Recommendations for Presentation Attack Detection (PAD): Mitigation of threats due to spoof attacks

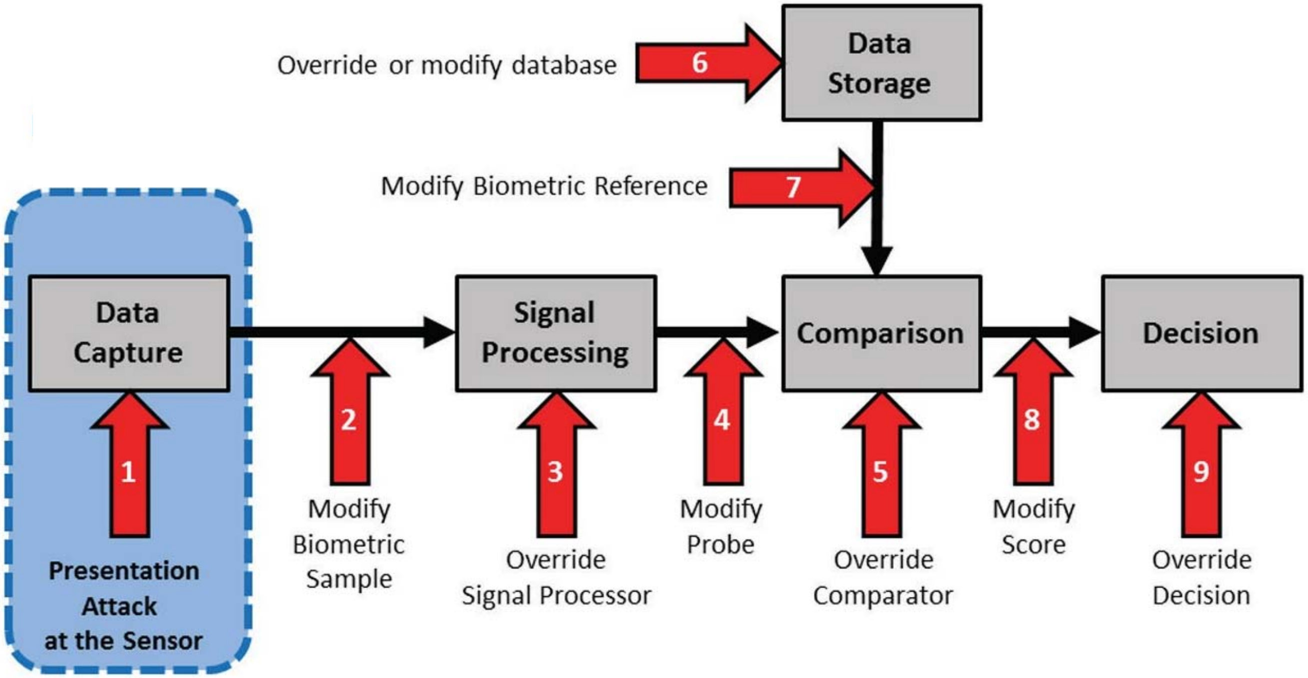
Elaine Newton, PhD | Stephanie Schuckers, PhD

NIST | Clarkson University

A Modest Proposal ~~Recommendations~~ for Presentation Attack Detection (PAD): Mitigation of threats due to spoof attacks

Elaine Newton, PhD | Stephanie Schuckers, PhD
NIST | Clarkson University

Key Attack Points in a Biometric System



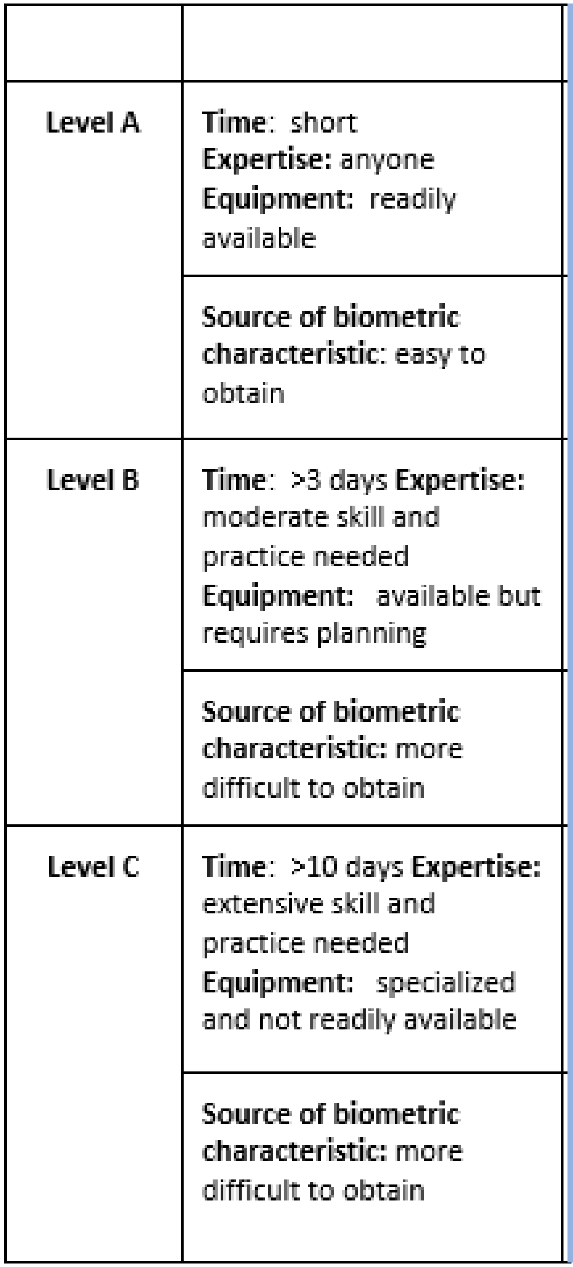
From ISO/IEC 30107-1, inspired by figure by Nalini Ratha from 2001 and Standing Document 11 of ISO/IEC JTC1 SC37.

