MICROTEC 2018 – 13. September 2018

Biometrische Bankkarte

Verfahren, Anwendungs- und Sicherheittsaspekte

Thomas Suwald

NXP Semiconductors Germany GmbH

Business Unit Security & Connectivity

Hamburg

Kennzahlen

9,25 Mrd US$ Umsatz

HQ in Eindhoven, NL

>44000 Mitarbeiter in >33 Ländern

Standorte Deutschland:

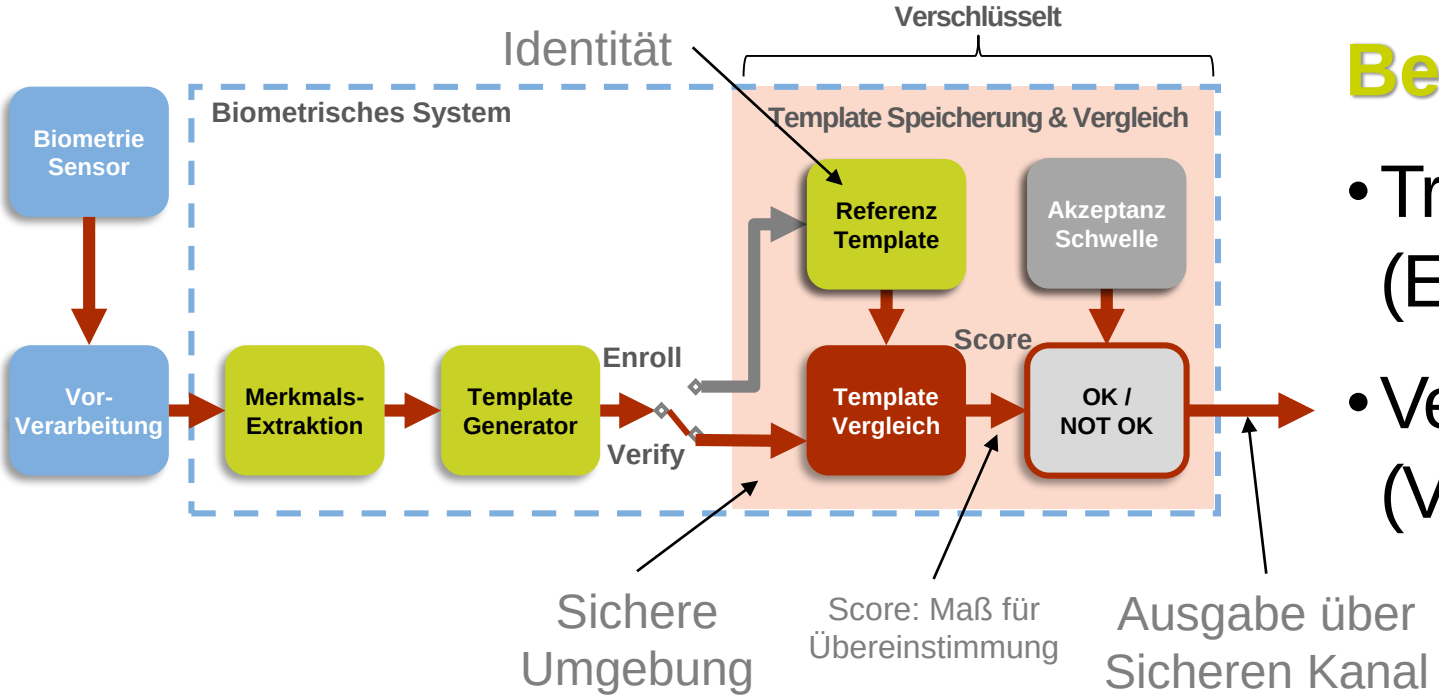
Böblingen, Dresden, Hamburg, München, Nürnberg, Wiesbaden

Stand: 12/2017

Themenauswahl

- Aufbau und Architektur
- Kontakt- und Kontaktlosanwendung
- Wie kommt der Fingerabdruck in die Karte
- Wie wird die Identität geschützt
- Wie gut ist die Erkennungsrate?
- Wie hoch ist der Sicherheitslevel?
- Zusammenfassung / Ausblick

