achelos
the experts in eID

TLS and IKE high performance security testing with Qumate

German Innovative Security Solutions 2018

Dr. Benjamin Eikel

© 2018 achelos

achelos – Segments and technologies

eIdentity

access control and security, administrative procedures with eID (nPA), NFC

eHealth

eGK, HBA, SMC, Connector, infrastructure security

ePayment

ePOS, eCash, EFT, home banking, NFC

Telecoms

Roaming, billing, apps/wallet, M2M, NFC

Mobility

Toll collection, Tachograph, eMobility, Car-to-Car com., NFC, eTicketing, public transport, M2M

eEnergy

Smart meter, smart meter gateways, service providers, roaming, PKI, M2M

achelos is an expert in eID-based authenticity and security:

- Technical attacks via data network
- Violation of privacy (data protection, profiling)
- Data corruption/service disruption
- Identity theft (person or thing)

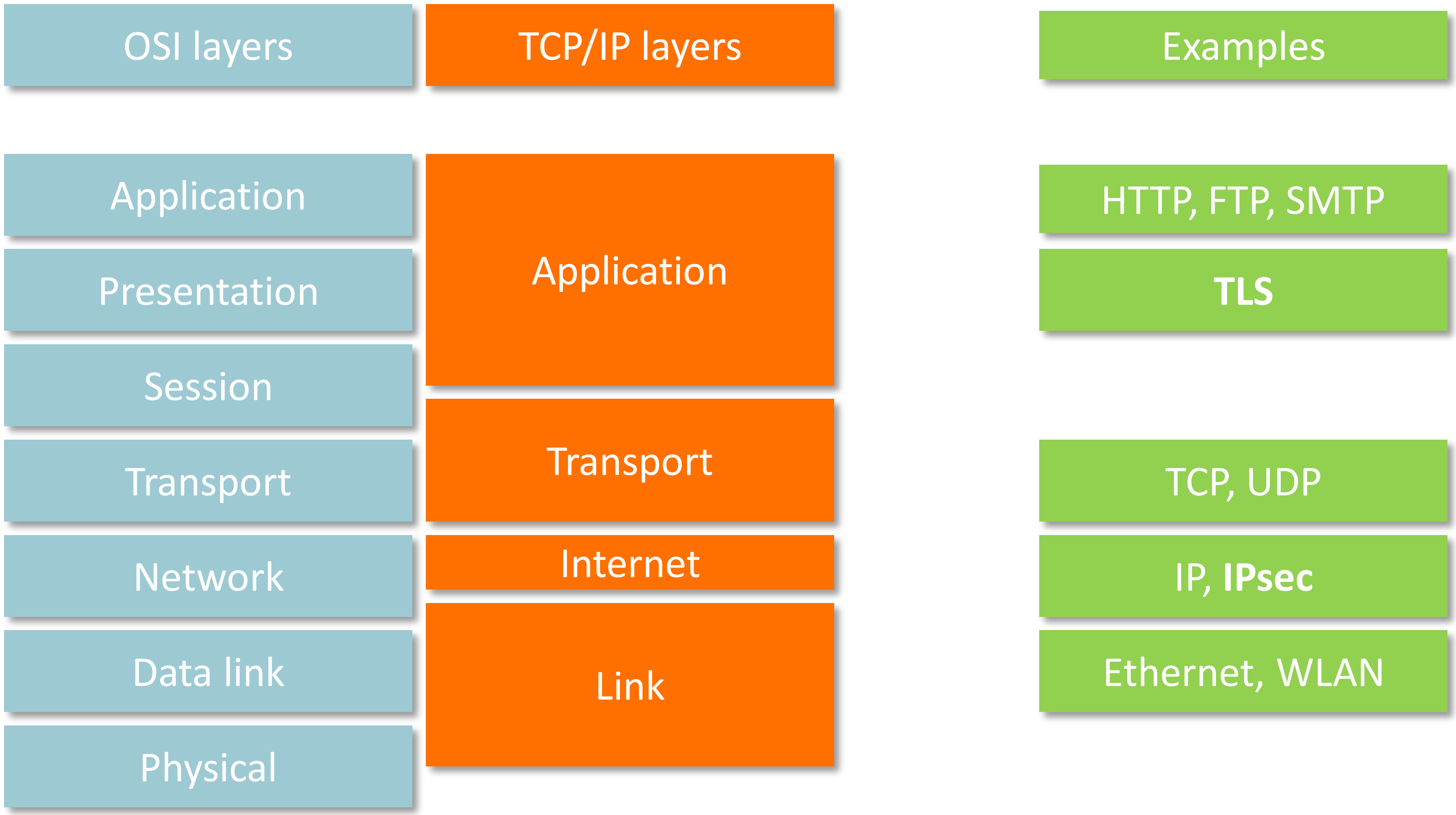
Potential threats

- **Systems communicate over public networks**
  - Internet, wireless networks
  - Data can be intercepted and manipulated
- **Protecting the data integrity**
  - Sensor data, control signals
- **Preventing data leakage to third parties**
  - Trade secrets, personal information
- **Identifying the communication peers**
  - Contracts
- **Often all of these measures are required**
  - Online banking

Protocols – TLS and IKE/IPsec

- **Transport Layer Security (TLS)**
  - Version 1.2 defined in RFC 5246
  - Successor of the Secure Sockets Layer (SSL)
  - Widely used on the Internet (e.g., web sites, e-mail)
- **Internet Key Exchange (IKE)**
  - Version 2 (IKEv2) defined in RFC 7296
  - Performs authentication and key exchange
- **Internet Protocol Security (IPsec) is a protocol family**
  - Encapsulating Security Payload (ESP) defined in RFC 4303
  - ESP secures IP packets
  - For example used by VPN gateways
- **Protocols guarantee authenticity, integrity, and confidentiality**

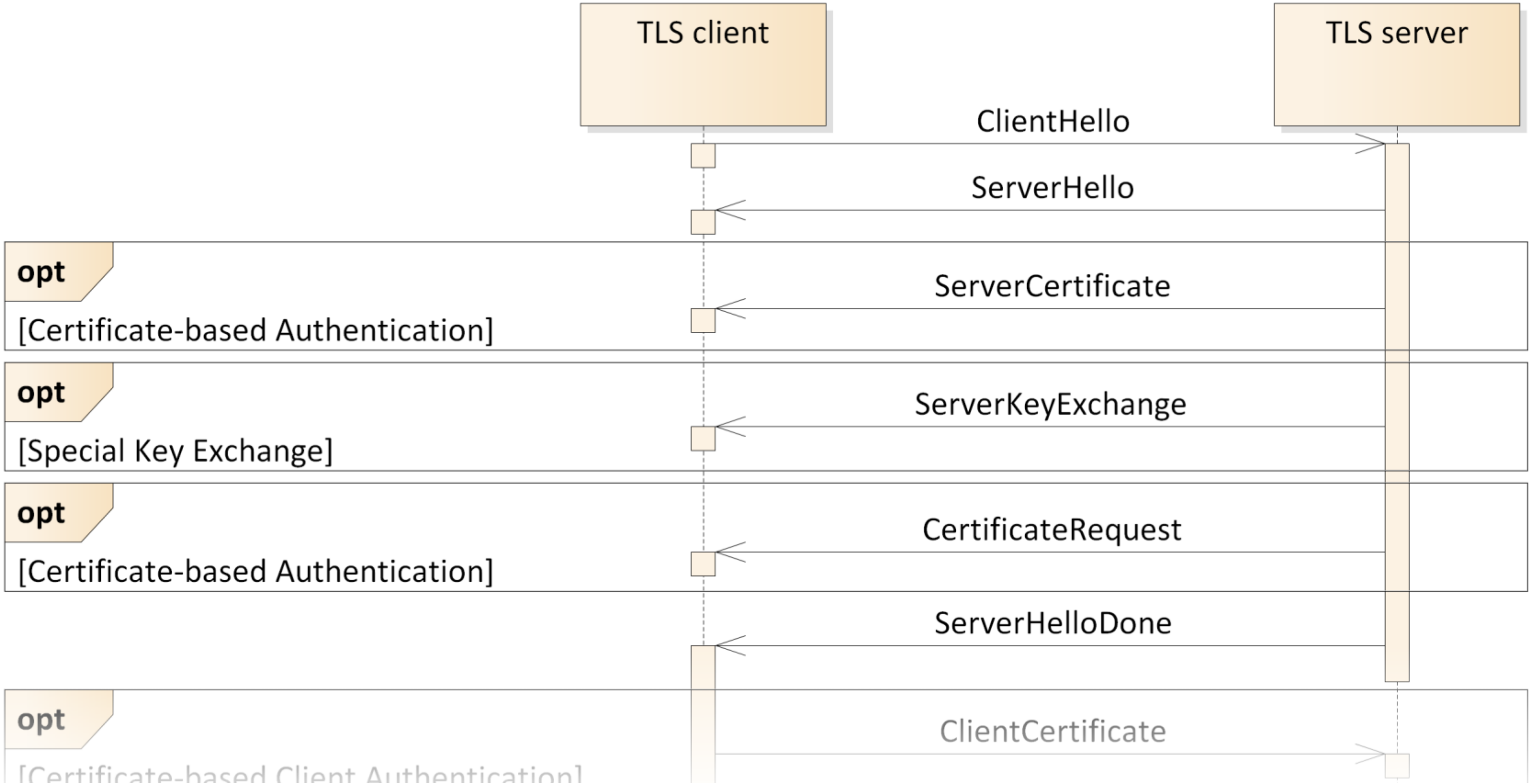
Protocols – Layer models and TLS, IKE/IPsec



OSI layers	TCP/IP layers	Examples
Application	Application	HTTP, FTP, SMTP
Presentation		**TLS**
Session		
Transport	Transport	TCP, UDP
Network	Internet	IP, **IPsec**
Data link	Link	Ethernet, WLAN
Physical		

© 2018 achelos

Protocols – TLS handshake 1



TLS client

TLS server

ClientHello

ServerHello

opt

[Certificate-based Authentication]

ServerCertificate

opt

[Special Key Exchange]

ServerKeyExchange

opt

[Certificate-based Authentication]

