Datenschutz und Biometrie

Dr. Thomas Probst

Unabhängiges Landeszentrum für Datenschutz
Schleswig-Holstein, Kiel
LD91@datenschutzzentrum.de



Biometrische Merkmale

- Fingerabdruck
- Iris
- Retina
- Handgeometrie
- Handvenenmuster
- Gesicht

physiologische Merkmale

- Stimme
- Handschrift
- Lippenbewegung
- Tipprhythmus

verhaltensbasierte Merkmale (z. T. mit Wissenkomponente)

Gesichtserkennung





Fingerabdruck









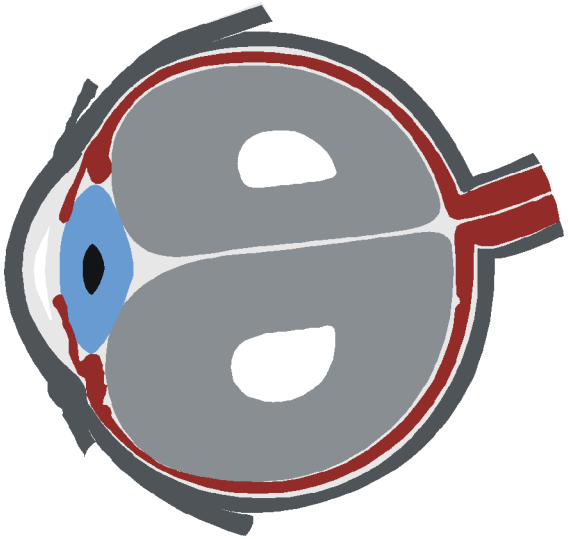
Quelle: www.bergdata.com



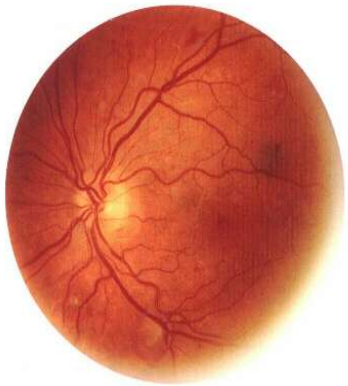


Quelle: www.bioscrypt.com

Auge: Retina





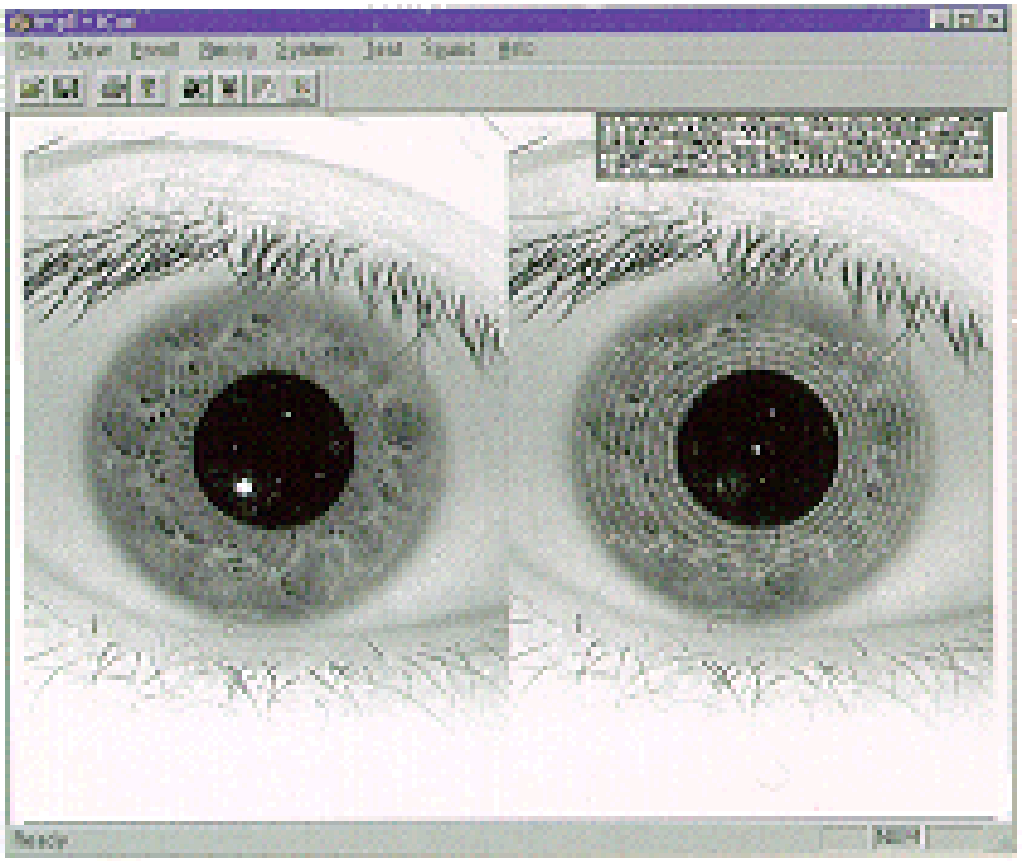


Quelle: Retica Systems

Auge: Iris







Quellen: www.iridian.com

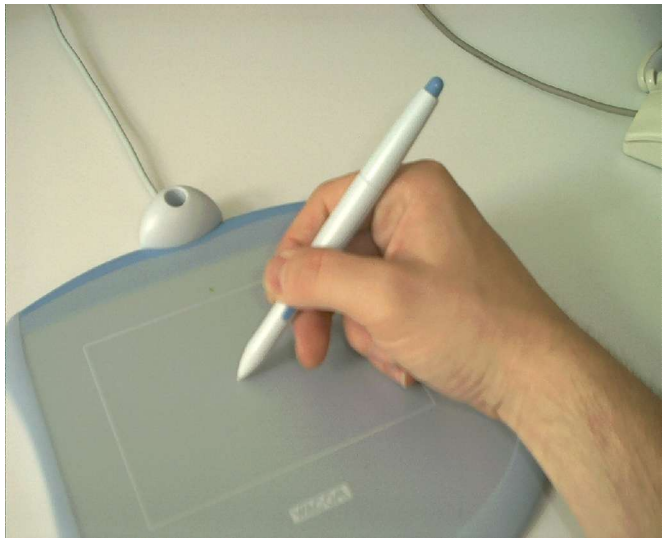
www.lgiris.com

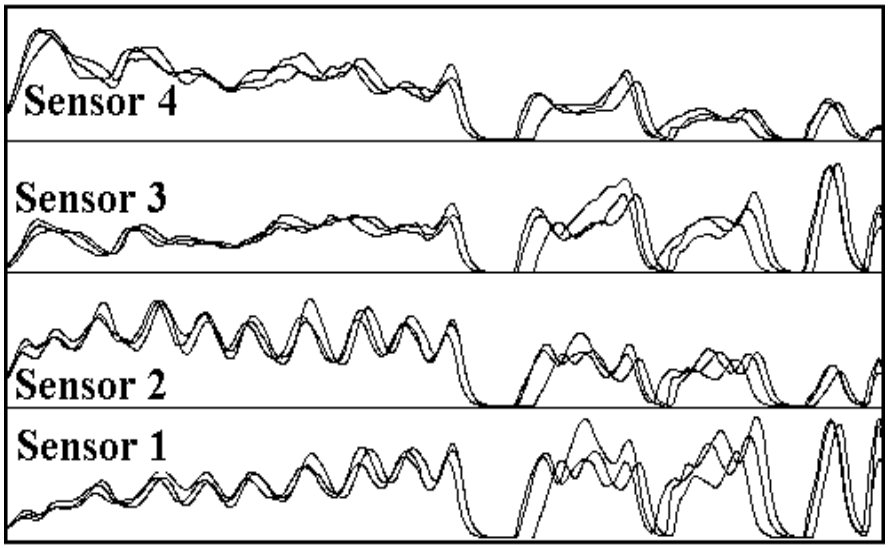
Auge: Iris




Power Indicator
VFD window
(graphical display enhances interactive interface, communicates authentication status)
Iris Camera
(exclusive autofocus iris image aquisition process delivers rapid two eye enrollment/recognition)
Facial Recognition Illuminator
Facial Recognition-Ready Camera
(captures facial image for facial recogniton)
Up/Down Button
(motorized auto-drive for easy height adjustment)
Alphanumeric Keypad
(supports PIN input and workforce management interface)
Device-Embedded SmartCard Reader
(delivers LG iDentity token authentication with leading smartcards)
Ethernet
USB
Serial (RS-232/422)
Wiegand
35°
20°