Biometrisches System



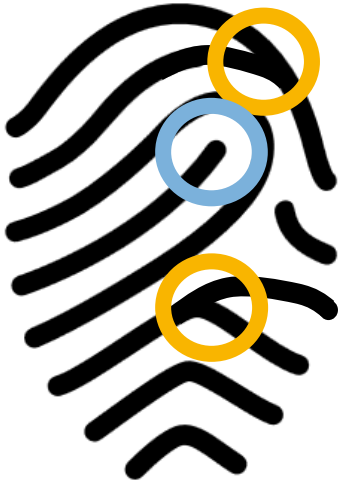
Betriebsarten

- Trainieren (Enroll)
- Verifizieren (Verify)

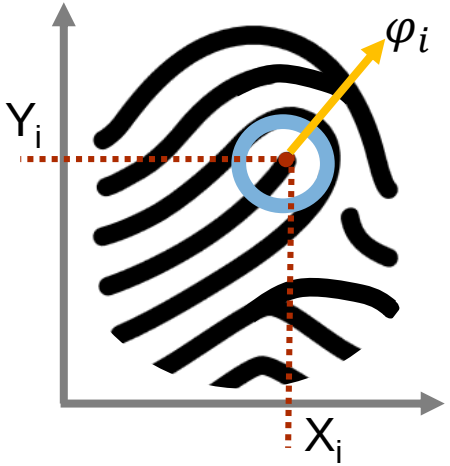
Sicherheitsanforderungen

Komponente	Funktion	Sicherheitsbedarf
Biometrie Sensor	Wandelt biometrische Merkmale in digitales Abbild (Merkmalsgehalt bleibt erhalten)	Keiner
Merkmals-Extraktion	Extrahiert Merkmale aus Abbild (Merkmalsgehalt bleibt erhalten)	**Training: Maximal** Verifikation: Keiner
Referenz Template	Repräsentiert eigene Identität	**Immer: Maximal**
Akzeptanz Schwelle, Template Vergleich	Entscheidet über Ausführung einer Transaktion	**Maximal** Bei hohem Transaktionsvolumen

