Update by Singapore member

By Mr. LIN, Yih

1. **Director, Digital Applied Research and Technology Pte Ltd**
2. **Chairman, Cards and Personal Identification Technical Committee (CPITC), under Singapore IT Standards Committee (ITSC)**
3. **Chairman, Singapore Telecommunications Standards Advisory Committee (TSAC) WG7 "Communications Security"**
4. **Convenor, ISO/IEC JTC1 SC17 WG11 "Biometrics on Cards"**

Overview of my presentation slides

- Updates from my international meetings
- Security alert – use of card serial number
- Standards developed in SC17 WG11
- Technical challenges of building contactless BSoC

Updates from ISO/IEC JTC1 SC17 Plenary

ISO/IEC JTC1 SC17 Plenary

Overview of ISO/IEC JTC1/SC17

English

International Organization for Standardization

Great things happen when the world agrees

Standards | All about ISO | Taking part | Store

Search

Who develops standards | Deliverables | Get involved | Resources

Taking part > Who develops standards > Technical Committees > ISO/IEC JTC 1 > SC 17

ISO/IEC JTC 1/SC 17

Cards and personal identification

About

Secretariat: BSI

Secretary: Ms Jean Stride

Chairperson (until end 2019): Dr Peter Waggett

ISO Technical Programme Manager : Mme Maho Takahashi

ISO Editorial Programme Manager : Ms Claudia Lueje

Creation date: 1987

Scope

The current area of work for JTC 1/SC 17 consists of:

- Identification and related documents
- Cards, and
- Devices associated with their use in inter-industry applications and international interchange

Quick links

Work programme
Drafts and new work items

Working area
on ISOTC and Public information folder

ISO Electronic applications
IT Tools that help support the standards development process

Structure of ISO/IEC JTC1/SC17

114	31	33	19
published ISO standards * under the direct responsibility of ISO/IEC JTC 1/SC 17	ISO standards under development * under the direct responsibility of ISO/IEC JTC 1/SC 17	Participating countries	Observing countries

* number includes updates

Structure | Liaisons

Reference	Title	Type
ISO/IEC JTC 1/SC 17/CAG 1	Chairman advisory group	Working group *
ISO/IEC JTC 1/SC 17/SWG 1	Registration Management Group (RMG)	Working group *
ISO/IEC JTC 1/SC 17/WG 1	Physical characteristics and test methods for ID-cards	Working group *
ISO/IEC JTC 1/SC 17/WG 3	Identification cards - Machine readable travel documents	Working group *
ISO/IEC JTC 1/SC 17/WG 4	Integrated circuit card with contacts	Working group *
ISO/IEC JTC 1/SC 17/WG 5	Identification cards — Identification of issuers	Working group *
ISO/IEC JTC 1/SC 17/WG 8	Integrated circuit cards without contacts	Working group *
ISO/IEC JTC 1/SC 17/WG 10	Motor vehicle driver licence and related documents	Working group *
ISO/IEC JTC 1/SC 17/WG 11	Application of biometrics to cards and personal identification	Working group *

* The convener can be reached through the secretariat (See contact information below)

ISO/IEC JTC1 SC17 Plenary, 12-14 Oct 2016

- I presented 3 reports – WG11 Convenor's, Singapore country report, SC17 to SC37 Liaison officer report
- Chairman Richard Mabbott (UK) steps down after 21 years of service
- New Chairman is Peter Waggett (UK)
- Next 2017 Plenary will be in Paris, France (9-20 Oct 2017)

Korea (Dr Tak) proposed a SIM based drone identification standard new work item

- Dr Tak presented a NWI to standardise Drone Operator's License, Drone Controller's License, Drone Driver's License, Drone Identify Module.
- Proposal has been approved by international ballot. Details in another presentation.

