Test Report

For the participants of the SDW InterOp 2016

Final Report, 2016.07.05

secunet
secunet Security Networks AG

Copyright © 2016 by secunet Security Networks AG

Contents

List of Figures

List of Tables

Preface

The SDW InterOp 2016 was held alongside the SDW 2016 on 10-12 May in London, UK. It continued the series of international ePassport interoperability testing. The event was organized by Science Media Partners Ltd; the technical aspects have been supervised by secunet Security Networks AG.

The interoperability tests were focused on Supplemental Access Control (SAC), a set of security protocols to protect personal data stored in electronic ID documents such as ePassports and ID cards. Although SAC has been implemented for some years, interoperability and conformity challenges still exist – particularly as more SAC enabled eMRTDs enter circulation, and with the introduction of new security mechanisms such as “Password Authenticated Connection Establishment with Chip Authentication Mapping” (PACE-CAM).

PACE-CAM is specified in Technical Report BSI TR-03110 “Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS token”. PACE-CAM combines PACE and Chip Authentication (CA) into one protocol leading to faster ID document verification. Global interoperability is important to ensure that new security mechanisms can be reliably checked by document verification systems.

This document summarizes the results of this event. Vendor specific results are only disclosed to the corresponding vendor.

1 Participants

The SDW InterOp 2016 targeted both document manufacturers and document verification system providers.

1.1 Registered Document Provider

Registered document manufacturers, listed below, could provide a maximum of two sets of documents. Each set contained three identical samples. For the event 17 vendors with 27 document configurations have been registered. During the registration process a unique ID (#1 – 27) was assigned to each set of documents.

- Arjo Systems
- Atos IT Solutions and Services
- Bundesdruckerei
- Canadian Bank Note Company
- cryptovision
- De La Rue
- Gemalto
- ID&Trust
- Imprimerie Nationale Group
- Iris Corporation Berhad
- MaskTech
- Morpho
- Mühlbauer
- NXP Semiconductors
- Oberthur Technologies
- PAV Card
- PWPW

1.2 Registered Document Verification System Provider

Registered document verification system providers, listed below, were identified by a unique ID (#1 – 15).

- 3M Security Systems

- Access IS
- ARH
- Canadian Bank Note Company
- cryptovision
- Dermalog Identification Systems
- Desko
- Gemalto
- InnoValor
- Iris Corporation Berhad
- Morpho
- MorphoTrust USA
- Oberthur Technologies
- Regula Baltija
- Toshiba Corporation

1.3 Registered Conformity Test Laboratories

The conformity testing was conducted by two independent test laboratories listed below:

- HJP Consulting / TÜViT
- Keolabs

2 Operations of tests

2.1 Registration Tests

Subsequent to the document registration, secunet started the initial registration test. All registered documents were read in a standard document verification scenario. For this purpose, the secunet Golden Reader Tool Platinum Edition 3.10.0.4 was used. Before document readout, all provided certificates have been imported into the application. All vendors provided the CSCA certificate for Passive Authentication; most vendors provided EAC certificates and keys for Terminal Authentication.

The reading process was started in “Auto Detect” mode. With this mode, the software used the PACE protocol if available; otherwise the BAC mechanism was used. Afterwards the Extended Access Control protocols were performed, if applicable. All data was read from the document and then logged to the hard disk.

The logged data is only provided to the corresponding document provider. Chapter 3.2 contains the summary of these tests.

2.2 Conformity Tests

Since the SDW InterOp 2016 event focused on the Supplemental Access Control mechanism (esp. PACE-CAM), the Conformity Tests applied an appropriate subset of the ICAO test plan for SAC (http://www.icao.int/Security/mrtd/Pages/TechnicalReports.aspx), Version 2.08RC2.

Two independent test laboratories performed the following test units:

Test Unit	Test scope
ISO7816_O	Security Conditions for PACE-enabled eMRTDs
ISO7816_P	Password Authenticated Connection Establishment
ISO7816_Q	Select and Read EF.CardAccess
ISO7816_S	Select and Read EF.CardSecurity
LDS_E	Data Group 14
LDS_I	EF.CardAccess
LDS_K	EF.CardSecurity

Table 1: Scope of the Conformity Tests

The test results were reported in a standardized CSV file format. The specific results for the documents are only provided to the corresponding document provider. Chapter 3.3 contains the summary of these tests.

2.3 Cross Over Tests

The Cross Over test was performed by the 15 registered document verification systems. All 27 registered document samples were sorted in 15 folders. Each folder contained 1 or 2 document samples.

