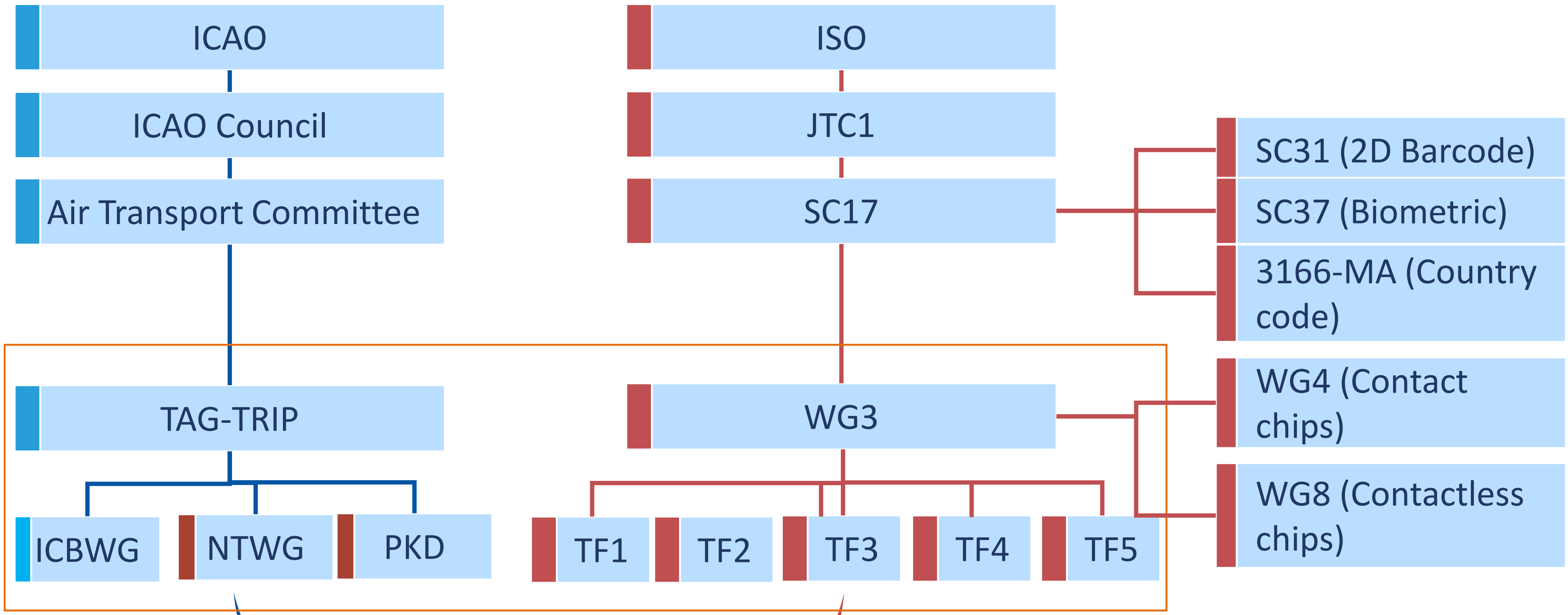
ISO Updates

R Rajeshkumar

Convener – ISO/IEC SC17/WG3

1. ICAO-ISO Relationship

Working Relationship between ICAO and ISO



ICAO

ICAO Council

Air Transport Committee

TAG-TRIP

ICBWG

NTWG

PKD

ISO

JTC1

SC17

SC31 (2D Barcode)

SC37 (Biometric)

3166-MA (Country code)

WG3

WG4 (Contact chips)

WG8 (Contactless chips)

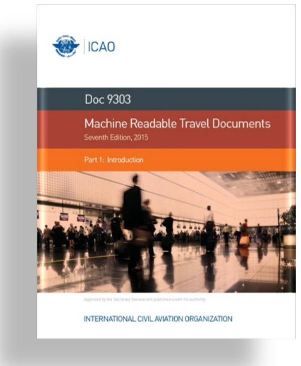
TF1

TF2

TF3

TF4

TF5



ICAO

Doc 9303

Machine Readable Travel Documents

Seventh Edition, 2015

Part 1: Introduction

INTERNATIONAL CIVIL AVIATION ORGANIZATION

ICAO Doc 9303 / ISO-IEC 7501

2. Governance

Meetings since TRIP 2023

- Wellington, NZ – March 2024
- Sydney, AU – October 2024

WG3 Structure

- Current Structure
  - TF1 – New Technologies
  - TF2 – Editorial
  - TF3 – Application Issues
  - TF4D – Test Specifications (Physical)
  - TF4R – Test Specifications (Logical)
  - TF5 – Logical (Chip and PKI)

- New Structure
  - TF1 – ~~New Technologies~~
  - TF2 – Editorial
  - TF3 – ~~Application Issues~~
  - TF4D – Test Specifications (Physical)
  - TF4R – Test Specifications (Logical)
  - TF5 – Logical (Chip and PKI)
  - TF6 – Physical Layout
  - TF7 – Optical Readable Data
  - TF8 - Biometrics

Editors and Liaisons

- Editors will have shadow editors – for load sharing and succession planning
- Liaisons
  - NTWG and TAG/TRIP – Convener – R Rajeshkumar (Singapore)
  - ICBWG – Patrick Beer (Switzerland)
  - SC17/WG4 – Kenichi Nakamura (Japan)
  - SC17/WG10 – Kenichi Nakamura (Japan)
  - SC37 – Andreas Wolf (Germany)
  - PKD – Peter Campbell (New Zealand)
  - SC27 – Gaetan Pradel (Luxembourg)

