ICAO UNITING AVIATION

European Commission

Regional Seminar on MRTDs and Traveller Identification Management
Madrid, Spain, 25 to 27 June 2014

Results Interop-Test 2014

Arnaldo Cremisini, fedpol Switzerland
Holger Funke, HJP Consulting

Interoperability Test

- Crossover Test
- Conformity Test

Objectives of Interoperability Test

- Test of Documents (Samples)
- Test of Inspection Systems
- Test of Test Tools
- Test of Specifications

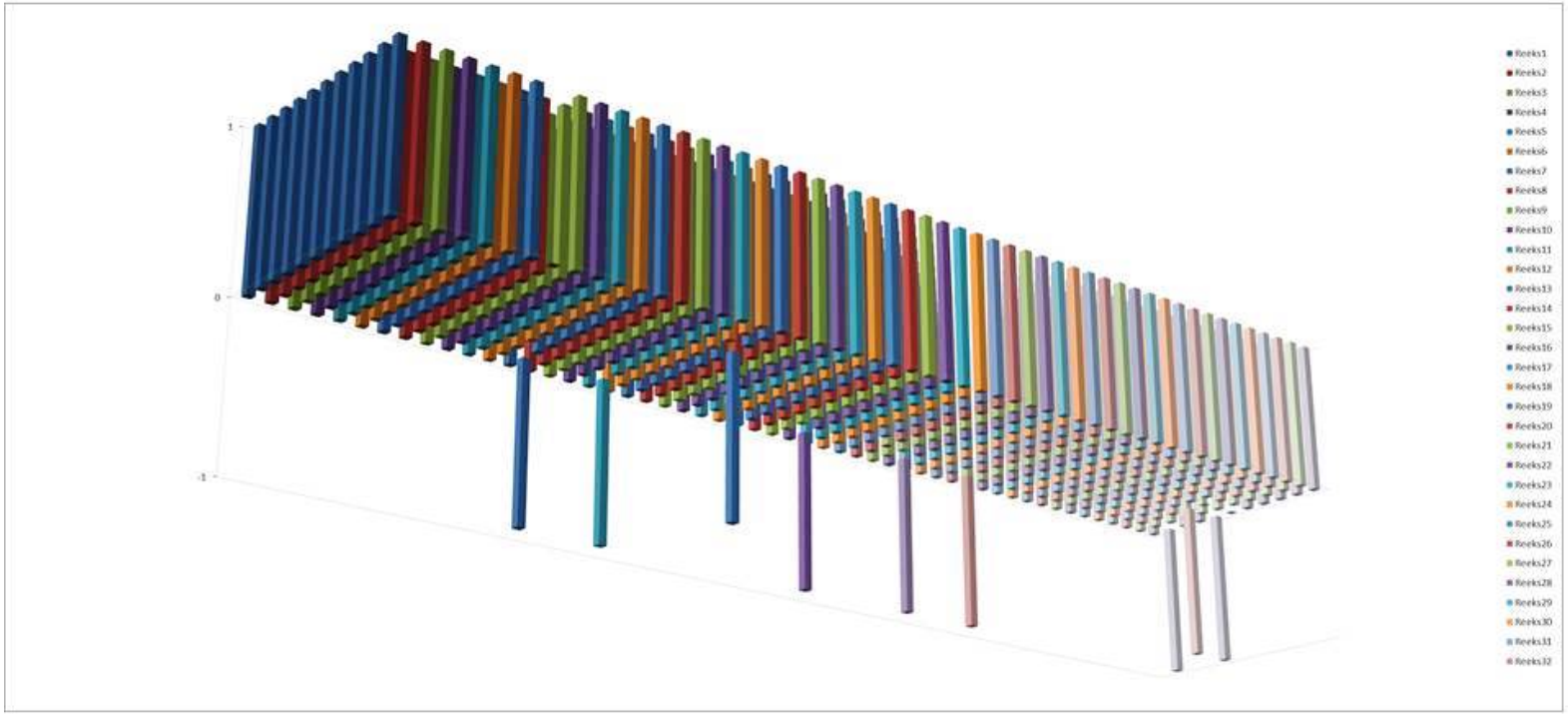
Participants

- 31 Document Providers
  - 18 Samples' Sets from Countries
  - 13 Samples' Sets from Industries
    - Total of 52 different document samples (One or two sets)
- 10 Inspection System Providers
  - 11 Inspection Systems stations
- 3 Test Labs for Conformity Testing