Introduction

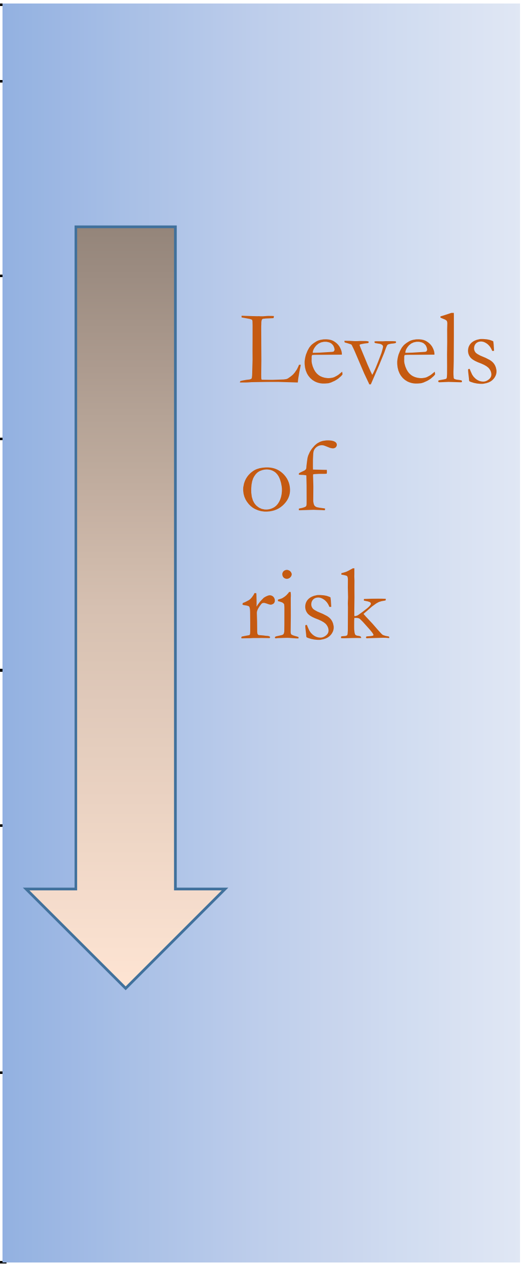
- Motivating Use Case
  - Remote, positive authentication using biometrics as a factor – e.g. using a smartphone to access bank account
    - Assuming that the attack is trying to match an enrollment template/image from a live person.
- Presentation Attack
  - presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system

    From ISO/IEC 30107-1: 2016
- Problem Statement
  - How can biometric verification systems be evaluated for their ability to reject a presentation attack?

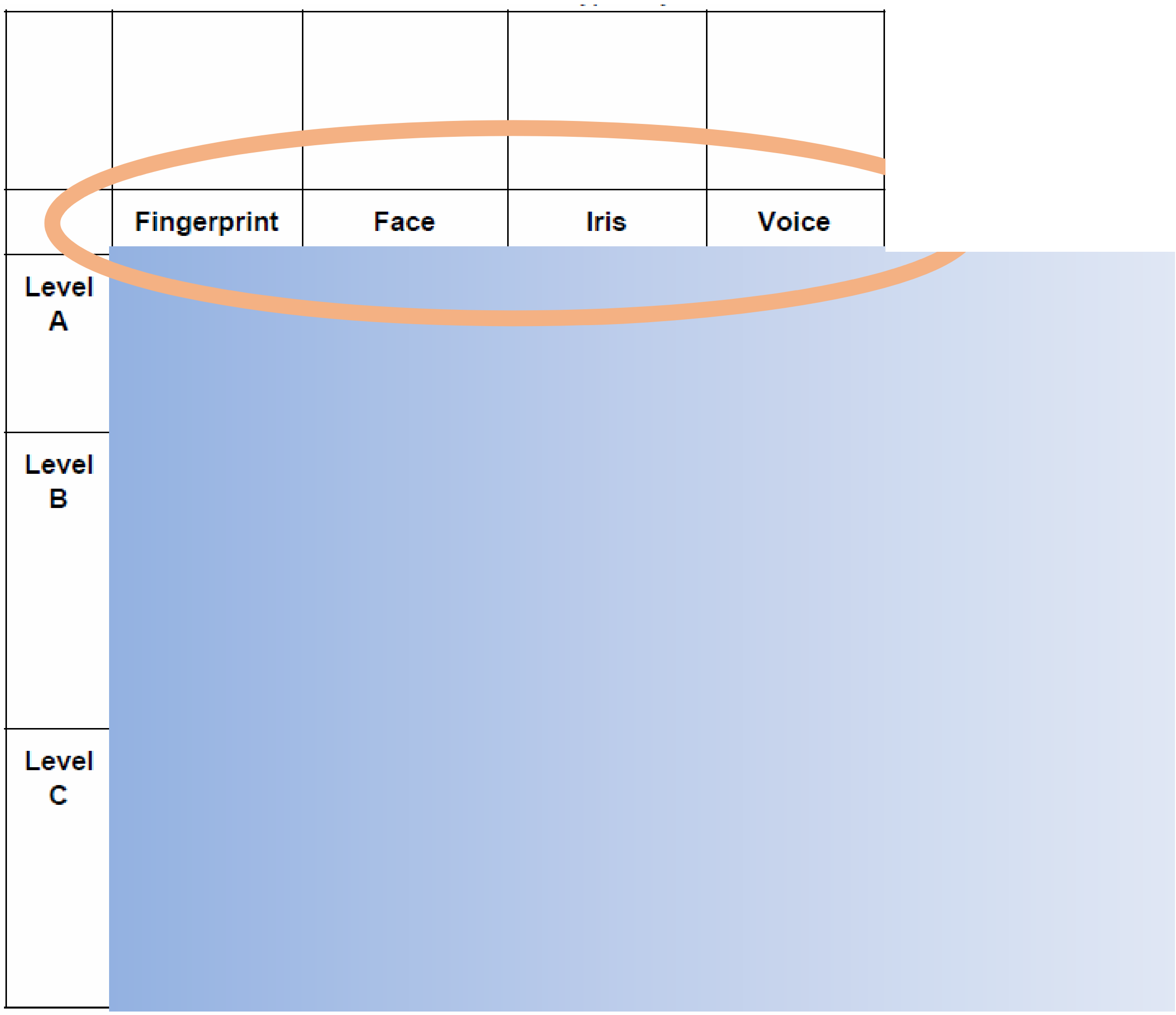
Introduction to the Testing Framework



Level A	**Time:** short **Expertise:** anyone **Equipment:** readily available
	Source of biometric characteristic: easy to obtain
Level B	**Time:** >3 days **Expertise:** moderate skill and practice needed **Equipment:** available but requires planning
	Source of biometric characteristic: more difficult to obtain
Level C	**Time:** >10 days **Expertise:** extensive skill and practice needed **Equipment:** specialized and not readily available
	Source of biometric characteristic: more difficult to obtain