Doc 9303 Fast Track

- Have submitted word versions to JTC1. Need to send pdf versions and editable graphics – ballot will open after about 6 weeks and will run for 8 weeks. If no major objections, ISO/IEC 7501 will be published and be in sync with 8th edition of Doc 9303
- ISO/IEC 18745-1 is published as ISO standard. Will be converted to an ICAO TR
- ISO/IEC 18745-2 is published by WG8 – transfer requested to WG3. Will also be converted to ICAO TR
- Then all parts of 18745 can be fast tracked using same process

3. TF2 Updates

Current Work

- FALP/13 decisions
  - Transition from ISO/IEC 19794-5 to 39794-5 for DG2 (facial image)
  - Deprecation of BAC & requirements to support PACE for eMRTDs
  - Adoption of the document type indicator’s 2nd character for passports
- FALP/13 timelines
  - are supposed to be adopted in Annex 9 “Facilitation” as standards
  - shall be specified in Doc 9303 as well
    - as Annex 9 and Doc 9303 address different audiences
  - are not yet adopted completely in Doc 9303 8th Edition
- Revision of Doc 9303 8th Edition – parts 4,8 and 11
  - To keep it consistent with the ICAO FALP/13 decisions for Annex 9

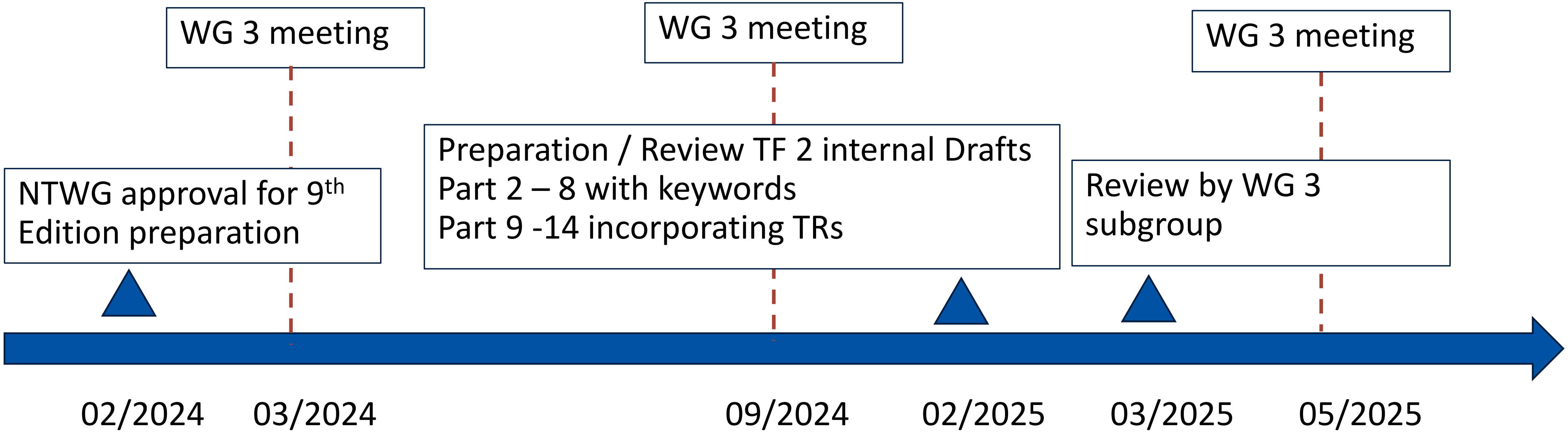
Further revisions

- Further Clarifications & Corrections to be included in this revision
  - Part 4: Description of the document type indicator (NTWG request)
    - “PT – Alien passport” → “PT – Alien/Non-Citizen passport”,
  - Part 11: Clarification on Chip Authentication → TF 5

Towards the 9th edition of Doc 9303

- Focus on editorial work
  - Incorporate published ICAO Technical Reports
  - Harmonize the terminology with the terms to be adopted in Annex 9 “Facilitation”
  - Express provisions in part 2 – 8 using the keywords SHALL, SHOULD, MAY etc.
  - Clarifications & correction of obvious errors / inconsistencies
  - Deprecate Doc 9303-6 for TD2 sized MROTDs

Doc 9303 9th Edition – Tentative Schedule



WG 3 meeting

WG 3 meeting

WG 3 meeting

NTWG approval for 9th Edition preparation

Preparation / Review TF 2 internal Drafts
Part 2 – 8 with keywords
Part 9 -14 incorporating TRs