Updates from ISO/IEC JTC1 SC17 WG11

ISO/IEC JTC1 SC17 WG11
"biometrics on cards"

ISO/IEC JTC1 SC17 WG11, 15-17 Mar 2017

- ISO/IEC 17839-3 has been published on 1 Nov
- ISO/IEC 17839 series covers Biometric System-On-Card (i.e. sensor and matcher)
- Current focus on revision of 24787 On-Card-Comparison, project editors from Singapore
- Next meeting – Oct 16-17, 2017 in Paris

Updates from ISO/IEC JTC1 SC17 WG11

Standards developed in SC17 WG11 and Challenges of building BSoC will be covered later

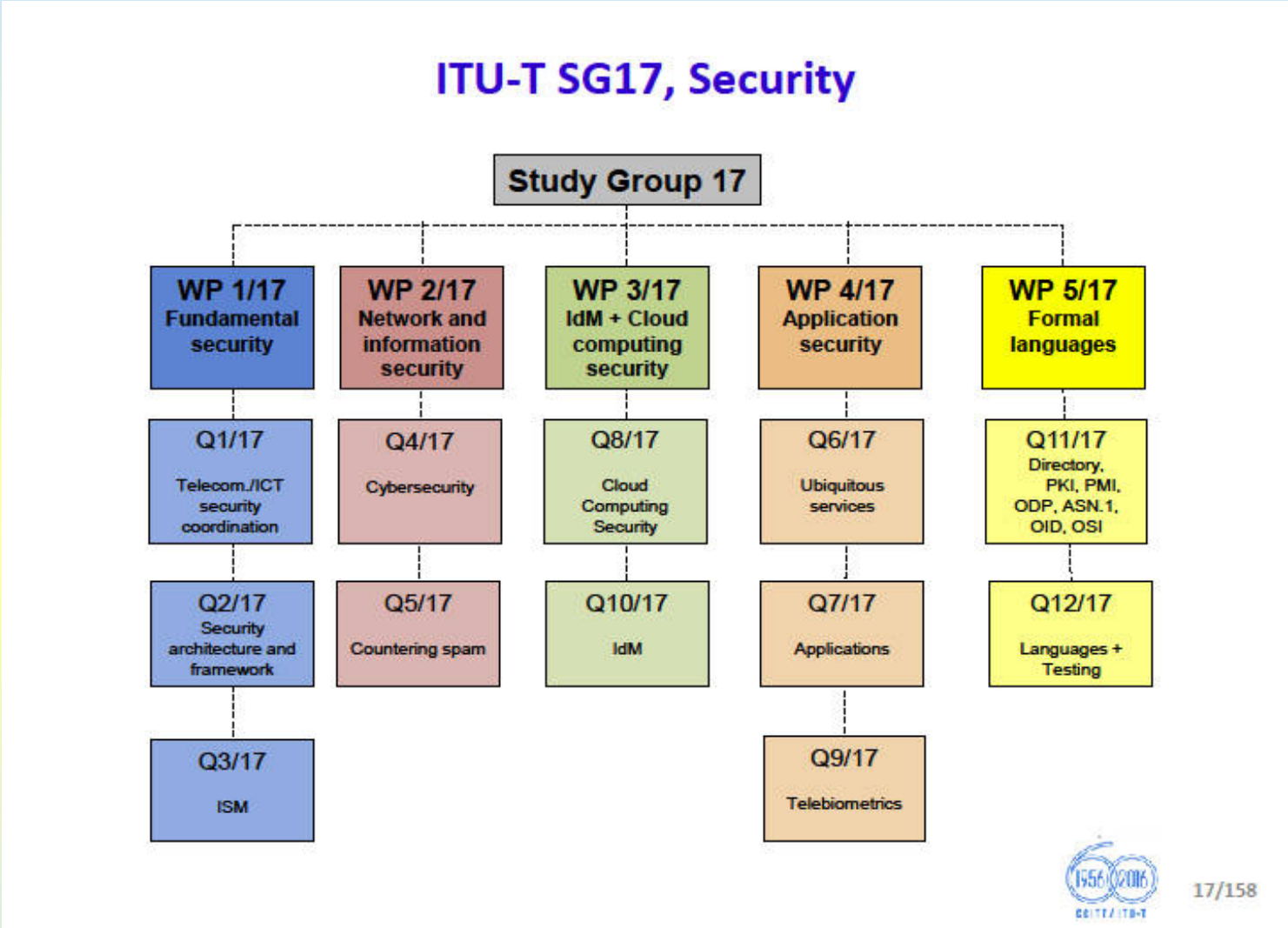
Updates from ITU-T SG17 “Security” meeting