Unterschriftserkennung





statische Verfahren: Schriftbild

dynamische Verfahren: Schreibdynamik

Unterschriftentablett SmartCardspeicherung



Quelle: www.softpro.de

Handgeometrie



Quelle: http://www.jaypeetex.com/

Biometrieanwendungen

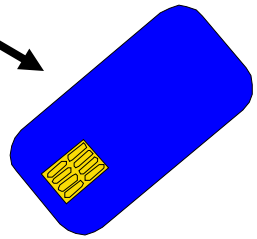
- öffentlicher Bereich:
  - Einsatz bei Strafverfolgung [AFIS]
  - verpflichtender Einsatz [Pässe, Visa]
  - freiwilliger Einsatz [bisher: Einreise von Vielfliegern]
- nicht-öffentlicher Bereich
  - Arbeitnehmerbereich [Zutrittskontrolle, Computerzugang]
  - Einsatz beim Kunden [Bankgeschäfte (SB/Home), Biergarten, Kontrolle des Hausrechts]
- private Anwendungen (Komfortbereich)
  - Auto, Mobiltelefon, Videorekorder
- elektronische/digitale Signatur (?)

Bindung an elektronische Signaturen

Person



- Besitz (im Zugriff des Benutzers)
- Wissen (PIN/Passwort)
- Sein (Biometrie)



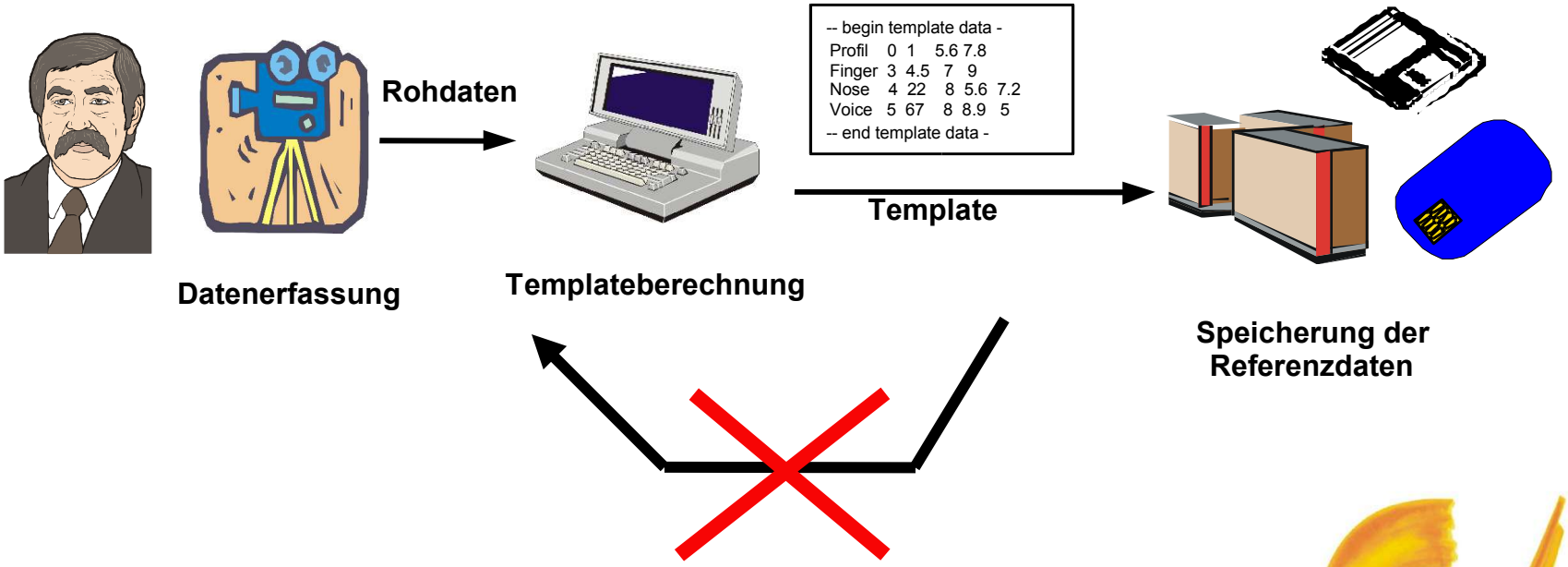
elektronisches Dokument



elektronische Signatur

e3kstx93hjdk2p2

Funktionsweise



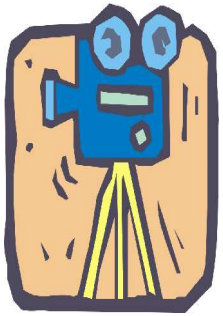
Beispiel: Fingerabdruckerkennung



Minutien

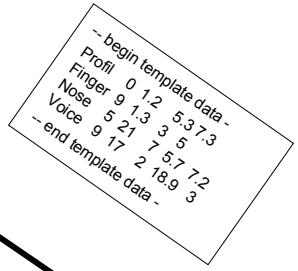
Kuhn, Markus: Security – Biometric Identification.
http://www.cl.cam.ac.uk/Teaching/2003/Security/guestslides/slides-biometric-4up.pdf

Kontrolle: Verifikation

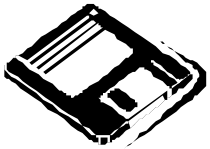


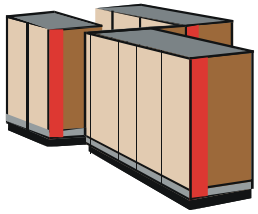


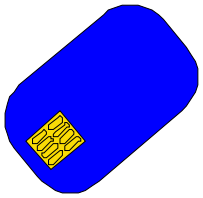


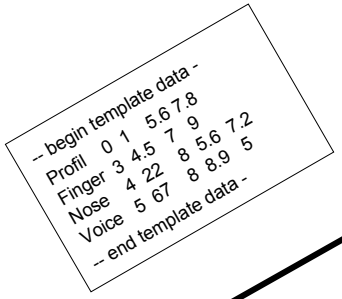






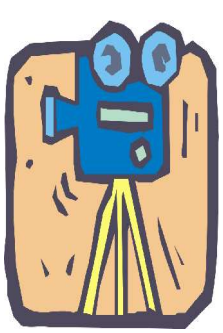








Kontrolle: Identifikation



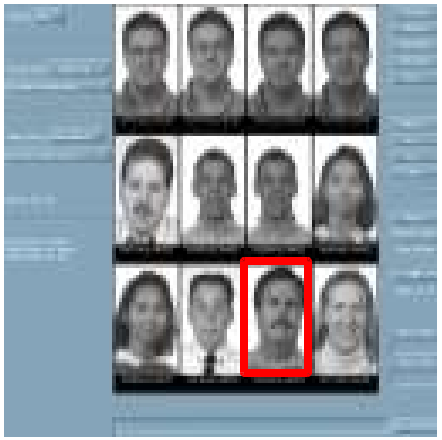




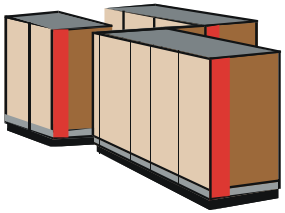
-- begin template data -
Profil 0 1.2 5.3 7.3
Finger 9 1.3 3 5
Nose 5 21 7 5.7 7.2
Voice 9 17 2 18.9 3
-- end template data -

?