Review by WG 3 subgroup

02/2024 03/2024 09/2024 02/2025 03/2025 05/2025

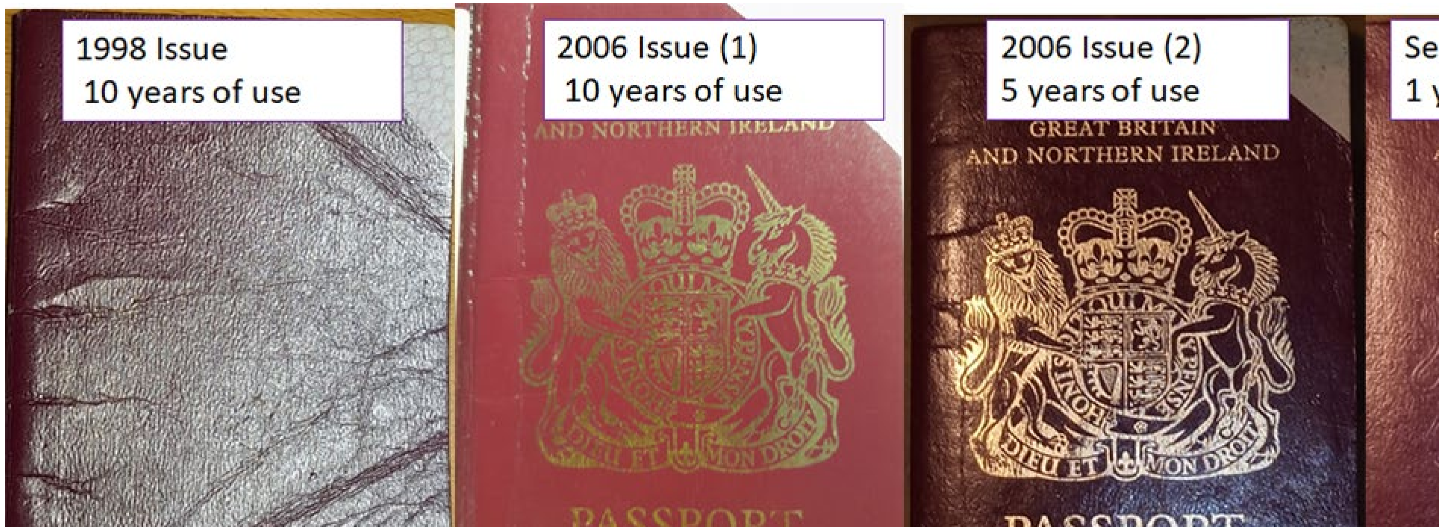
4. Other work items

Technical Reports in progress

- eMRTD Bound DTC-VC Extended – add additional photo to the VC
- DTC-VC – Transmission Protocol
  - 2 existing protocol (OpenID4VP, ISO/IEC 23220-4 REST API) and 1 protocol under development (Browser API) are candidates
- DTC-PC Phase 2 – defining a Physical Component with alternate form factor (mobile phone)
  - Focus on security and certification of the device before defining the protocols

ISO/IEC 18745-1 revision – Physical Test Specifications

- Test for Hot Stamp on the cover to be investigated



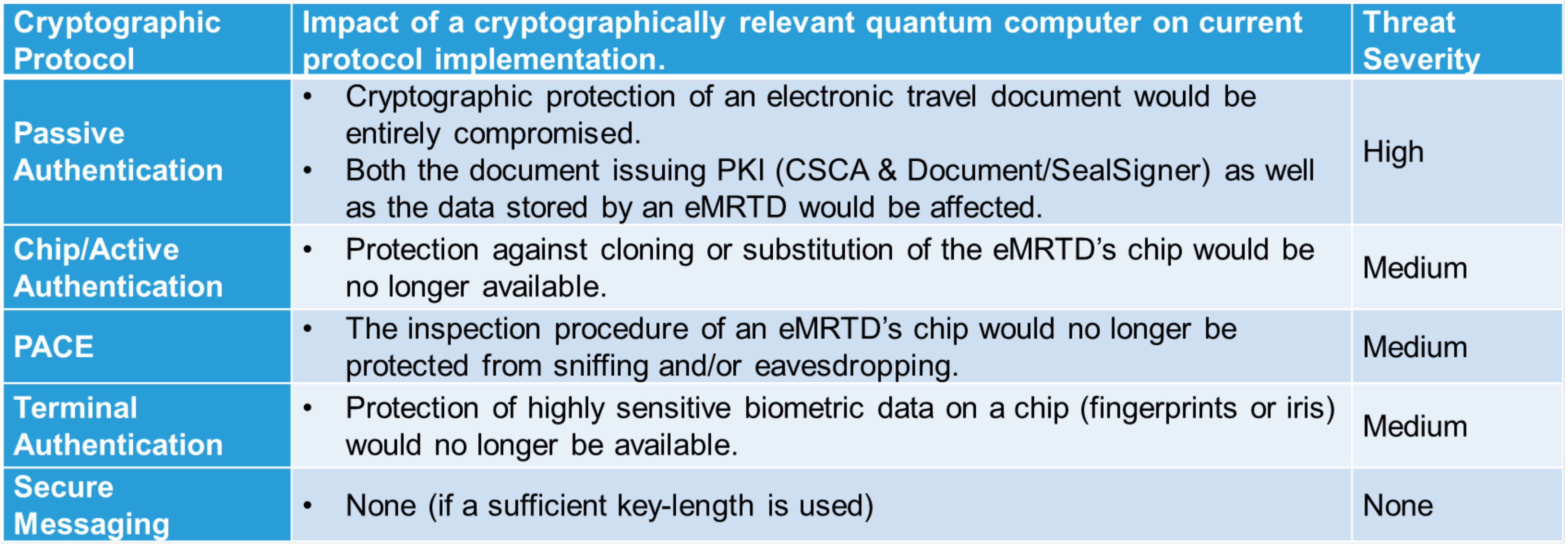
1998 Issue
10 years of use

2006 Issue (1)
10 years of use

2006 Issue (2)
5 years of use

Se
1 y

Research on Post Quantum Cryptography



Cryptographic Protocol	Impact of a cryptographically relevant quantum computer on current protocol implementation.	Threat Severity
Passive Authentication	• Cryptographic protection of an electronic travel document would be entirely compromised. • Both the document issuing PKI (CSCA & Document/SealSigner) as well as the data stored by an eMRTD would be affected.	High
Chip/Active Authentication	• Protection against cloning or substitution of the eMRTD's chip would be no longer available.	Medium
PACE	• The inspection procedure of an eMRTD's chip would no longer be protected from sniffing and/or eavesdropping.	Medium
Terminal Authentication	• Protection of highly sensitive biometric data on a chip (fingerprints or iris) would no longer be available.	Medium
Secure Messaging	• None (if a sufficient key-length is used)	None