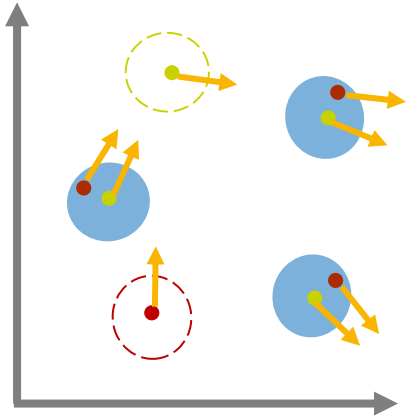
Fingerabdruck Minutien Merkmale



Minutien:
- Verzweigung
- Endung

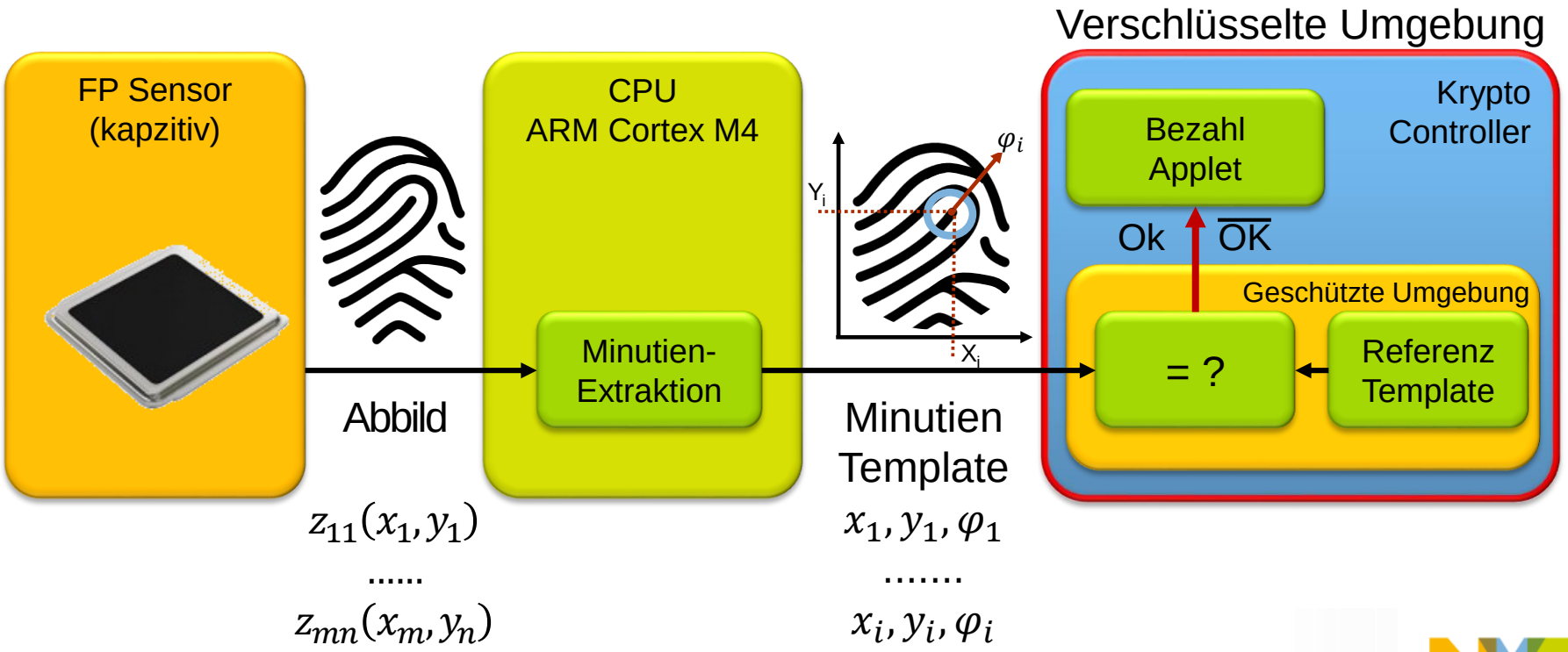


Typ	=	Endung
X-Pos	=	X_i
Y-Pos	=	Y_i
Winkel	=	φ_i



Vergleich
- = Life-Bild
- = Referenz
- = Übereinstimmung

System Architektur



Kontaktbetrieb (Traditionelle Anwendung)

Weiterhin Betrieb als PIN-Karte

Sensor verdeckt

Mechanische Belastung

ESD-Entladung

Bank vertraut weiter auf PIN (bestehende Infrastruktur)

Kontaktlosbetrieb (Hauptanwendung)

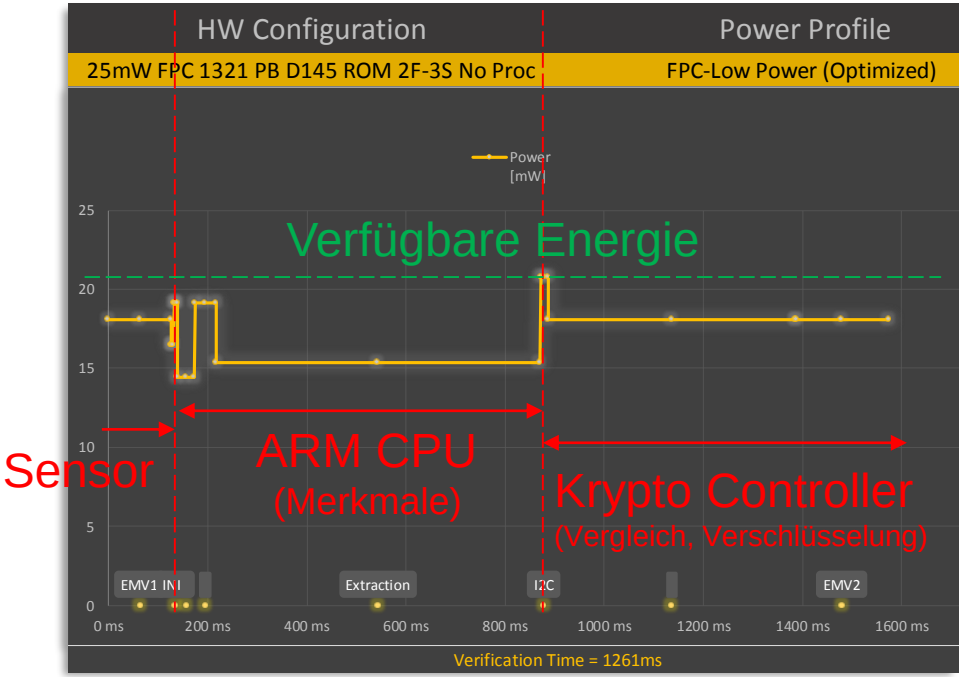
Anspruch

- Schnell
- Bequem
- Sicher

Genauere Betrachtung:

- für Daumen
- Für gepflegte Finger

Herausforderung: Energie

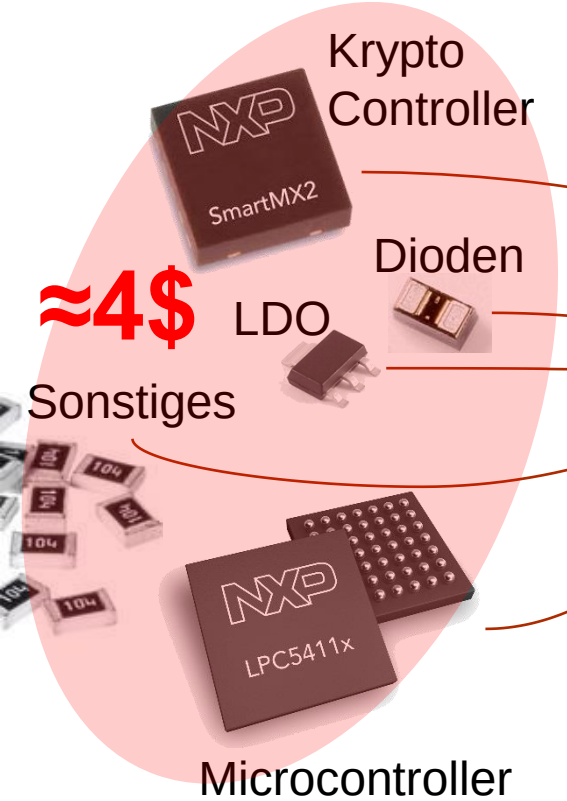


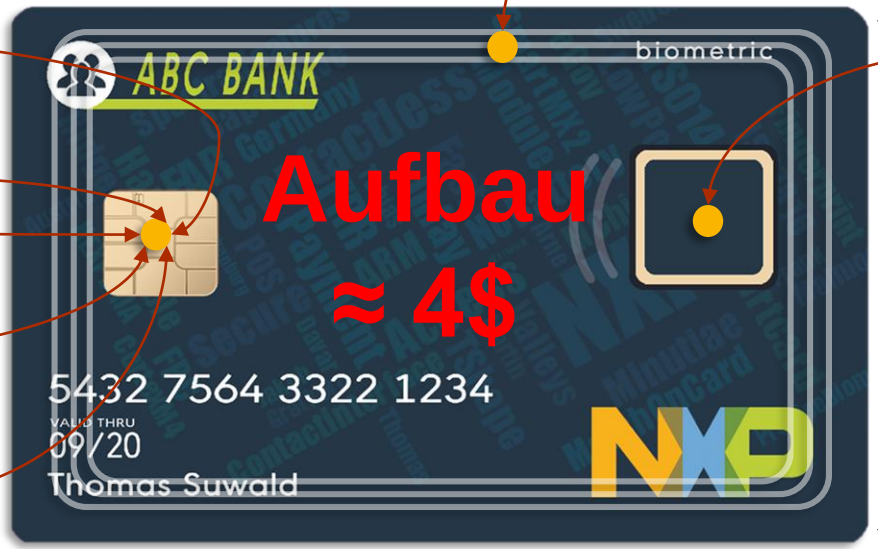
Versorgung über Magnetfeld (energiekritisch)

Abarbeitung phasenweise

- Transaktion starten
- Abbild erzeugen
- Merkmale extrahieren
- Merkmale vergleichen
- Transaktion beenden