CertificateRequest

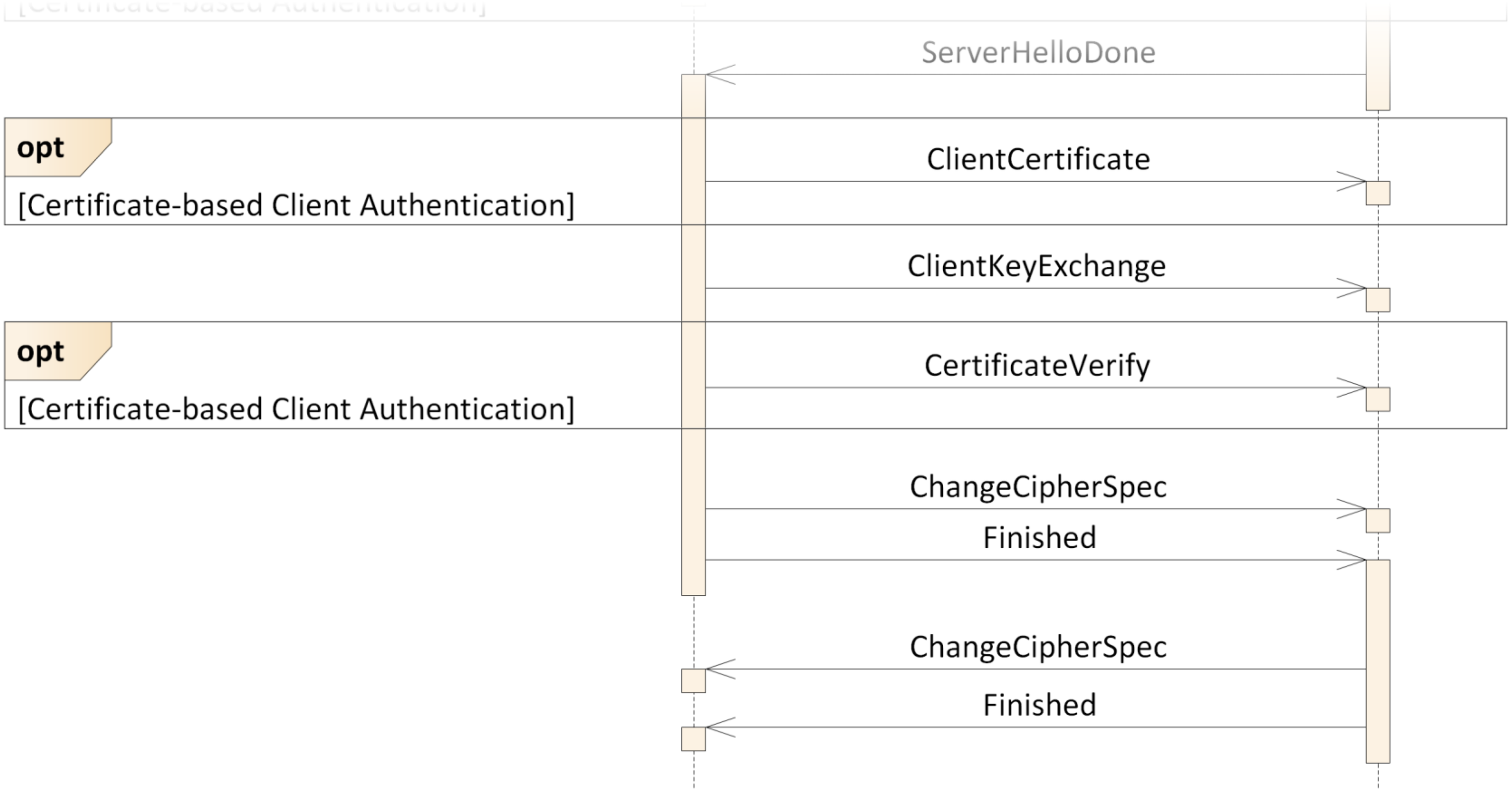
ServerHelloDone

opt

[Certificate-based Client Authentication]

ClientCertificate

Protocols – TLS handshake 2



[Certificate-based Authentication]

ServerHelloDone

opt

[Certificate-based Client Authentication]

ClientCertificate

ClientKeyExchange

opt

[Certificate-based Client Authentication]

