FINGERPRINTS

Fingerprint Biometrics in Mobiles

A request for input to Certification and Testing.

May 3, 2016

IBPC

NIST
Gaithersburg
Fingerprint Technology in Smartphones

- **World’s #1 Fingerprint System Market**
  - Strong Underlying Market
    - Smartphones sell >100 M Units per month
    - Smartphones sell at prices of 100 to 1000 USD
  - Riding the Mobile Market Biometry Wave
    - Inflexion Point early 2015
    - 24 OEMs launched 53 Smartphones with FPC Sensors alone in second half of 2015
    - 24 Further Smartphones released in Q1 2016 with FPC Sensors
    - TAM Growth YoY 15-16 is 105%
    - FPC alone Shipped 1M sensors daily in December, 2015
  - Strong End-User Pull.
    - Ease of Use
- **Fingerprint Authentication on Smartphones is Trusted.**
  - Endorsed by Banks,
  - Generalized through Password Managers, BankID and FIDO
  - Federation of identity
Fingerprint as an Authentication Subsystem

- **Purpose Built for Authentication of the User**
- **Widely Accepted**
  - End Users
  - Relying Parties
- **Integrated in Device’s security Architecture**
  - Android CPP guidelines met with TEE and/or proprietary solutions
- **OS-Level APIs Widely Used by App Developers**
  - Android Marshmallow
  - iOS
  - Global Platform TEE Biometric API under construction
- **Well Defined Envelope – Black Box**
  - Sensor
  - Stored Templates
  - Matching Algorithm
- **Privacy Enhancing - through End User Owned Device**
- **Performance Proven in the Field**
Goals and Objectives of Certification

• Trust
  – End User trusts the selected Brandname, OEM
  – Functional Intermediaries: FIDO, GP, EMVCo, GSMA...
  – Relying Party

• Transparency

• Quality Now and into the Future
  – Continued Evolution

• Fit into a demanding Ecosystem and Production Process
Issues with Testing Fingerprint Biometric Performance in Mobiles

- Short development and sales cycles
  - Integration into Product Development Process
- Privacy by Design
  - Images are not available in COTS products
- Close Performance Relationship in Optimized Subsystem
  - Sensor size and shape, Enrollment interaction, Matcher
Relevant Measures

• Security Measures
  – False Acceptance Rate (FAR)
  – Spoof Rejection
    – Attack testing

• User Convenience Measures – Leave to Marketplace!
  – False Rejection (FRR)
  – Failure to Enroll (FTE)
  – Speed of Matching
Self Test in Development Process

- Biometric Subsystem
  - Sensor
  - Image Processing
  - Enrollment S/W
  - Matching Algorithm

- Matching
  - Proprietary Algorithm and Templates
  - Decision by Threshold

- Setting of Threshold
  - Statistical analysis of image DB
  - DB Collected on relevant Sensor with relevant S/W Stack
Verified Self Test Certification

• Black Box Performance Test of Biometric Subsystem
  – Performed by the Biometric Supplier as part of the Design and development Process
  – Submitted to independent review by recognized test houses.
  – Best Practice guidelines and methodology

• OEM can refer to Certification by supplier product identifier.

• Physical security and integration of sensor and matching is part of TEE certification of handset.
Issues and Concerns

- Legal and Privacy Concerns in image DB from Self Test
  - Contractual framework
- Best Practice in Supplier Self Testing
- Control over Certification Process
  - Relying Parties, Relevant Security Community
  - FIDO, Global Platform
- Evolving Certification Targets
- Measure Effect on Performance of OEM Integration
Organisation

• Certification Board (Stewards of the Process)
  – To maintain and evolve the measures and requirements of the Certification in order to remain relevant.
  – Participation
    – EMVCo
    – GP
    – FIDO
    – GSMA
    – Governments
    – Enterprise Security

• Biometric Expertise (advisory to the Board)
  – Fingerprint Sensor Suppliers
  – Academia
  – Government
Participation

• Work is starting
• Contact me to discuss how you could participate
  – Jonas.andersson@fingerprints.com
  – Phone: +46-730 35 67 24
Thank you for your attention!

jonas.andersson@fingerprints.com

BEYOND KEYS AND PINS