Status quo of Post-Quantum Cryptography

- First cryptographic primitives for digital signatures and key encapsulation are available
  - Stateful hash-based signature schemes: XMSS, LMS
  - NIST competition on Post-Quantum Encryption Standards released first 3 final standards: ML-KEM (CRYSTALS-Kyber), ML-DSA (CRYSTALS-Dilithium), SLH-DSA (Sphincs+)
- Primitives must be implemented into cryptographic protocols
  - Specifications for using PQC algorithms in X.509 certificates or CMS are still mostly in draft status

Doc 9303 cryptographic key length review

- Review all currently allowed cryptographic algorithms, domain parameters and key lengths in Doc 9303 (part 11, 12 and 13)
- Analyze the impact of further cryptographic primitives (e.g. SHA-3), key-lengths or domain parameters (e.g. finite fields > 2048 bits)
- Ad-hoc group prepared first draft
  - Only covers review of currently allowed algorithms
  - Idea: Map each algorithm & key length to a security strength
- Document is still under discussion
  - Challenge: Keep balance between raising security and technical feasibility
  - No recommendations for the time being

ICAO Datastructure for Barcodes (IDB)

- In previous version 1.1, two documentType were introduced:
  - “NH” for healthproof messages
  - “NA” for travel document messages
- Issue for countries that need to differentiate visa signer from other travel documents (Iceland)
  - In version 1.2, new documentType "NB“ introduced for visa and/or DTA
- New worked example for TD1 MRZ
- In future, new worked examples will be created and published to Github site – no revision of TR for each example. Major revision will incorporate the worked examples

5. 39794-5 Application Profile

39794-5 Application Profile

- New encoding for DG2 agreed by NTWG and endorsed by TAG/TRIP
- Inspection Systems need to be ready by 2026 to handle the new encoding
- Issuers to switch to new encoding by 2030
- Interoperability event for testing readiness of Issuers and Inspection Systems – Sydney, October 2024

Preparation

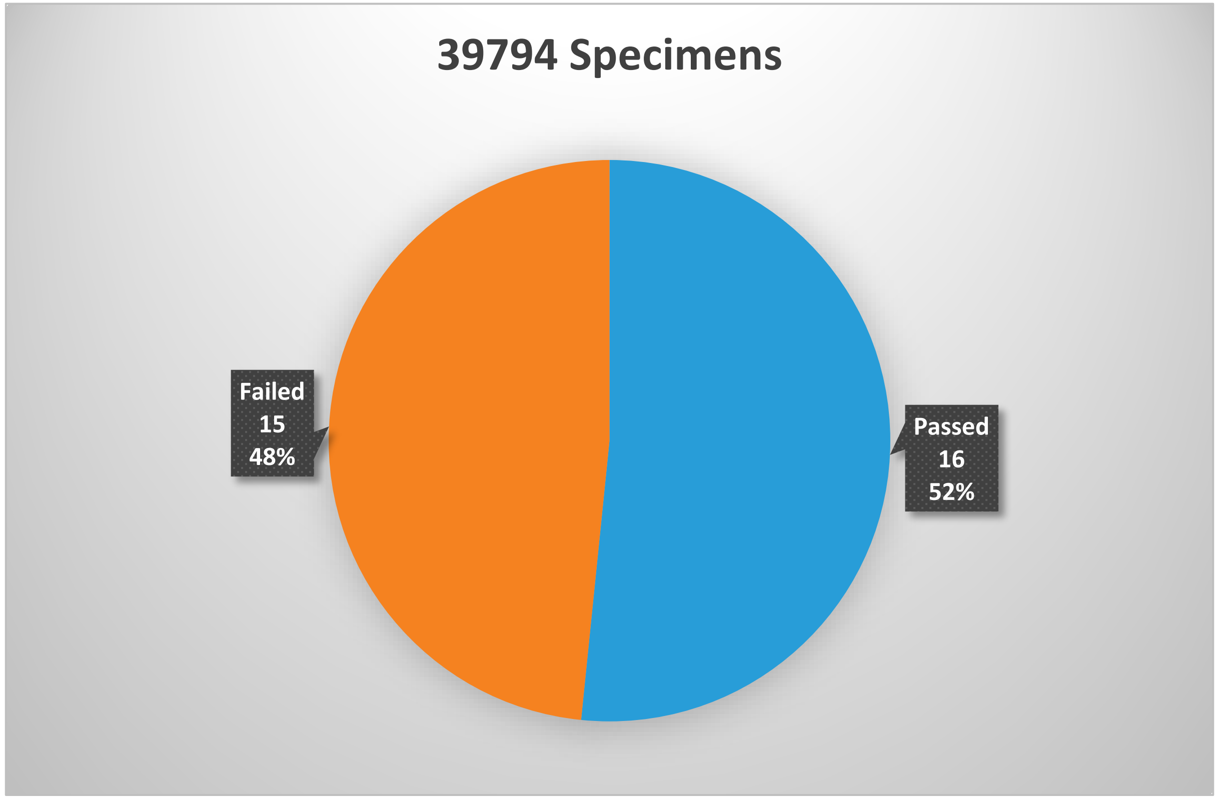
- Silver dataset created and published to WG3 github site
- Additional test data created to simulate future extensions that might be defined by SC37
- Quite good participation
  - 13 eMRTD participants
  - 12 Inspection participants