ITU-T SG17 Meeting
29 Aug - 7 Sep 2016
Geneva, Switzerland

ITU-T SG17, 29 Aug – 7 Sep, Geneva, Switzerland

- About 120 delegates over 8 working days
- China, Korea, Japan sent most delegates
- Many African countries attended too

ITU-T SG17 structure and work areas



- PKI, identity management, application security are relevant to AICF activities

ITU-T SG17 structure and work areas

- ITU-T SG17 meets twice a year
- Singapore plans to attend at least once a year (Sep / Oct)

- ITU-T SG17 has work items that overlap with ITU-T SG16 "Media, Systems and Applications"
- ITU-T SG16 also covers "Intelligent Transport System"
- ITU-T SG17 also has work items that overlap with ITU-T SG20 "IoT"
- Singapore will monitor all these SGs and align our "LOHEI" work accordingly

Next ITU-T SG17 “Security” meetings

ITU-T SG17 Meetings
(Geneva, Switzerland)

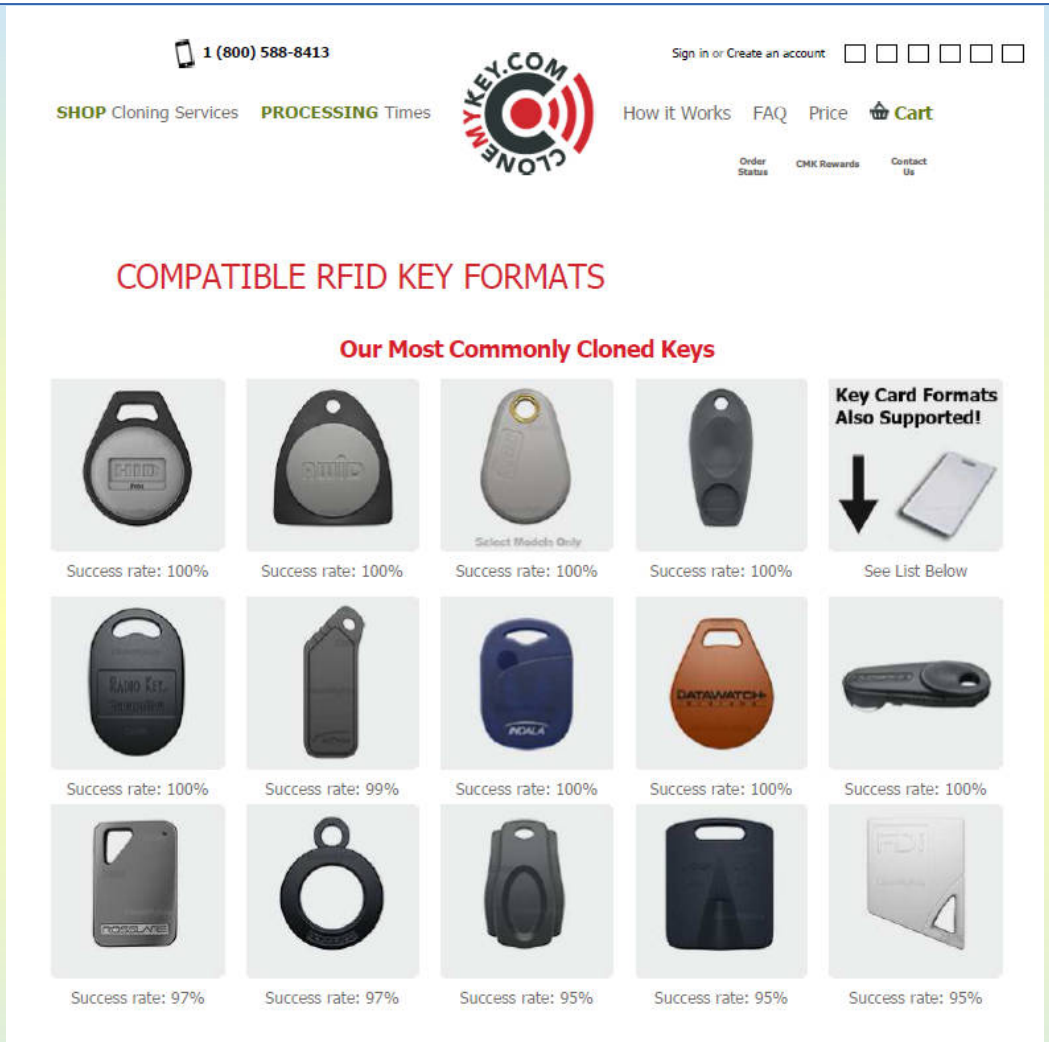
- 22-30 Mar 2017
- 21 Mar, Workshop on Security Aspects of Blockchain
- 29 Aug – 6 Sep 2017
- 28 Aug, Workshop on ITS Security

