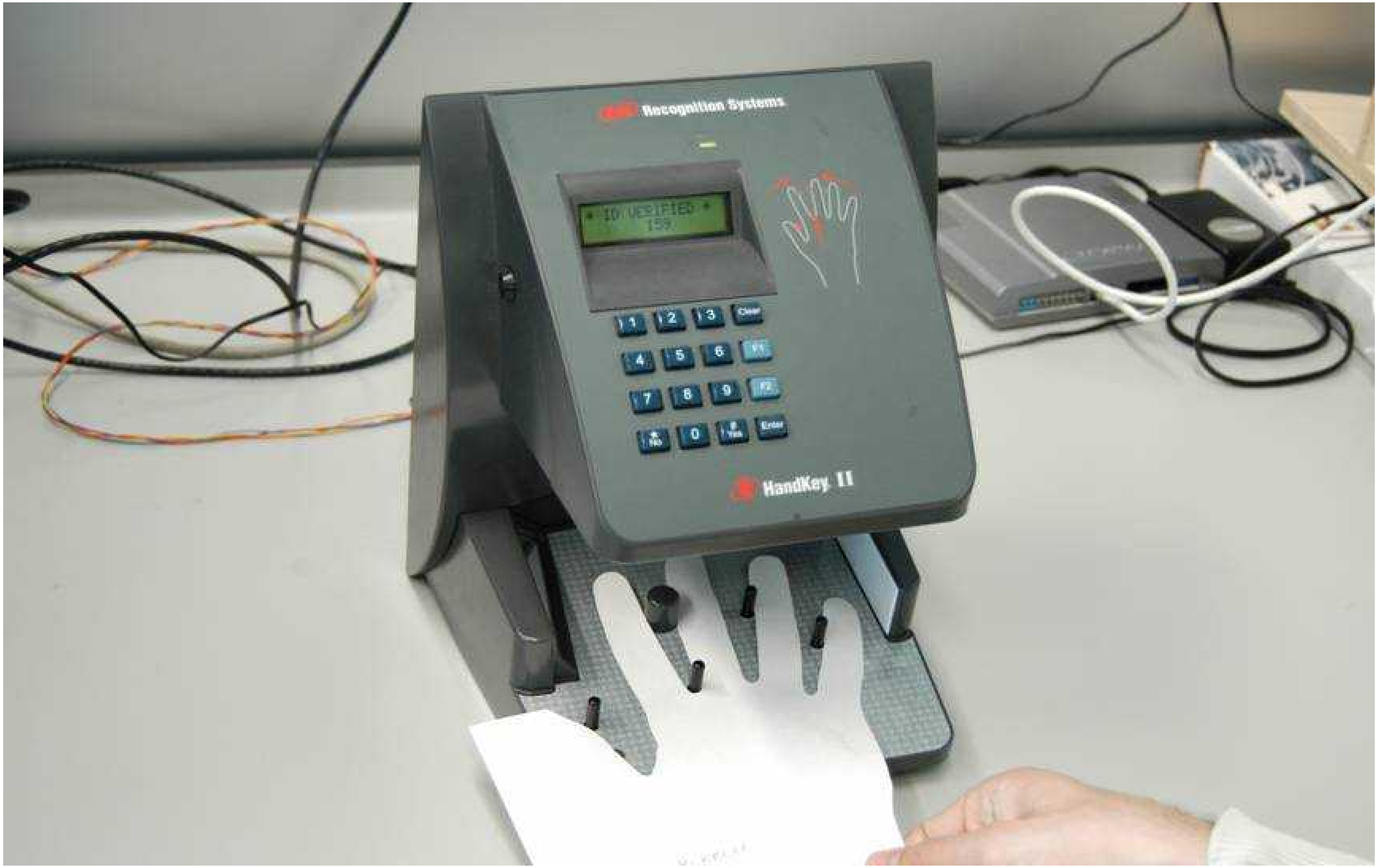


Rubber Stamp

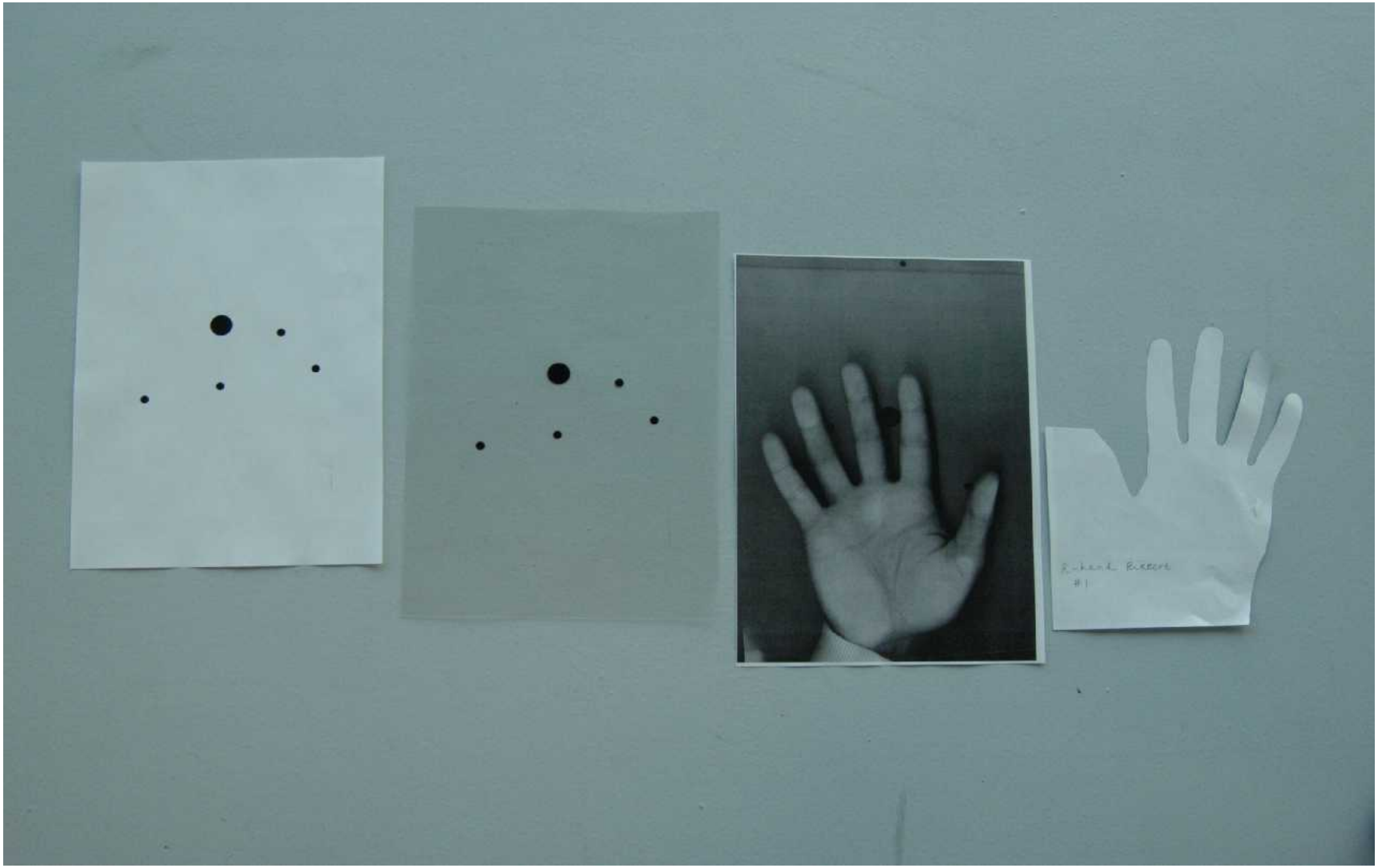
- Just send your fingerprint by email to a stamp manufacturer