Conduct of the Test

- Reference implementation of Inspection System
  - Used to do a smoke test to pick out issues with eMRTD samples brought by issuers
- Reference implementation of eMRTDs for testing inspection systems
- Additional eMRTDs to do negative tests
- Anonymized – Result not linked back to a company or product

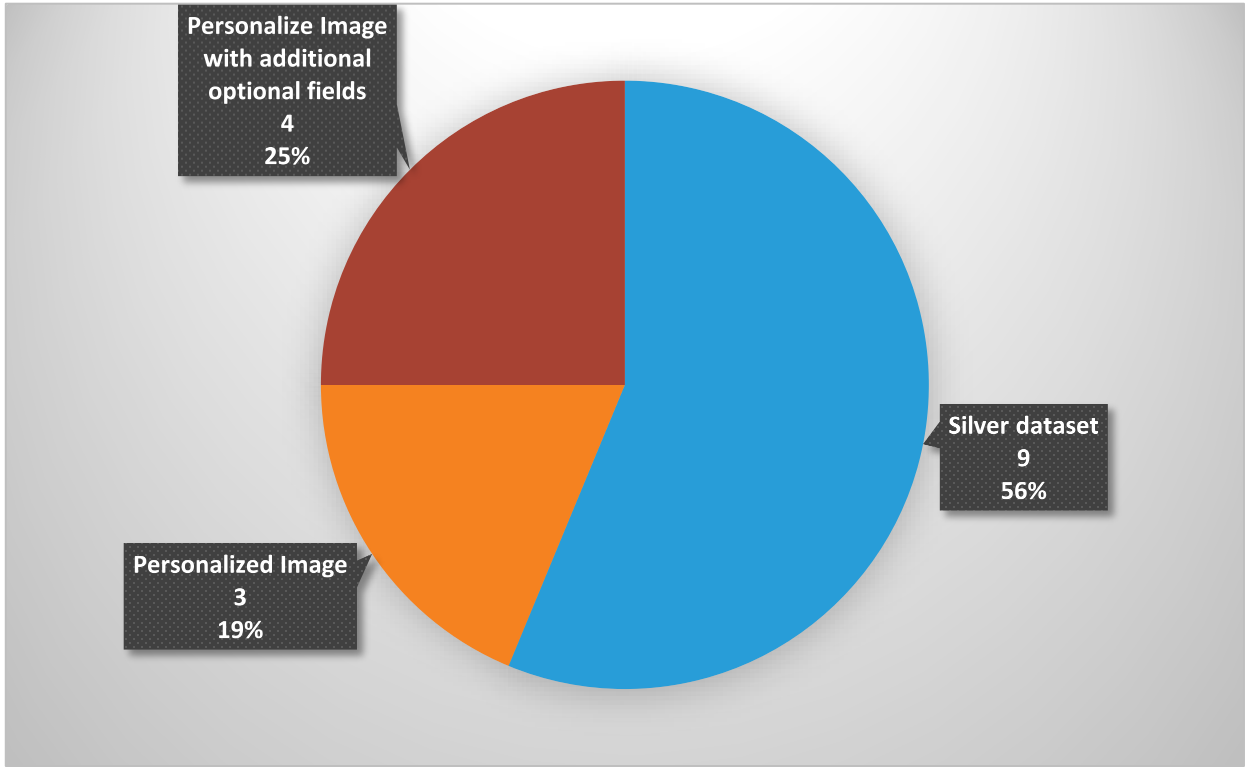
eMRTDs – 39794 Specimens

- Correctly encoded specimens – 52%
- Wrongly encoded – 48%