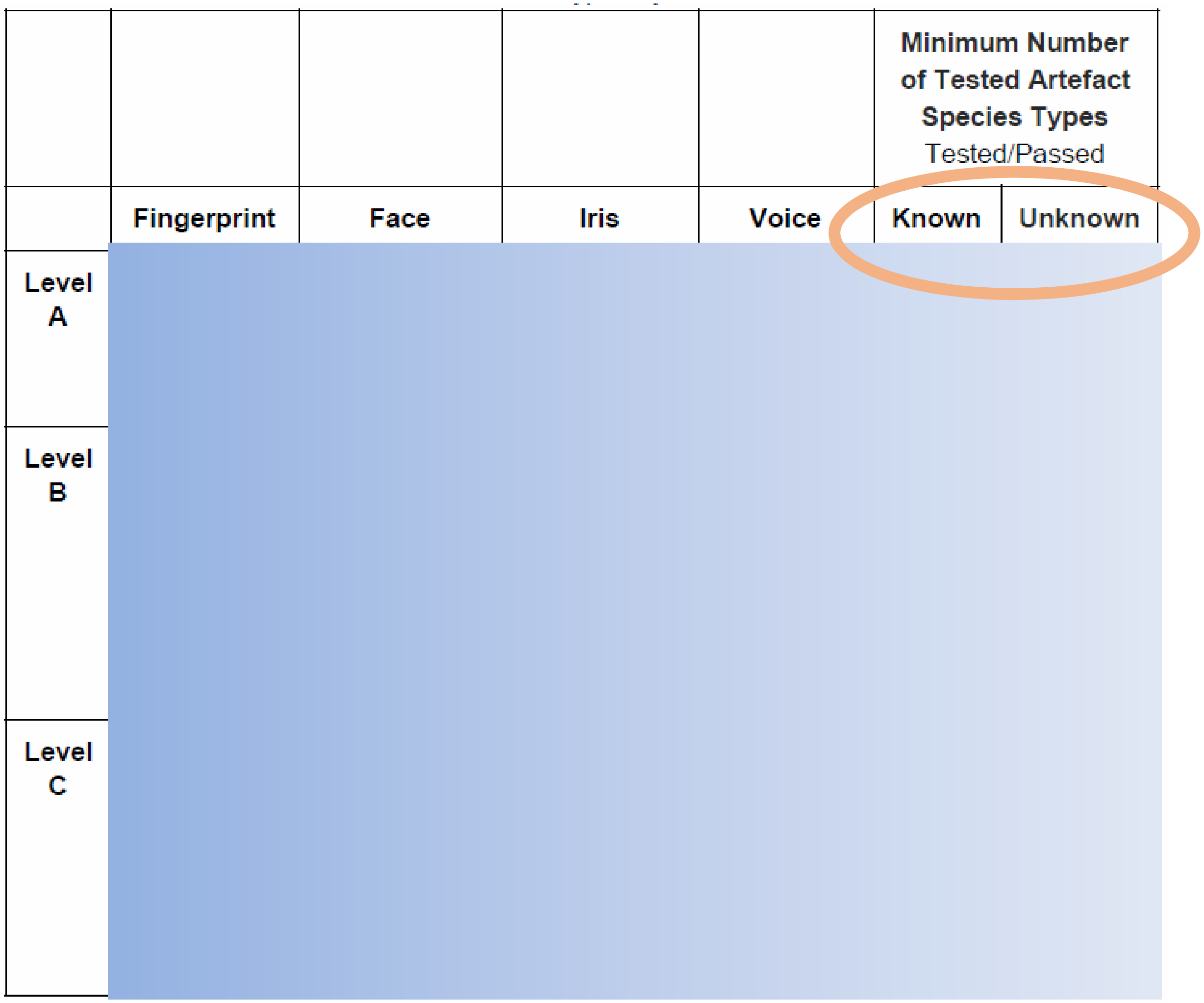


Introduction to the Testing Framework



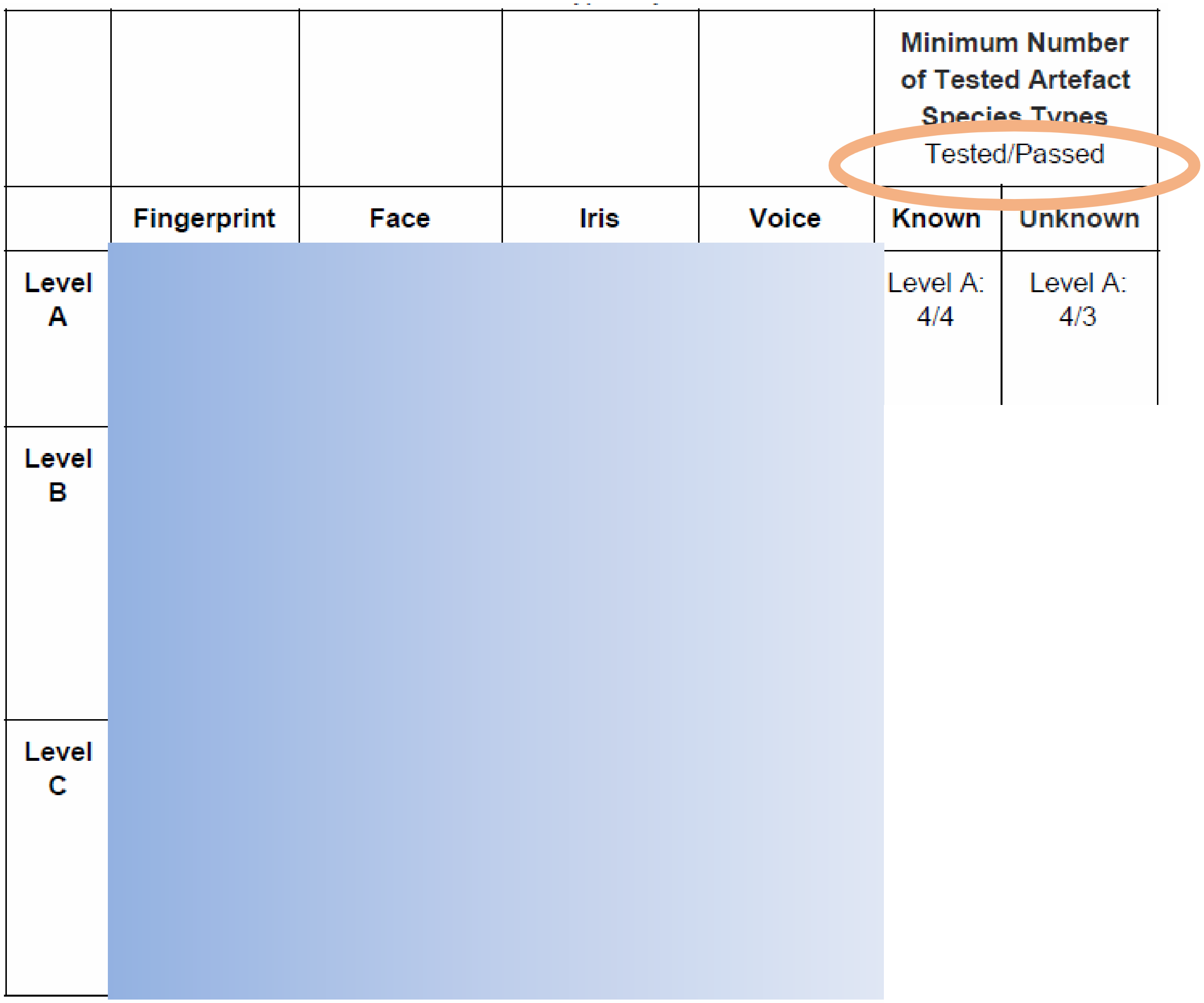
	Fingerprint	Face	Iris	Voice
Level A				
Level B				
Level C				