Security Alert – use of card serial number

Special Security Alert

Card Serial Number
an be cloned easily
use with caution

Companies openly advertise card cloning



- **Produce another device with same serial number as old one**

Companies openly advertise card cloning

95% Success

Formats and brands below have been supported for less than 1 year or have a success rate between 95% to 99%.

Aptus	BlueWave Security	Cardax	Casi-Rusco
Comelit	Community Controls	Corby (Ibutton & Prox)	Deister Electronics
DKS (Select Models Only)	Doorking (Select Models Only)	Farpointe Data	FDI
Fermax	Force	GProx-II	Hexact
ICT	Identiv	IDTECK	IntelleQt®
IoProx	Kaba	Keri W Format	Key-Rite Security
Mango	Mifare® Classic 1K	Mifare® Classic 4K (CSN Only)	Mifare® Ultralight (Non C)
MicroPlus 8069	Miwa	Monarch †	Mul-T-Lock®
NexKey	NexWatch	Noralsy	PassPoint
Position Technology	Prox Lite	Pyramid (Farpointe Data)	Rosslare
RSS (Rapid Security Solutions)	Select Engineered Systems †	XceedID	

- **Mifare serial number can be cloned**

Security Alert – use of card serial number

Card Serial Number is now typically reported by the card operating system software

Hence a card can be programmed to report <u>any</u> serial number of your choosing

Security Alert – use of card serial number

Simple Card Serial Number should <u>not</u> be used for identification application unless supplemented by cryptographic mechanism to prevent cloning, replay