The Interop Test Room

SAC Cross Over test Overview results

BAC Cross Over test Overview results



Crossover Test

Samples

- Mismatches between EF.CardAccess and DG14 (i.e. declared algorithms)
- Some EF.CardAccess contained additional or unexpected information
- Open questions on use of extended length (specification and support by IS and samples)

General

- The quality of the used certificates varied widely (CSCA, DS and CVCA)

Crossover Test

Inspection Systems

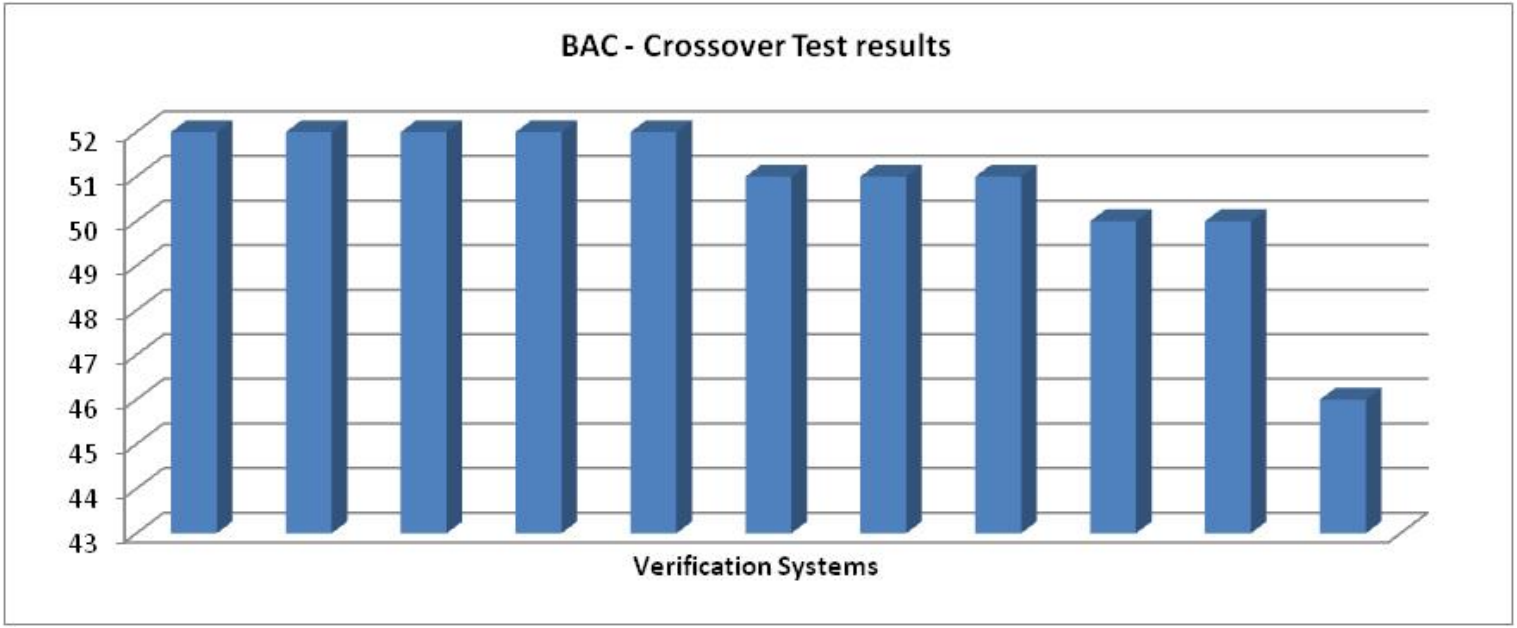
- Some were upgraded during tests (end result after the tests: improved the interoperability)
- Some were definitely not doing EAC and PA
- Some were able to read the samples even if samples were not fully compliant (IS were compensating for errors)