=



-- begin template data -
Profil 0 1 5.6 7.8
Finger 3 4.5 7 9
Nose 4 22 8 5.6 7.2
Voice 5 67 8 8.9 5
-- end template data -



-- begin template data -
Profil 0 1 5.6 7.8
Finger 3 4.5 7 9
Nose 4 22 8 5.6 7.2
Voice 5 67 8 8.9 5
-- end template data -

Sicherheit durch Templateverwendung?

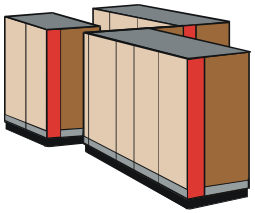
Oft gehörtes “Beruhigungs”argument:

“Wir speichern nur Templates, keine Rohdaten; aus den Templates können die Rohdaten nicht gewonnen werden.”

- **Dies ist vermutlich richtig (bei der Templaterzeugung geht “Information” verloren – aber vielleicht lassen sich mit Teilen der Templateinformationen Teile der Rohdaten rekonstruieren (z. B. Minutien)?)**
- **Templates gleichartiger Algorithmen lassen sich elektronisch weiterverwenden (z. B. “rastern”). Bei Iris-Verfahren gibt es nur einen Algorithmus**

Verfahren funktioniert auch mit Rohdaten (ohne Speicherung der Templates) z. B. in Reisepässen. Zukünftig Verzicht auf Templates, wenn Verarbeitungs- und Speicherkapazität steigen?

Datenabgleich mit Templates



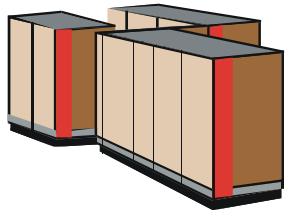
-- begin template data -
Profil 0 1 5.6 7.8
Finger 3 4.5 7 9
Nose 4 22 8 5.6 7.2
Voice 5 67 8 8.9 5
-- end template data -

=?

-- begin template data -
Profil 0 1 5.6 7.8
Finger 3 4.5 7 9
Nose 4 22 8 5.6 7.2
Voice 5 67 8 8.9 5
-- end template data -

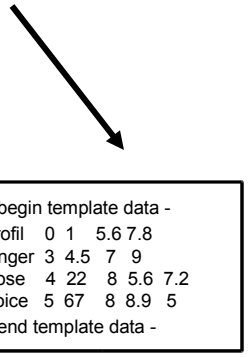
-- begin template data -
Profil 0 1 5.6 7.8
Finger 3 4.5 7 9
Nose 4 22 8 5.6 7.2
Voice 5 67 8 8.9 5
-- end template data -

-- begin template data -
Profil 0 1 5.6 7.8
Finger 3 4.5 7 9
Nose 4 22 8 5.6 7.2
Voice 5 67 8 8.9 5
-- end template data -

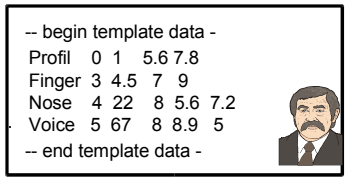


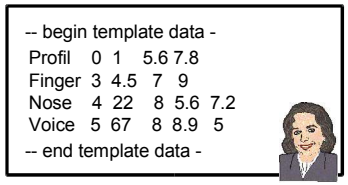
Datenabgleich mit Rohdaten und Templates