Each document verification system received one folder and conducted Cross Over tests with the received samples and their verification system. The findings of the Cross Over tests were noted on test protocol sheets. After each 20 minute time slot, the folders/samples were passed to the next desk. During the day, all samples have been tested by all verification systems.

The specific results reported by the verification system provider are only disclosed to the corresponding document provider. Chapter 3.4 contains a summary of these tests.

3 SDW InterOp 2016 Result Summary

3.1 General Statistics

Test participants	Quantity
Registered conformity test laboratories	2
Registered document verification systems	15
Registered document provider	17
Number of different document samples	27
Total number of document samples	81

Table 2: General statistics

3.2 Registration Test Results

During the registration tests, all **27** different sample configurations have been read. For **all** samples the PACE protocol has been performed successfully.

3.2.1 SAC/PACE Results

The ICAO standard for Supplemental Access Control (SAC) defines three different variants of the PACE protocol: Generic Mapping (GM), Integrated Mapping (IM), and the new Chip Authentication Mapping (CAM). The mapping function used by the samples was distributed as follows:

PACE Mapping functions	Samples
Generic Mapping (GM) only	8
Integrated Mapping (IM) only	0

Chip Authentication Mapping (CAM)	**19**
GM + CAM	18
IM + CAM	1
GM + IM + CAM	4

Table 3: PACE Mapping functions

The PACE algorithms that are supported by the document are defined with the EF.CardAccess. It is possible that more than one algorithm is supported; in this case the EF.CardAccess file contains more than one PACEInfo element. For PACE-CAM enabled passports it is mandatory to support at least two PACE algorithms.

From the 27 documents, 20 document configurations support at least 2 PACE algorithms, one document type supports 5 PACE OIDs, two documents types support 9 PACE OIDs and two other document types support 10 PACE OIDs.

The provided documents support 17 different PACE algorithms. DH was supported by only two document configurations (and even these are just optional). All document configurations support PACE-ECDH algorithm family. Triple-DES PACE algorithms are still supported by 7 document configurations. 26 document configurations support AES PACE algorithm, just one supports Triple-DES PACE only.

Many verification systems use the first PACEInfo element listed in the EF.CardAccess. The following algorithms were listed in the first position of the EF.CardAccess:

Algorithm	Samples
id-PACE-DH-GM-3DES-CBC-CBC	2
id-PACE-ECDH-CAM-AES-CBC-CMAC-128	3
id-PACE-ECDH-GM-3DES-CBC-CBC	3
id-PACE-ECDH-GM-AES-CBC-CMAC-128	10
id-PACE-ECDH-GM-AES-CBC-CMAC-192	2
id-PACE-ECDH-GM-AES-CBC-CMAC-256	7

Table 4: First PACE Algorithm in EF.CardAccess

The following Table 5 contains all algorithms included in the EF.CardAccess:

Algorithm	Samples
id-PACE-ECDH-GM-AES-CBC-CMAC-128	13
id-PACE-ECDH-CAM-AES-CBC-CMAC-128	12
id-PACE-ECDH-GM-AES-CBC-CMAC-256	11
id-PACE-ECDH-CAM-AES-CBC-CMAC-256	9
id-PACE-ECDH-GM-3DES-CBC-CBC	5
id-PACE-ECDH-CAM-AES-CBC-CMAC-192	4
id-PACE-ECDH-IM-3DES-CBC-CBC	4
id-PACE-ECDH-IM-AES-CBC-CMAC-256	4
id-PACE-ECDH-GM-AES-CBC-CMAC-192	3
id-PACE-ECDH-IM-AES-CBC-CMAC-128	3
id-PACE-DH-GM-3DES-CBC-CBC	3
id-PACE-DH-GM-AES-CBC-CMAC-128	3
id-PACE-DH-GM-AES-CBC-CMAC-192	2
id-PACE-DH-GM-AES-CBC-CMAC-256	2
id-PACE-DH-IM-AES-CBC-CMAC-256	2
id-PACE-ECDH-IM-AES-CBC-CMAC-192	2

Table 5: Complete list of all used PACE algorithms

3.2.2 Other Security Mechanisms and Personalization Features

Besides SAC, the following security mechanisms were supported by the registered samples.

Algorithm	Samples
Chip Authentication supported	25
Terminal Authentication supported	21
Active Authentication supported	14
CSCA certificate provided for Passive Authentication	27

Table 6: Other security mechanisms

With regard to the personalization of the chip data the following coding versions were supported:

- 25 LDS 1.7 encoded document configurations
- One LDS 1.8 encoded document configuration (with EF.COM still in place, LDS version also encoded in EF.SOD)
- One LDS 2.0 compliant document configuration with LDS 1.7 backward compatibility

Table 7 gives a summary on the files that are contained in the documents.