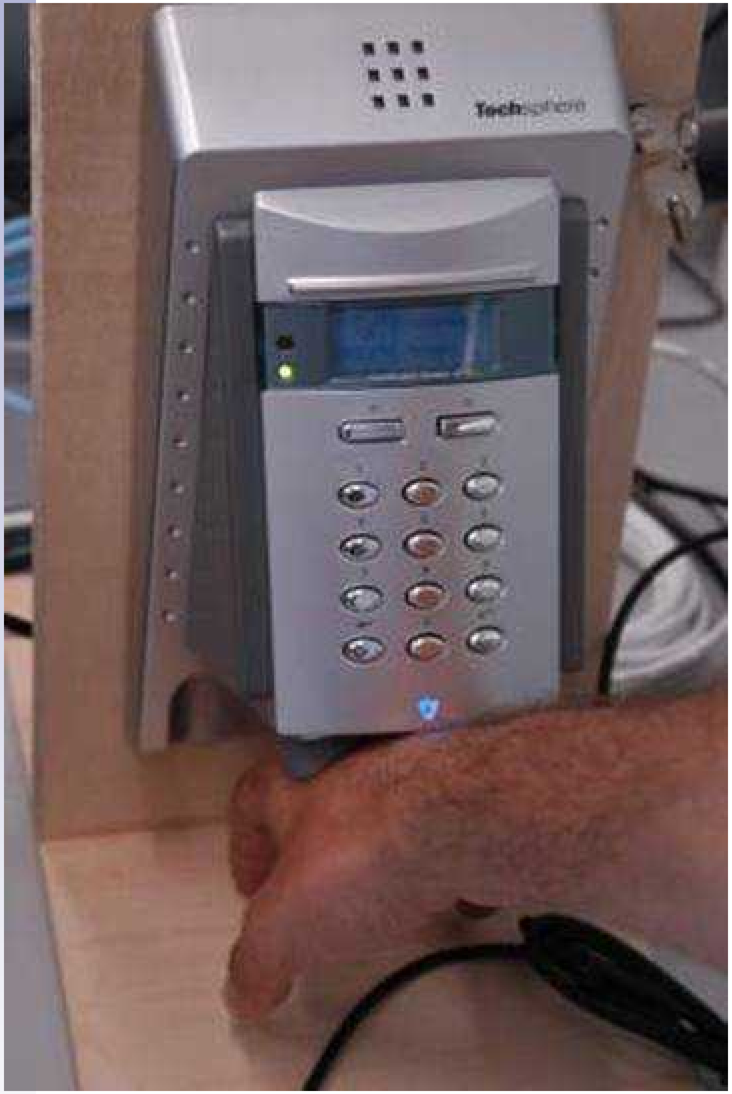
Hand copy

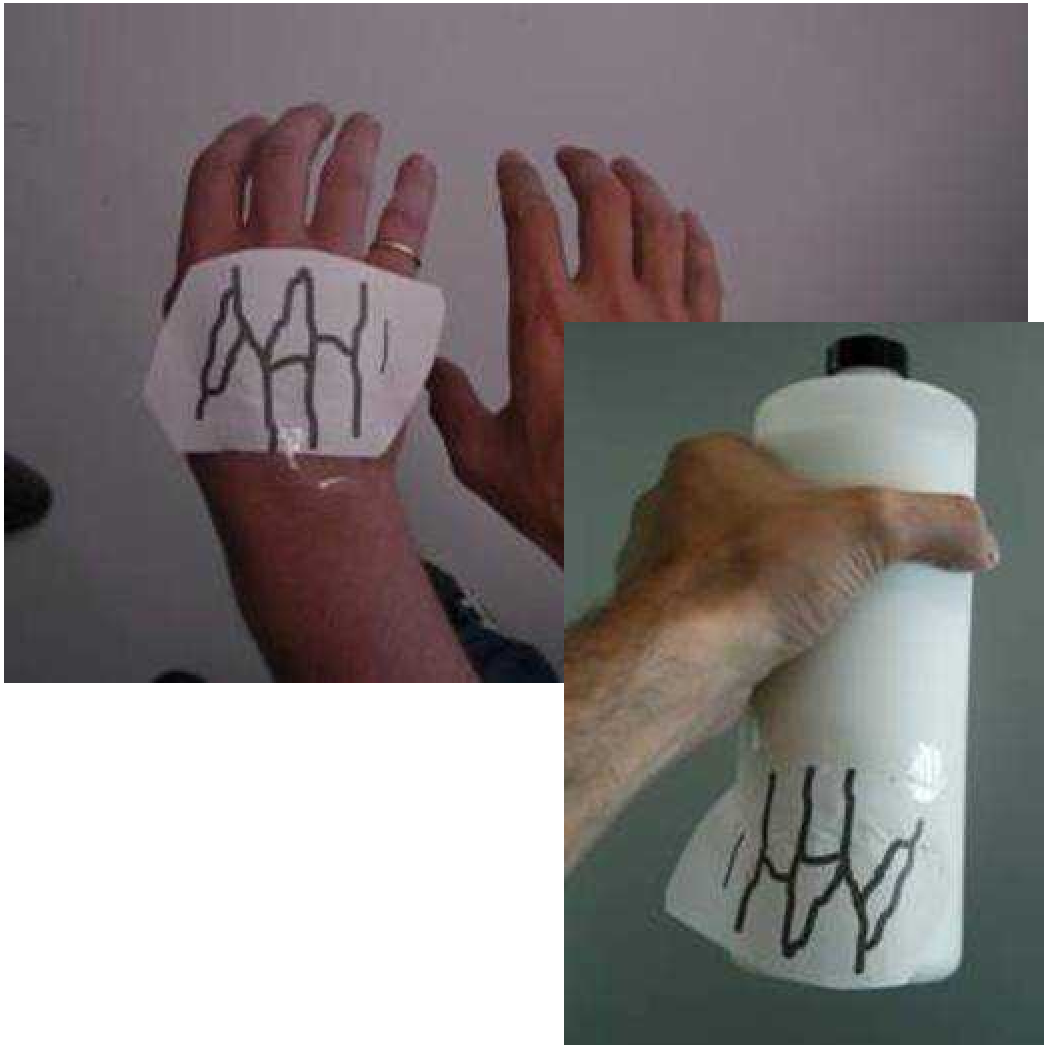

Recognition Systems
* ID VERIFIED *
159
1 2 3 Clear
4 5 6 F1
7 8 9 F2
No 0 Yes Enter
HandKey II