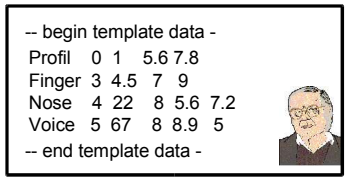


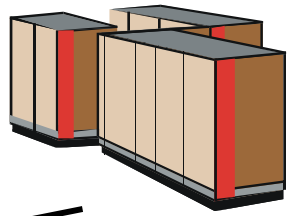




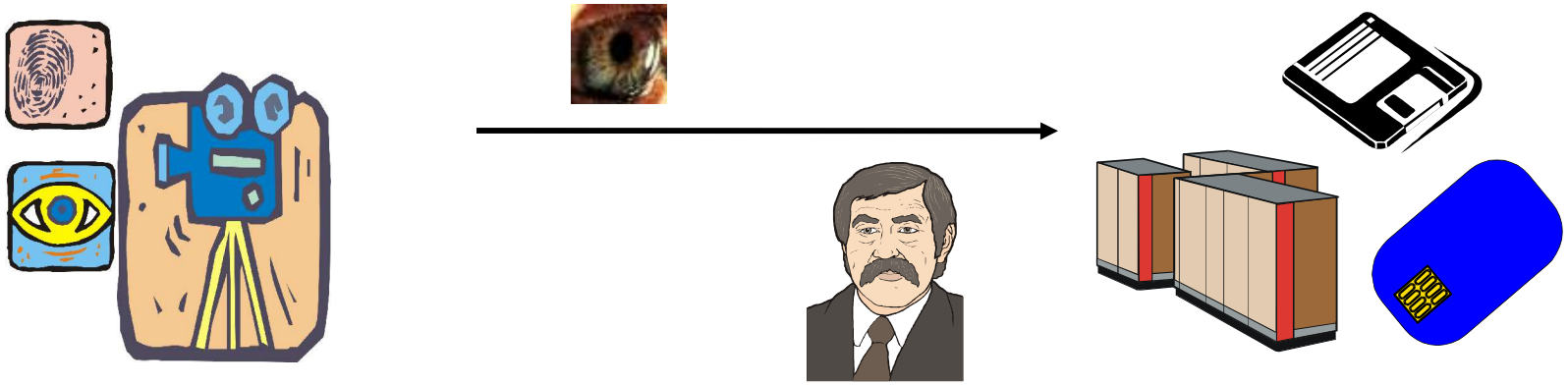




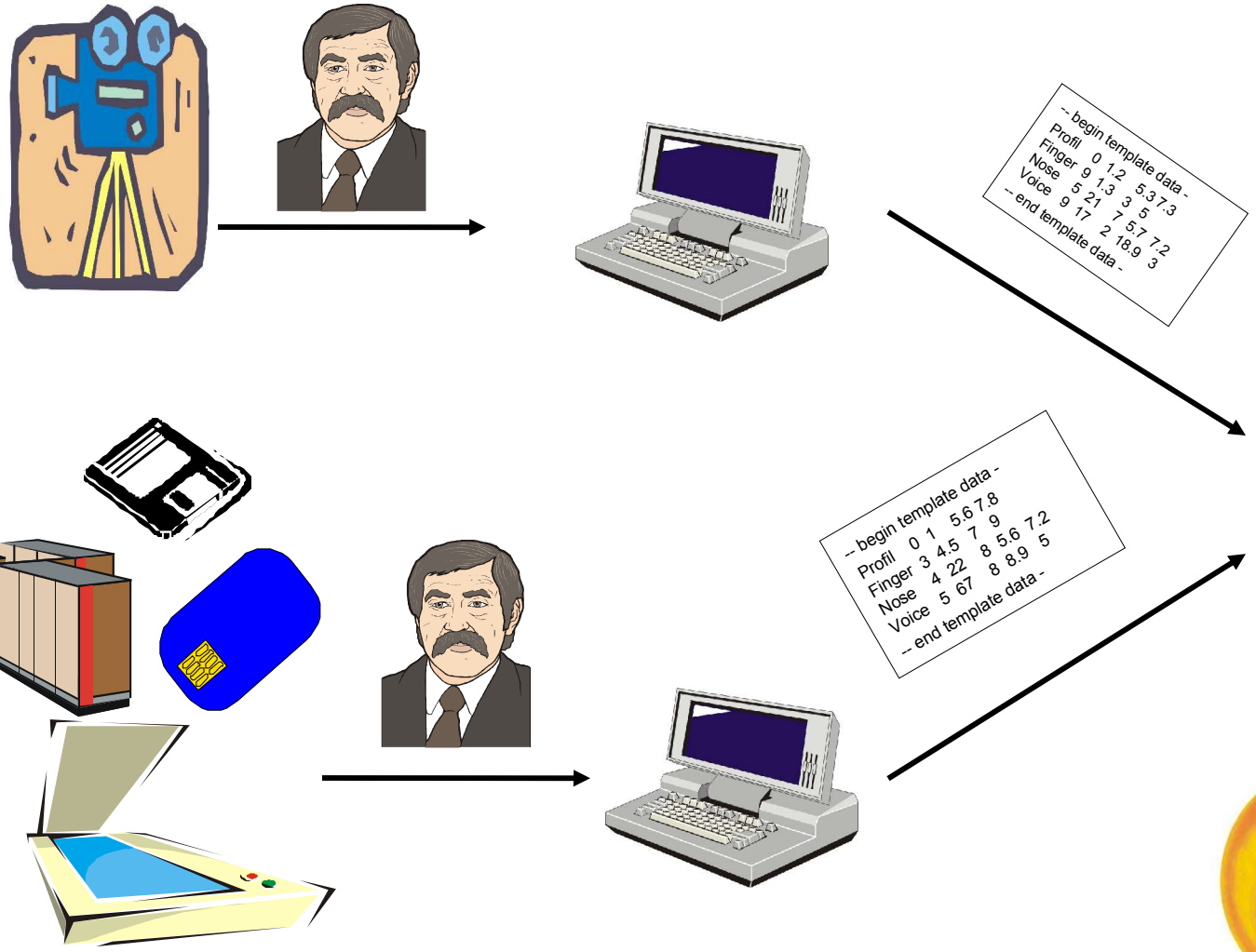




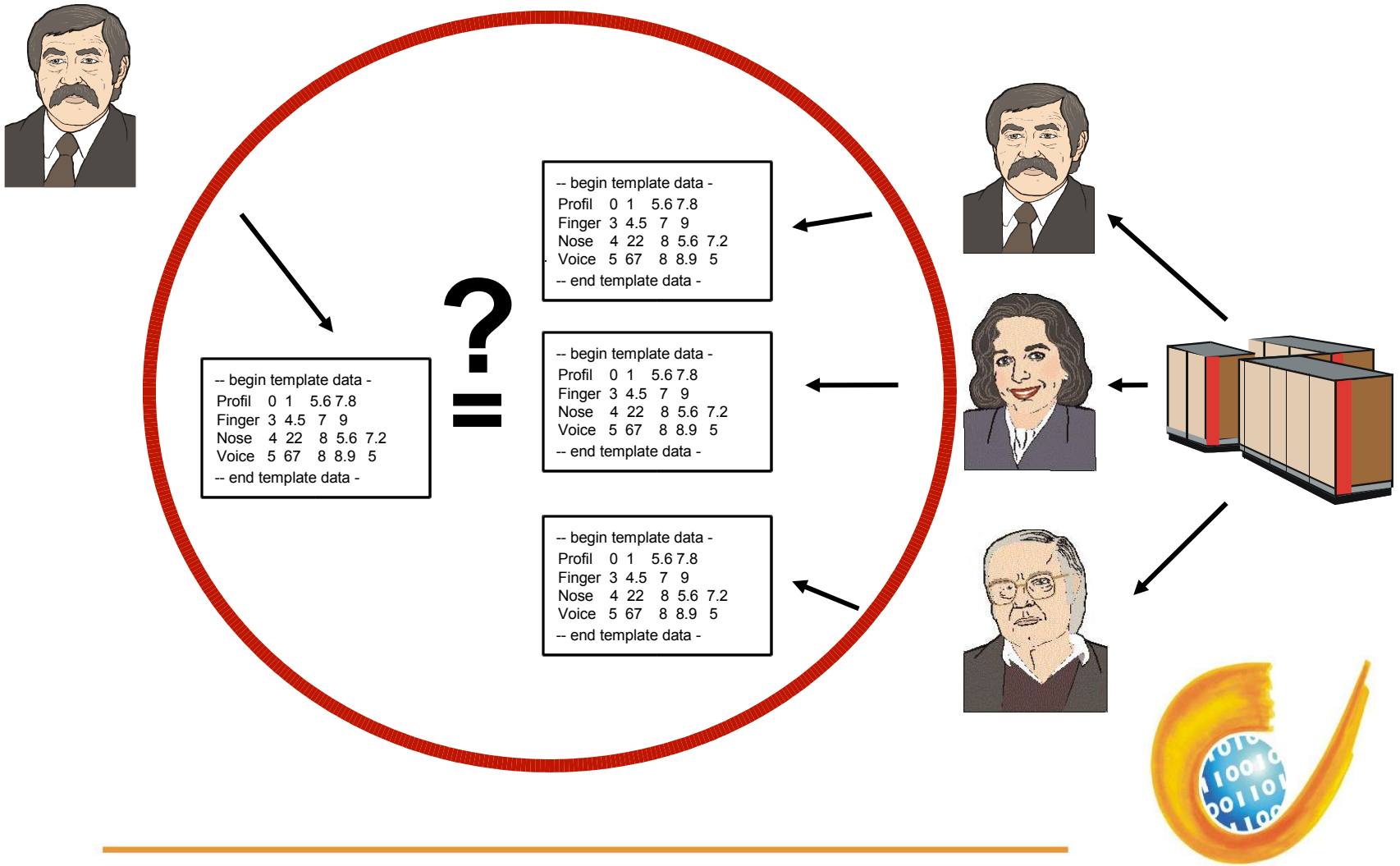
Einlernen der Rohdaten



Verifikation der Rohdaten



Datenabgleich mit Rohdaten

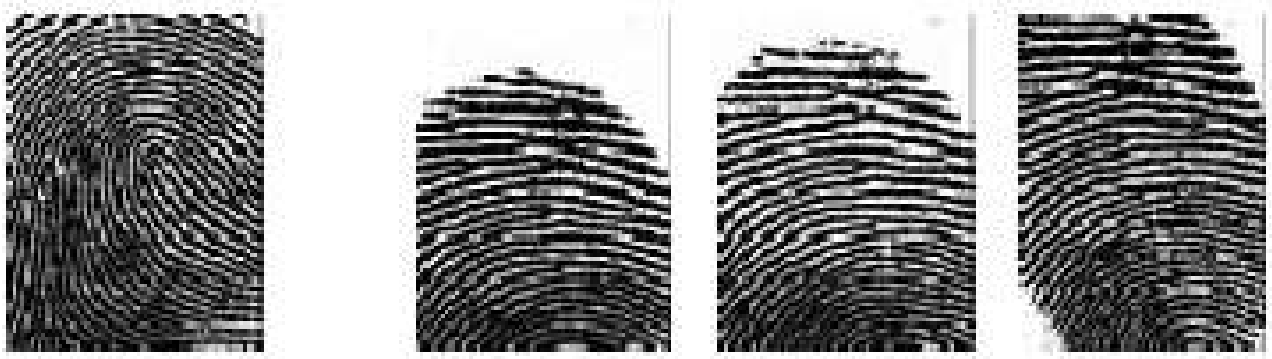


Probleme beim Einlernen und der Erfassung

- nicht alle Personen lassen sich biometrisch erfassen ("failure to enroll")
- kaum Probleme: Gesichtserkennung
- mehr Probleme: Fingerabdruck ("Abrieb", Verschmutzungen)
- Diskriminierung von Seh-, Sprachbehinderten?
- Widersprüchliche statistische Angaben

Probleme beim Einlernen und der Erfassung

- Fehler bei der Erfassung (“Failure-to-aquire”):
  - Fingerabdrücke: Verletzungen, Verschmutzungen, “Abrieb”
  - Stimme: Heiserkeit
  - Schrift: Handverletzungen



Quelle: Mike Fairhurst : Document identity, authentication and ownership: *The future of biometric verification*

Failure-to-enroll /Failure-to-acquire

•**Failure-To-Enroll Rate (FTE):** proportion of enrollment transactions in which the device is unable to complete the enrollment process

•**Failure-To-Acquire Rate (FTA):** proportion of recognition attempts in which the device is unable to capture or locate an image or signal of sufficient quality

• **Transactional Failure-To-Acquire Rate (T–FTA):** proportion of recognition transactions in which the device is unable to capture or locate an image or signal of sufficient quality
