FIGI Security Clinic

FIGI › FINANCIAL INCLUSION GLOBAL INITIATIVE

FIDO Certification

Dr. Rolf Lindemann, Nok Nok Labs
rolf@noknok.com

4-5 December 2019
#financialinclusion

Sponsored by

BILL & MELINDA GATES foundation

Organized by

Committee on Payments and Market Infrastructures
BANK FOR INTERNATIONAL SETTLEMENTS

WORLD BANK GROUP

ITU

Benefits to certification

- Validation
- Interoperability
- Rigorous testing
- Trust
- Competitive edge
- Market expansion

FIDO Certified Ecosystem (Sample)

PHONES & PCs

FUJITSU

HUAWEI

intel

Lenovo

LG

SAMSUNG

SHARP

SONY

SECURITY KEYS

egis Technology

FEITIAN WE BUILD SECURITY

Ledger

SurePass id

OneSpan

yubico

CLOUD/SERVER SOLUTIONS

Daon

Google

ING

mastercard

nok nok

RAON SECURE

RSA

SAMSUNG SDS

Over 550 FIDO Certified Solutions Available Today

FIDO Metadata Service

- Web-based tool where FIDO authenticator vendors can publish metadata statements for FIDO servers to download
- Provides organizations deploying FIDO servers with a centralized and **trusted source** of information about FIDO authenticators
- Validate the integrity of a device population by periodically downloading a digitally signed metadata to verify individual metadata statements