Elementary File	Samples
EF.ATR	12
EF.DIR	6
EF.COM	27
EF.SOD	27
Datagroup 1	27
Datagroup 2	27
Datagroup 3	19

Elementary File	Samples
Datagroup 4	2
Datagroup 5	0
Datagroup 6	0
Datagroup 7	4
Datagroup 8	0
Datagroup 9	0
Datagroup 10	0
Datagroup 11	7
Datagroup 12	7
Datagroup 13	0
Datagroup 14	27
Datagroup 15	14

Table 7: Elementary Files and Datagroups

3.3 Conformity Results

Results from **8502** individual test cases were collected by the conformity test laboratories. Depending on the sample configuration (for example supported algorithm), the number of applicable test cases is different between the samples. Therefore an effective number of **5725** test cases were performed, 2777 test cases were not applicable. **98%** of these tests were passed successful, while 2% failed. The tests provided fairly consistent results between the different labs.

The following diagram shows the number of passed (green) vs. failed (red) test cases for each sample:[1]

[1] A test case was rated as passed if at least one of the two labs rated this test case as passed. A test case is rated as failed if both of the labs rated this test case as failed.

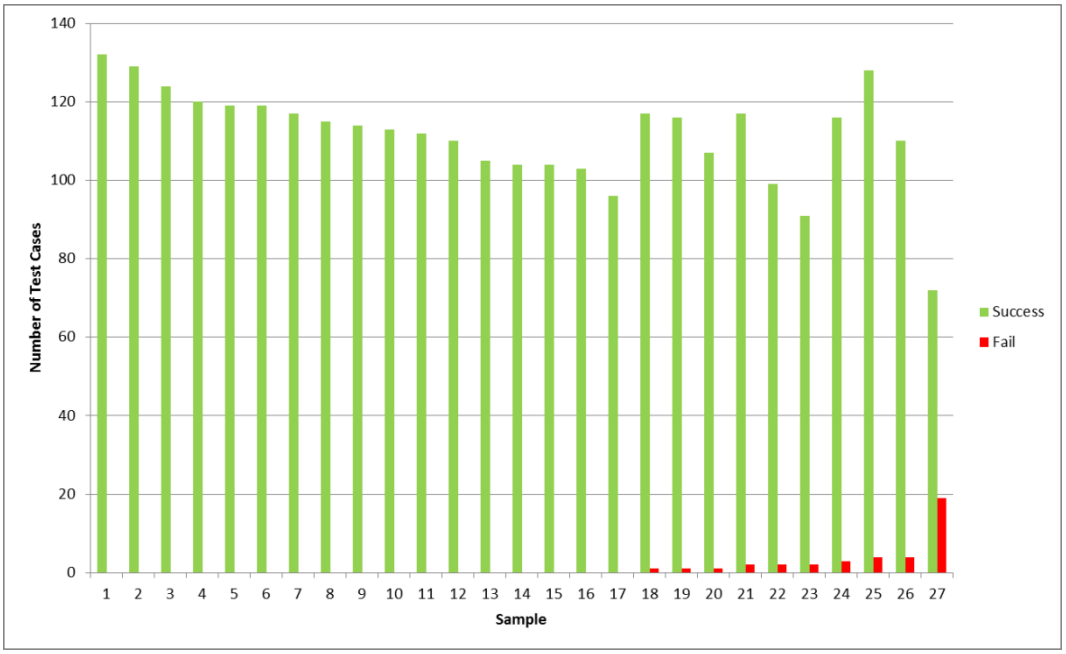

Figure 1: Conformity testing – Passed vs. Failed test cases

The test results in Figure 1 can be summarized as follows:

- 17 samples have 100% positive test results
- 26 samples have more than 95% positive test results
- Just 1 sample had 20% failed test cases

There was no test case failed for more than 3 samples for both laboratories. However, for one test case the results of both laboratories differ for 12 of the 27 samples: Test case LDS_K_2 (EF.CardSecurity: Verify the ASN.1 encoding of the chipAuthenticationPublicKey) allows for different interpretations by document vendors and test labs, and thus clarification is needed.

One important outcome of the SDW InterOp 2016 is the appropriate change of this test case specification in the final version of ICAO test plan 2.08.