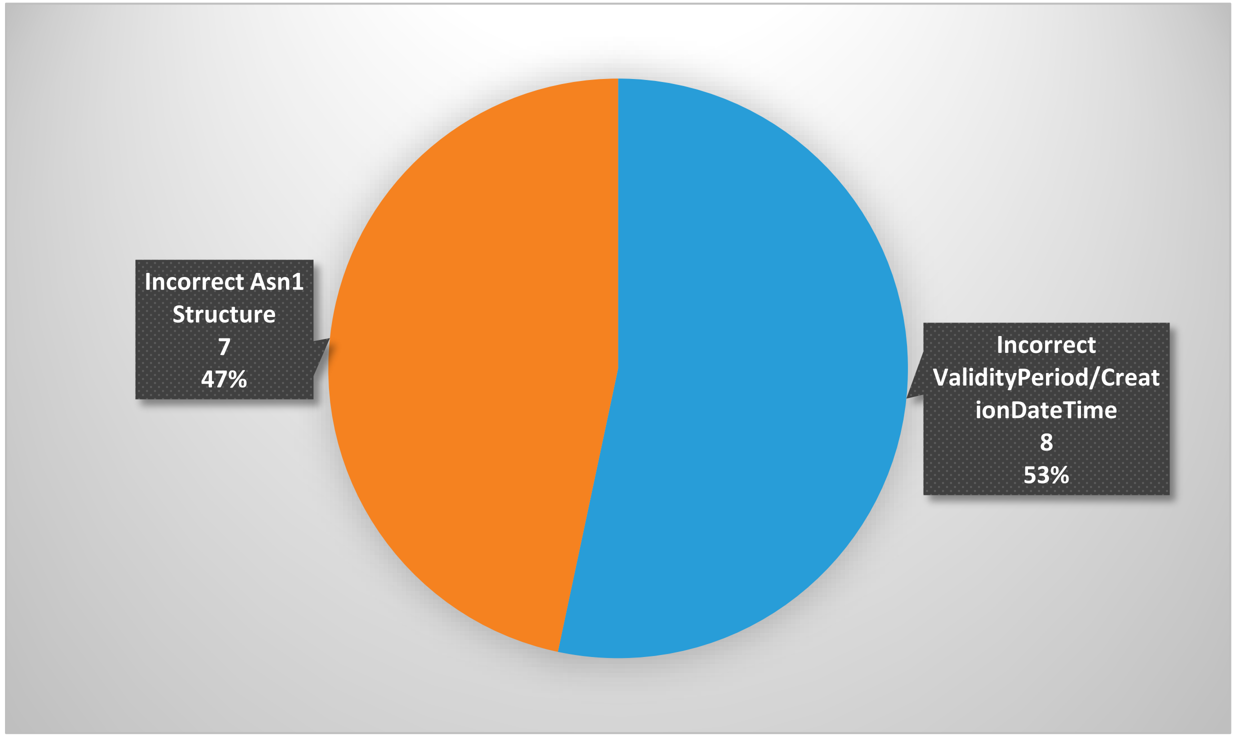
eMRTDS – Specimens that passed

- 56% simply re-used the silver data set
- 19% used the same metadata as the silver data set but with different images
- 25% created new DG2 from scratch and got it right



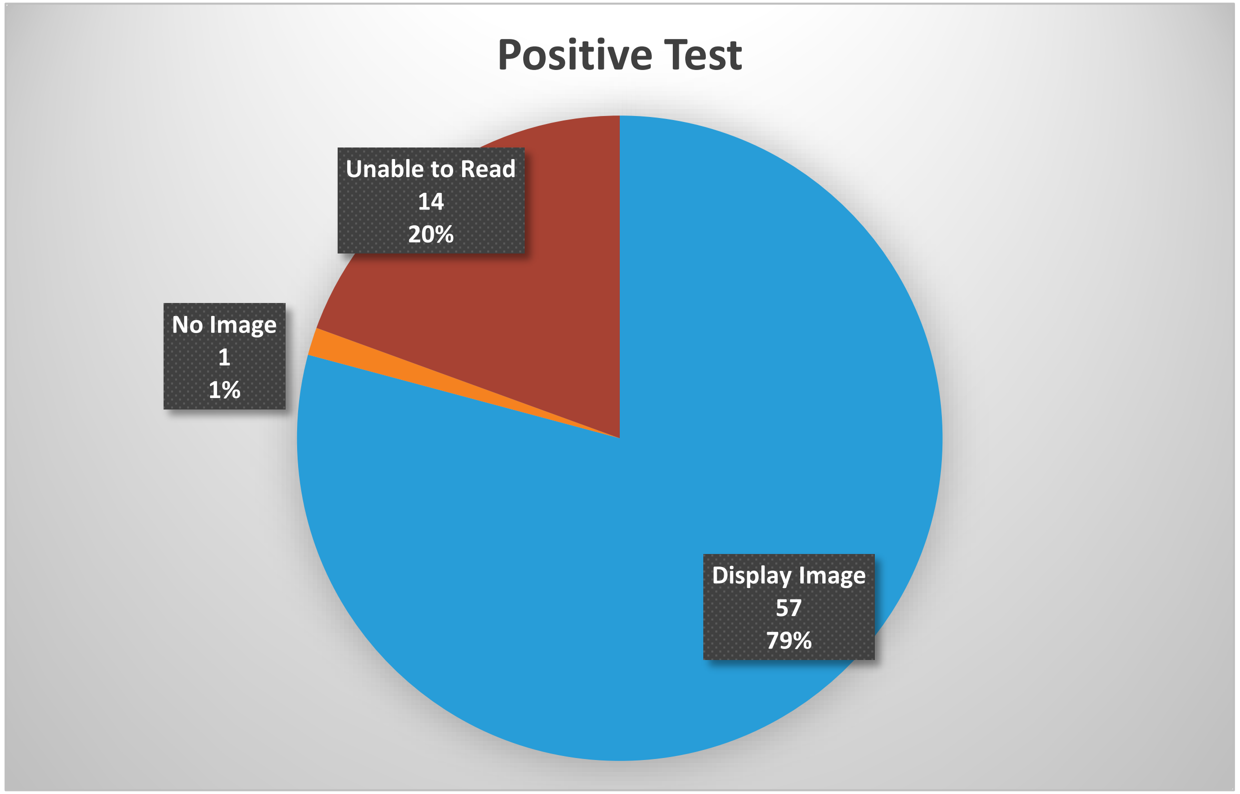
eMRTDs – Failed specimens

- 47% of failed specimens used an incorrect encoding of the metadata
- 53% of failed specimens had incorrect encoding in the header of DG2