How to

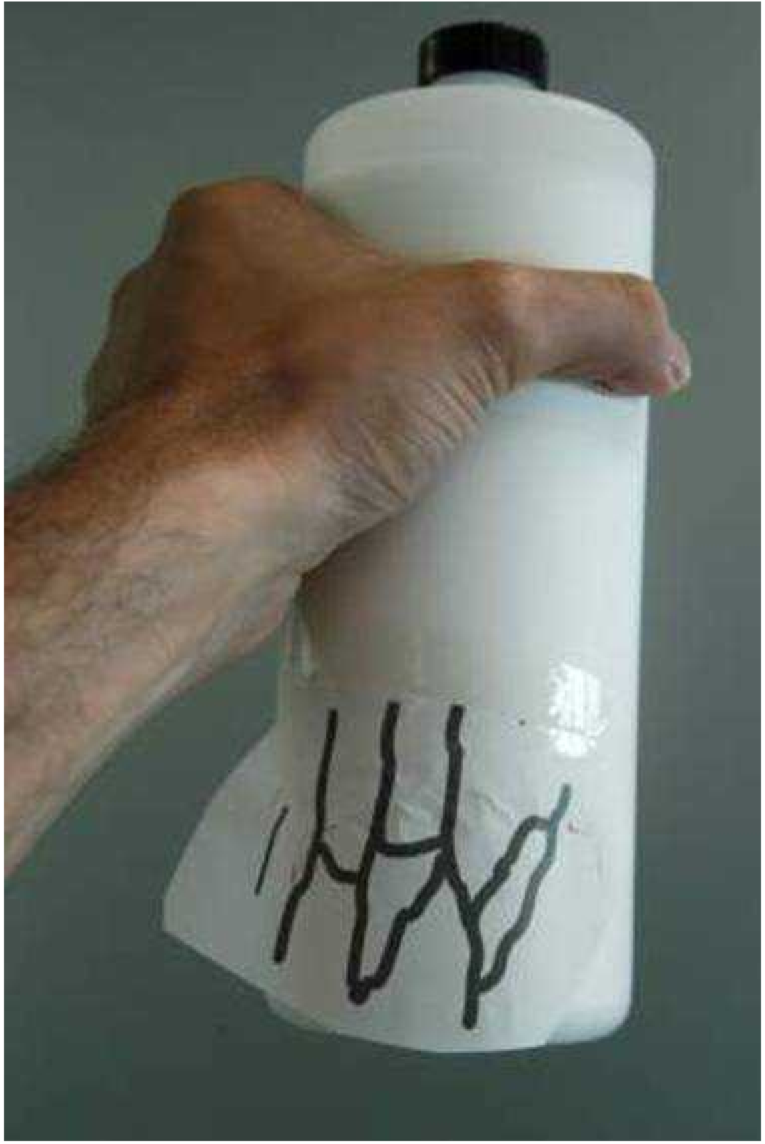


Vein scanner





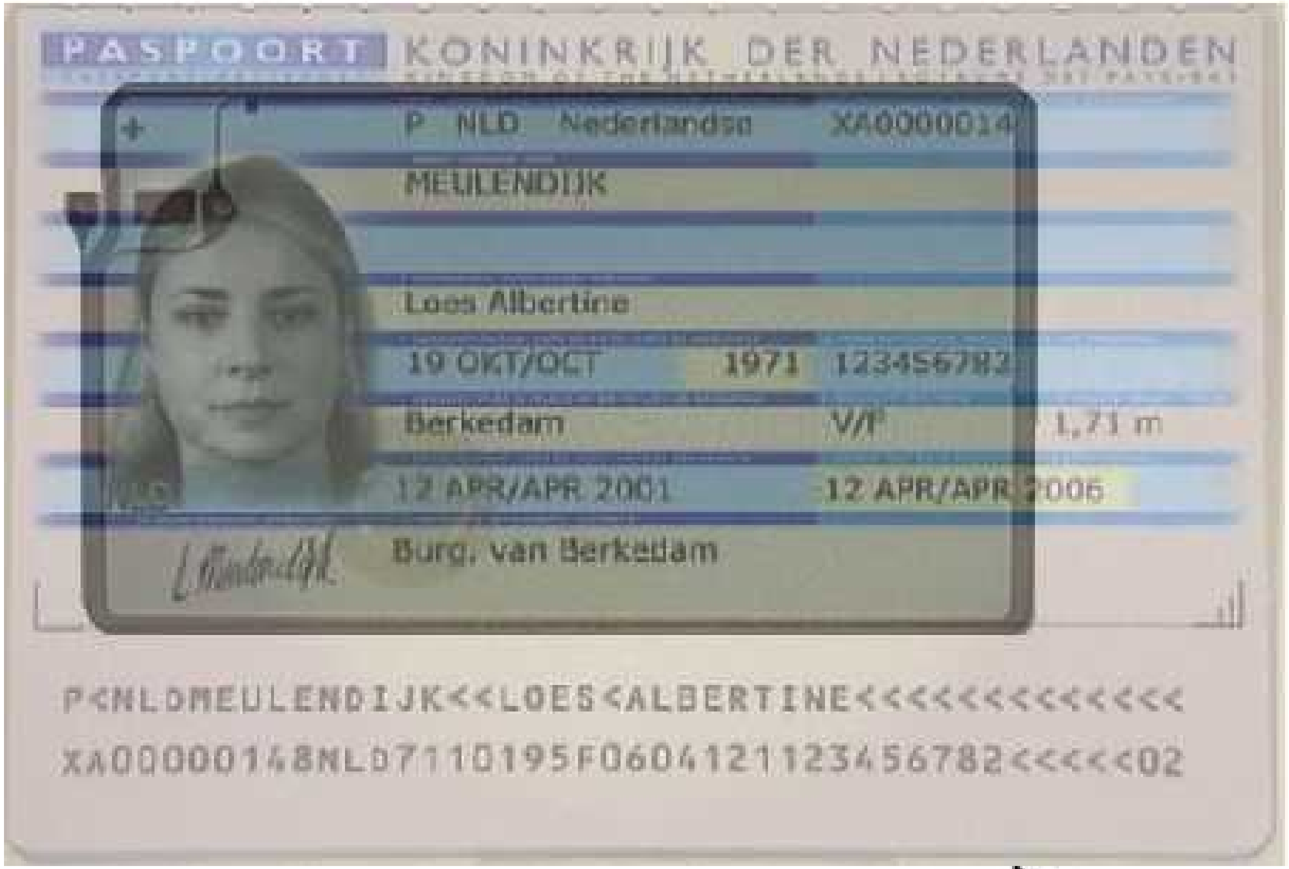
Vein Scanner (2)



ICAO Standards

- Face recognition
  - Image in stead of template
- Contactless chiptechnology
  - ISO/IEC 14443 type A or B
- Logical Data Structure
  - Design of the chip
- PKI for MRTDs
  - Secure and authenticate information on the chip
- Optional 2nd biometric features
  - Fingerprint & Iris