CertificateVerify

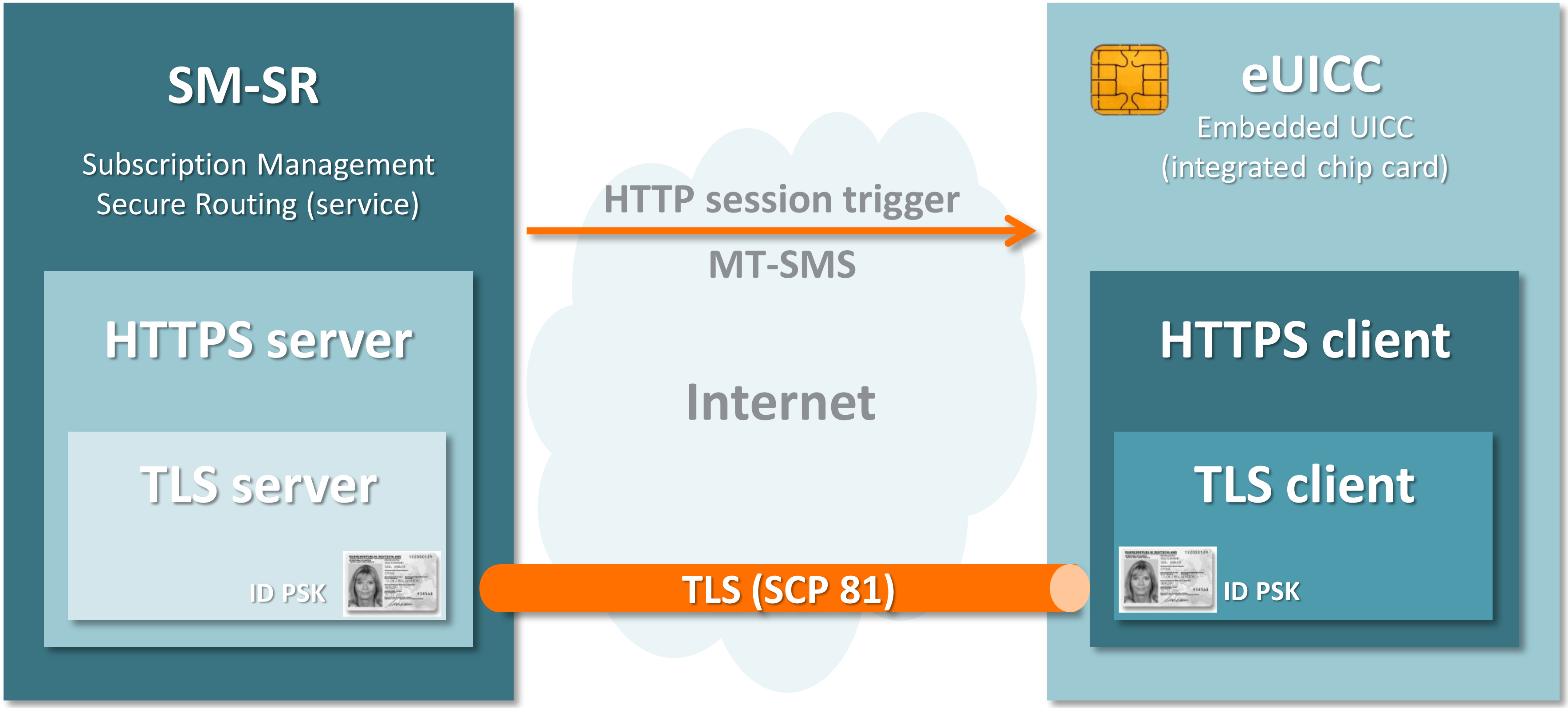
ChangeCipherSpec

Finished

ChangeCipherSpec

Finished

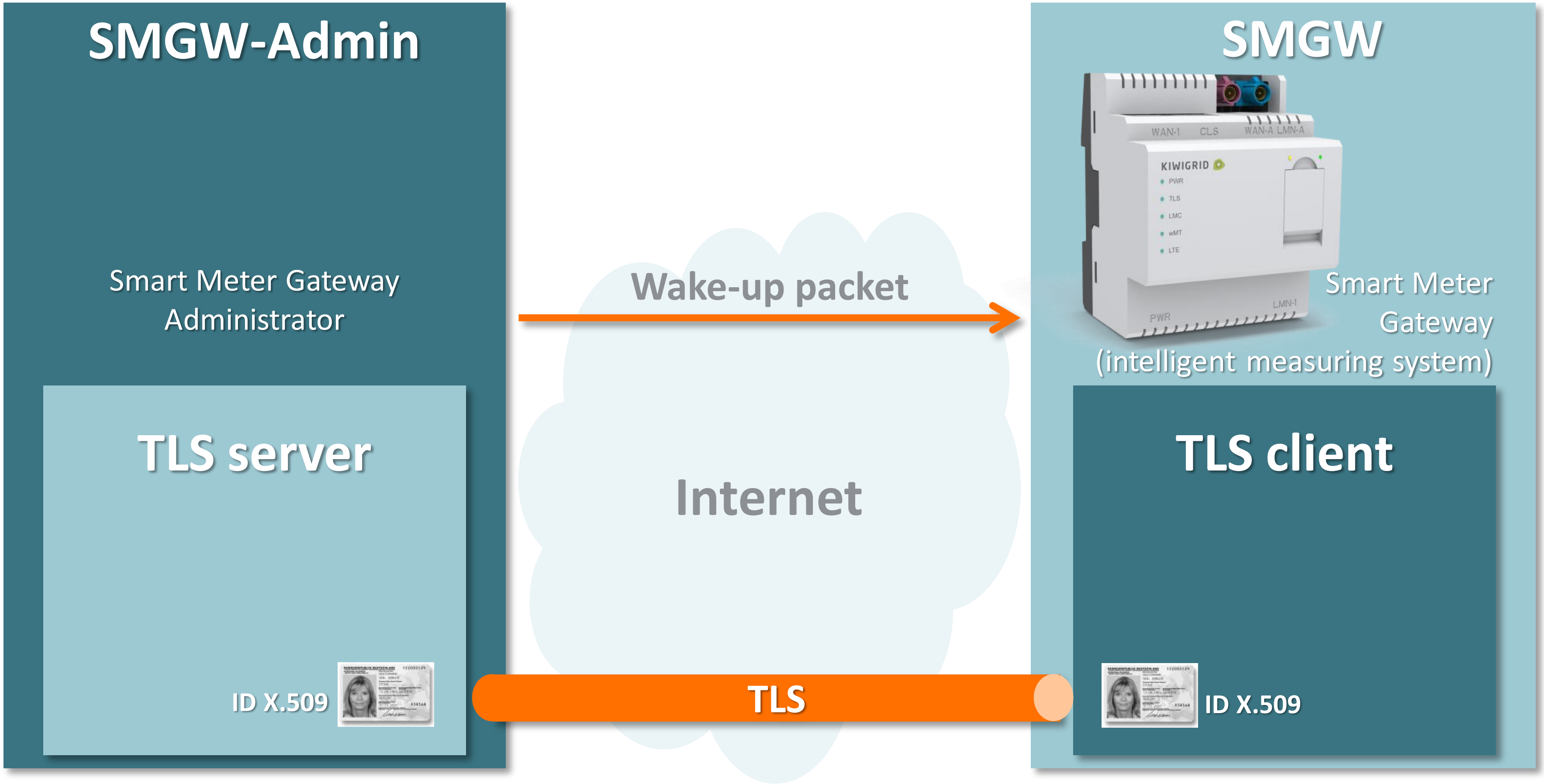
Applications – Telecommunications



© 2018 achelos

achelos
the experts in eID

Applications – Energy sector



SMGW-Admin

Smart Meter Gateway Administrator

TLS server

ID X.509

Wake-up packet

Internet

TLS

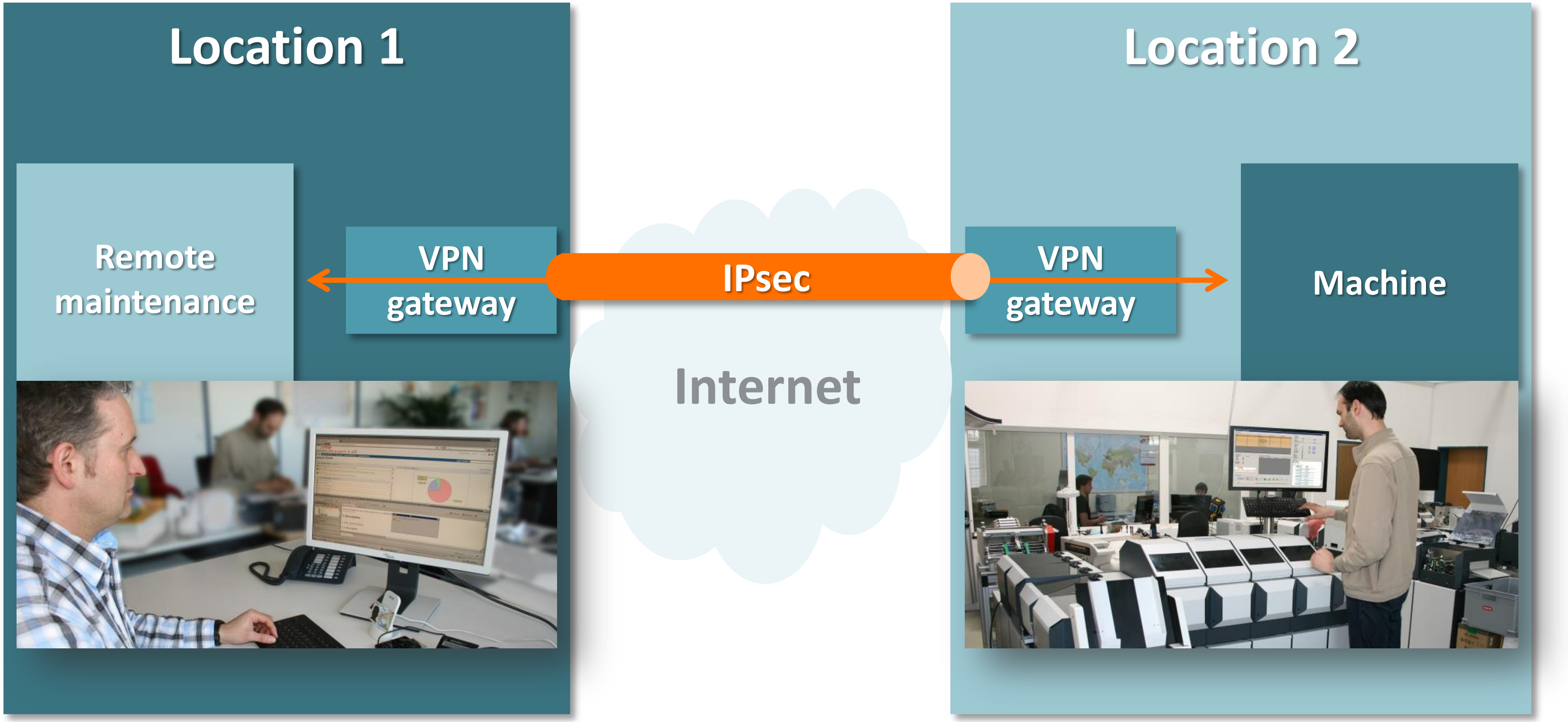
SMGW

Smart Meter Gateway (intelligent measuring system)

TLS client

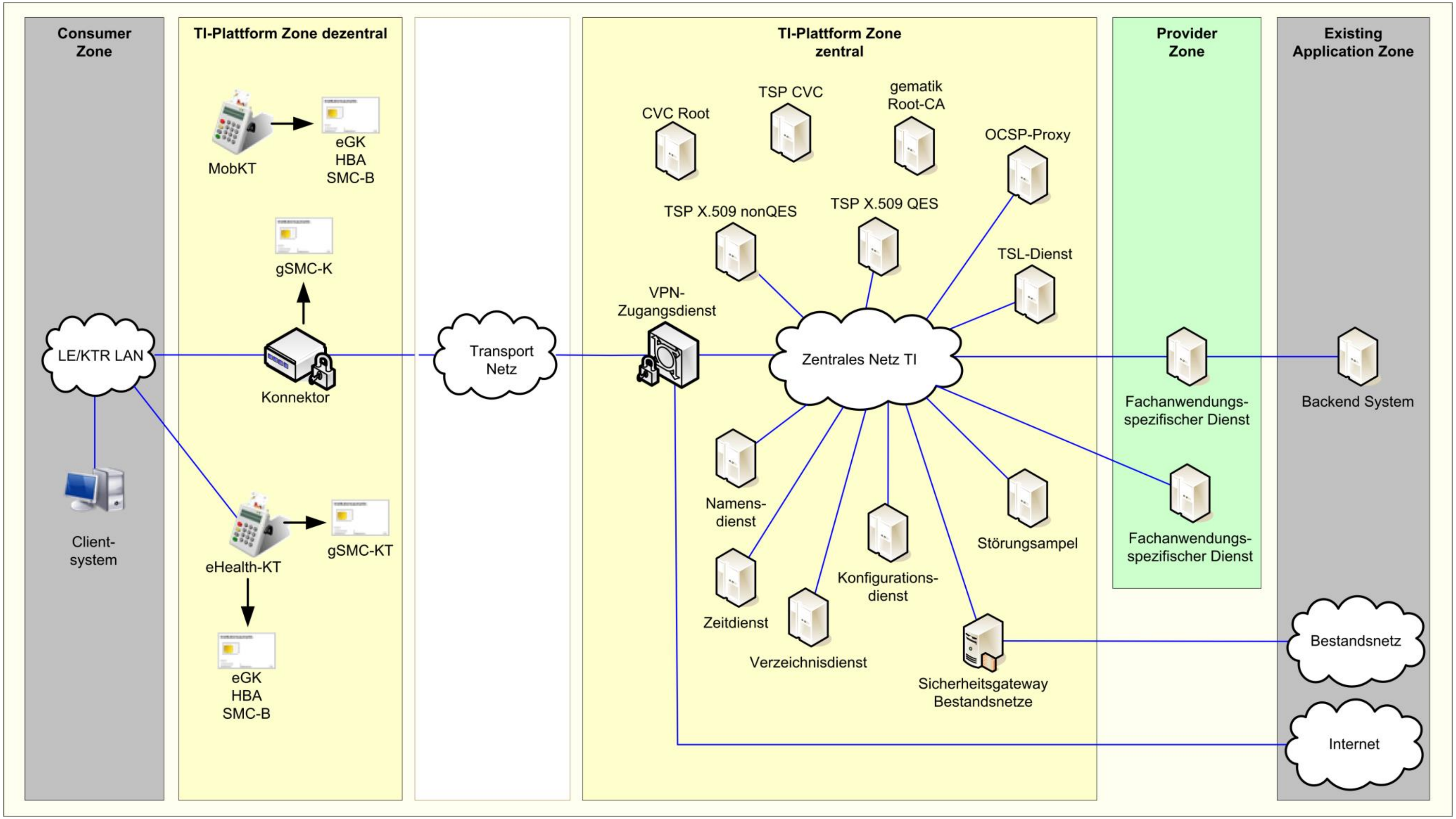
ID X.509

Applications – Industry



© 2018 achelos

Applications – German health system



Source: [gemKPT_Arch_TIP], v1.8.0, Fig. 7

Problem: Configuration

- Different methods and combination possibilities
  - Authentication: PSK, X.509 certificates, EAP, …
  - Key exchange: RSA, DHE, ECDHE, …
  - Encryption: 3DES, AES-CBC, AES-GCM, …
  - Key lengths: 256 bit AES, 2048 bit RSA, 521 bit EC, …
- Different protocol versions
  - IKEv1, IKEv2
  - SSL 3.0, TLS 1.0, 1.1 and 1.2, soon TLS 1.3
- Implementations support a lot of protocol variants and extensions
- An application often needs only a small subset
- Secure configuration necessary

Problem: Implementation

- **Secure implementation of the protocols is required**
  - Keys in secure storage
  - Non predictable random numbers
  - No side channels, e.g., timing, padding oracles
  - No downgrade to the behavior of old protocol versions
- **Even widely used libraries regularly contain security holes**
  - Attacks: Lucky Thirteen (2013), Heartbleed (2014),
    POODLE against TLS (2014), …

Security tests – Necessity

- **Exclude the existence of known security weaknesses**
  - Secure configuration based on guidelines (e.g., NIST, BSI)
  - Check the implementation for known security holes
- **Certifications require security tests**
  - Protection Profiles (PP) for Common Criteria (CC)
  - PCI-DSS
  - ISO/IEC 27000

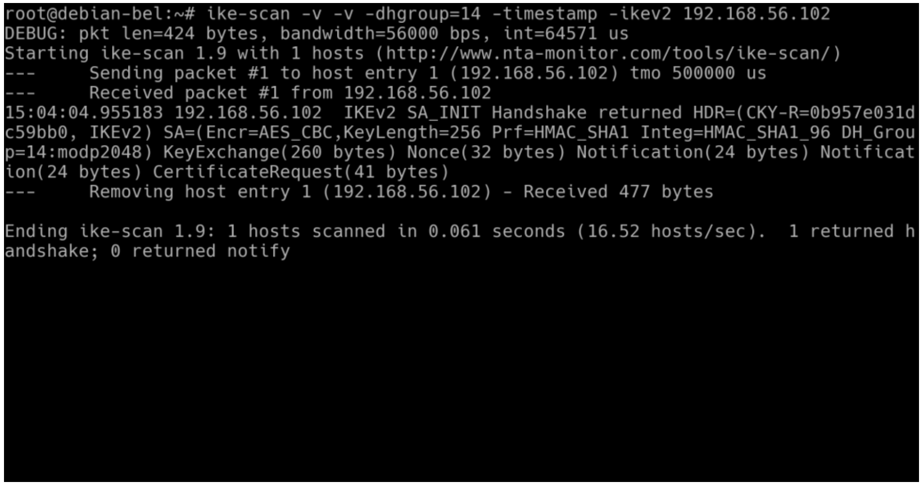
© 2018 achelos

Security tests – Automation

- **Some checks can only be done manually**
  - Source code review (e.g., secure deletion of internal data)
- **Many procedures can be checked automatically**
  - Outside behavior on the system‘s interface
- **Advantages of test automation**
  - Fast execution
  - Uniform test reports
  - Reproducibility

Market overview – IKE tools

ike-scan

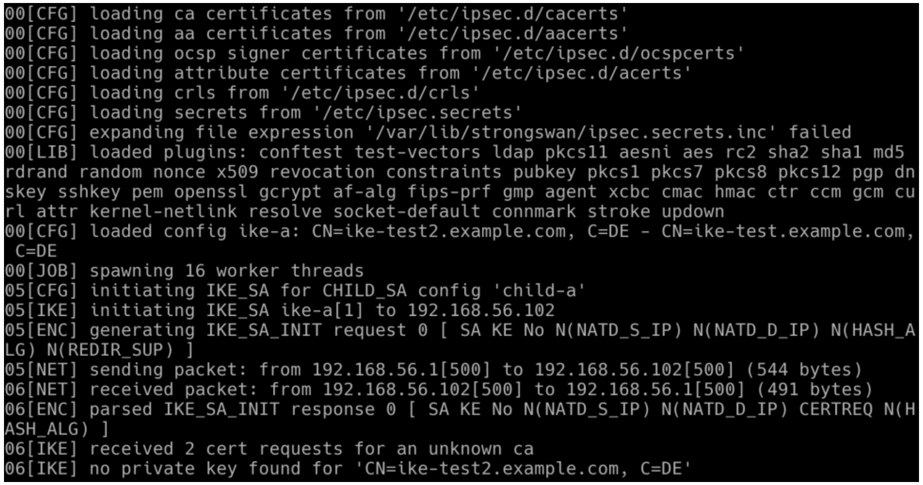


```
root@debian-bel:~# ike-scan -v -v -dhgroup=14 -timestamp -ikev2 192.168.56.102
DEBUG: pkt len=424 bytes, bandwidth=56000 bps, int=64571 us
Starting ike-scan 1.9 with 1 hosts (http://www.nta-monitor.com/tools/ike-scan/)
---     Sending packet #1 to host entry 1 (192.168.56.102) tmo 500000 us
---     Received packet #1 from 192.168.56.102
15:04:04.955183 192.168.56.102  IKEv2 SA_INIT Handshake returned HDR=(CKY-R=0b957e031d
c59bb0, IKEv2) SA=(Encr=AES_CBC,KeyLength=256 Prf=HMAC_SHA1 Integ=HMAC_SHA1_96 DH_Grou
p=14:modp2048) KeyExchange(260 bytes) Nonce(32 bytes) Notification(24 bytes) Notificat
ion(24 bytes) CertificateRequest(41 bytes)
---     Removing host entry 1 (192.168.56.102) - Received 477 bytes

Ending ike-scan 1.9: 1 hosts scanned in 0.061 seconds (16.52 hosts/sec).  1 returned h
andshake; 0 returned notify
```