CEPAS provides a mechanism for authenticated reading of CAN and CSN

Overview of standards Developed in ISO/IEC JTC1 SC17 WG11

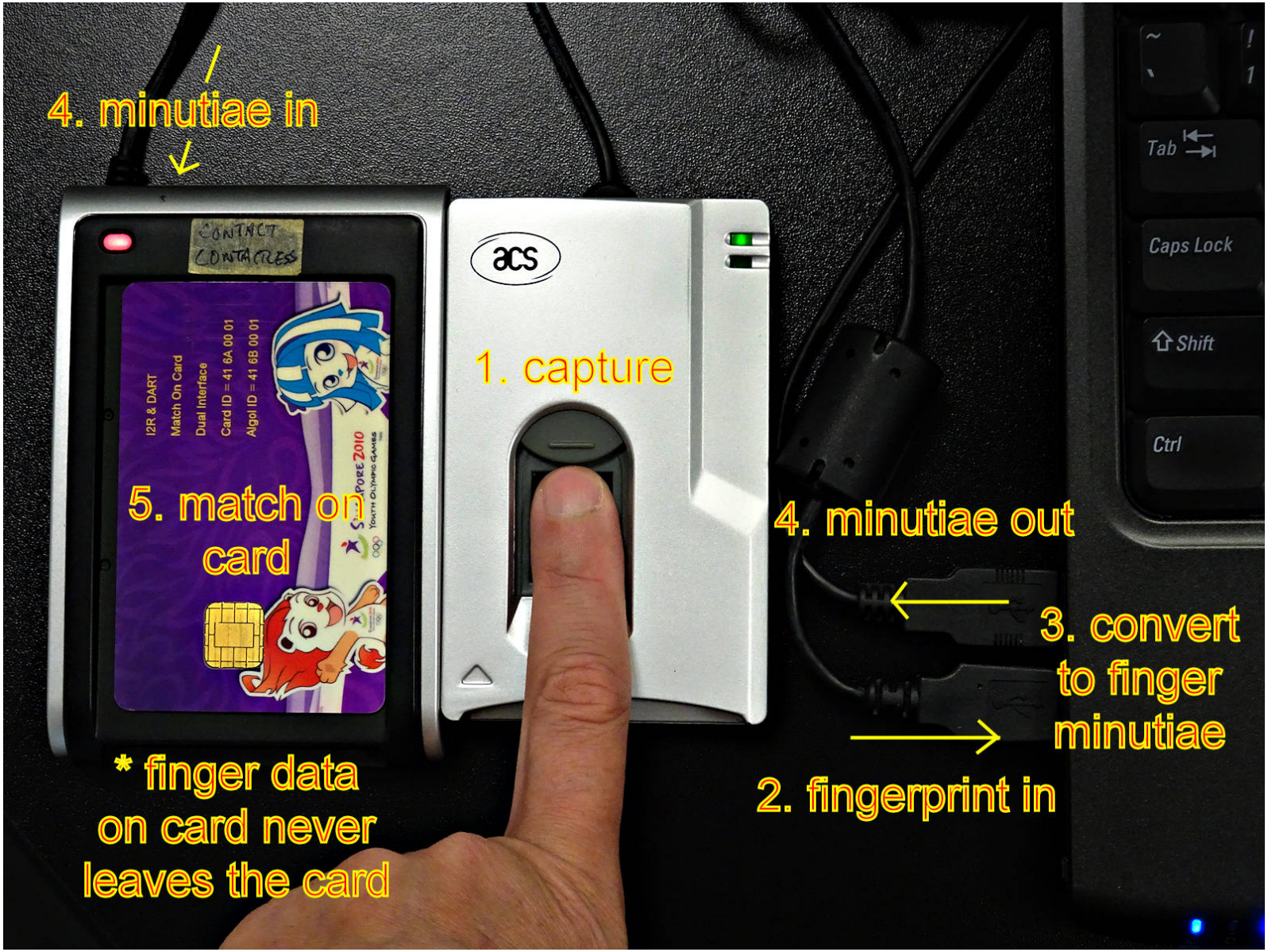
Standards developed in SC17 WG11

- ISO/IEC 24787:2010 - On-card biometric comparison
- ISO/IEC TR 30117:2014 - Guide to on-card biometric comparison standards and applications
- ISO/IEC 18584:2015 - Conformance test requirements for on-card biometric comparison applications
- ISO/IEC 17839-1:2014 - Biometric System-on-Card -- Part 1: Core requirements
- ISO/IEC 17839-2:2015 - Biometric System-on-Card -- Part 2: Physical characteristics
- ISO/IEC 17839-3:2016 - Biometric System-on-Card -- Part 3: Logical information interchange mechanism

What is Match on Card ?

(also known as “biometric on card comparison”)

Overview of Match on Card (MoC)



ISO/IEC 24787:2010

- ISO/IEC 24787:2010 covers topics such as
  - Mandatory retry counter to prevent repeated brute force attack
  - Return of comparison status in a trusted, secured manner
  - Security policies for on-card biometric comparison
  - Commands and rules to permit pre-comparison computations to be done off-card ("work sharing", useful for Java card implementation)
  - Single storage of biometric data shared by multiple applications
- ISO/IEC 24787:2010 is currently being revised (updated)

TR 30117:2014

- ISO/IEC TR 30117:2014 summarizes how the international standards, recommendations and technical reports dealing with identification cards, biometrics and/or information security relate to each other with regard to the joint use of biometrics and integrated circuit cards
- Also provides further recommendations and policies needed by developers to integrate applications related to on-card biometric comparison.