- Note that Integrated Mapping was NOT supported by all Inspection Systems
- Not all algorithms were supported

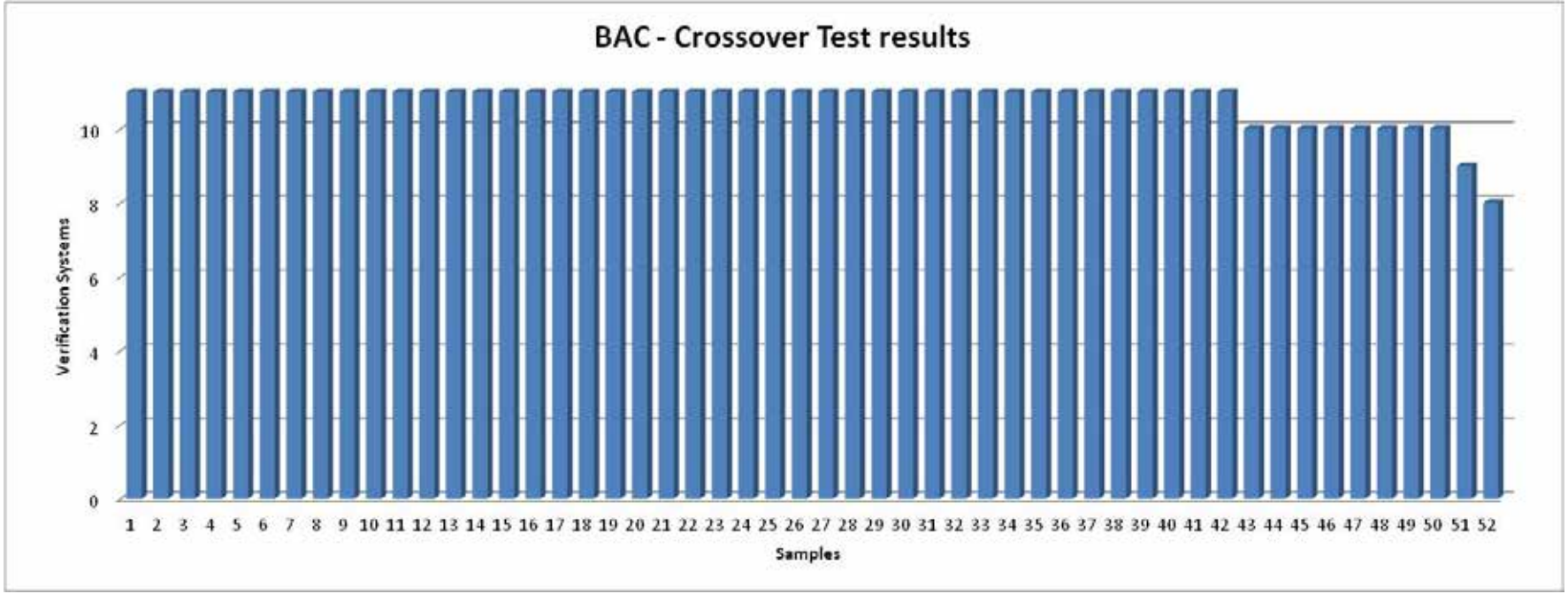
General

- Make sure that IS support all algorithms

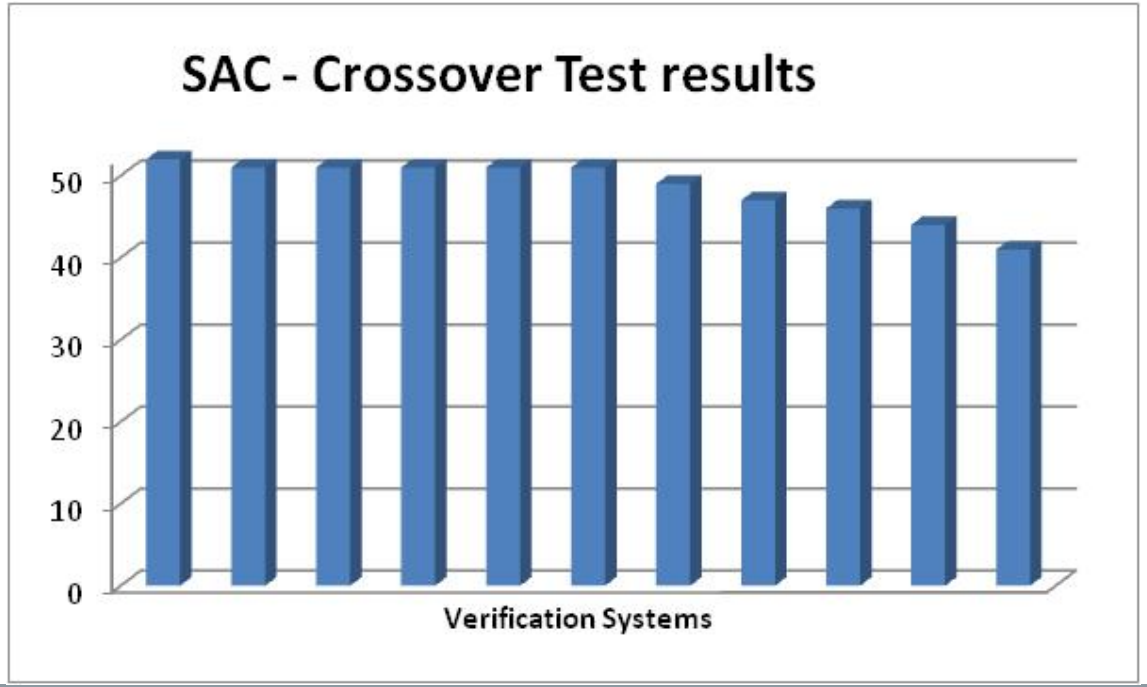
Crossover Test



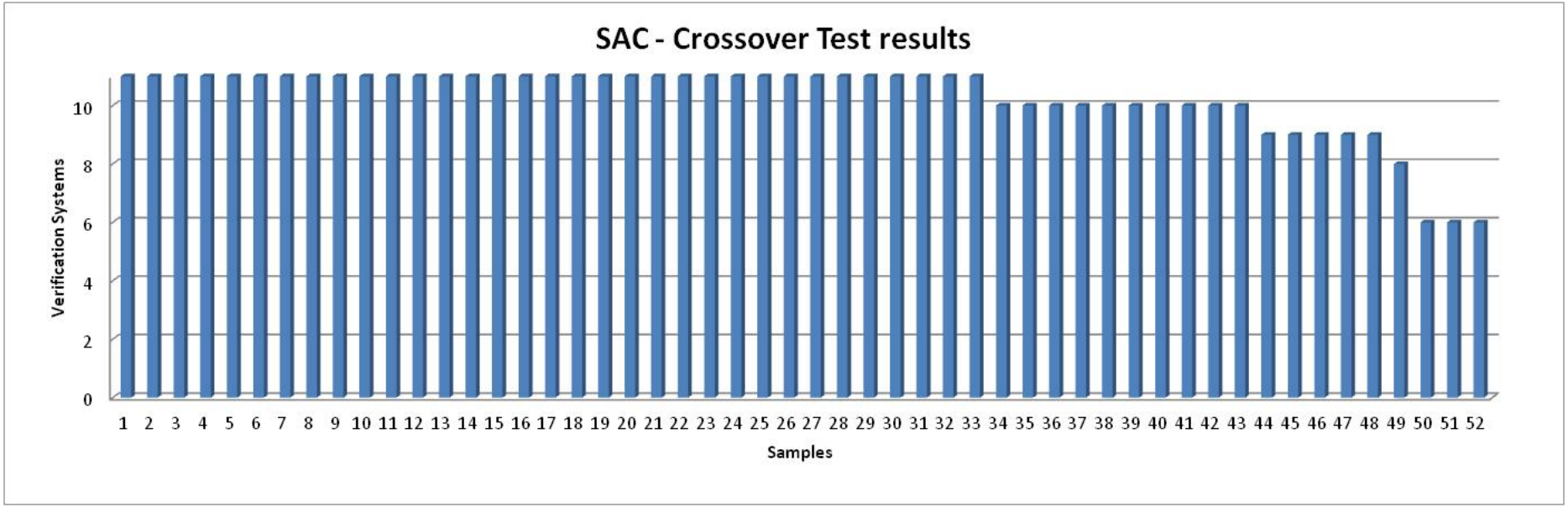
Crossover Test



Crossover Test



Crossover Test



Crossover Test

Notes

- Almost all IS tested both BAC and PACE but some did not plan to support BAC
- In comparison with the Interop in London many more IS were supporting Integrated Mapping
- The expectations of the Interop session was that IS vendors would provide systems representative of functional border control systems