Contact less Chip Technology



PASPOORT KONINKRIJK DER NEDERLANDEN

P NLD Nederlandse XA0000014

MEULENDIJK

Loes Albertine

19 OKT/OCT 1971 123456782

Berkedam V/F 1,71 m

12 APR/APR 2001 12 APR/APR 2006

Burg. van Berkedam

P<NLDMEULENDIJK<<LOES<ALBERTINE<<<<<<<<<<<<<

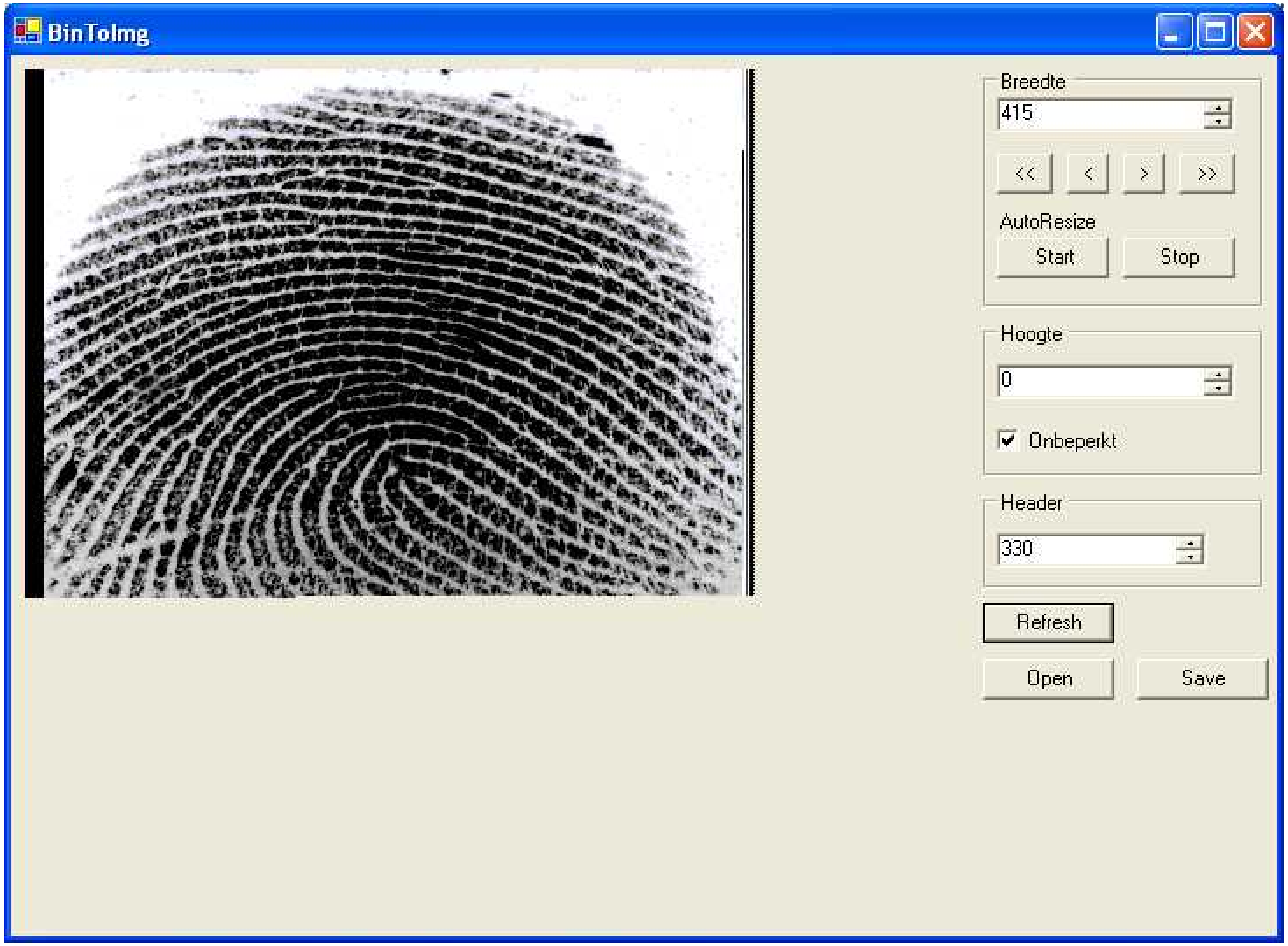
XA00000148NLD7110195F0604121123456782<<<<<02

Threats for biometric systems (summarized)

