



secunet Security Networks AG

Detailed report of e-passport conformity testing:
Layer 6-7

Michael Schlueter

01.06.2006

www.secunet.com

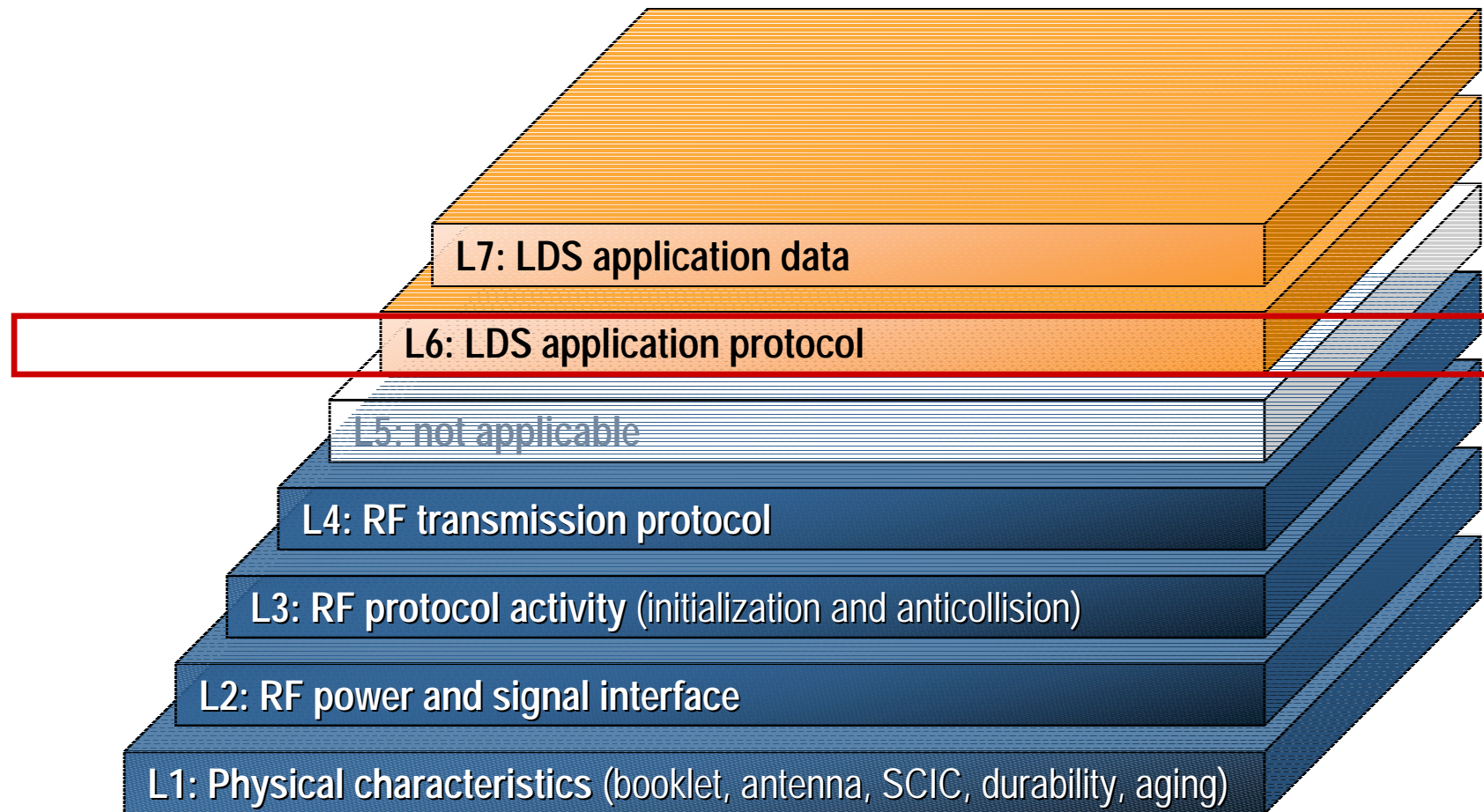
- **Conformity Specification Layer 6**
 - **Scope and Structure**
 - **Interop Conformity Test Summary**