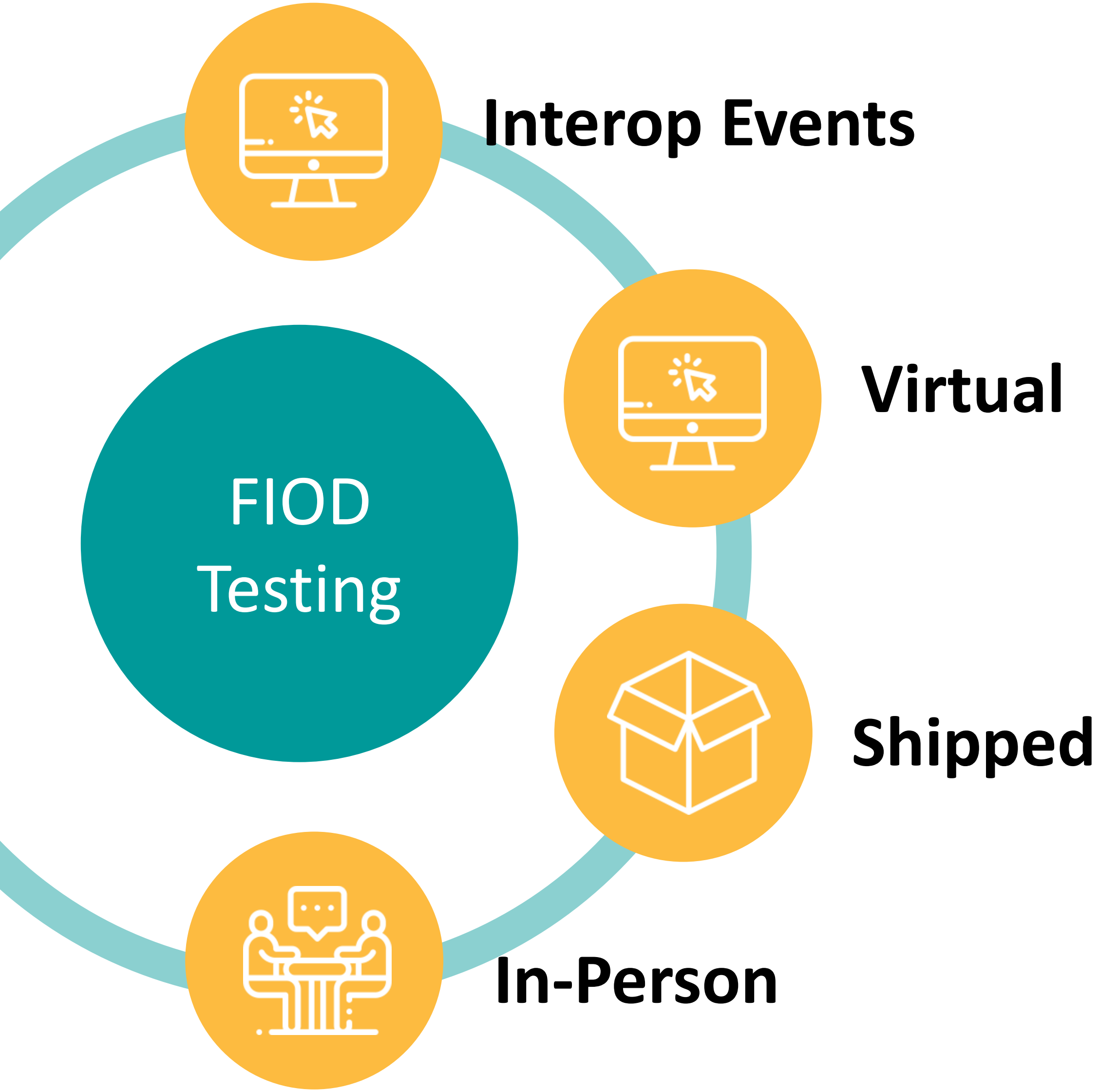
fido™
CERTIFIED

FIDO Certification Programs

Functional Certification

- Available to members and non-members
- Measures compliance among products and services that support FIDO specifications
- Validates interoperability within the ecosystem
- Certify products such as authenticators, servers, clients, and combos

Interop Testing Overview



FIOD Testing

Interop Events

Virtual

Shipped

In-Person

- **Existing Process – Interop Testing Events**
  - Interop every 90 days
  - Plan ahead! May impact product schedules…

- **New Process – On Demand Testing**
  - Pick your testing date from a calendar
  - Servers: remote / virtual testing
  - Authenticators: ship device or in-person testing
  - Convenience and fast turn-around

FIDO Authenticator Certification

- The FIDO Authenticator Certification Program validates that Authenticators conform to the FIDO specifications (UAF/U2F/FIDO2) and allows vendors to certify the security characteristics of their implementations
- After completing certification, vendors may use the FIDO logo on their products

Authenticator Certification Levels

SAMPLE DEVICE HARDWARE & SOFTWARE REQUIREMENTS		DEFENDS AGAINST
Protection against chip fault injection, invasive attacks…	L3+	Captured devices (chip-level attacks)
Circuit board potting, package on package memory, encrypted RAM…	L3	Captured devices (circuit board level attacks)
Restricted Operating Environment (ROE) (e.g., TEE or Secure Element in a phone, USB token or Smart Card which are intrinsically ROEs, other…)	L2+	Device OS compromise (defended by ROE)
	L2	
Any device HW or SW	L1+	Device OS compromise (defended by white-box cryptography)
	L1	Phishing, server credential breaches & MiTM attacks (better than passwords)

Level 1

- Better than passwords
  - FIDO is unfishable and biometrics are more convenient
- Keys and biometric templates are protected similar to passwords stored by a browser or password manager app
- Requires best facilities offered by hosting OS
- L1+ adds white-box cryptography (obfuscation and other techniques) to defend against compromise of hosting OS

Examples

- Android or iOS applications
- Platform built-in authenticators
- Level 2- or Level 3-capable authenticators that yet been certified at Level 2 or Level 3

Certification Process
Vendor documents their design in detail
L1+ only: Evaluation by FIDO-accredited lab, penetration testing (L1+ program still in development)
Evaluation by FIDO Alliance Security Secretariat

Level 2

In addition to L1

- A restricted operating environment like a TEE gives security even if OS is compromised.
- Separate USB, BLE and NFC authenticators are considered to use a restricted operating environment
- Gives defense against larger scale attacks
- Additional assurance at L2+

Examples

- Android apps using FIDO Level 2 certified phone (there aren't any yet)
- USB, BLE and NFC Security Keys
- Level 3-capable authenticators that haven't yet been certified at Level 3