- Detection of IKE responders
- Manipulation of payloads (e.g., transforms)

strongSwan conftest

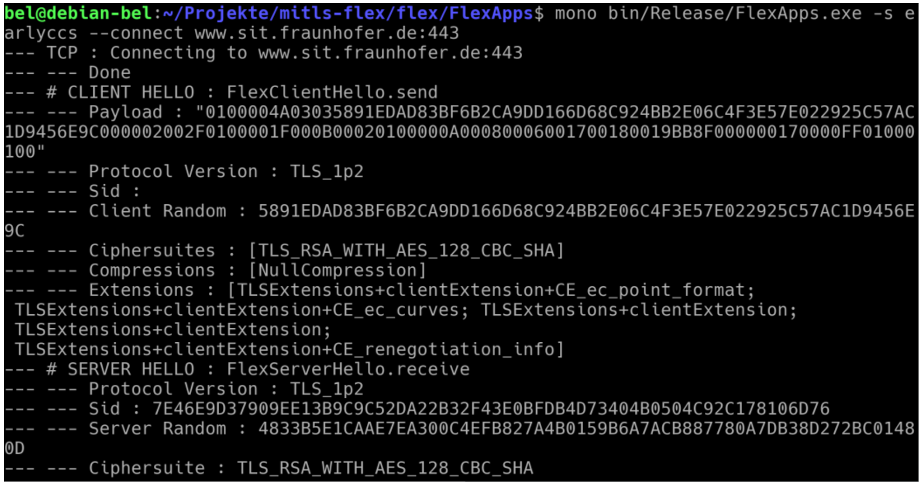


```
00[CFG] loading ca certificates from '/etc/ipsec.d/cacerts'
00[CFG] loading aa certificates from '/etc/ipsec.d/aacerts'
00[CFG] loading ocsp signer certificates from '/etc/ipsec.d/ocspcerts'
00[CFG] loading attribute certificates from '/etc/ipsec.d/acerts'
00[CFG] loading crls from '/etc/ipsec.d/crls'
00[CFG] loading secrets from '/etc/ipsec.secrets'
00[CFG] expanding file expression '/var/lib/strongswan/ipsec.secrets.inc' failed
00[LIB] loaded plugins: conftest test-vectors ldap pkcs11 aesni aes rc2 sha2 sha1 md5
rdrand random nonce x509 revocation constraints pubkey pkcs1 pkcs7 pkcs8 pkcs12 pgp dn
skey sshkey pem openssl gcrypt af-alg fips-prf gmp agent xcbc cmac hmac ctr ccm gcm cu
rl attr kernel-netlink resolve socket-default connmark stroke updown
00[CFG] loaded config ike-a: CN=ike-test2.example.com, C=DE - CN=ike-test.example.com,
 C=DE
00[JOB] spawning 16 worker threads
05[CFG] initiating IKE_SA for CHILD_SA config 'child-a'
05[IKE] initiating IKE_SA ike-a[1] to 192.168.56.102
05[ENC] generating IKE_SA_INIT request 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) N(HASH_A
LG) N(REDIR_SUP) ]
05[NET] sending packet: from 192.168.56.1[500] to 192.168.56.102[500] (544 bytes)
06[NET] received packet: from 192.168.56.102[500] to 192.168.56.1[500] (491 bytes)
06[ENC] parsed IKE_SA_INIT response 0 [ SA KE No N(NATD_S_IP) N(NATD_D_IP) CERTREQ N(H
ASH_ALG) ]
06[IKE] received 2 cert requests for an unknown ca
06[IKE] no private key found for 'CN=ike-test2.example.com, C=DE'
```

- Configuration file
- Invalid values
- Wrong protocol behavior

Market overview – TLS test scripts

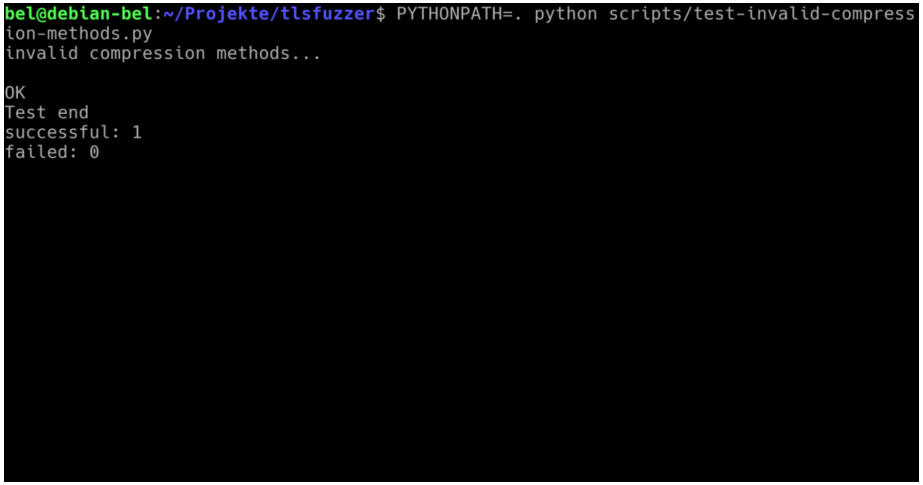
FlexApps



```
bel@debian-bel:~/Projekte/mitls-flex/flex/FlexApps$ mono bin/Release/FlexApps.exe -s e
arlyccs --connect www.sit.fraunhofer.de:443
--- TCP : Connecting to www.sit.fraunhofer.de:443
--- --- Done
--- # CLIENT HELLO : FlexClientHello.send
--- --- Payload : "0100004A03035891EDAD83BF6B2CA9DD166D68C924BB2E06C4F3E57E022925C57AC
1D9456E9C000002002F0100001F000B00020100000A000800060017001800019BB8F000000170000FF01000
100"
--- --- Protocol Version : TLS_1p2
--- --- Sid :
--- --- Client Random : 5891EDAD83BF6B2CA9DD166D68C924BB2E06C4F3E57E022925C57AC1D9456E
9C
--- --- Ciphersuites : [TLS_RSA_WITH_AES_128_CBC_SHA]
--- --- Compressions : [NullCompression]
--- --- Extensions : [TLSExtensions+clientExtension+CE_ec_point_format;
 TLSExtensions+clientExtension+CE_ec_curves; TLSExtensions+clientExtension;
 TLSExtensions+clientExtension;
 TLSExtensions+clientExtension+CE_renegotiation_info]
--- # SERVER HELLO : FlexServerHello.receive
--- --- Protocol Version : TLS_1p2
--- --- Sid : 7E46E9D37909EE13B9C9C52DA22B32F43E0BFDB4D73404B0504C92C178106D76
--- --- Server Random : 4833B5E1CAAE7EA300C4EFB827A4B0159B6A7ACB887780A7DB38D272BC0148
0D
--- --- Ciphersuite : TLS_RSA_WITH_AES_128_CBC_SHA
```

- Known vulnerabilities
- Fuzzing with SmackTLS
- Wrong protocol behavior
- Test cases in F# based on miTLS

tlsfuzzer



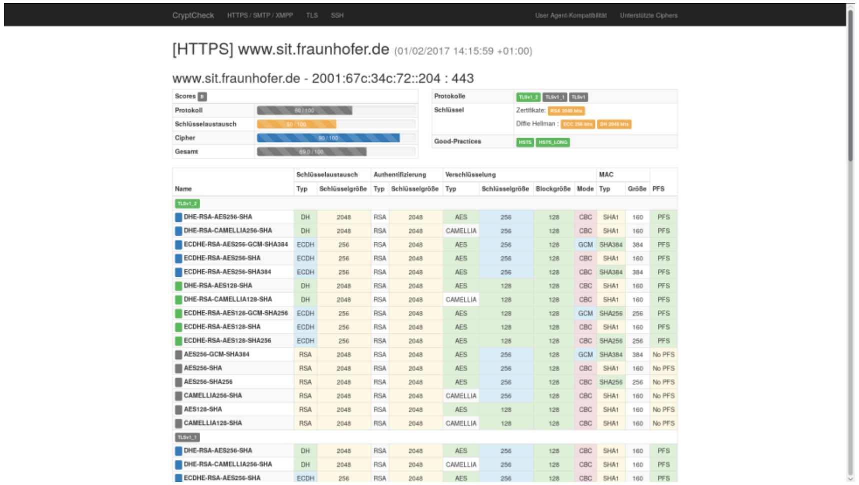
```
bel@debian-bel:~/Projekte/tlsfuzzer$ PYTHONPATH=. python scripts/test-invalid-compress
ion-methods.py
invalid compression methods...

OK
Test end
successful: 1
failed: 0
```

- Known vulnerabilities
- Fuzzing
- Wrong protocol behavior
- TLS configuration
- Test cases as Python scripts

Market overview – Web sites for TLS tests 1

CryptCheck



CryptCheck HTTPS / SMTP / XMPP TLS SSH User Agent-Kompatibilität Unterstützte Ciphers

[HTTPS] www.sit.fraunhofer.de (01/02/2017 14:15:59 +01:00)

www.sit.fraunhofer.de - 2001:67c:34c:72::204 : 443

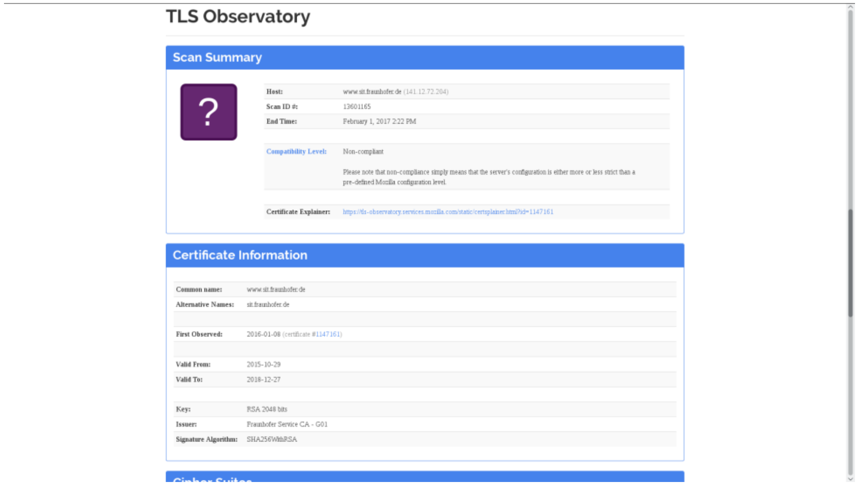
Scores B	
Protokoll	60 / 100
Schlüsselaustausch	50 / 100
Cipher	90 / 100
Gesamt	69.0 / 100