Herausforderung: Kosten*





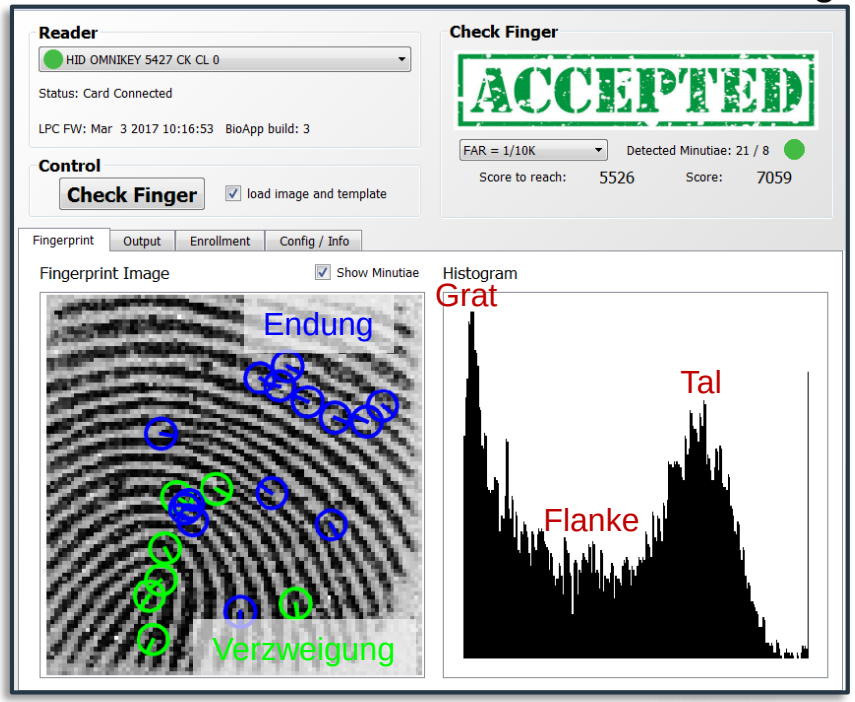
Fingerabdruck
Sensor 8*8mm²

*Schätzung Preisbasis Jan 2018

Sensorbild (kapazitiv 100mm²)

Rohbild

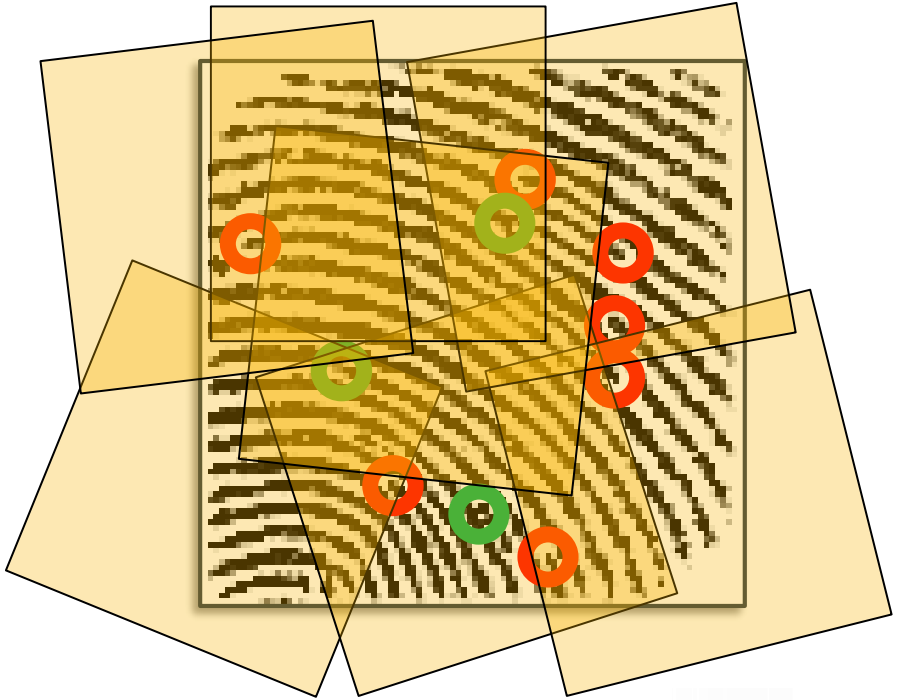
Extrahierte Merkmale mit Übereinstimmung



Referenzabbild (kleiner Sensor 64mm²)