1: User.	Authorized user provides own biometric sample, unknowingly, unwillingly or willingly (collusion), to imposter.
2: User/capture.	Authorized user tries to enroll a weak biometric template. Imposter presents own biometric sample in an attempt to impersonate an authorized user. Imposter modifies own biometric in an attempt to impersonate. Imposter presents an artificial biometric sample. Imposter uses a residual biometric in an attempt to impersonate the last user (e.g. latent fingerprint).
3: Capture/extraction.	Imposter intercepts an authorized biometric sample, and inserts the authorized biometric sample (replay).
4: Extraction/comparison.	Imposter intercepts extracted biometric features, and inserts these into the comparison subsystem.
5: Enrollment Extraction/Template storage	Imposter intercepts an authorized biometric template. Unauthorized user is enrolled due to error or by replacement of an authorized user template
6: Template storage.	Attacker modifies templates in storage. Imposter presents own biometric after manipulation of a template storage device. Imposter steals the biometric template of an authorized user from a storage device.
7: Template Retrieval.	Imposter intercepts an authorized biometric template during transmission between Storage and Comparison subsystems. Imposter inserts own template directly into the comparison subsystem.
8: Administrator/Resource manager.	A hostile unauthorized user may acquire administrator privileges Non-hostile administrator or hostile unauthorized user or imposter incorrectly modifies matching thresholds, incorrectly modifies user privileges, allows unauthorized access to template storage, allows unauthorized modification of audit trail, enrolls unauthorized user. Administrator fails to properly review and respond to audit trail anomalies.
9: User policy/management.	Imposter authenticates as authorized user through collusion, coercion, password, backup system,
10: Policy management.	Audit data collection inadequate to detect attacks, attacker modifies user identity.
11: Policy management/portal.	Attacker bypasses biometric system by inserting appropriate “grant privileges” signal directly into portal. Attacker disables system, and defeats backup system or alternative authentication method
12: Portal.	Attacker gains unauthorized access with the willing or unwilling aid of an authorized user User gains access to unauthorized privileges after improper modification of privileges.
13: Hardware components.	Attacker tampers, modifies, bypasses, or deactivates one or more components, and exploits hardware “back-door”, design flaw, environmental conditions, or failure mode. Attacker floods one or more components with noise (e.g. electromagnetic energy). Imposter intercepts or inserts authorized biometric templates to one or more hardware components.
14: Software/firmware components.	Attacker tampers, modifies, bypasses, or deactivates one or more executables, and exploits software “back-door”, algorithm quirk, design flaw, or failure mode. A virus or other malicious software is introduced into the system. Imposter intercepts or inserts authorized biometric template to one or more software or firmware components.
15: Connections (including network).	Attacker tampers, modifies, bypasses, or deactivates one or more connections between components. Imposter intercepts or inserts authorized biometric sample or template during transmission.

Common Methodology for Information Technology Security Evaluation, The Biometric Evaluation Methodology Working Group, 2002

USB Sniffing example from fingerprint



BinToImg

Breedte

415

AutoResize

Hoogte

0

☑ Onbeperkt

Header

330

Biometric system Issues

- Biometrics not absolute identification
- Biometrics are not secret
- Biometrics cannot be changed/revoked (theft/spoofing)
- Biometric algorithms are not validated
- How to know when security level falls

Tony Mansfield, Philip Statham Biovision,2003

User Concerns

- Biometric may be stolen
- Identity theft
- Increased chance of capture/coercion
- Authentication failure
- Operator/administrator misuse
- Audit trail reveals personal information
- Use without consent
  - Giving biometric by accident
  - Covert collection of biometric
- Function creep
  - Database searched for criminal suspects

Tony Mansfield, Philip Statham Biovision,2003

Outline

- Definition of Biometrics
- Biometrics at the NFI
- Biometric systems
- Automatic verification
- Privacy issues
- Future of biometrics

Future developments

- Biometrics mandatory in travel documents
- Mass introduction of biometric systems?
- Large datasets
- Statistics about features from biometric systems available for forensic identification research
- Knowledge base for biometric features and systems

Discussion

- Most test with people that cooperate

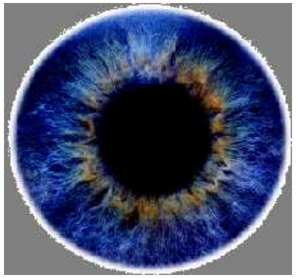
- What if people damage the sensor
- Damage the chip
- Fall back system

Summary

- In some cases expectations of biometric systems are still too high
- Consensus about biometric systems testing is growing*, but implementation is still lacking
- Current mass-market products are relatively easy to ‘spoof’
- Privacy issues depend on technology and system implementation
- Multimodal biometrics (3D + 2D + IR of face)
- Biometry is gaining importance in forensics

*http://www.cesg.gov.uk

Image Analysis and Biometrics



Questions?
zeno@holmes.nl