- **Conformity Specification Layer 7**
 - **Scope and Structure**
 - **Interop Conformity Test Summary**

- **Future Prospects**



- RF Protocol and Application Test Standard for e-Passport Part 3



- Test specification based on international standards
 - ISO 7816-4 : 2005 Organization, security and commands for interchange
 - ICAO Doc 9303 MRTD Part 1 – Machine Readable Passports

- Command set required by the LDS specification (Annex A.12)
 - Select File
 - Read Binary

- Additional commands required by the PKI report (for BAC only)
 - Get Challenge
 - External Authenticate



- Document structure consists of five test units
 - A – Selection of the ICAO LDS Application
 - B – File Access Control for ePassport with BAC protection
 - C – BAC specific commands (Get Challenge, Mutual Authenticate)
 - D – Implementation of the Select File command
 - E – Implementation of the Read Binary command

Specification of status words should be avoided if interoperability is not affected

Supplement to 9303 Part 1 6th Edition



ISO 7816 Status Byte Categories

Normal processing	90 00	Process completed
Warning processing	62 00 – 63 FF	
Execution error	64 00 – 66 FF	Process aborted
Checking error	67 00 – 6F FF	

Two exceptions to the rule

A MRTD chip that supports Basic Access Control MUST respond to unauthenticated read attempts (including *selection* of (protected) files in the LDS) with ‘Security status not satisfied’ (**0x6982**).

TR PKI 3.2.2 Inspection process flow

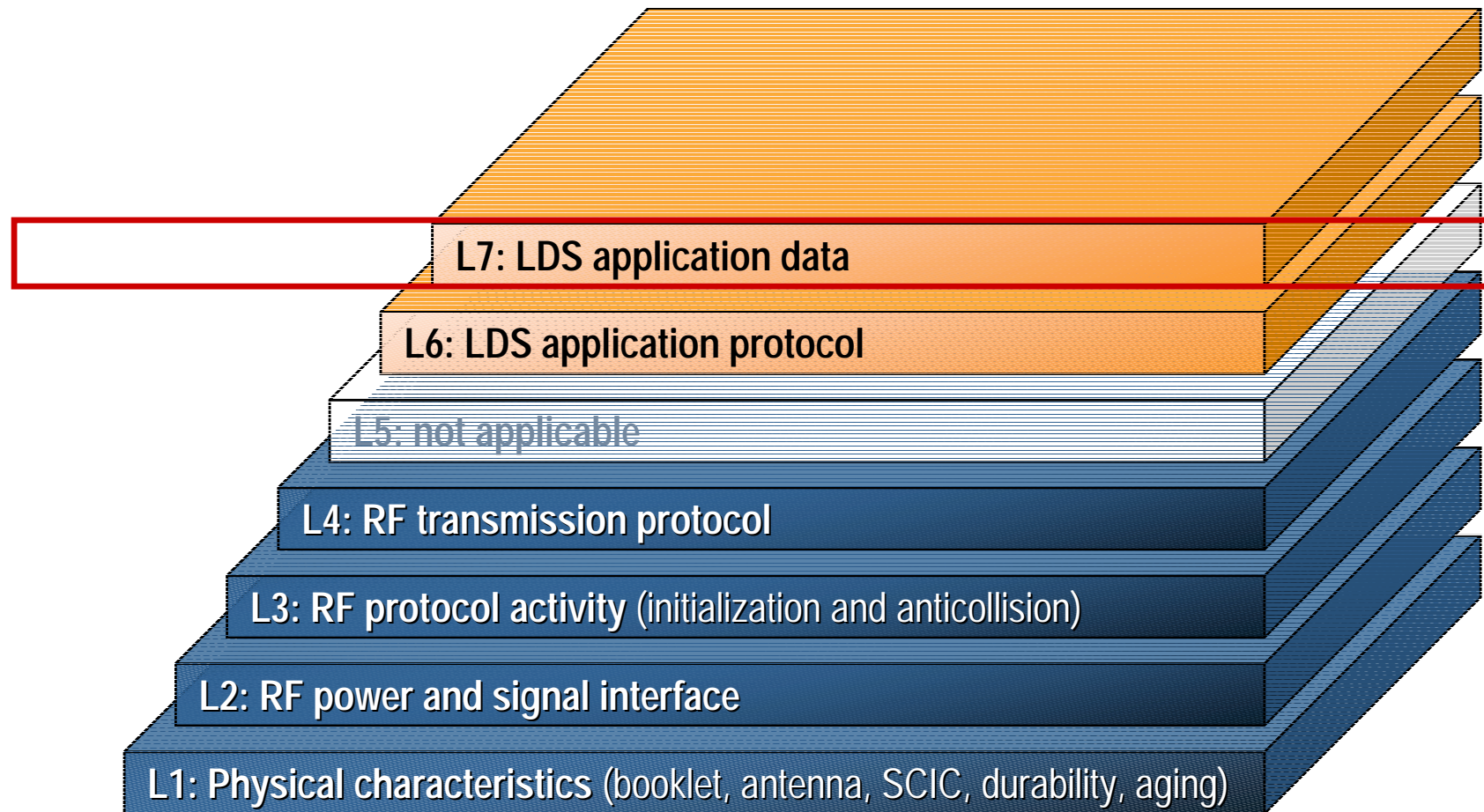
The session is only aborted on a SM error. At incorrect P1 or P2, which is not a SM error, the session is not aborted and the return must be in with SM