Bankkarte = Kleiner Sensor

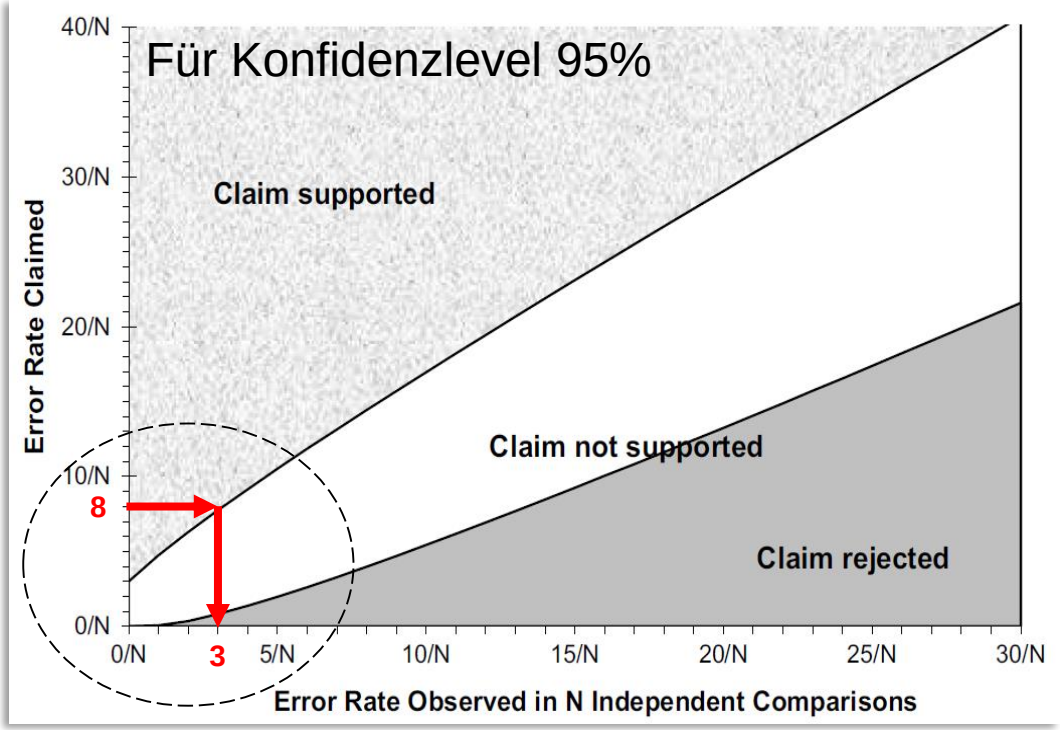
- überlappende Bilder erforderlich
- Merkmale rotationsinvariant extrahieren
- Merkmale zusammenfassen
- Im **Secure Element** ablegen (verschlüsselt)



Fehlerrate Eigenerkennung

- Vom Karteneigner trainiert
- Karteneigner meldet sich an
- $\boldsymbol{F_{alse}R_{eject}R_{ate}} = \frac{\boldsymbol{Anzahl\ Fehlversuche}}{\boldsymbol{Alle\ Versuche}} * \mathbf{100}\%$
- $\boldsymbol{FRR_{typisch}} = \mathbf{3}\%$
- FRR ist Indikator für die Benutzerfreundlichkeit
- $FRR > 5\%$ führt zur Ablehnung des Systems

Ermittlung Erkennungs Fehlerrate



Aus ISO/IEC 19795

Abschätzen der Fehlerrate:
z.B. $FRR = 3\%$

Wieviele <u>unkorrelierte</u> Versuche erforderlich?

$$\frac{8}{N} = \frac{3}{100} \rightarrow N = 8 * \frac{100}{3} = 267$$

Max Fehler: 3

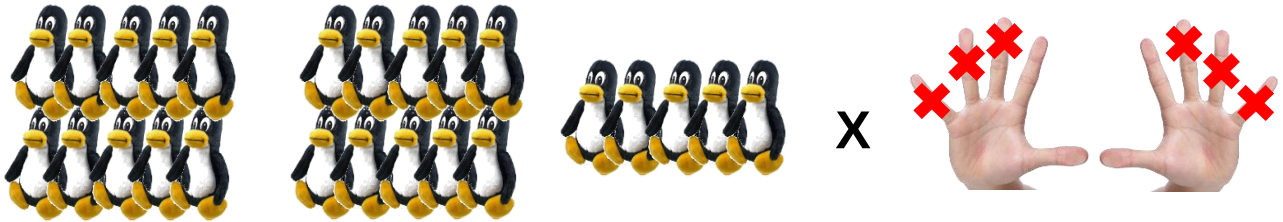
99 Tests:	0 Fehler
158 Tests:	1 Fehler
208 Tests:	2 Fehler

Test Eigenerkennung (False-Positive)

Schnell-Test
(13 Probanden)