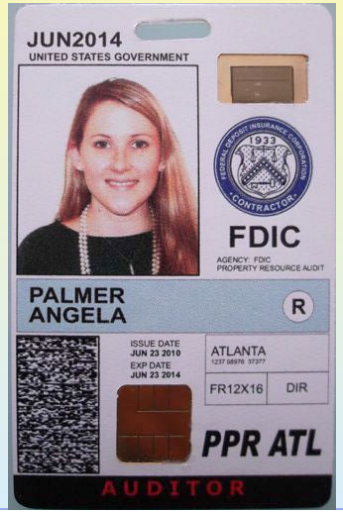
ISO 18584:2015

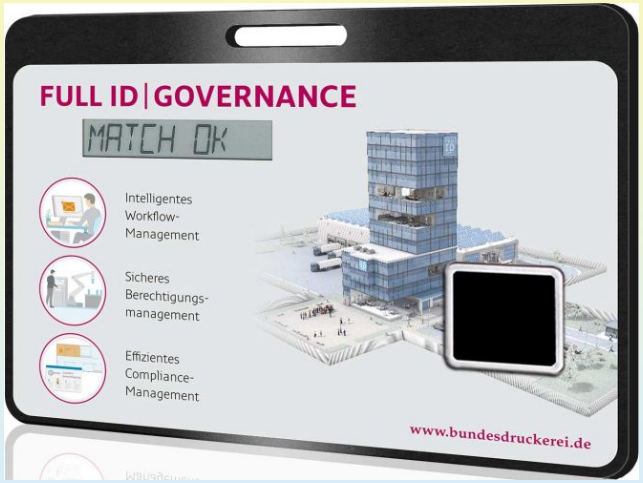
- ISO 18584:2015 establishes
  - Conformance test requirements for using general framework for on-card comparison applications,
  - Conformance test requirements for using work-sharing mechanism for on-card comparison applications, and
  - Conformance test requirements to check accomplishment of security policies for on-card biometric comparison that are specified in ISO/IEC 24787:2010

What is Biometric System On Card ?

Biometric System on Card (BSoC)

- **Biometric capture, feature extraction, comparison all on the card**
- **The samples shown here may not conform with ISO/IEC 17839-x**





ISO 17839-1:2014

- Defines two different types of system-on-card: Type S1 and Type S2
- Type S1 (“conventional”)
  - Dimensions (thickness, width and height) in accordance with the ID-1 format as specified in ISO/IEC 7810 (e.g. 0.76mm thick)
  - Card withstands torsion and bending tests specified in ISO/IEC 7816-1
  - Communication Interface may be any of the following:
    - Contact interface as specified in ISO/IEC 7816-3
    - USB interface as specified in ISO/IEC 7816-12
    - Contactless interface as specified in ISO/IEC 14443

ISO 17839-1:2014

- Type S2 ("new, thicker")
  - Card must be 2.5mm thick, more than the one defined in ISO/IEC 7810
  - Maximum width and height are within the boundaries of an ISO/IEC 7810 card as specified in ISO/IEC 17839-2
  - Need not conform to the ISO/IEC 7816-1 flexibility requirements
  - Supports *only* contactless interface specified in ISO/IEC 14443
  - 2.5mm thick card cannot be inserted into standard card slot by mistake
- Regardless of S1 or S2, a card with swipe sensor must have some form of feedback mechanism such as LCD display, LED or buzzer