(transaction: up to 6 attempts)

Definitionen und folgende Tabellen aus eine Feldtest mehrerer Verfahren :

Independent Testing of Iris Recognition Technology (ITIRT), Final Report, May 2005, http://www.biometricgroup.com/reports/public/ITIRT.html

OKI IRISPASS-WG	Enrollment Transaction 1		Enrollment Transaction 2		Sum: Enrollment Transactions 1&2	
Total # Transactions	1682	100.00%	1682	100.00%	3364	100.00%
Transactions with Zero Irides Enrolled	42	2.50%	43	2.56%	85	2.53%
Transactions with One Iris Enrolled	129	7.67%	133	7.91%	262	7.79%
Transactions with Two Irides Enrolled	1511	89.83%	1506	89.54%	3017	89.68%

Figure 31: OKI Enrollment Results

LG IrisAccess 3000	Recognition Attempts	Recognition Attempts with Sample Acquired	Recognition Attempts with No Sample Acquired	FTA
Transaction 1	10075	9571	504	5.00%
Transaction 2	10054	9583	471	4.74%
Transaction 3	10063	9616	447	4.48%
Total	**30192**	**28770**	**1422**	**4.74%**

Figure 38: LG Failure to Acquire Rates (FTA)

OKI IRISPASS-WG	Recognition Transaction 1		Recognition Transaction 2		Recognition Transaction 3		Recognition Transactions 1-3	
	#	%	#	%	#	%	#	%
Total Transactions	1681	100.00%	1680	100.00%	1679	100.00%	**5040**	**100.00%**
Zero Iris Samples Acquired	8	0.48%	4	0.24%	4	0.24%	**16**	**0.32%**
≥ 1 Left or ≥ 1 Right Iris Sample Acquired	17	1.01%	14	0.84%	15	0.89%	**46**	**0.91%**
≥ 1 Left and ≥ 1 Right Iris Samples Acquired	1654	98.51%	1658	98.93%	1657	98.87%	**4969**	**98.77%**

Figure 42: OKI Transactional Failure to Acquire (T–FTA)