Recent WG3 TF4 Q & A

Test Case	Pass	Fail
ISO7816_B_4	68,52%	31,48%
ISO7816_C_23	96,30%	3,70%
ISO7816_D_3	96,36%	3,64%
ISO7816_E_5	98,18%	1,82%

- ISO7816_B_4
 - Verify the file protection for BAC protected e-Passports

- RF Protocol and Application Test Standard for e-Passport Part 3



- Test specification based on international standards
 - ICAO Doc 9303 MRTD Part 1 – Machine Readable Passports

- ICAO defines four mandatory elements
 - EF.COM – Common Data Elements
 - EF.SOD – LDS Security Data
 - Data Group 1 – Machine Readable Zone Information
 - Data Group 2 – Encoded Face Image

- Data Group 2
 - CBEFF coding according to ISO 7816-11
 - Biometric data coding according to ISO 19794-5

- EF.SOD
 - ASN.1 coding of the LDS Security Object
 - Certificate profile as defines in the PKI report
 - Calculation of the signature

Test Case	Pass	Fail
LDS_A_3	85,45%	14,55%
LDS_C_7	100,00%	0,00%
LDS_C_8	85,45%	14,55%
LDS_D_7	69,09%	30,91%

- LDS_D_7
 - Key usage extension SHOULD be digitalSignature only
 - DS certificate validity period should cover the passports validity.

- All members of ISO and ICAO / NTWG are invited to contribute to the test standards
- Results from this test event will be used for improvements
- Finalization of the test standard parts 2 and 3 is planned for WG3
TF4 meeting in Graz 12th to 13th of June 2006

- Extend specification to cover
 - Read Binary with odd instruction byte
 - ISO 7816 commands required by EAC
 - Additional security mechanisms like
 - Active Authentication
 - Extended Access Control
 - Additional data groups
 - Data Group 3 (Fingerprint)
 - Data Group 11, 12
 - Data Group 14, 15 (AA, EAC)



For any further information you can contact me

Michael Schlüter
secunet Security Networks AG
Kronprinzenstrasse 30
45128 Essen
Germany

Michael.Schlueter@secunet.com