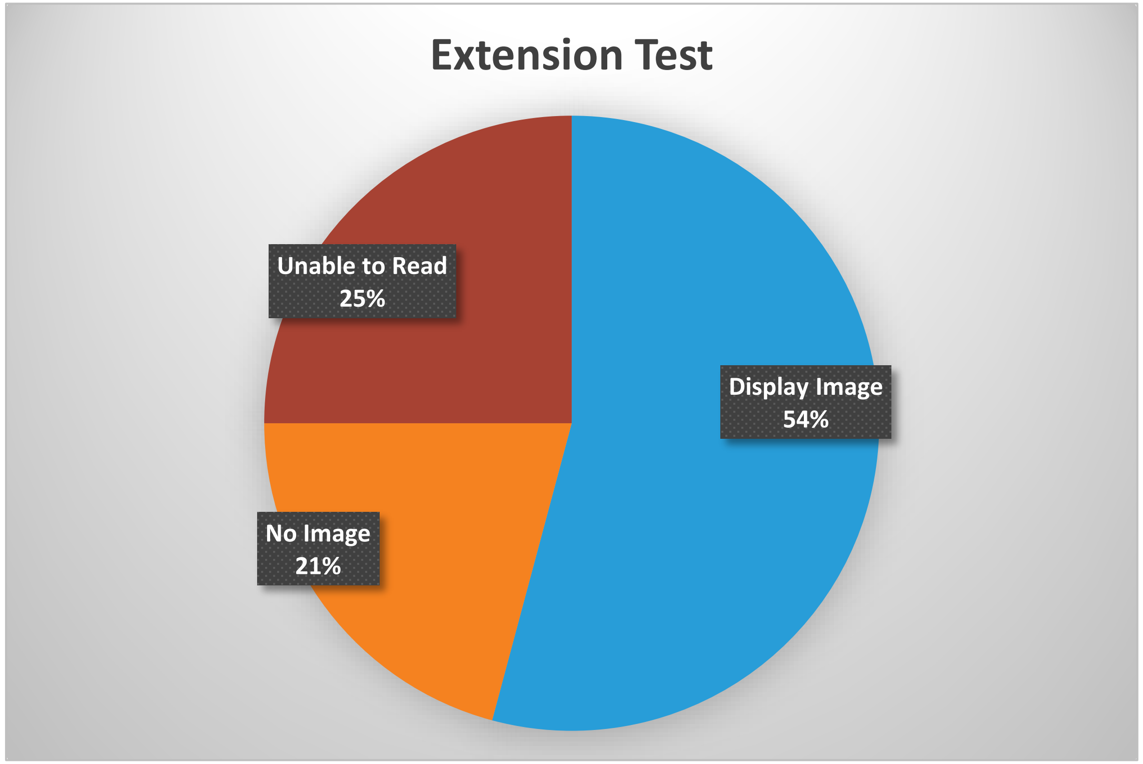
Inspection Systems – Positive Test

- Sample eMRTDS that are fully compliant to 39794-5 Application Profile
- Expectation is that Inspection system should be able to read DG2 and display the image



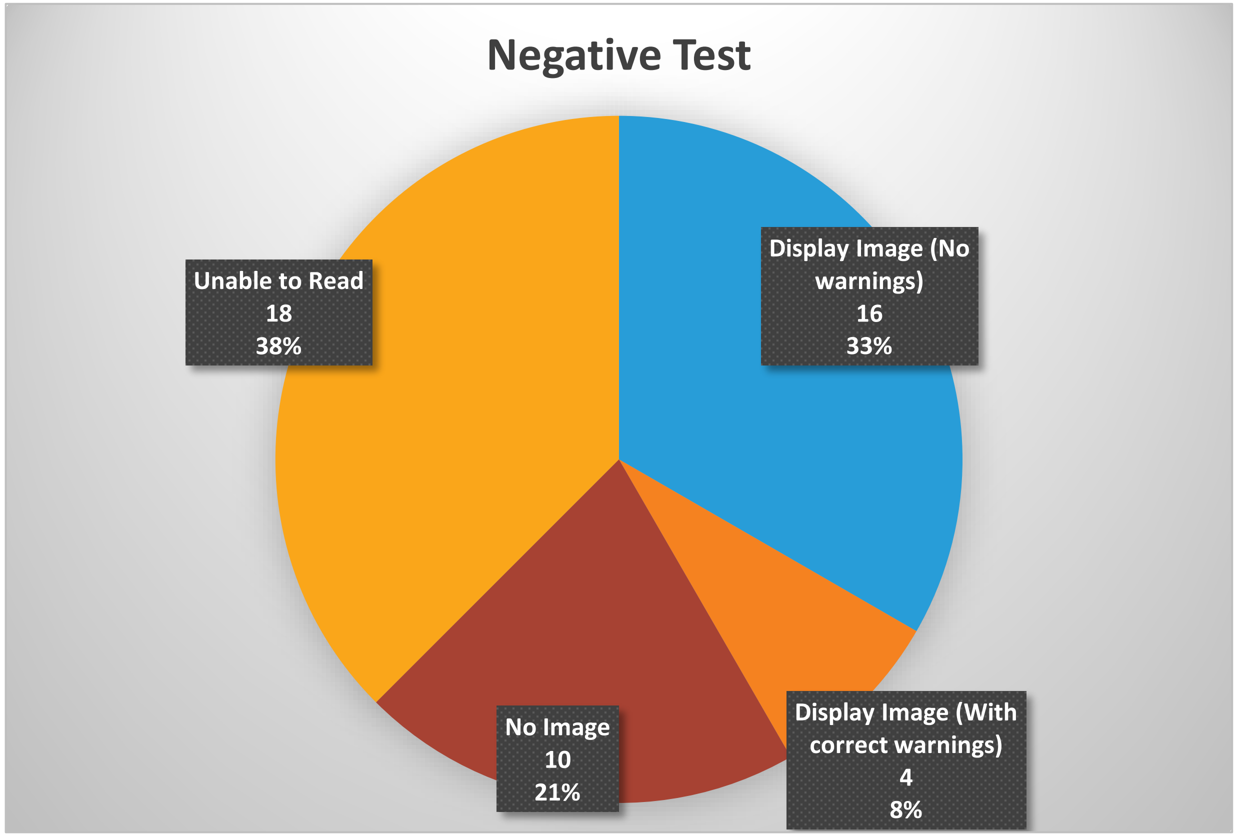
Inspection Systems – additional Extensions