3.4 Cross Over Results

The **15** document verification system providers returned a total number of **402** protocol sheets. The verification system providers claimed for their systems the following capabilities:

- 15 claimed to support SAC
- 15 claimed to support PACE-Generic Mapping

- 12 claimed to support PACE-Integrated Mapping
- 12 claimed to support PACE-CAM
- 14 claimed to support EAC

The results of the cross over test can be summarized as follows:

- 4 verification systems were able to perform SAC successfully for all 27 samples
- 4 verification systems were able to perform SAC successfully for nearly 2/3 of the samples (for 17 out of 27 documents)
- 1 verification system was able to perform PACE-CAM successfully for all 19 documents supporting PACE-CAM
- 3 verification systems were not able to perform PACE-CAM

In detail, Figure 2 shows the number of samples for each verification system that could be read successfully.

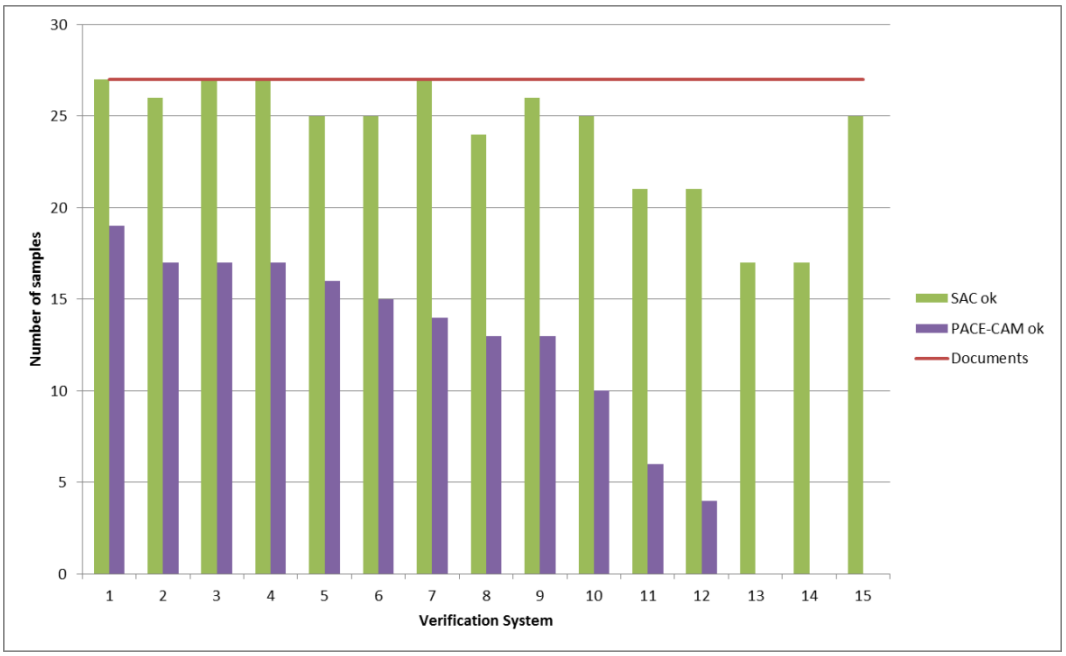

Figure 2: Number of samples read successfully per verification system

The following Figure 3 shows the successful operations of PACE for each sample.