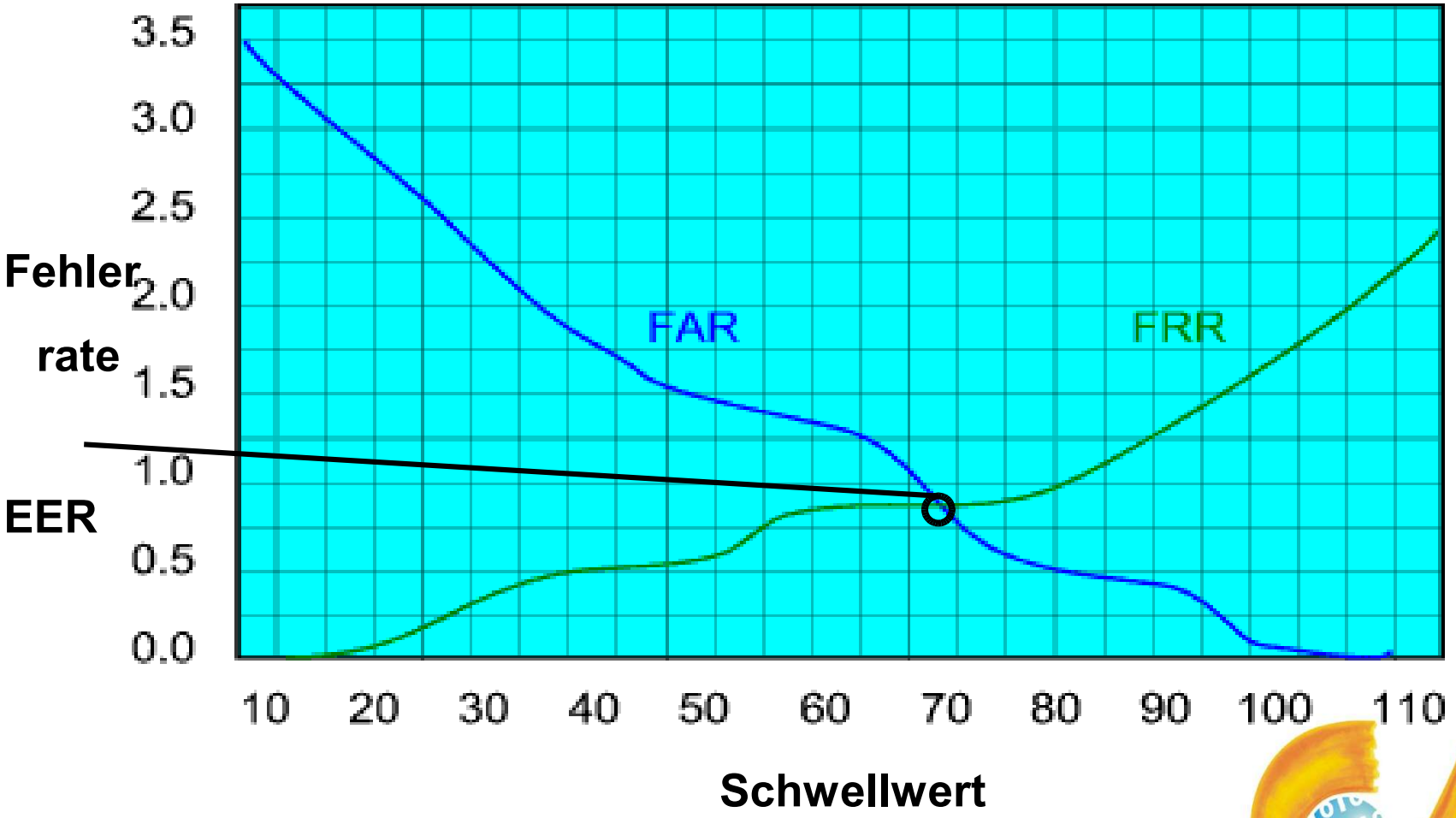
Problem: Falsch (Nicht-)erkennungen

- Biometrische Datensätze sind nie identisch (außer Kopien von Datensätzen), sondern nur ähnlich (Identität wäre Hinweis auf “Angriff”)
- Erkennung: Prüfung, ob Templates “ähnlich genug” sind
- Mögliche Fehlentscheidungen:
  - Falscherkennung („**false match**“):
    keine Gleichheit der biometrischen Daten, aber der Algorithmus entscheidet “ja”
  - Falsch-Nichterkennung („**false non-match**“):
    Trotz Gleicheit entscheidet der Algorithmus “nein”

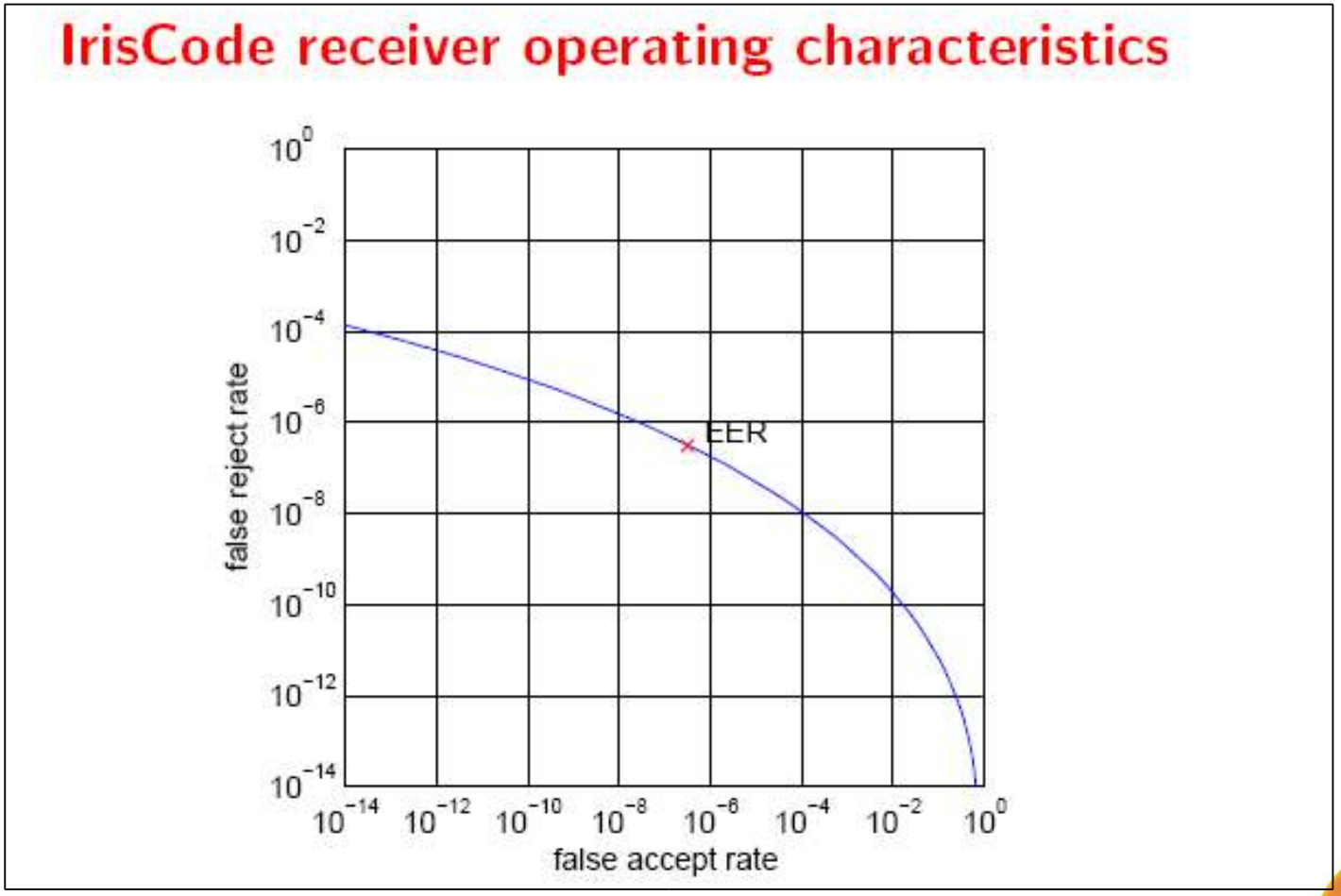
Konsequenzen von Falsch-(Nicht-)erkennungen

- **Konsequenzen:**
  - Falschzurückweisung (oder: falscher Nicht-Treffer bei einer Suchliste) oder
  - Falschakzeptanz (oder: falscher Treffer auf der Suchliste)
- **Statistik:**
  - Falschzurückweisungsrate (“false rejection rate”, (FRR))
  - Falschakzeptanzrate (“false acceptance rate”, (FAR))
  - abhängig von Schwellwert, der die “genügende Ähnlichkeit” für einen Treffer festlegt
  - Fehlerraten bedingen sich gegenseitig und müssen ausbalanciert werden
  - Gleichfehlerrate (equal error rate, EER): Fehlerrate bei der Schwellwerteinstellung, bei der FAR=FRR gilt
- **Schätzen Sie Fehlerraten!**