Protokolle	TLSv1_2 TLSv1_1 TLSv1
Schlüssel	Zertifikate: RSA 2048 bits Diffie Hellman : ECC 256 bits DH 2048 bits
Good-Practices	HSTS HSTS_LONG

	Schlüsselaustausch		Authentifizierung		Verschlüsselung				MAC		
Name	Typ	Schlüsselgröße	Typ	Schlüsselgröße	Typ	Schlüsselgröße	Blockgröße	Mode	Typ	Größe	PFS
TLSv1_2											
DHE-RSA-AES256-SHA	DH	2048	RSA	2048	AES	256	128	CBC	SHA1	160	PFS
DHE-RSA-CAMELLIA256-SHA	DH	2048	RSA	2048	CAMELLIA	256	128	CBC	SHA1	160	PFS
ECDHE-RSA-AES256-GCM-SHA384	ECDH	256	RSA	2048	AES	256	128	GCM	SHA384	384	PFS
ECDHE-RSA-AES256-SHA	ECDH	256	RSA	2048	AES	256	128	CBC	SHA1	160	PFS
ECDHE-RSA-AES256-SHA384	ECDH	256	RSA	2048	AES	256	128	CBC	SHA384	384	PFS
DHE-RSA-AES128-SHA	DH	2048	RSA	2048	AES	128	128	CBC	SHA1	160	PFS
DHE-RSA-CAMELLIA128-SHA	DH	2048	RSA	2048	CAMELLIA	128	128	CBC	SHA1	160	PFS
ECDHE-RSA-AES128-GCM-SHA256	ECDH	256	RSA	2048	AES	128	128	GCM	SHA256	256	PFS
ECDHE-RSA-AES128-SHA	ECDH	256	RSA	2048	AES	128	128	CBC	SHA1	160	PFS
ECDHE-RSA-AES128-SHA256	ECDH	256	RSA	2048	AES	128	128	CBC	SHA256	256	PFS
AES256-GCM-SHA384	RSA	2048	RSA	2048	AES	256	128	GCM	SHA384	384	No PFS
AES256-SHA	RSA	2048	RSA	2048	AES	256	128	CBC	SHA1	160	No PFS
AES256-SHA256	RSA	2048	RSA	2048	AES	256	128	CBC	SHA256	256	No PFS
CAMELLIA256-SHA	RSA	2048	RSA	2048	CAMELLIA	256	128	CBC	SHA1	160	No PFS
AES128-SHA	RSA	2048	RSA	2048	AES	128	128	CBC	SHA1	160	No PFS
CAMELLIA128-SHA	RSA	2048	RSA	2048	CAMELLIA	128	128	CBC	SHA1	160	No PFS
TLSv1_1											
DHE-RSA-AES256-SHA	DH	2048	RSA	2048	AES	256	128	CBC	SHA1	160	PFS
DHE-RSA-CAMELLIA256-SHA	DH	2048	RSA	2048	CAMELLIA	256	128	CBC	SHA1	160	PFS
ECDHE-RSA-AES256-SHA	ECDH	256	RSA	2048	AES	256	128	CBC	SHA1	160	PFS

- Certificate checks
- TLS configuration
- Grades for the overall result and for partial results

Observatory by Mozilla



TLS Observatory

Scan Summary

Host:	www.sit.fraunhofer.de (141.12.72.204)
Scan ID #:	13601165
End Time:	February 1, 2017 2:22 PM
Compatibility Level:	Non-compliant Please note that non-compliance simply means that the server's configuration is either more or less strict than a pre-defined Mozilla configuration level.
Certificate Explainer:	https://tls-observatory.services.mozilla.com/static/certsplainer.html?id=1147161

Certificate Information

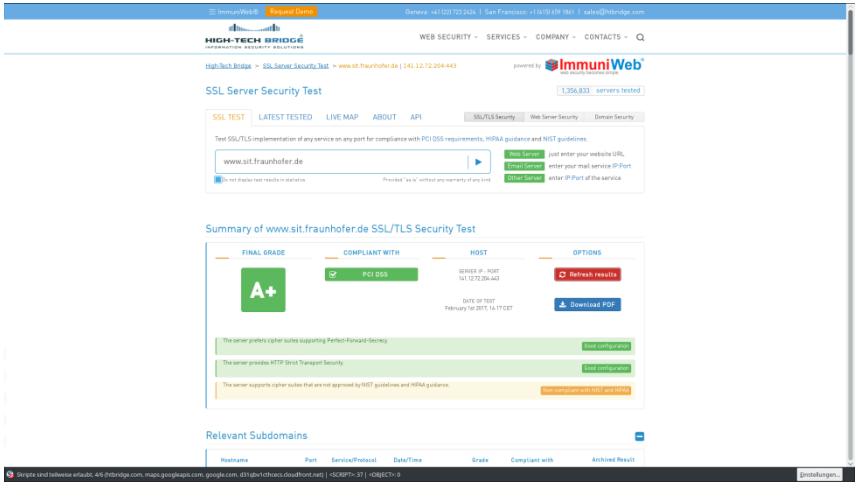
Common name:	www.sit.fraunhofer.de
Alternative Names:	sit.fraunhofer.de
First Observed:	2016-01-08 (certificate #1147161)
Valid From:	2015-10-29
Valid To:	2018-12-27
Key:	RSA 2048 bits
Issuer:	Fraunhofer Service CA - G01
Signature Algorithm:	SHA256WithRSA

Cipher Suites

- Certificate checks
- TLS configuration
- Comparison with Mozilla guidelines
- Grade for the overall result

Market overview – Web sites for TLS tests 2

HT Bridge SSL Server Security Test



☰ ImmuniWeb® Request Demo Geneva: +41 (22) 723 2424 | San Francisco: +1 (415) 659 1861 | sales@htbridge.com

HIGH-TECH BRIDGE INFORMATION SECURITY SOLUTIONS

WEB SECURITY ⌄ SERVICES ⌄ COMPANY ⌄ CONTACTS ⌄

High-Tech Bridge > SSL Server Security Test > www.sit.fraunhofer.de | 141.12.72.204:443

powered by ImmuniWeb® web security becomes simple

SSL Server Security Test

1,356,833 servers tested

SSL TEST | LATEST TESTED | LIVE MAP | ABOUT | API — SSL/TLS Security | Web Server Security | Domain Security

Test SSL/TLS implementation of any service on any port for compliance with PCI DSS requirements, HIPAA guidance and NIST guidelines.

www.sit.fraunhofer.de ▶

☑ Do not display test results in statistics — Provided "as is" without any warranty of any kind

Web Server	just enter your website URL
Email Server	enter your mail service IP:Port
Other Server	enter IP:Port of the service

Summary of www.sit.fraunhofer.de SSL/TLS Security Test

FINAL GRADE	COMPLIANT WITH	HOST	OPTIONS
A+	☑ PCI DSS	SERVER IP : PORT 141.12.72.204:443	Refresh results
		DATE OF TEST February 1st 2017, 14:17 CET	Download PDF

The server prefers cipher suites supporting Perfect-Forward-Secrecy.	Good configuration
The server provides HTTP Strict Transport Security.	Good configuration
The server supports cipher suites that are not approved by NIST guidelines and HIPAA guidance.	Non-compliant with NIST and HIPAA

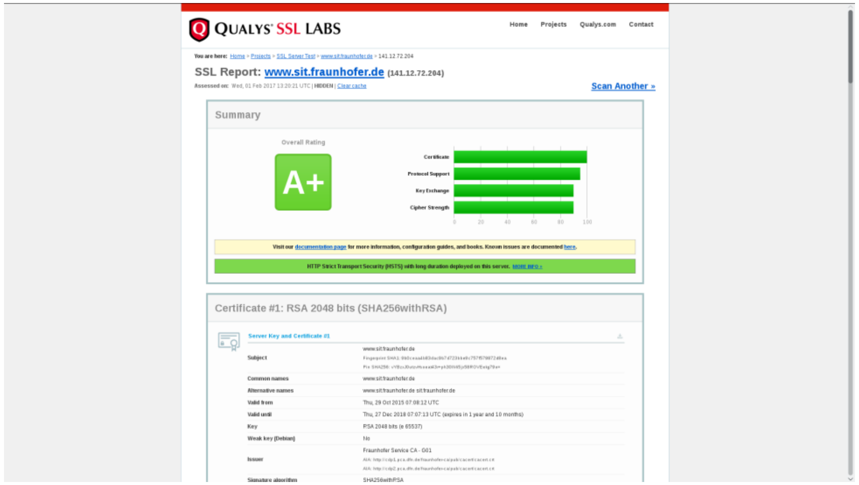
Relevant Subdomains

Hostname	Port	Service/Protocol	Date/Time	Grade	Compliant with	Archived Result

Skripte sind teilweise erlaubt, 4/6 (htbridge.com, maps.googleapis.com, google.com, d31qbv1cthcecs.cloudfront.net) | <SCRIPT>: 37 | <OBJECT>: 0 Einstellungen...

- … + known vulnerabilities
- Comparison with HIPAA, NIST, and PCI-DSS guidelines

Qualys SSL Labs



QUALYS® SSL LABS

Home Projects Qualys.com Contact

You are here: Home > Projects > SSL Server Test > www.sit.fraunhofer.de > 141.12.72.204

SSL Report: www.sit.fraunhofer.de (141.12.72.204)

Assessed on: Wed, 01 Feb 2017 13:20:21 UTC | HIDDEN | Clear cache

Scan Another »

Summary

Overall Rating

A+

Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. MORE INFO »

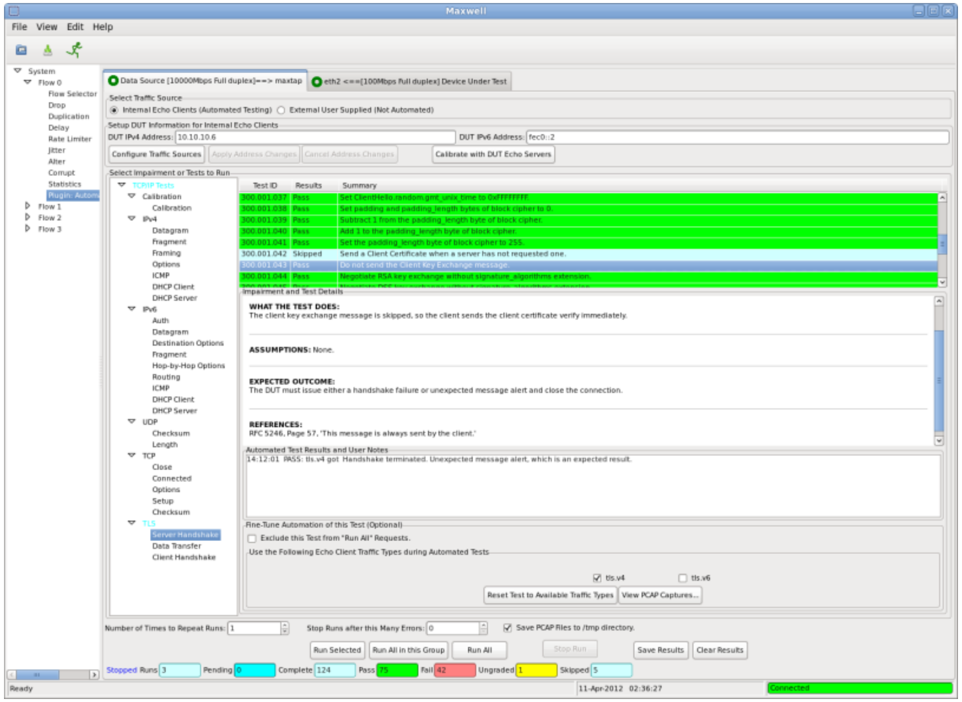
Certificate #1: RSA 2048 bits (SHA256withRSA)