13 Personen trainieren jeweils 8 Finger = 104 bei 0 Fehlern

Besserer Test
(25 Probanden)



25 Personen trainieren jeweils 4 Finger = 100 bei 0 Fehlern

Anwendungsnaher
Test
(50 Probanden)

50 Personen trainieren jeweils 2 Daumen = 100 bei 0 Fehlern

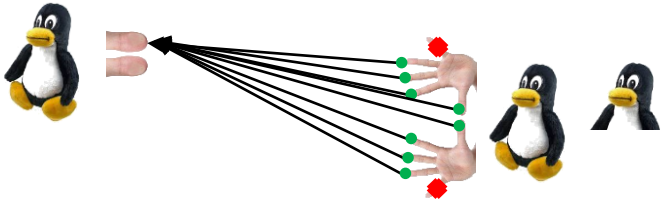
Fehlerrate Fremdabweisung

- Vom Karteneigner trainiert
- Fremder meldet sich an (ohne Betrugsaufwand)
- $\boldsymbol{F_{alse}A_{cceptance}R_{ate}} = \frac{\boldsymbol{Anzahl\ zu\ Unrecht\ akzeptierter\ Finger}}{\boldsymbol{Alle\ Versuche}} * \mathbf{100\%}$
- $\boldsymbol{FAR_{typisch}} = \mathbf{0.01\%} \quad (= \frac{1}{10000}, \quad entspricht\ 4 - stelliger\ PIN)$
- FAR ist Indikator für den Sicherheitslevel
- Über $FAR = 0.01\%$ wird Fingerabdruck unsicherer als 4-stellige PIN

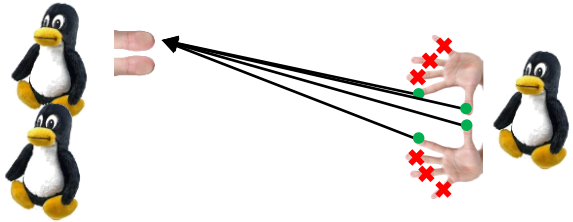
Sicherheit

Test Fremderkennung (False-Non-Match)

Schnell-Test
(50 Trainierte gegen
75 Probanden)