Certification Process
Vendor documents their design in detail L2+ only: Vendor submits source code (L2+ program still in development)
Evaluation by a FIDO-accredited lab L2+ only: Attack potential calculation, pen testing

Level 3

- In addition to L2
- Defends against physically captured authenticators
- Defenses against disassembling, probing, glitch and other such physical attacks
- L3+ adds defense against chip-level physical attacks, such as decapping and probing the chip

Examples

- USB, BLE and NFC Security Keys using Secure Elements or other means of defending HW attacks
- In some case phone or platform authenticators may achieve L3, but is difficult

Certification Process
Vendor documents their design in detail Vendor submits source code
Evaluation by a FIDO-accredited lab (L3, L3+) Attack potential calculation and penetration testing L3+ only: Higher attack potential requirements

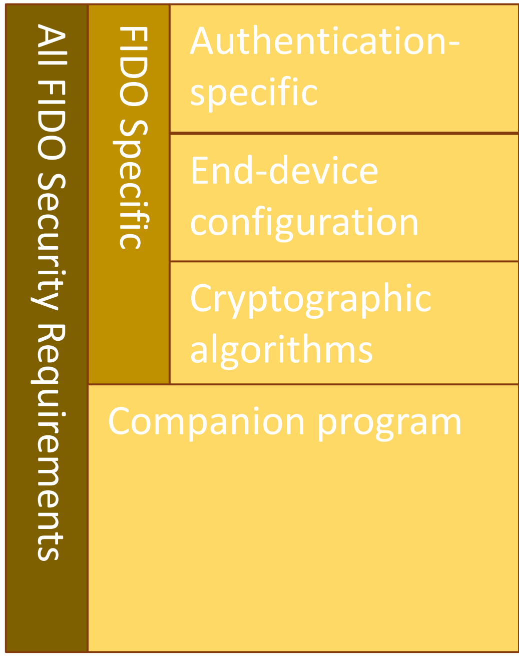
Companion Programs

Re use as much as possible from other programs like Common Criteria

- Reduces time, effort and cost of certification for authenticator vendors, sometimes by quite a lot

Companion programs never cover all FIDO requirements; they were not developed specifically for authenticators

- Even with advanced companion programs, vendors will have to go through additional certification with the FIDO Alliance



Companion Program	FIDO Security Level	Program Status
Common Criteria AVA_VAN 3	L3	Operating
Common Criteria AVA_VAN 4	L3+	Operating
FIPS	L2+, L3	In development
Global Platform TEE Protection Profile	L2+, L3	In development

FIDO Accredited LABS – Security

Applus laboratories

BCTC 国家金融IC卡安全检测中心 National Financial IC Card Security Test Center 银行卡检测中心 Bank Card Test Center

DOPLS Lab

brightsight® the number one security lab in the world

CCLAB

BCTC 国家金融IC卡安全检测中心 National Financial IC Card Security Test Center 银行卡检测中心 Bank Card Test Center

CAICT 中国信息通信研究院

leti ceatech

UL

TÜViT® TÜV NORD GROUP

riscure

TTA 한국정보통신기술협회 Telecommunications Technology Association

All labs that do FIDO certification must pass accreditation by the FIDO Alliance

FIDO Accredited LABS – Biometric

BCTC 国家金融IC卡安全检测中心
National Financial IC Card Security Test Center
银行卡检测中心
Bank Card Test Center