ISO 17839-2:2015

- ISO 17839-2:2015 covers “Physical characteristics”
  - The minimum size of an fingerprint area sensor shall be 13x13 mm^2 (0.512x0.512 in^2)
  - In the case of a swipe sensor, the effective area of fingerprint capture is bigger than the sensor size. A swipe sensor shall have a minimum width of 13 mm (0.512 in)
- Allows fingerprint sensor, voice microphone, camera for facial image, signature input pad

ISO 17839-3:2016

- ISO 17839-3:2016 covers “Logical information interchange mechanism”
  - Commands and data structures
  - Internal Enrollment and External Enrollment
  - Initiation of verification
  - Status feedback
  - Processing time management and extension
  - Capability discovery mechanism

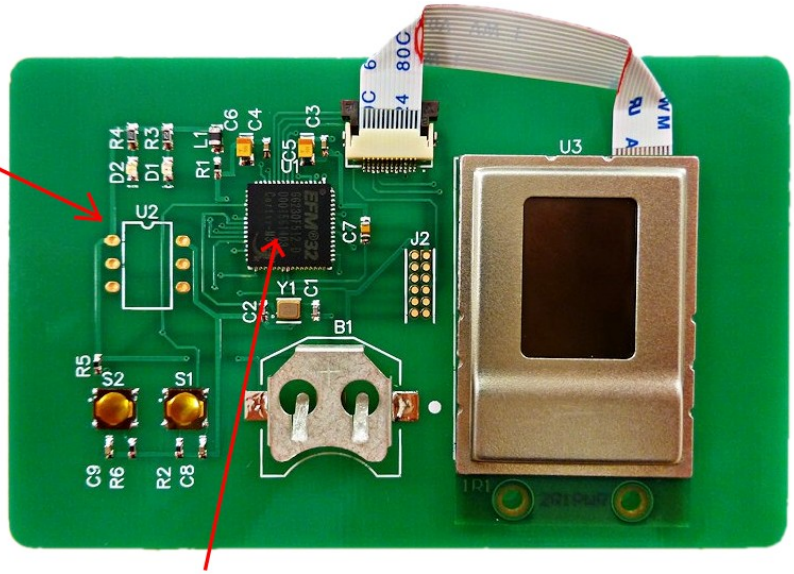
Summary and conclusion

- Biometric Match on Card and Sensor on Card prevents sensitive data (e.g. fingerprint) from leaving the card
- Demand has been around for decades, and technology continues to grow and improve
- Standards are available to ensure – interoperability, confidence in products and services, etc.
- Although the context here is “card”, the technology can be applied to other form factors – key chain, wrist band, other wearable devices with secure element capability

Technical challenges of building contactless BSoC

“Home made” BSoC prototype

There is a dual-interface smartcard sandwitched behind green PCB !



Multi-IC system : EFM32 is the main controller, not the smartcard

- Fingerprint data needs “large” RAM space
- With / without a battery, low power operation is a challenge

Technical challenges

- Fingerprint data is not small: 13 x 13 mm square @ 512 dpi = 68KB
- Most smart card MCU RAM limited to 32KB
- RAM not NVM because the fingerprint data needs to be processed for matching (e.g. rotation, shift, image processing, etc.)
- Low power operation is another challenge – the main MCU must "sleep" as much as possible in between operations, even when doing data transfer – the MCU should provide many options for power management
- Best case architecture – main MCU, smart card MCU, sensor controller all integrated into one (but need to have a few companies work together)

Technical challenges

- Example choice of main MCU: Silicon Labs EFM32 family
- 48MHz, 1.98–3.8 V supply voltage
- RAM: 128KB, Flash: 512KB
- Flexible energy management system with 5 different energy modes
  - 20 nA shutoff mode (0.4 µA with RTC)
  - 0.6 µA stop mode, including power-on-reset, brown-out detector, RAM and CPU retention
  - 0.9 µA deep sleep mode, including RTC with 32.768 kHz oscillator, power-on-reset, brown-out detector, RAM and CPU retention
  - 45 µA/MHz sleep mode
  - 180 µA/MHz run mode with code executed from flash

THE END

THANK YOU

Q&A