Server Key and Certificate #1

Subject	www.sit.fraunhofer.de Fingerprint SHA1: 9b0ceaa4b83dac9b7d723bbe9c757f579872d8ea Pin SHA256: [illegible]
Common names	www.sit.fraunhofer.de
Alternative names	www.sit.fraunhofer.de sit.fraunhofer.de
Valid from	Thu, 29 Oct 2015 07:08:12 UTC
Valid until	Thu, 27 Dec 2018 07:07:13 UTC (expires in 1 year and 10 months)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	Fraunhofer Service CA - G01 AIA: http://cdp1.pca.dfn.de/fraunhofer-ca/pub/cacert/cacert.crt AIA: http://cdp2.pca.dfn.de/fraunhofer-ca/pub/cacert/cacert.crt
Signature algorithm	SHA256withRSA

- … + known vulnerabilities
- Simulation of different clients
- Browser test

Market overview – IWL Maxwell Pro TLS Test Suite



Select Traffic Source

● Internal Echo Clients (Automated Testing) ○ External User Supplied (Not Automated)

Setup DUT Information for Internal Echo Clients

DUT IPv4 Address: 10.10.10.6 DUT IPv6 Address: fec0::2

Select Impairment or Tests to Run

Test ID	Results	Summary
300.001.037	Pass	Set ClientHello.random.gmt_unix_time to 0xFFFFFFFF.
300.001.038	Pass	Set padding and padding_length bytes of block cipher to 0.
300.001.039	Pass	Subtract 1 from the padding_length byte of block cipher.
300.001.040	Pass	Add 1 to the padding_length byte of block cipher.
300.001.041	Pass	Set the padding_length byte of block cipher to 255.
300.001.042	Skipped	Send a Client Certificate when a server has not requested one.
300.001.043	Pass	Do not send the Client Key Exchange message.
300.001.044	Pass	Negotiate RSA key exchange without signature_algorithms extension.

Impairment and Test Details

WHAT THE TEST DOES:
The client key exchange message is skipped, so the client sends the client certificate verify immediately.

ASSUMPTIONS: None.

EXPECTED OUTCOME:
The DUT must issue either a handshake failure or unexpected message alert and close the connection.

REFERENCES:
RFC 5246, Page 57, 'This message is always sent by the client.'

Automated Test Results and User Notes

```
14:12:01  PASS: tls.v4 got  Handshake terminated. Unexpected message alert, which is an expected result.
```

Fine-Tune Automation of this Test (Optional)

□ Exclude this Test from "Run All" Requests.

Use the Following Echo Client Traffic Types during Automated Tests

☑ tls.v4 □ tls.v6

Number of Times to Repeat Runs: 1 Stop Runs after this Many Errors: 0 ☑ Save PCAP Files to /tmp directory.

Stopped Runs 3 Pending 0 Complete 124 Pass 75 Fail 42 Ungraded 1 Skipped 5

Ready 11-Apr-2012 02:36:27 Connected

- TLS configuration
- Known vulnerabilities
- Invalid values
- Wrong protocol behavior
- Test report with the description of the test idea and a reference to the RFC

achelos test environment – Test suites

achelos
the experts in eID
Qumate.Security.IKE

achelos
the experts in eID
Qumate.Security.TLS-Client

achelos
the experts in eID
Qumate.Security.TLS-Server

- Test case specification in cooperation with TÜViT
- Targeted at CC evaluation procedures
- Automatic tests for BSI requirements

achelos
the experts in eID
Qumate.Security.World
TLS.Checklist

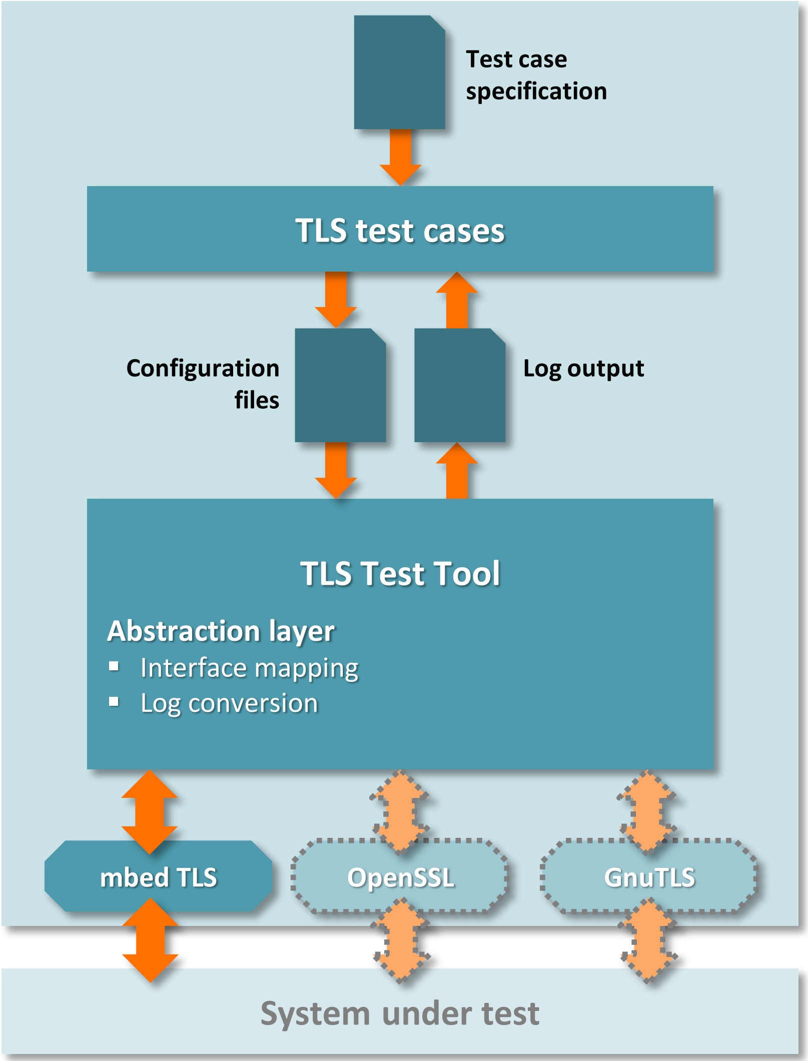
- TLS check list according to BSI TR-03116-4

© 2018 achelos

achelos test environment – Test coverage

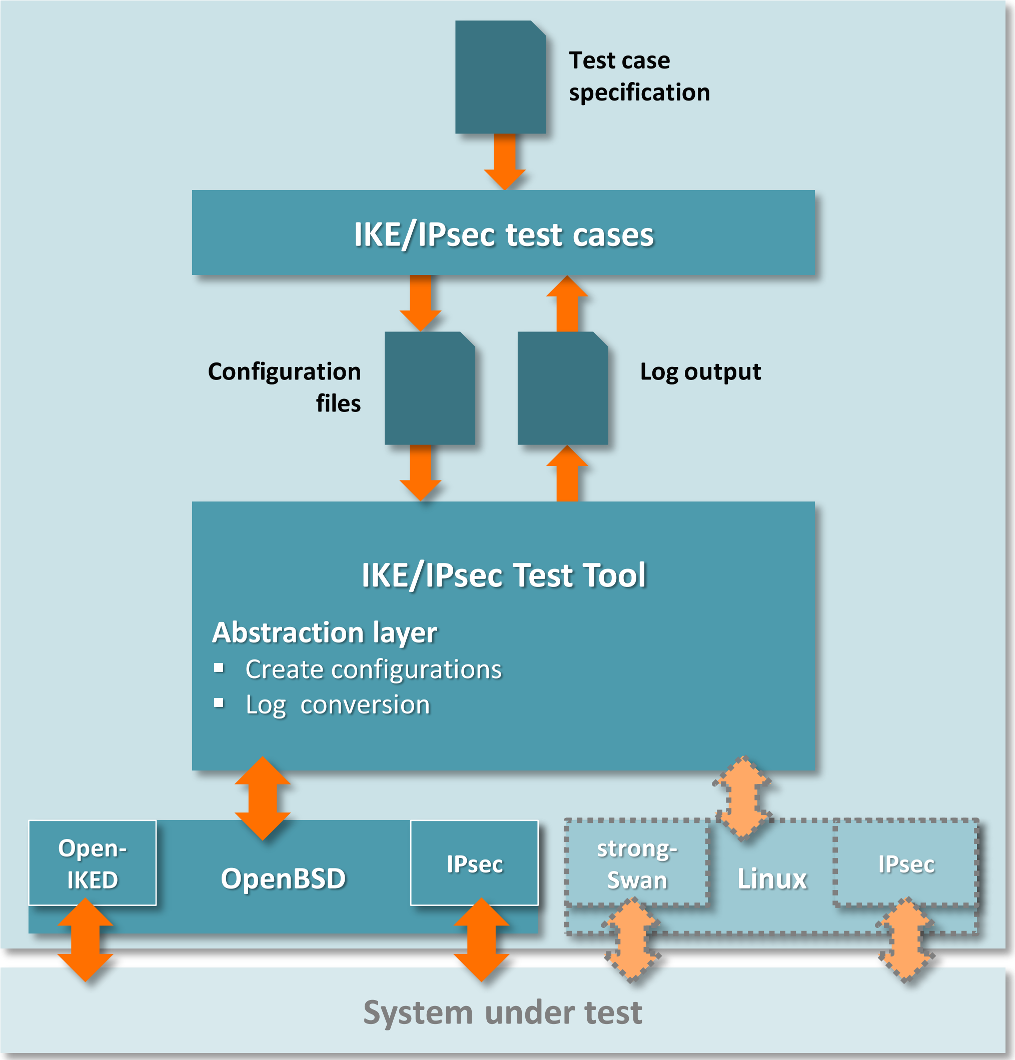
- **Checks for the TLS configuration**
  - Protocol version (no SSL 3.0, TLS 1.0, …)
  - Cipher suites (no EXPORT cipher suites, no weak cryptographic algorithms, …)
  - Cryptographic parameters (RSA key length ≥ 2048 bit, …)
  - Protocol extensions (TLS compression, Heartbeat, …)
- **Tests for correct implementation**
  - Robust protocol implementation (manipulated message order, …)
  - Correct padding/data checks (adding invalid padding values, sequence counters, …)
  - Cryptographic checks (point that is not on the elliptic curve, bad MAC, …)
  - Constant-time implementation (e.g., Lucky Thirteen attack)