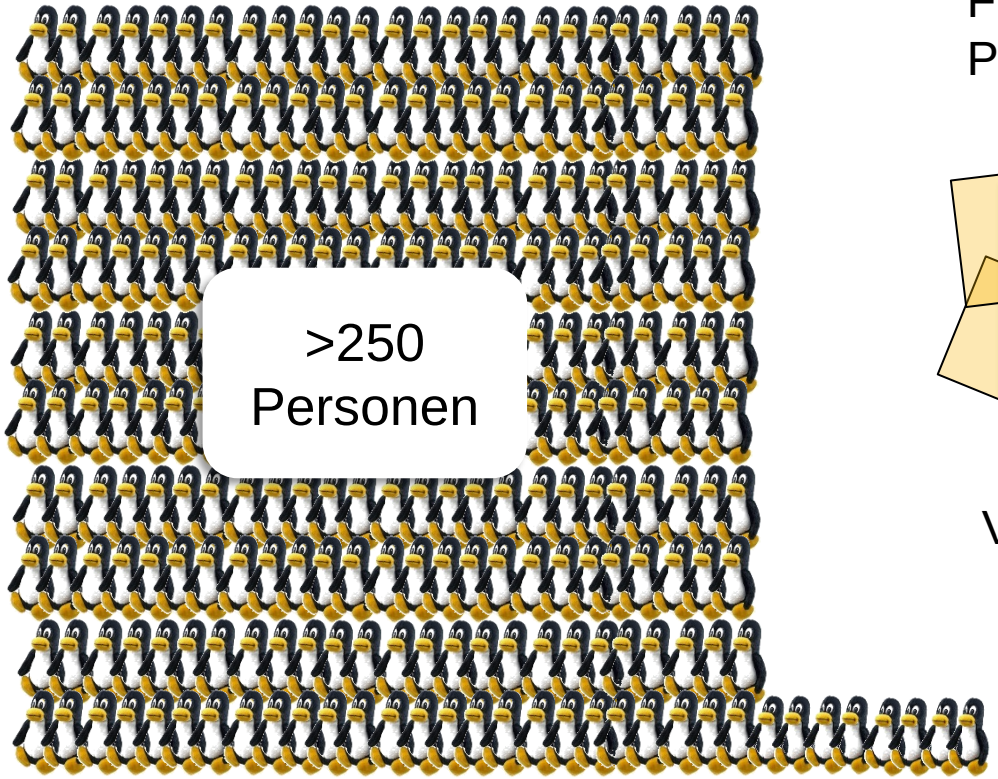


50 Pers. x 2 Finger gegen 75 Personen x 8 Finger / 2 = 30000 bei 0 Fehlern

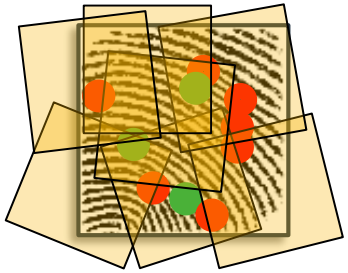


100 Pers. x 2 Finger gegen 75 Personen x 4 Finger / 2 = 30000 bei 0 Fehlern
gegen 115 Personen x 4 Finger / 2 = 46000 bei 1 Fehler
gegen 158 Personen x 4 Finger / 2 = 62500 bei 2 Fehlern

Praktische Test-Auslegung



FRR bestimmt Anzahl zu trainierender Personen (ca. 100 bei 3% FRR)



Trainig benötigt bis zu 20 Teil-Bilder (je kleiner der Sensor, desto mehr)

Verifikation erfordert nur 1 Bild/Finger

Für FRR: 1-14 Tage zwischen Training und Verifikation

Erzielbares Sicherheitsniveau

$$FAR = \frac{1}{10000}$$ bei 95% Konfidenz

Bis zu 5 Fehlversuche akzeptiert:

$$FAR = \frac{5}{10000} = \frac{1}{2000}$$

Spanne trocken zu feucht, Faktor 2:

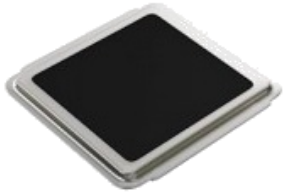
$$FAR = \frac{5*2}{1000} = \frac{1}{1000}$$

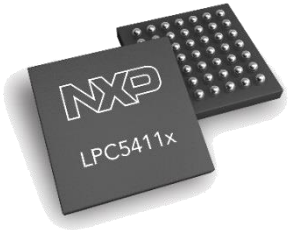
Weitere Faktoren:

Fingerabnutzung, Verschmutzung, ...

COMPANY PUBLIC

Optimales Erkennungssystem (Ausblick)





Sensor: Groß, Flexibel, Preis <1$

Erwartung

- Sensor → 30mm²
- Biometrie: Minutiuen → Korrelation → HW CoProcessing (Widerspruch: hohe Procesinganforderungen)

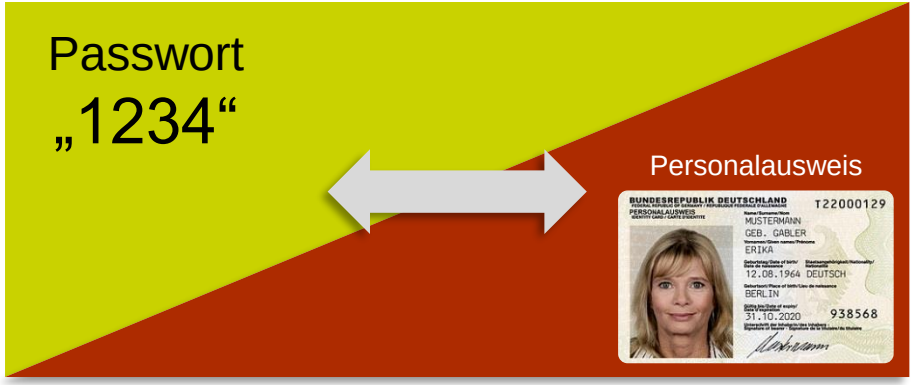
Biometrie: $FRR < 1\%,\ FAR < \frac{1}{50000}$

Energiebedarf < 10mW
Immun gegen Common Mode Noise

Sicherheit? Der Nutzer entscheidet

Bequem

Unbequem



Unsicher

Sicher

Kosten?

Mit Unterstützung der Master Studenten Andy Eckhoff / Moritz Dyballa (HAW/Uni Westküste)

SECURE CONNECTIONS
FOR A SMARTER WORLD