Proposed Minimum Number of Tested Artefact Types by Risk Level



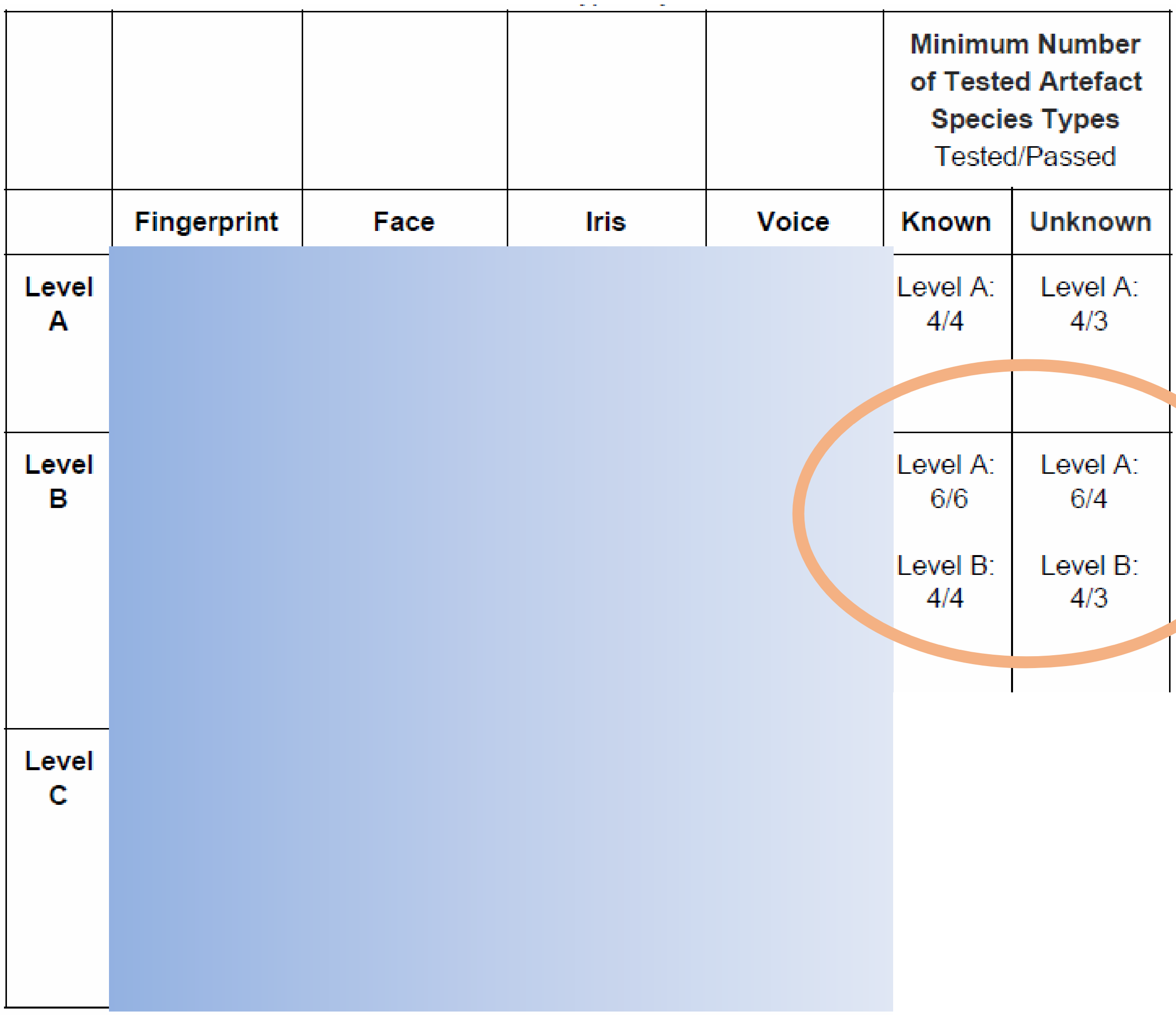
					Minimum Number of Tested Artefact Species Types Tested/Passed	
	Fingerprint	Face	Iris	Voice	Known	Unknown
Level A						
Level B						
Level C						

Proposed Minimum Number of Tested Artefact Types by Risk Level



					Minimum Number of Tested Artefact Species Types Tested/Passed	
	Fingerprint	Face	Iris	Voice	Known	Unknown
Level A					Level A: 4/4	Level A: 4/3
Level B						
Level C						