achelos test environment – TLS Test Tool



© 2018 achelos

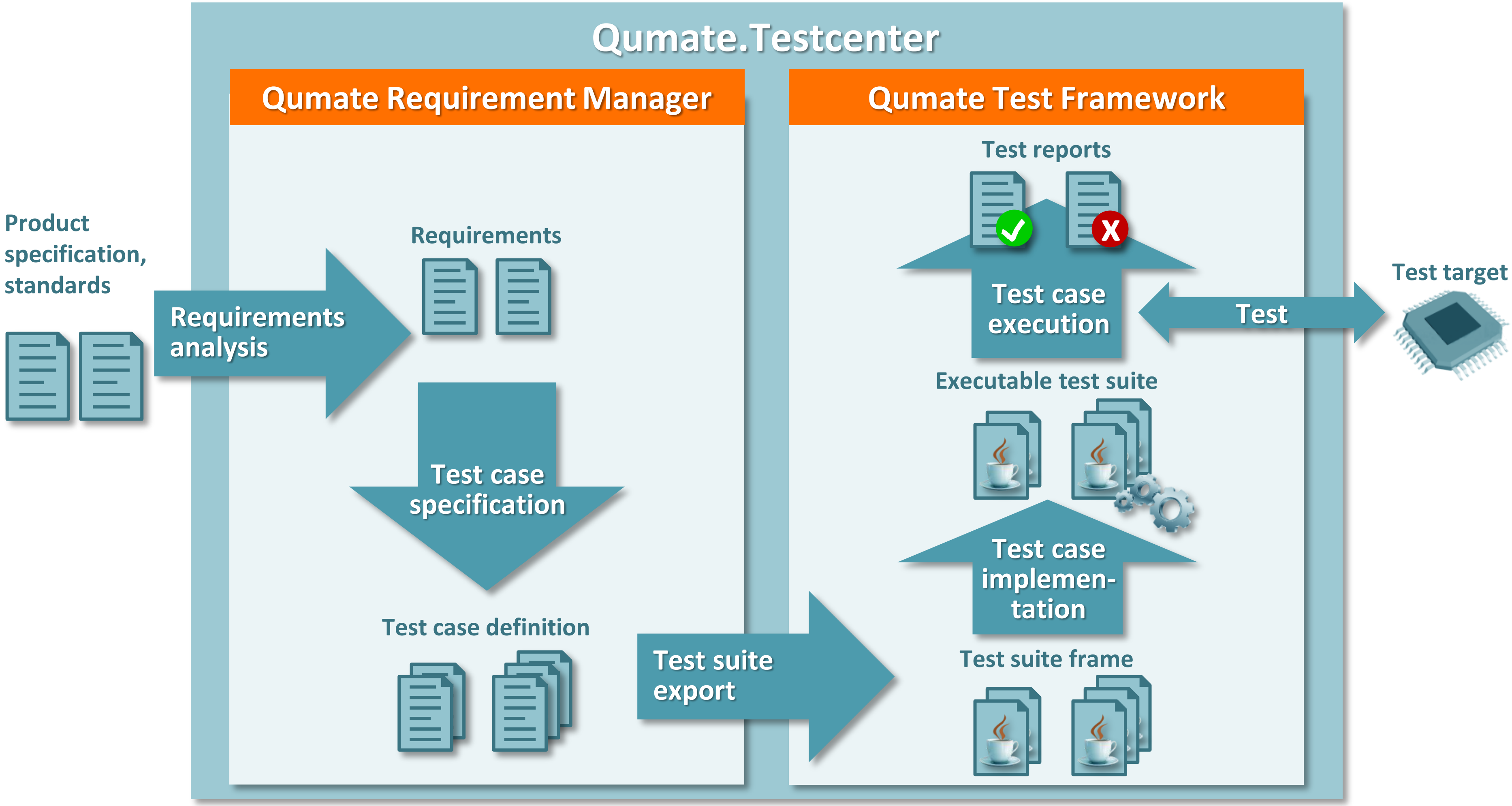
achelos test environment – IKE Test Tool



achelos test environment – Traceability

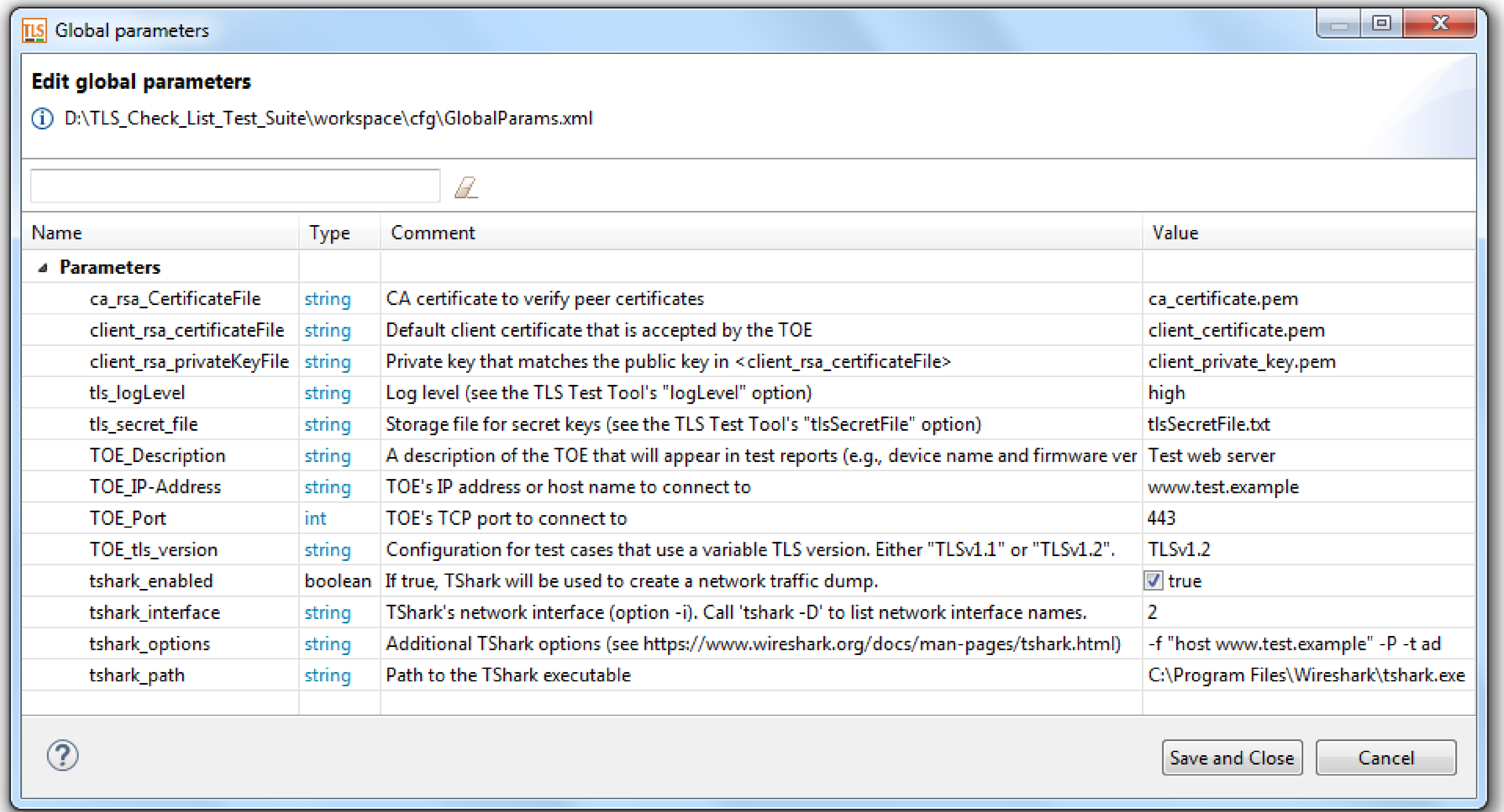
- Test case specification uses wording of the relevant RFCs
  - No implementation details
- Test report contains …
  - … test case idea and specification
  - … checks performed by the test case (expected/actual result)
  - … details of the network communication
- Additionally, a network traffic dump (PCAP file) for every test case