Fehlerraten



FAR/FRR der Iriserkennung



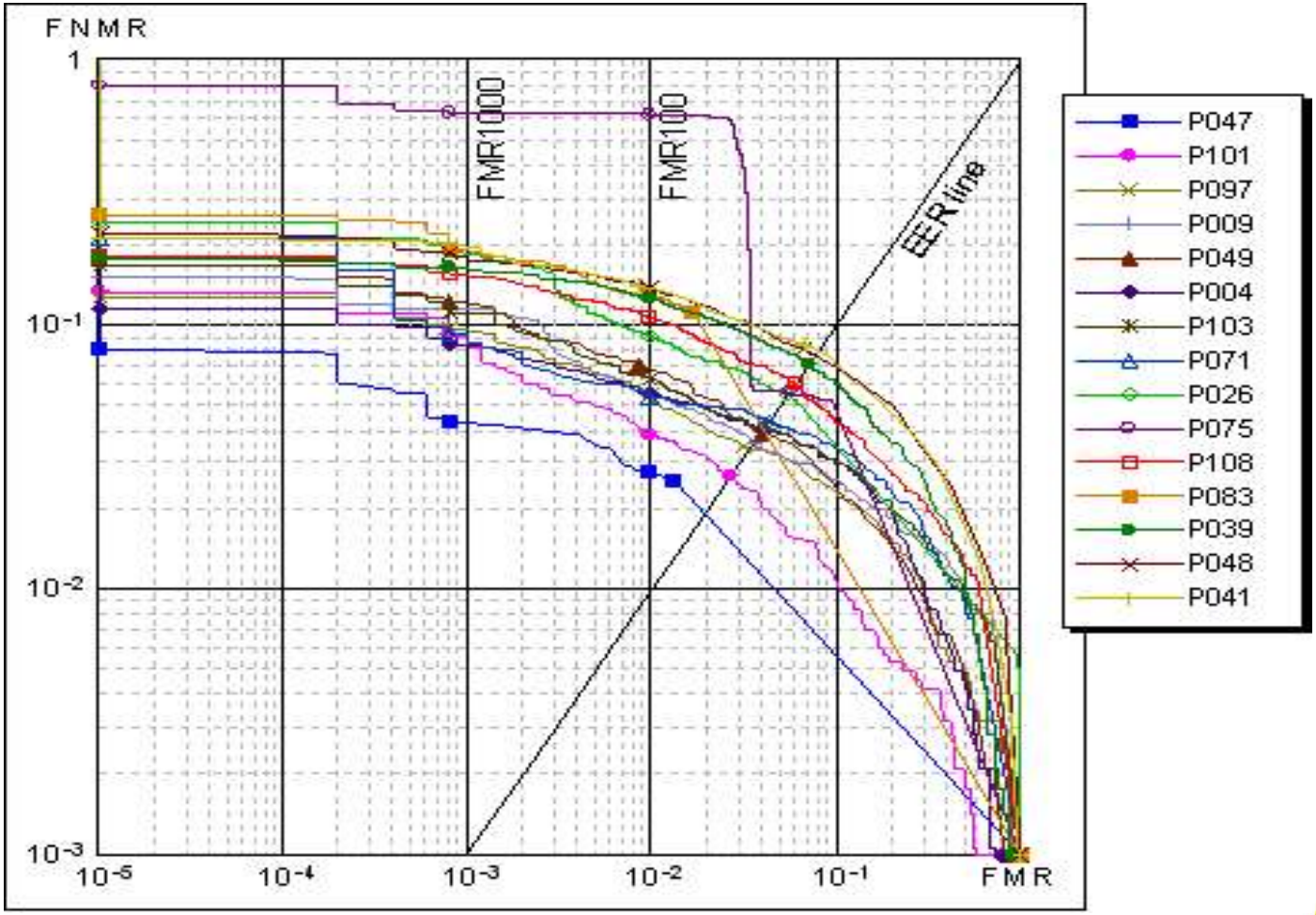
Kuhn, Markus: Security – Biometric Identification.
http://www.cl.cam.ac.uk/Teaching/2003/Security/guestslides/slides-biometric-4up.pdf

	Metric	Attempt-Level				Transaction-Level
		Intra-Visit Enrollment Comparisons	Cross-Visit Enrollment Comparisons	Intra-Visit Recognition Comparisons	Cross-Visit Recognition Comparisons	Cross-Visit Recognition Transactions
LG-LG	FNMR	0.964%	1.636%	4.784%	5.293%	T–FNMR: 1.570%
	FMR	0.00058%	0.00058%	0.00095%	0.00092%	T–FMR: 0.00875%
OKI-OKI	FNMR	1.117%	1.980%	6.655%	6.726%	T–FNMR: 1.038%
	FMR	0.00014%	0.00001%	0.00010%	0.00006%	T–FMR: 0.00035%
PAN-PAN	FNMR	0.759%	1.422%	4.039%	2.906%	T–FNMR: 0.583%
	FMR	0.00013%	0.00031%	0.00023%	0.00024%	T–FMR: 0.00129%
LG-OKI	FNMR	4.090%	5.303%	8.912%	9.384%	T–FNMR: 2.454%
	FMR	0.00021%	0.00025%	0.00028%	0.00032%	T–FMR: 0.00161%
LG-PAN	FNMR	3.617%	3.928%	8.460%	8.520%	T–FNMR: 2.301%
	FMR	0.00035%	0.00023%	0.00043%	0.00038%	T–FMR: 0.00199%
OKI-LG	FNMR	4.141%	4.900%	10.779%	11.283%	T–FNMR: 3.241%
	FMR	0.00021%	0.00019%	0.00019%	0.00016%	T–FMR: 0.00090%
OKI-PAN	FNMR	4.209%	4.031%	9.763%	9.036%	T–FNMR: 2.298%
	FMR	0.00018%	0.00015%	0.00015%	0.00012%	T–FMR: 0.00062%
PAN-LG	FNMR	3.572%	4.371%	7.518%	6.971%	T–FNMR: 2.678%
	FMR	0.00036%	0.00034%	0.00033%	0.00029%	T–FMR: 0.00154%
PAN-OKI	FNMR	4.200%	5.382%	8.212%	7.313%	T–FNMR: 2.644%
	FMR	0.00023%	0.00022%	0.00016%	0.00016%	T–FMR: 0.00083%

Figure 49: Accuracy at .330 HD

F(N)MR: false (non)match rate
Quelle: ITIRI -Studie

Fingerabdruck: *ROC* mehrerer Verfahren



http://bias.csr.unibo.it/fvc2004/results/O_res_db1_a.asp

Fehlerraten bei 1:1 und 1:n-Vergleichen

- ein “gutes” Verfahren für Verifikationen ist noch lange kein gutes Verfahren für Identifikationen
- dazu braucht man “sehr sehr gute” Verfahren
- Beispiel:

  Verifikationsverfahren mit Falscherkennungsrate von 0,1%

  Falscherkennungswahrscheinlichkeit: P = 0,001

  Wahrscheinlichkeit, dass *keine* Falscherkennung auftritt:

  (1-P) =0,999 = 99,9 %

Fehlerraten bei 1:1 und 1:n-Vergleichen

Bei N Vergleichen:

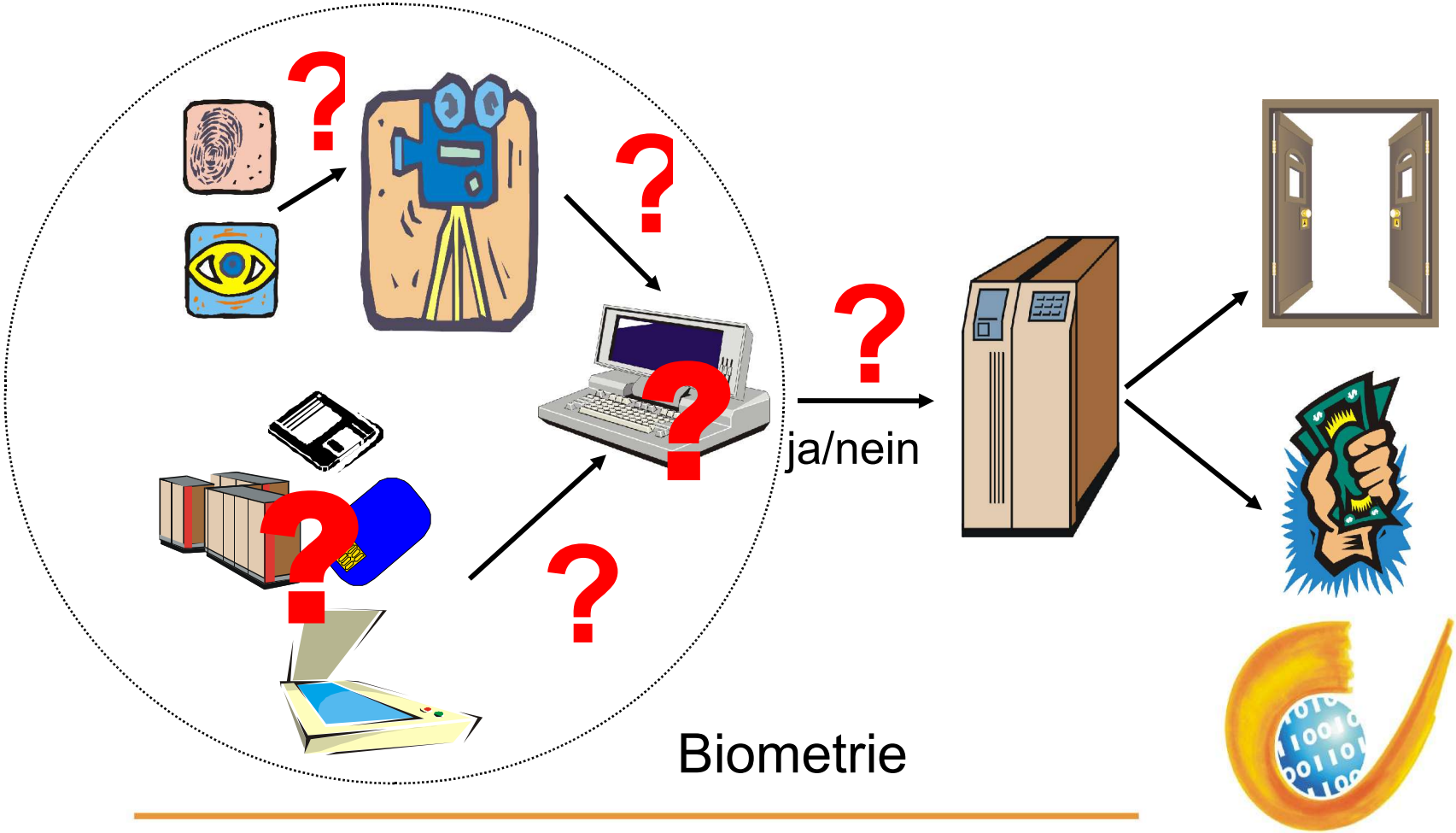
Wahrscheinlichkeit, dass *keine* Falscherkennung auftritt: $(1-P)^N$