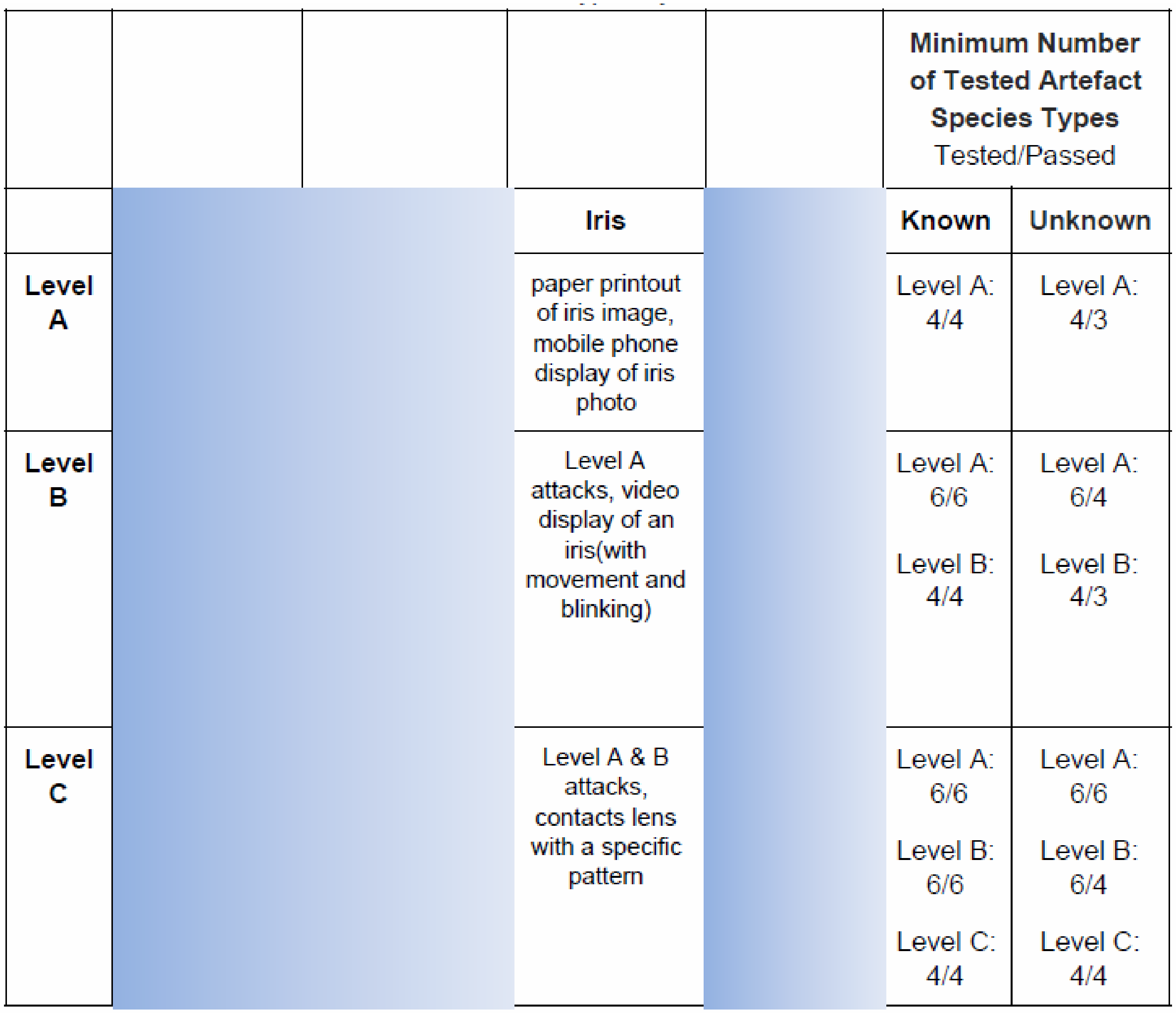
Proposed Minimum Number of Tested Artefact Types by Risk Level



					Minimum Number of Tested Artefact Species Types Tested/Passed	
	Fingerprint	**Face**	**Iris**	**Voice**	**Known**	**Unknown**
Level A					Level A: 4/4	Level A: 4/3
Level B					Level A: 6/6 Level B: 4/4	Level A: 6/4 Level B: 4/3
Level C						

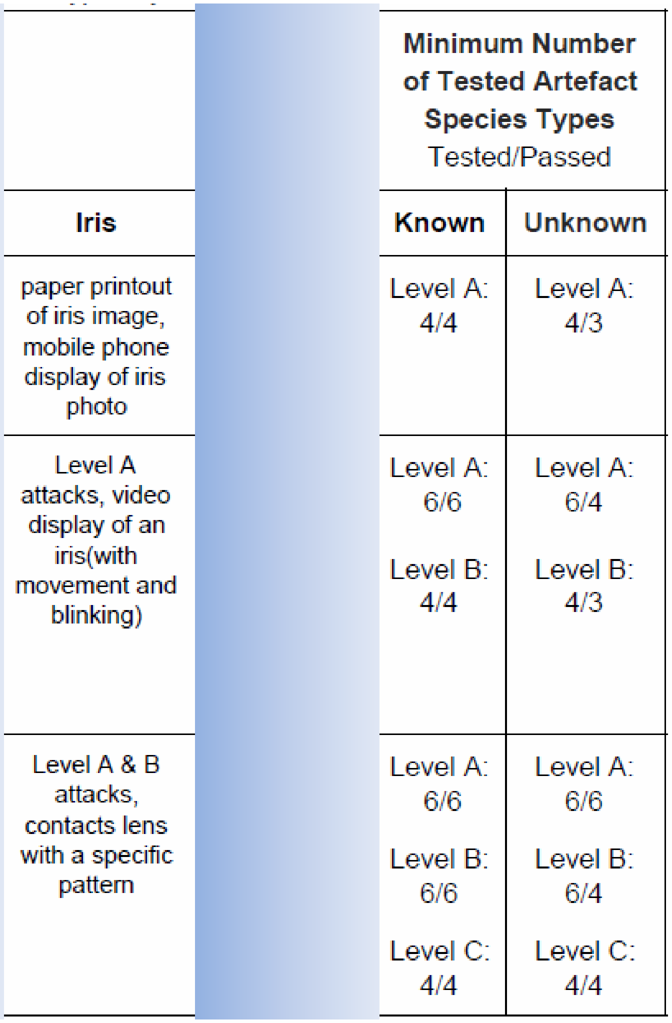
Each subsequent (higher) level should be testing attacks from lower levels.