- Extensions added to simulate future additions by SC37
- Expectation is that extensions are detected and image is displayed



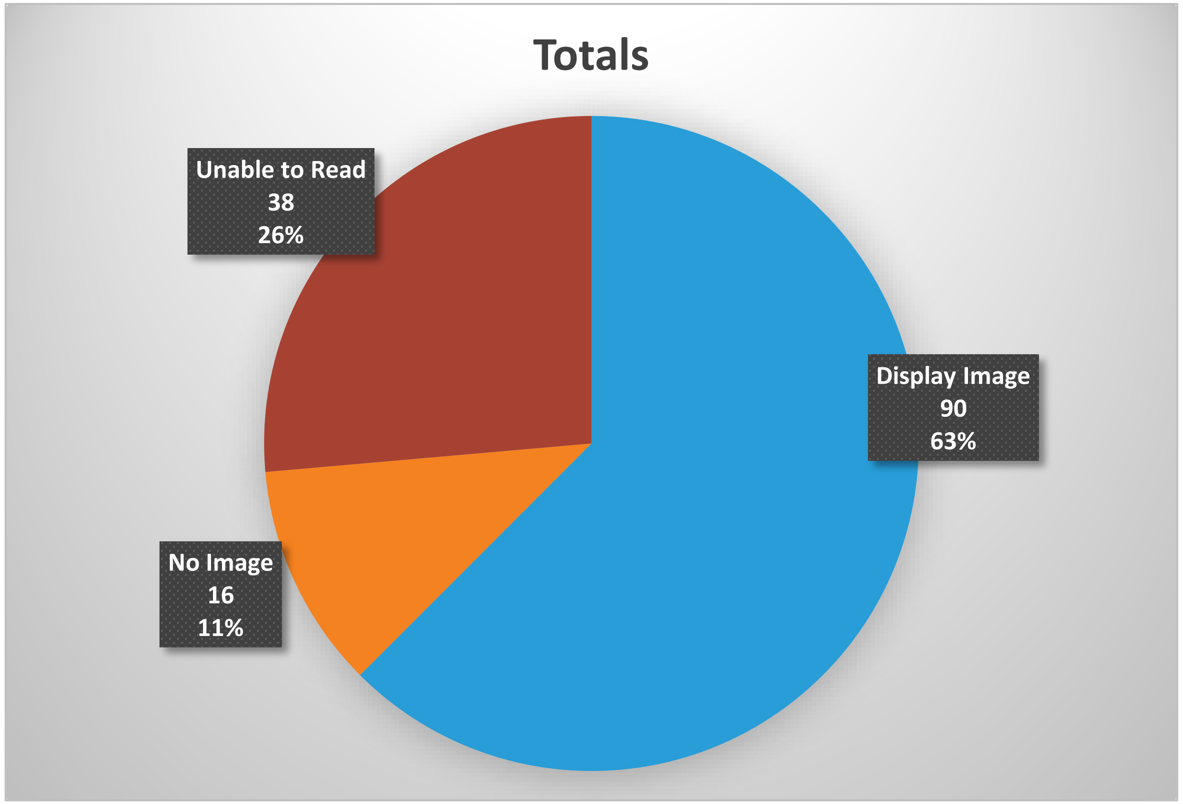
Inspection Systems – Negative Test

- Errors introduced in encoding to simulate real life scenarios
- Expectation is that errors are detected and reported, but image is displayed



Inspection System - Overall

- Some interesting results
  - Not consistent with different extensions – Can read DG2 with Hair color extension, but not with Eye color extension
  - One Inspection System displayed all images – but found errors with even correct data
  - Some Inspection Systems could not detect chip!!!!!



Results

- Only 25% of the eMRTD specimens tried to create DG2 from scratch and succeeded – raises a question on whether issuers are ready for the switch
- 79% of inspection systems managed to read correctly formatted DG2
- When extension is added (as will happen in future) 54% of inspection systems managed to display image from DG2
- With slight encoding errors (which can happen) only 41% managed to display the image

Appreciations

- Andy Hing – Auctorizium
  - Creating the silver datasets/negative test cases and the reference implementation of the Inspection system
- Ralph Lessmann – Hid Global
  - Helping verify the silver dataset
- Jeen de Swart – JustID, NL
  - Creating the eMRTD samples based on the silver datasets and negative test cases

- Stephane Jobard (iCube Test Centre) and Holger Funke (Secunet)
  - Lending their expertise in doing interop testing
- Kenichi Nakamura (Panasonic Japan)
  - Excellent co-ordination and conduct of the event
- Andreas Wolf (Bundesdruckerei)
  - Excellent support and co-ordination between SC17/WG3 and SC37

Next steps

- MORE TESTING IS REQUIRED !!!!!!
- Next interop event planned for February 14 in Singapore – watch out for the formal announcement
- Inspection system test procedures will be published for comments before the event – will be used for conducting the tests
- Will not be anonymous

Thank You

R.Rajeshkumar@auctorizium.com

RRaj88@gmail.com

ICAO
Headquarters
Montréal
European and
North Atlantic
(EUR/NAT) Office
Paris
Asia and Pacific
(APAC) Sub-office
Beijing
Middle East
(MID) Office
Cairo
Western and
Central African
(WACAF) Office
Dakar
North American
Central American
and Caribbean
(NACC) Office
Mexico City
Asia and Pacific
(APAC) Office
Bangkok
Eastern and
Southern African
(ESAF) Office
Nairobi
South American
(SAM) Office
Lima

ICAO