Wahrscheinlichkeit, dass *eine* Falscherkennung auftritt: $P_N=1-(1-P)^N$

Datenbankgröße	W. einer Falscherkennung
N = 200	P_N= 18%
N = 2.000	P_N=86%
N = 10.000	P_N=99,995%

Quelle: Daugman, Biometric Decisionlandscapes, Technical Report 482, UCAM-CL-TR-482, ISSN 1476-2986, 2000

Sicherheit: Angriffspunkte



“Fake biometrics” – nachgemachte Merkmale

Repliken biometrischer Merkmale (vor dem Sensor)

- Gummifinger
- Gesichtsmasken
- Kontaktlinsen
- Fotographien von Gesichtern, Iris, etc.
- Videoaufnahmen
- Stimmaufnahmen

- Relevanz: in nicht-überwachten Situationen (Homebanking, Telefon [Voice-over-IP?])

Abhilfe

- Überwindungssicherheit abhängig von Sensortechnik
  - Beispiel Fingerabdruck:
    thermische, optische, kapazitive, Ultraschall- Sensoren
  - Kamera: Normallicht, Infrarot
- z. T. Live-Tests möglich:
  - Augenbewegung bei Gesichtserkennung
  - Pulsmessung bei Fingerabdruckerkennung
  - Pupillenbewegung bei Iriserkennung
- Berichte über Unwirksamkeit (c't)
- z.T. Interaktive Verfahren möglich:
  - Vorgabe nachzusprechnder Worte
  - "Zwinkern auf Befehl"

Datenschutzrechtliche Problemfelder I

- **„überschießende Informationen“:**
  - **Welcher Zusatzgehalt (Krankheiten, persönliche Informationen, ethnische Hintergründe etc.) steckt in biometrischen Daten?**
  - **Bisher nur wage statistische Zusammenhänge bekannt, aber: Langzeitproblematik, Verbesserung der Forschungsmöglichkeiten!**
- **lebenslange Bindung** der Daten (bisher keine „Rückrufmöglichkeit“, solange keine „Beimischung“ von Zufallsdaten)
- neue **Qualität** und **Quantität**: automatisiere Auswertbarkeit und Überwachung möglich

Datenschutzrechtliche Problemfelder II

- **Datensicherheit**: Datenbesitz = Berechtigung?
- ggf. umfangreiche **Datenbestände** (Mißbrauchsgefahr)
- Sicherstellung der **Zweckbindung**? (auch eventueller **Protokolldaten**!)
- ggf. **blindes Technikvertrauen**: Entscheidungen sind ggf. manuell schwer oder gar nicht nachvollziehbar

Datenschutzgerechte Biometrie I

- aktive Mitwirkung des Nutzer bei Datenerhebung
- Nutzung verhaltensbasierter Merkmale mit einer Wissenkomponente

- Verschlüsselung biometrischer Daten
- frühe Löschung von Rohdaten

- keine „Vortäuschbarkeit“ von Aktionen des Nutzers
- sichere (revisionsfeste) Protokollierung von Eingabe/Parameteränderungen

Datenschutzgerechte Biometrie II

- transparente Gestaltung, Information des Nutzers
- Qualitätskontolle, z.B. durch Zertifizierungen, Evaluation, Auditierungen, Verwendung offengelegter Algorithmen und Verfahren

- enge Zugriffsbefugnisse bei zentraler Speicherung
- Nutzung von Anonymisierungs- und Pseudonymisierungsverfahren
- templatefreie Verfahren (Biometrie als kryptographischer Schlüssel); Zumischung zufälliger Informationen in einzelnen Verwendungen
- Speicherung unter Nutzerhoheit (z.B. Chipkarten)

Ort der Datenspeicherung

- **zentrale** oder **dezentrale** Datenspeicherung möglich
  Vorteile einer zentralen Speicherung:
  - keine Kartenpersonalisierung mit biometrischen Daten
  - einfachere Handhabung (kartenlos)

- ggf. einfacherer Umgang mit den biometrischen Daten
- ggf. besserer Schutz der einzelnen Daten als in Karte

Nachteile zentraler Datenspeicherung

- **Akzeptanzprobleme** bei Kunden/Bürgern/Arbeitnehmern
- Datenbank ist begehrtes Objekt bei **Ermittlungsbehörden** (komplizierte Fragestellungen bei Beschlagnahme oder „freiwilliger“ Weitergabe biometrischer Daten)
- Kompromittierung des **gesamten** Datensatzes denkbar - biometrische Datenbank ist (begehrter!) „single point of failure“
- Fragestellung des **Informationsüberschusses** ungeklärt

Verbraucherschutzaspekte

- **Nutzungsfreundlichkeit**
  - Wahlfreiheit
  - Information
  - Alltagstauglichkeit/Robustheit/(Geräte)Sicherheit
  - Komfort
  - Rückfallpositionen

- **Haftung/Beweislastverteilung**
  - kein (Mit-)Verschulden des Verbrauchers:
    - unzumutbar, körperliches Merkmal „missbrauchssicher“ zu verwenden und zu gebrauchen
    - System-Sicherheit in der Sphäre des Systembetreibers (z. B. eines Geldinstituts)

Ausblick

Differenzierte Betrachtungen notwendig!

Einflussfaktoren:

- **Art der Anwendung** (PC-Sicherung, Elektronische Signatur, Datenspeicherung, Zutrittsschutz)
- **Größe** und **Zusammensetzung** der Anwendergruppe
- **Rechtsstatus** des Anwenders (öffentlich/nichtöffentlich) und der Anwendung (freiwillig/verpflichtend)