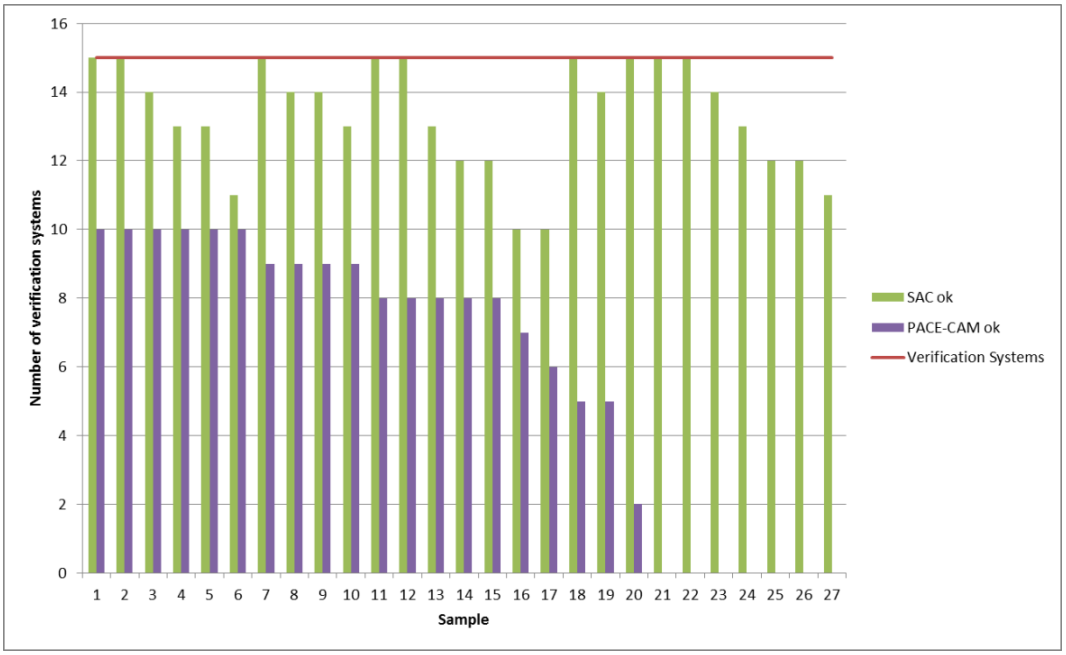

Figure 3: Successful reads of PACE per passport

The evaluation of the Cross Over results indicates that on some samples PACE + CA + Terminal Authentication works, while PACE-CAM + Terminal Authentication fails. A possible explanation: PACE is specified within ICAO documents while TA is specified within BSI TR documents. Therefore the combination of these two protocols requires special handling as specified in BSI-TR03110:

TR-03110-1, Version 2.20:

"If Chip Authentication has not been performed before Terminal Authentication (**because PACE with Chip Authentication Mapping was performed**), C is set to Comp(~PK$_{PCD}$PACE), i.e. the compressed representation of the terminal's ephemeral public key of PACE."

Figure 4: Explanation of TA in combination with PACE-CAM in BSI TR-03110

Conformity Tests as well as Cross Over Tests showed problems with access/read of EF.CardSecurity during PACE-CAM. This could be a problem of documents or verification systems (or both).

A third observation was relating to EF.CVCA. 5 document samples defined an alternative File-ID for EF.CVCA in the Terminal Authentication Info. Even this is fully compliant to the specification, it seems to be a potential interoperability issue for verification systems.

4 Conclusion

4.1 Documents

The quality of the provided passport samples was very good. Compared to SDW InterOp 2013 PACE is well understood by document providers and no longer poses a problem for them.

For PACE-CAM there is still a need for some clarification work. For the conformity test plan, the conclusions of the test laboratories will be applied to the final release of the test case specification. For the implementation of PACE-CAM in combination with Terminal Authentication the special handling of the terminal's ephemeral public key may need more attention.

4.2 Verification Systems

The document verification system providers have still some work to do. It was obvious during the tests that access to a wide variety of document samples is vital for them to achieve good interoperability. They have to be prepared for the point in time when the first PACE documents without BAC fall-back will appear in the real world.

Due to a mistake while preparing the Cross Over tests a wrong country signer certificate had been assigned to one of the document samples. Nevertheless almost **50%** of the verification systems claimed to successfully perform Passive Authentication for that specific sample. This is also a major problem that has been spotted in actual border control processes. Just to make that clear again: Passive Authentication is the most important security mechanism to detect forged electronic travel documents. Please ensure to signal any failure in verification of the Passive Authentication protocol unambiguously (missing CSCA certificate, invalid CSCA certificate, invalid signature verification etc. pp.)!

4.3 Statement regarding performance tests

The organisers of SDW InterOp 2016 would like to, in the strongest terms, clarify that any vendor claims concerning the reading speed of ePassports are not in any way a result of the official interoperability tests. Measurement of any reading times was **not** performed, in either the crossover or conformity parts of the event.

This kind of test was dropped after the Berlin InterOp event in 2006 for several good reasons. A performance metric requires a strictly defined sample configuration, since many parameter like data size (facial image) and the chosen algorithms have a great impact on the results. Furthermore the SDW 2016 InterOp focused on the

new PACE-CAM mechanism. The organisers were positively surprised that many samples already supported PACE-CAM. However, it is common practice to implement new mechanisms as patches to the original chip application during the pre-production phase. Such implementations are great for testing purposes like this event, but slower than the final version used for later production. Therefore the speed of the InterOp samples cannot be used to judge the final performance and so no performance data has been collected during the SDW event.

4.4 Feedback

We are happy to receive your feedback regarding the SDW Interop 2016. Please contact us at

interop@secunet.com