Proposed Minimum Number of Tested Artefact Types by Risk Level



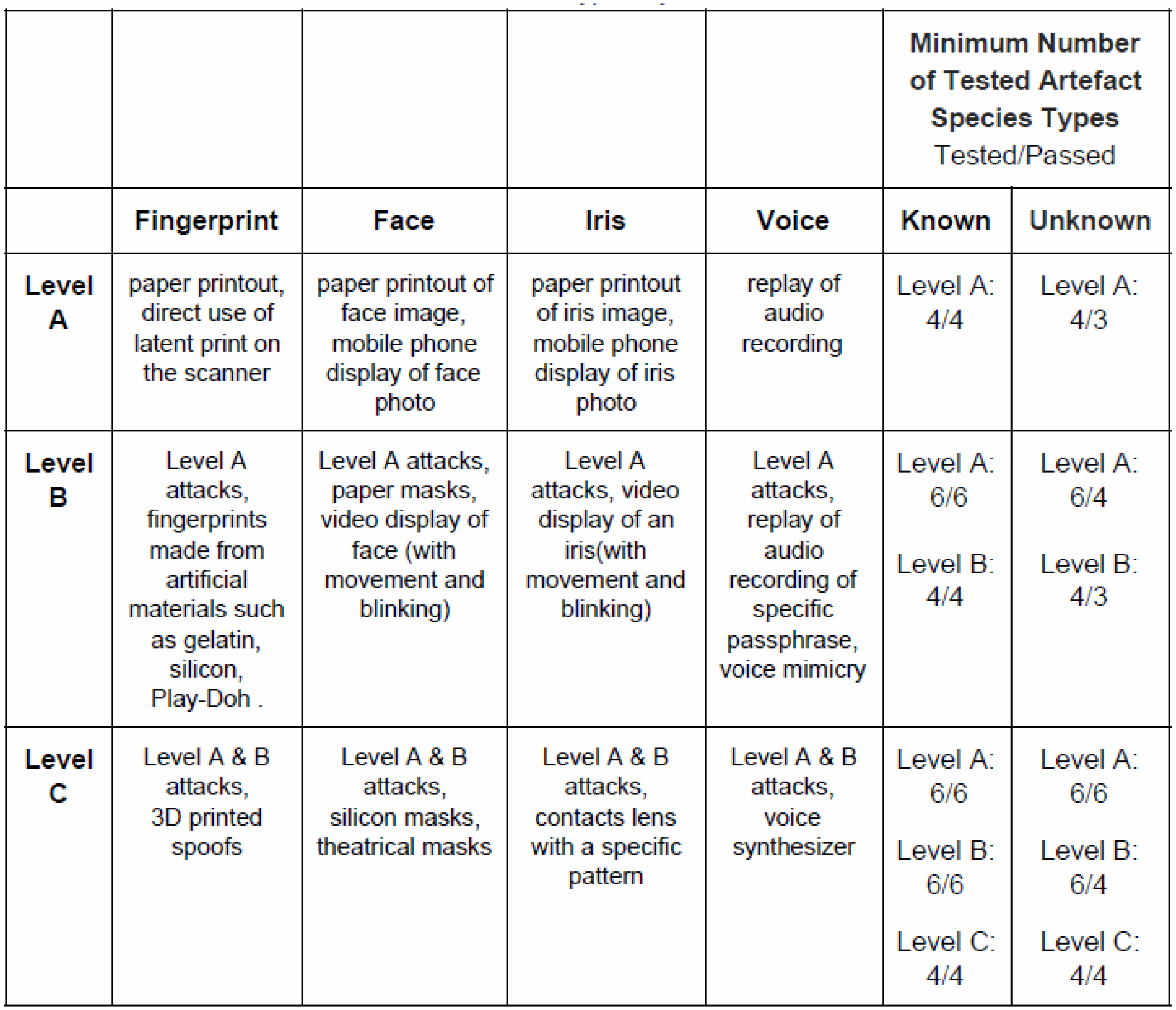
					Minimum Number of Tested Artefact Species Types Tested/Passed	
			Iris		Known	Unknown
Level A			paper printout of iris image, mobile phone display of iris photo		Level A: 4/4	Level A: 4/3
Level B			Level A attacks, video display of an iris(with movement and blinking)		Level A: 6/6 Level B: 4/4	Level A: 6/4 Level B: 4/3
Level C			Level A & B attacks, contacts lens with a specific pattern		Level A: 6/6 Level B: 6/6 Level C: 4/4	Level A: 6/6 Level B: 6/4 Level C: 4/4

- Each species should be tested …
  - With a minimum of 100 attempts
    - A series of 10 for 10 different people
      - 5 men, 5 women



	Minimum Number of Tested Artefact Species Types Tested/Passed	
Iris	**Known**	**Unknown**
paper printout of iris image, mobile phone display of iris photo	Level A: 4/4	Level A: 4/3
Level A attacks, video display of an iris(with movement and blinking)	Level A: 6/6 Level B: 4/4	Level A: 6/4 Level B: 4/3
Level A & B attacks, contacts lens with a specific pattern	Level A: 6/6 Level B: 6/6 Level C: 4/4	Level A: 6/6 Level B: 6/4 Level C: 4/4

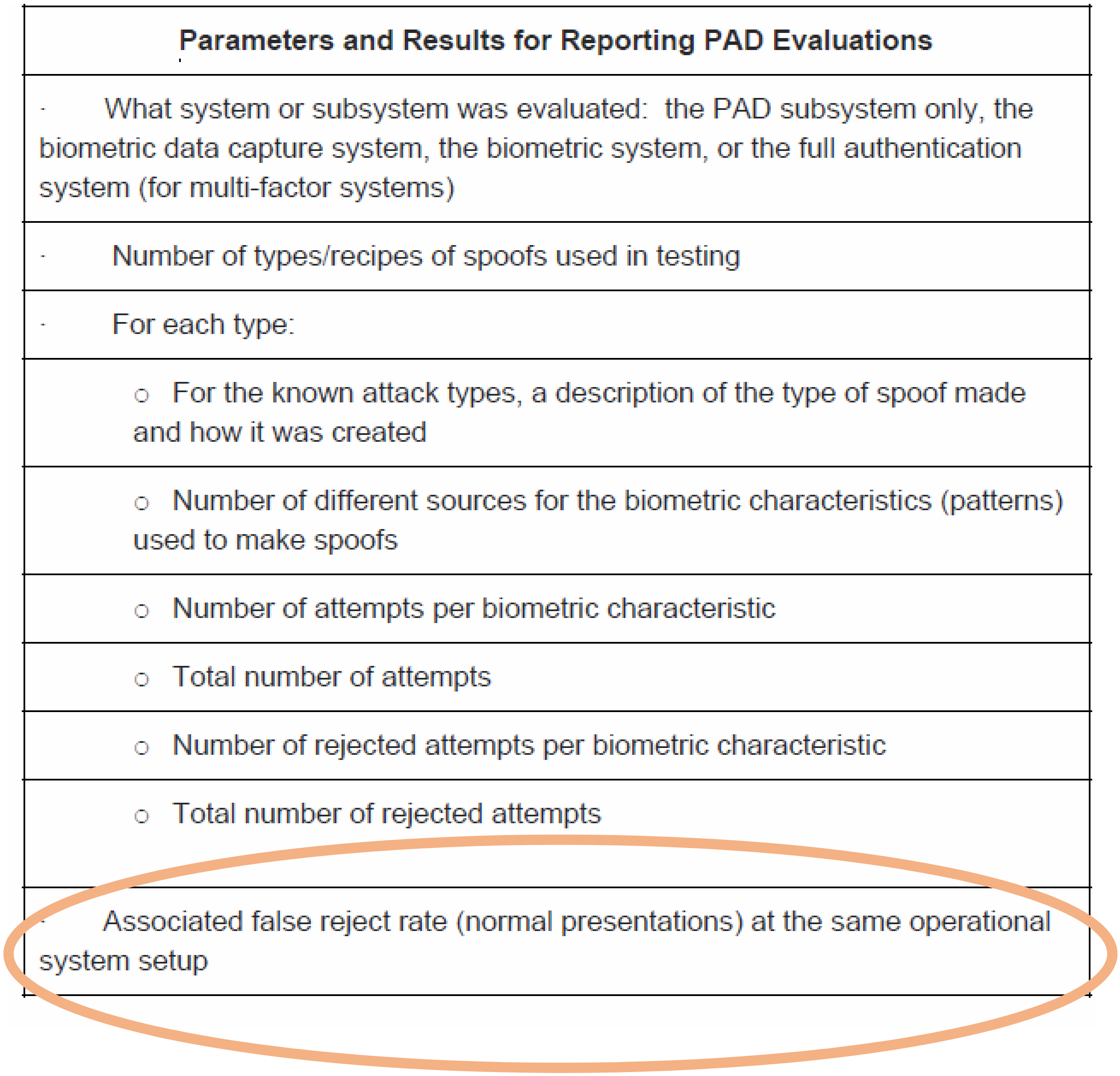
Proposed Minimum Number of Tested Artefact Types by Risk Level