- Not all samples were representative of Governmental issued eMRTD (some were more like development cards)

Crossover Test

Some more statistical information

BAC
- 80% of the samples have been successfully read by all IS with BAC
- but only 45% of the IS could read all samples with BAC

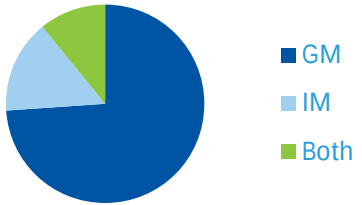
SAC
- 63% of the samples have been successfully read by all IS with SAC(PACE)
- but only 55% of the IS could successfully read 98% of samples with SAC(PACE)
- note that 1 IS could successfully read all samples with SAC(PACE)

Conformity Test

- 3 Test Labs with Conformity Test Tools
  - Keolabs (France): „ICAO Conformance Solution“
  - TÜViT + HJP Consulting (Germany): „GlobalTester“
  - UL (Netherlands): „Collis eMRTD Test Tool“
- Subset of „ICAO TR RF Protocol and Application Test Standard for e-Passports, Part 3“ Version 2.01:
  - Test suite ISO7816_O: Security conditions for PACE protected MRTDs
  - Test suite ISO7816_P: PACEv2
  - Test suite ISO7816_Q: SELECT and READ file EF.CardAccess
  - Test suite LDS_E: Matching between DG14 and EF.CardAccess
  - Test suite LDS_I: Structure of EF.CardAccess

Document Information (1/2)

- Generic Mapping vs. Integrated Mapping*
- SAC may use either IM or GM to map the nonce
  - Samples supporting GM: 34
  - Samples supporting IM: 7
  - Samples supporting GM and IM: 5

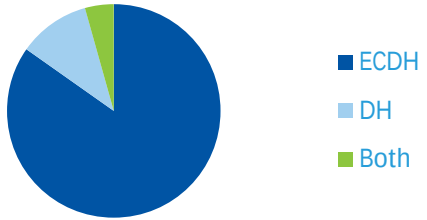


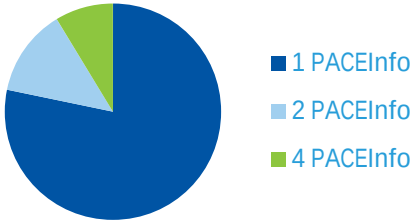
- Additional in 2014: Chip Authentication Mapping