iBeta QUALITY ASSURANCE

idiap

elitt You innovate We validate

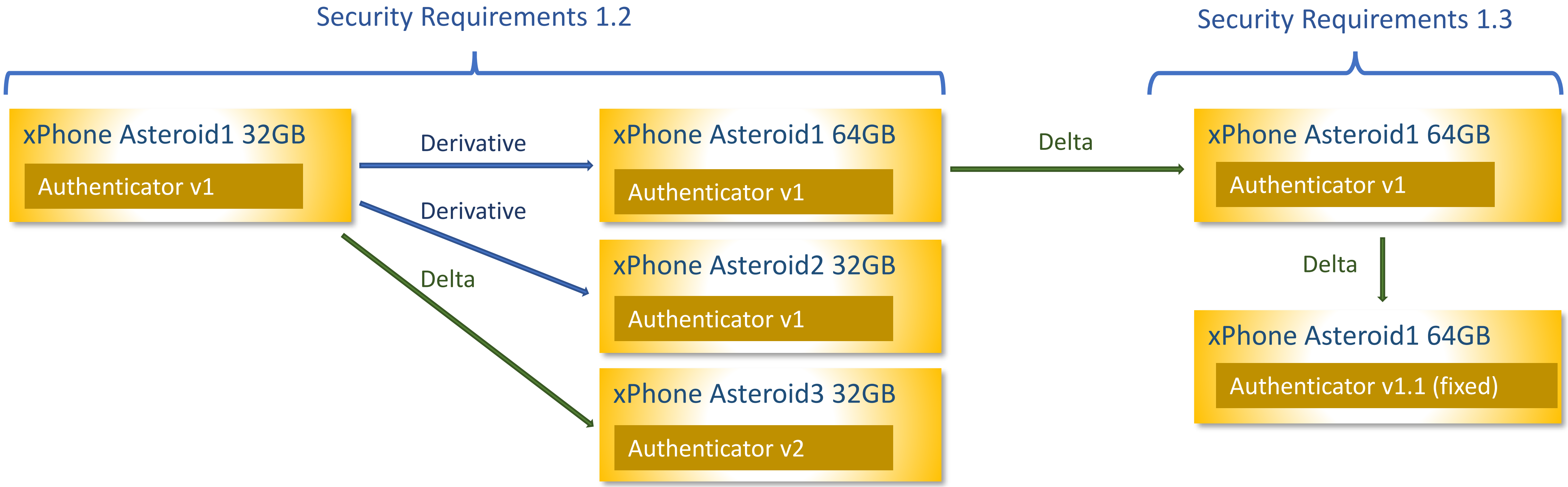
leti CEA tech

TTA 한국정보통신기술협회
Telecommunications Technology Association

All labs that do FIDO certification must pass accreditation by the FIDO Alliance

FIGI › FINANCIAL INCLUSION GLOBAL INITIATIVE

Expiration, Derivative & Delta certification



No Expiration

- Certification of a given product never expires
- Recertification against new versions of the requirements is optional

Derivative certification

- No change to FIDO functionality allowed
- Surrounding functionality may change
- Packaging & product name may change
- No re evaluation of security

Delta Certification

- When the FIDO functionality changes
- Recertification against new requirements
- After fix to close a vulnerability
- Reevaluation of security is required

FIDO Biometric Certification

- The FIDO Biometric Certification Program is intended to certify biometric components and/or subsystems and is independent from Authenticator Certification Program

Relevant Biometric Definitions

- False Accept Rate (FAR): The proportion of verification transactions with wrongful claims of identity that are incorrectly confirmed
  - The requirement of less than 1:10,000 for the upper bound of a 80% confidence interval
- False Reject Rate (FRR): The proportion of verification transactions with truthful claims of identity that are incorrectly denied
  - the requirement of less than 3:100 for the upper bound of a 80% confidence interval
- Impostor Attack Presentation Match Rate (IAPMR): Proportion of presentation attacks in which the target reference is matched
  - evaluation measures the Impostor Attack Presentation Match Rate for each presentation attack type, as defined in ISO 30107 Part 3

Self-attestation – Optional

- Biometric Requirements:
- False Accept Rate (FAR): The vendor SHALL attest to an FAR of [1:25,000 or 1:50,000 or 1:75,000 or 1:100,000] at an FRR of 3% or less.
- False Reject Rate (FRR): The vendor SHALL attest to an FRR at no greater than 3% as measured when determining the self-attested FAR. In other words, self attestation for FRR is only possible when self attesting for FAR.

- NOTE: Self-attestation for FAR and FRR shall be supported by test data and documented in a report submitted to lab from vendor.

Connect with FIDO

fidoalliance.org