					Minimum Number of Tested Artefact Species Types Tested/Passed	
	Fingerprint	**Face**	**Iris**	**Voice**	**Known**	**Unknown**
Level A	paper printout, direct use of latent print on the scanner	paper printout of face image, mobile phone display of face photo	paper printout of iris image, mobile phone display of iris photo	replay of audio recording	Level A: 4/4	Level A: 4/3
Level B	Level A attacks, fingerprints made from artificial materials such as gelatin, silicon, Play-Doh .	Level A attacks, paper masks, video display of face (with movement and blinking)	Level A attacks, video display of an iris(with movement and blinking)	Level A attacks, replay of audio recording of specific passphrase, voice mimicry	Level A: 6/6 Level B: 4/4	Level A: 6/4 Level B: 4/3
Level C	Level A & B attacks, 3D printed spoofs	Level A & B attacks, silicon masks, theatrical masks	Level A & B attacks, contacts lens with a specific pattern	Level A & B attacks, voice synthesizer	Level A: 6/6 Level B: 6/6 Level C: 4/4	Level A: 6/6 Level B: 6/4 Level C: 4/4

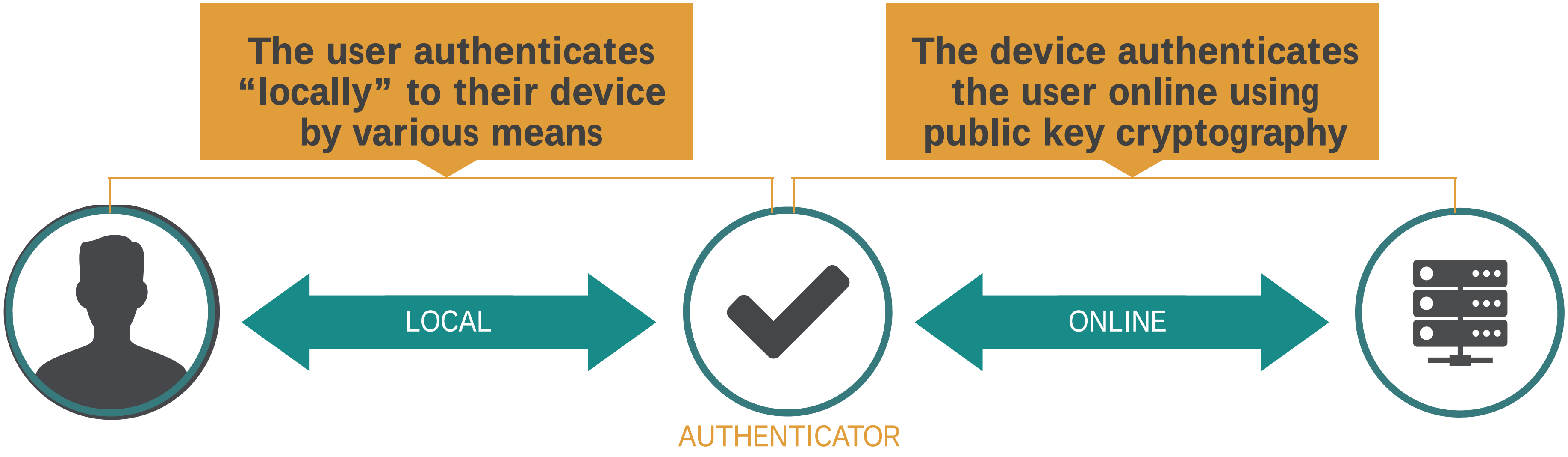
An attack presentation match rate (APMR) of less than 5% shall be achieved for each attack type.

Common Set of Elements for PAD Evaluation Reporting



Parameters and Results for Reporting PAD Evaluations
· What system or subsystem was evaluated: the PAD subsystem only, the biometric data capture system, the biometric system, or the full authentication system (for multi-factor systems)
· Number of types/recipes of spoofs used in testing
· For each type:
o For the known attack types, a description of the type of spoof made and how it was created
o Number of different sources for the biometric characteristics (patterns) used to make spoofs
o Number of attempts per biometric characteristic
o Total number of attempts
o Number of rejected attempts per biometric characteristic
o Total number of rejected attempts
· Associated false reject rate (normal presentations) at the same operational system setup