*Based on 46 ICS

Document Information (2/2)

- PACE with
  - ECDH: 39
  - DH: 5
  - Both: 2
- Number of PACEInfos
  - One PACEInfo: 36
  - Two PACEInfos: 6
  - Four PACEInfos: 4

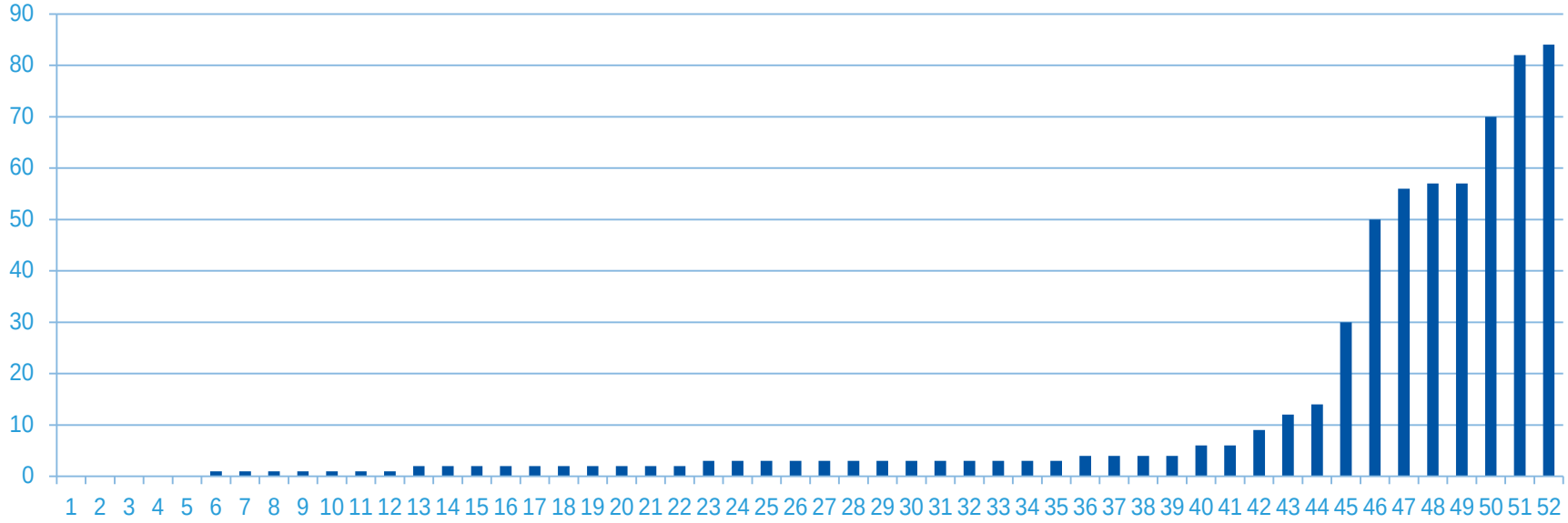




Overall Test Results (Conformity)

- Number of test cases performed: 21.282
- Results:
  - Passed: 9.203 (13.925)
  - Failed: 615 (713)
  - Not performed: 4.514 (6.644)

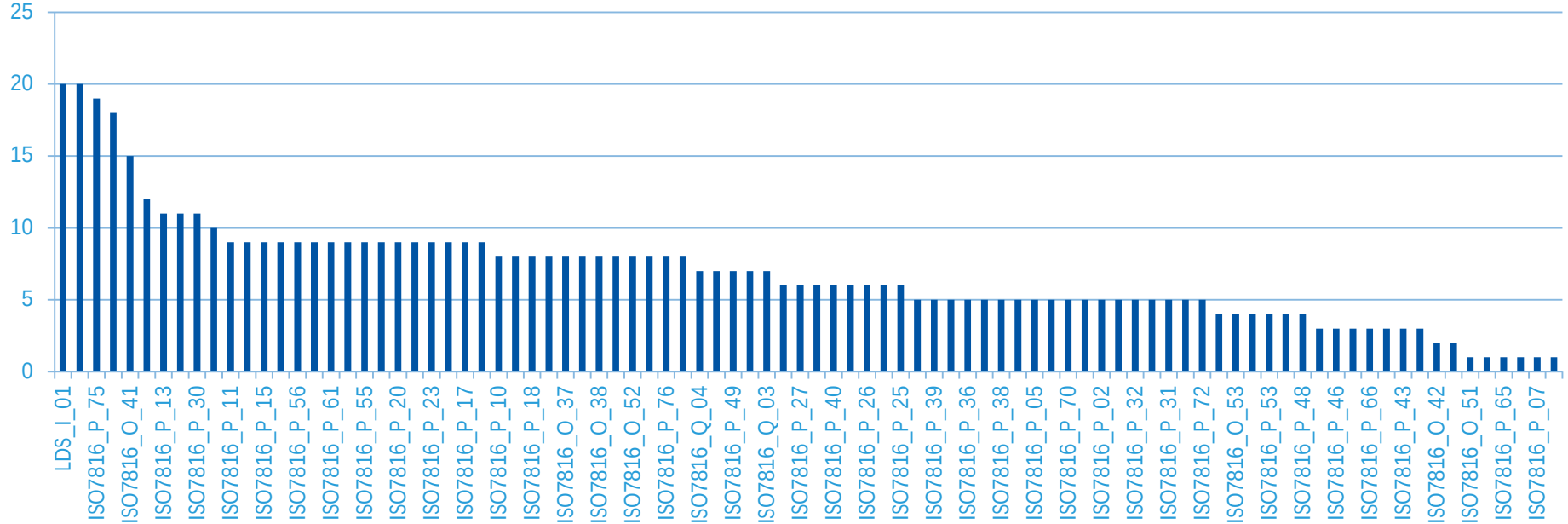
Failed Test Cases per Document



Test Cases with failures (Top 7)

Test Case	#Fail	Description
LDS_I_01	20	Test of ASN.1 encoding of security infos in EF.CardAccess
LDS_I_03	20	Test of ASN.1 encoding of PACEDomainParameterInfo
7816_P_75	19	Positive test without domain parameter reference (DO 84) and eMRTD supports only one set of domain parameters
LDS_I_02	18	Test of ASN.1 encoding of PACEInfo
7816_O_41	15	Accessing the EF.DG3 file with Read Binary. The test verifies the enforcement of SM after the PACE protocol has been performed successfully.
7816_P_64	12	MSE: Set AT command without data object 80
7816_P_13	11	General Authenticate to get the encrypted nonce command with an additional object data

Number of Failures per Test Case



Observations Conformity Testing

- Document quality varies from
  - Close to Release State vs. Experimental State
- Test results differ between test labs
  - Quality process to identify deltas
- Different interpretations of
  - Padding in EF.CardAccess and EF.DG14
  - Encoding of TerminalAuthenticationInfo in EF.DG14
  - Use of DO 84 in PACE
  - Use of ParameterID in PACE when proprietary or standardized domain parameters are used
- Certificates for EAC protocol were missing or not usable
- Use of Test Specification Version 2.01 (two test labs) and 2.06 (one test lab)

With special thanks to

Alan Bennett, DFAT
Cor de Jonge, justid
Jeen de Swart, justid
Mark Stafford, Infineon
Nicolas Meuwly, fedpol
Philipp Bättig, fedpol
Stefan Brandl, OeSD

Contact Details

Arnaldo Cremisini
arnaldo.cremisini@fedpol.admin.ch
Holger Funke
holger.funke@hjp-consulting.com