HOW FIDO AUTHN WORKS

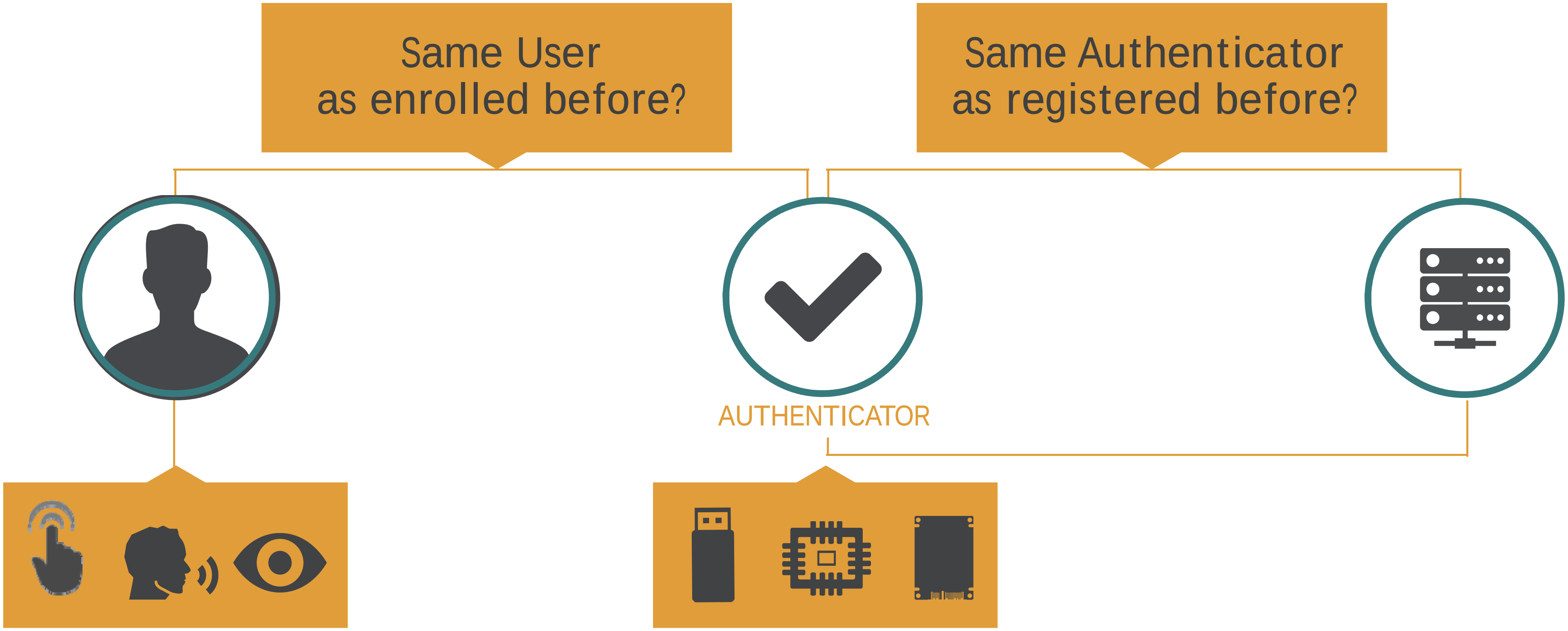


The user authenticates "locally" to their device by various means

The device authenticates the user online using public key cryptography

FIDO UAF

UNIVERSAL AUTHENTICATION FRAMEWORK



Same User as enrolled before?

Same Authenticator as registered before?

AUTHENTICATOR

FIDO Alliance Mission

1

Develop Specifications

2

Operate Adoption Programs

3

Pursue Formal Standardization

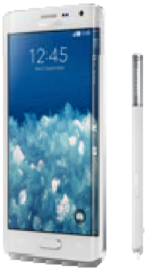
OEMs Now Shipping FIDO Certified Devices

SAMSUNG

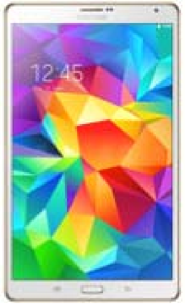
S5, Mini

Alpha

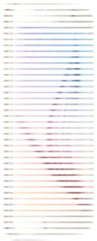
Note 4, 5



Note Edge



Tab S, Tab S2



S6, S6 Edge

Sharp Aquos Zeta

Sony Experia Z5

Fujitsu Arrows
(Iris Biometrics)

fido U2F UAF Certified

AUTHASAS We make authentication work

BLUINK LTD.

CrucialTec

Daon

egis Technology

Entersekt

ETRI Electronics and Telecommunications Research Institute

FEITIAN WE BUILD SECURITY

Google

GO-Trust Trust in a Mobile World

HAPPLINK SOLUTIONS FOR DIGITAL LIFE

HYPERSECU®

InCOMM

infineon

LG Electronics

RAONSECURE

MicroStrategy

Nok Nok LABS

NTT docomo

NXP

QUALCOMM

SK planet

SAMSUNG

SAMSUNG SAMSUNG SDS

SECURE METRIC TECHNOLOGY

sensory™

SHARP

Synaptics®

Sonavation®

SONY

ST life.augmented

StrongAuth® Securing the Core

SurePass id

FUJITSU

TendyRon

Yahoo! JAPAN

yubico Trust the Net.

Feedback welcome

- General approach/levels of risk?
- Relax requirements for minimum species types tested and passed? Or require more and/or that all unknown testing is passed?
- Examples for each modality for different levels of attacks?
- Should these numbers be relaxed or strengthened:
  - Each species should be tested with a minimum of 100 attempts, using a series of 10 for 10 different people, 5 men and 5 women.
- Attack presentation match rate (APMR) of less than 5% shall be achieved for each attack type?

References

- ISO/IEC JTC 1/SC 37: 30107 Information technology — Biometric presentation attack detection, Parts 1 and 3.
- Measuring Strength of Authentication, NIST ITL, Workshop: Applying Measurement Science in the Identity Ecosystem, Version: 1, December 16, 2015,

http://www.nist.gov/nstic/NSTICstrengthauthenticationdiscussiondraft.pdf

- O Henniger, D Scheuermann, and T Kniess. On security evaluation of fingerprint recognition systems, IBPC, 2010.

http://biometrics.nist.gov/cs_links/ibpc2010/pdfs/Henniger2_Olaf_IBPC_Paper.pdf

Thank you

Questions or Comments?

enewton@nist.gov and sschucke@clarkson.edu

Back up slides

		Fingerprint	Face	Iris	Voice
Level A	Source of biometric characteristic: easy to obtain	lift of fingerprint	photo from social media	photo from social media	recording of voice
Level B	Source of biometric characteristic: more difficult to obtain	latent print, stolen fingerprint image	video of subject, high quality photo	video of subject, high quality photo	recording of voice of specific phrase
Level C	Source of biometric characteristic: more difficult to obtain	3D fingerprint information from subject	3D face information from subject	high quality photo in Near IR	multiple recordings of voice to train synthesizer

Presentation Attack Detection (PAD)

- **Presentation attack**

presentation to the biometric data capture subsystem with the goal of interfering with the operation of the biometric system

- **Presentation attack detection (PAD)**

automated determination of a presentation attack.

- Artefact and Liveness Detection are types of PAD.

From ISO/IEC 30107-1: 2016

Proposed Testing Framework

- Qualitative risk levels A, B, and C
- Covers four modalities
  - Fingerprint, face, iris, & voice
  - Others could be developed if the modality passes the requirements for FAR and FRR if determined by a third party.
- Known and unknown methods must be tested
  - Lesson learned from LivDet