achelos test environment – Workflow using Qumate



achelos
the experts in eID

achelos test environment – Test configuration

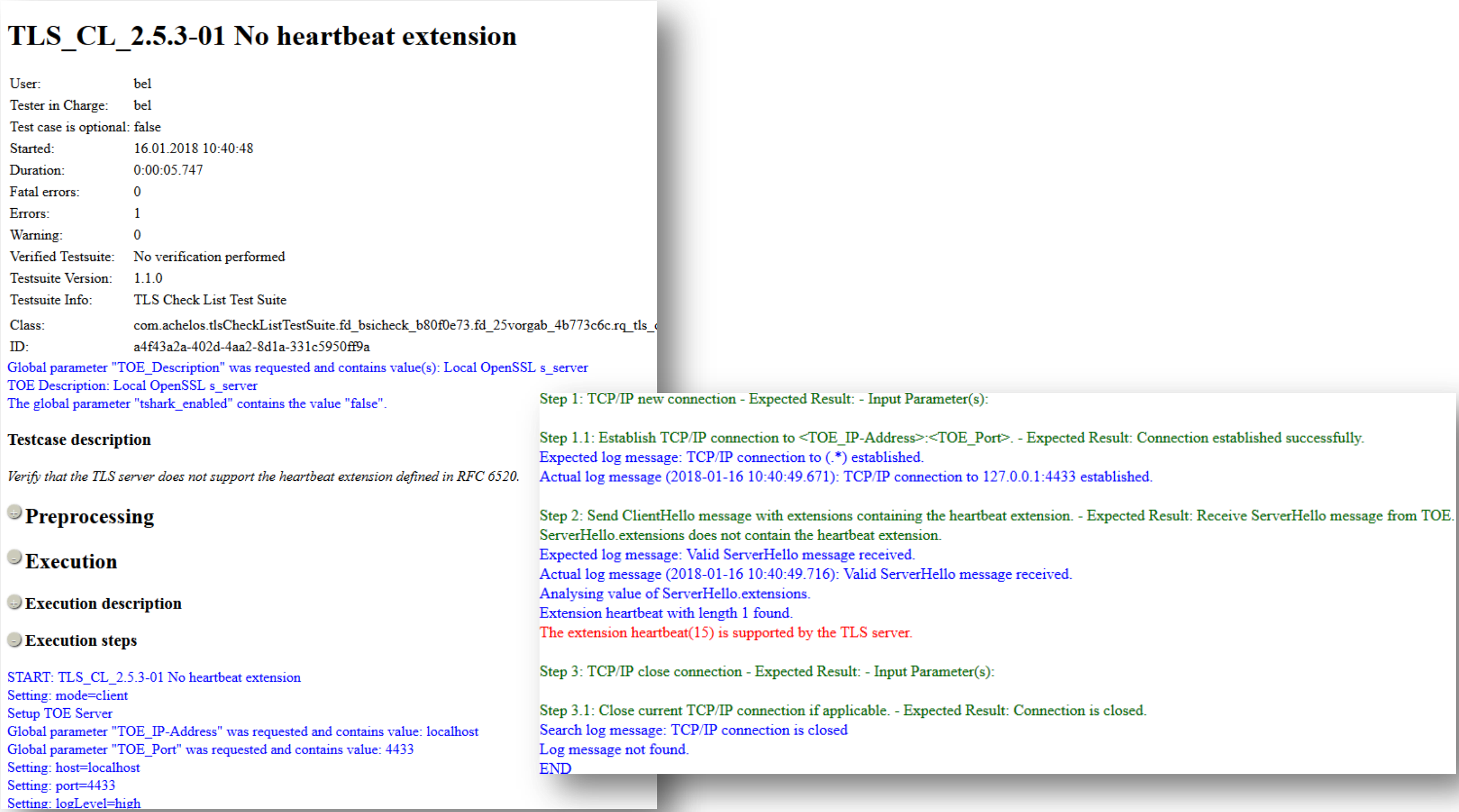


Edit global parameters

ⓘ D:\TLS_Check_List_Test_Suite\workspace\cfg\GlobalParams.xml

Name	Type	Comment	Value
Parameters			
ca_rsa_CertificateFile	string	CA certificate to verify peer certificates	ca_certificate.pem
client_rsa_certificateFile	string	Default client certificate that is accepted by the TOE	client_certificate.pem
client_rsa_privateKeyFile	string	Private key that matches the public key in <client_rsa_certificateFile>	client_private_key.pem
tls_logLevel	string	Log level (see the TLS Test Tool's "logLevel" option)	high
tls_secret_file	string	Storage file for secret keys (see the TLS Test Tool's "tlsSecretFile" option)	tlsSecretFile.txt
TOE_Description	string	A description of the TOE that will appear in test reports (e.g., device name and firmware ver	Test web server
TOE_IP-Address	string	TOE's IP address or host name to connect to	www.test.example
TOE_Port	int	TOE's TCP port to connect to	443
TOE_tls_version	string	Configuration for test cases that use a variable TLS version. Either "TLSv1.1" or "TLSv1.2".	TLSv1.2
tshark_enabled	boolean	If true, TShark will be used to create a network traffic dump.	☑ true
tshark_interface	string	TShark's network interface (option -i). Call 'tshark -D' to list network interface names.	2
tshark_options	string	Additional TShark options (see https://www.wireshark.org/docs/man-pages/tshark.html)	-f "host www.test.example" -P -t ad
tshark_path	string	Path to the TShark executable	C:\Program Files\Wireshark\tshark.exe

achelos test environment – Test reports



TLS_CL_2.5.3-01 No heartbeat extension

```
User:                   bel
Tester in Charge:       bel
Test case is optional:  false
Started:                16.01.2018 10:40:48
Duration:               0:00:05.747
Fatal errors:           0
Errors:                 1
Warning:                0
Verified Testsuite:     No verification performed
Testsuite Version:      1.1.0
Testsuite Info:         TLS Check List Test Suite
Class:                  com.achelos.tlsCheckListTestSuite.fd_bsicheck_b80f0e73.fd_25vorgab_4b773c6c.rq_tls_
ID:                     a4f43a2a-402d-4aa2-8d1a-331c5950ff9a
Global parameter "TOE_Description" was requested and contains value(s): Local OpenSSL s_server
TOE Description: Local OpenSSL s_server
The global parameter "tshark_enabled" contains the value "false".
```

Testcase description

Verify that the TLS server does not support the heartbeat extension defined in RFC 6520.

⊕ **Preprocessing**

⊖ **Execution**

⊕ **Execution description**

⊖ **Execution steps**

```
START: TLS_CL_2.5.3-01 No heartbeat extension
Setting: mode=client
Setup TOE Server
Global parameter "TOE_IP-Address" was requested and contains value: localhost
Global parameter "TOE_Port" was requested and contains value: 4433
Setting: host=localhost
Setting: port=4433
Setting: logLevel=high
```

```
Step 1: TCP/IP new connection - Expected Result: - Input Parameter(s):

Step 1.1: Establish TCP/IP connection to <TOE_IP-Address>:<TOE_Port>. - Expected Result: Connection established successfully.
Expected log message: TCP/IP connection to (.*) established.
Actual log message (2018-01-16 10:40:49.671): TCP/IP connection to 127.0.0.1:4433 established.

Step 2: Send ClientHello message with extensions containing the heartbeat extension. - Expected Result: Receive ServerHello message from TOE.
ServerHello.extensions does not contain the heartbeat extension.
Expected log message: Valid ServerHello message received.
Actual log message (2018-01-16 10:40:49.716): Valid ServerHello message received.
Analysing value of ServerHello.extensions.
Extension heartbeat with length 1 found.
The extension heartbeat(15) is supported by the TLS server.

Step 3: TCP/IP close connection - Expected Result: - Input Parameter(s):

Step 3.1: Close current TCP/IP connection if applicable. - Expected Result: Connection is closed.
Search log message: TCP/IP connection is closed
Log message not found.
END
```

Summary

- Widespread use of the protocols TLS and IKE/IPsec
- Configuration and implementation can contain security holes
- Automatic tests reduce test time and give reproducibility
- Different solutions on the market
- achelos test environment with detailed test reports targeting CC evaluation procedures

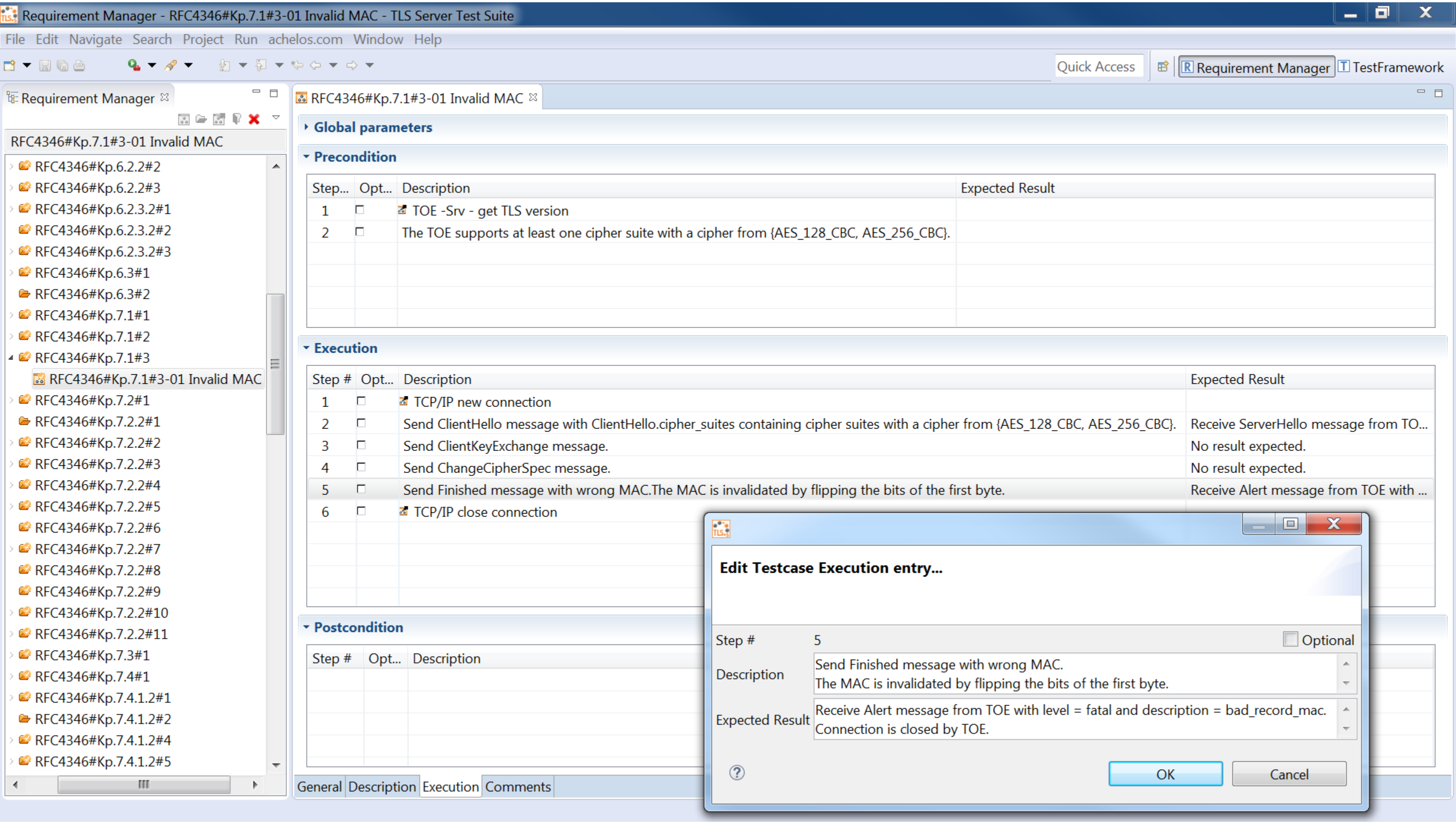
achelos
the experts in eID

achelos GmbH

Dr. Benjamin Eikel

Vattmannstraße 1
33100 Paderborn
Germany
Phone: +49 5251 14212-342
E-mail: benjamin.eikel@achelos.de

www.achelos.de


Requirement Manager - RFC4346#Kp.7.1#3-01 Invalid MAC - TLS Server Test Suite
File Edit Navigate Search Project Run achelos.com Window Help
Quick Access
Requirement Manager
TestFramework
Requirement Manager
RFC4346#Kp.7.1#3-01 Invalid MAC
General
Description
Execution
Comments

RFC4346#Kp.7.1#3-01 Invalid MAC

- RFC4346#Kp.6.2.2#2
- RFC4346#Kp.6.2.2#3
- RFC4346#Kp.6.2.3.2#1
- RFC4346#Kp.6.2.3.2#2
- RFC4346#Kp.6.2.3.2#3
- RFC4346#Kp.6.3#1
- RFC4346#Kp.6.3#2
- RFC4346#Kp.7.1#1
- RFC4346#Kp.7.1#2
- RFC4346#Kp.7.1#3
  - RFC4346#Kp.7.1#3-01 Invalid MAC
- RFC4346#Kp.7.2#1
- RFC4346#Kp.7.2.2#1
- RFC4346#Kp.7.2.2#2
- RFC4346#Kp.7.2.2#3
- RFC4346#Kp.7.2.2#4
- RFC4346#Kp.7.2.2#5
- RFC4346#Kp.7.2.2#6
- RFC4346#Kp.7.2.2#7
- RFC4346#Kp.7.2.2#8
- RFC4346#Kp.7.2.2#9
- RFC4346#Kp.7.2.2#10
- RFC4346#Kp.7.2.2#11
- RFC4346#Kp.7.3#1
- RFC4346#Kp.7.4#1
- RFC4346#Kp.7.4.1.2#1
- RFC4346#Kp.7.4.1.2#2
- RFC4346#Kp.7.4.1.2#4
- RFC4346#Kp.7.4.1.2#5

Global parameters

Precondition

Step...	Opt...	Description	Expected Result
1	□	TOE -Srv - get TLS version	
2	□	The TOE supports at least one cipher suite with a cipher from {AES_128_CBC, AES_256_CBC}.	

Execution

Step #	Opt...	Description	Expected Result
1	□	TCP/IP new connection	
2	□	Send ClientHello message with ClientHello.cipher_suites containing cipher suites with a cipher from {AES_128_CBC, AES_256_CBC}.	Receive ServerHello message from TO...
3	□	Send ClientKeyExchange message.	No result expected.
4	□	Send ChangeCipherSpec message.	No result expected.
5	□	Send Finished message with wrong MAC.The MAC is invalidated by flipping the bits of the first byte.	Receive Alert message from TOE with ...
6	□	TCP/IP close connection	

Postcondition

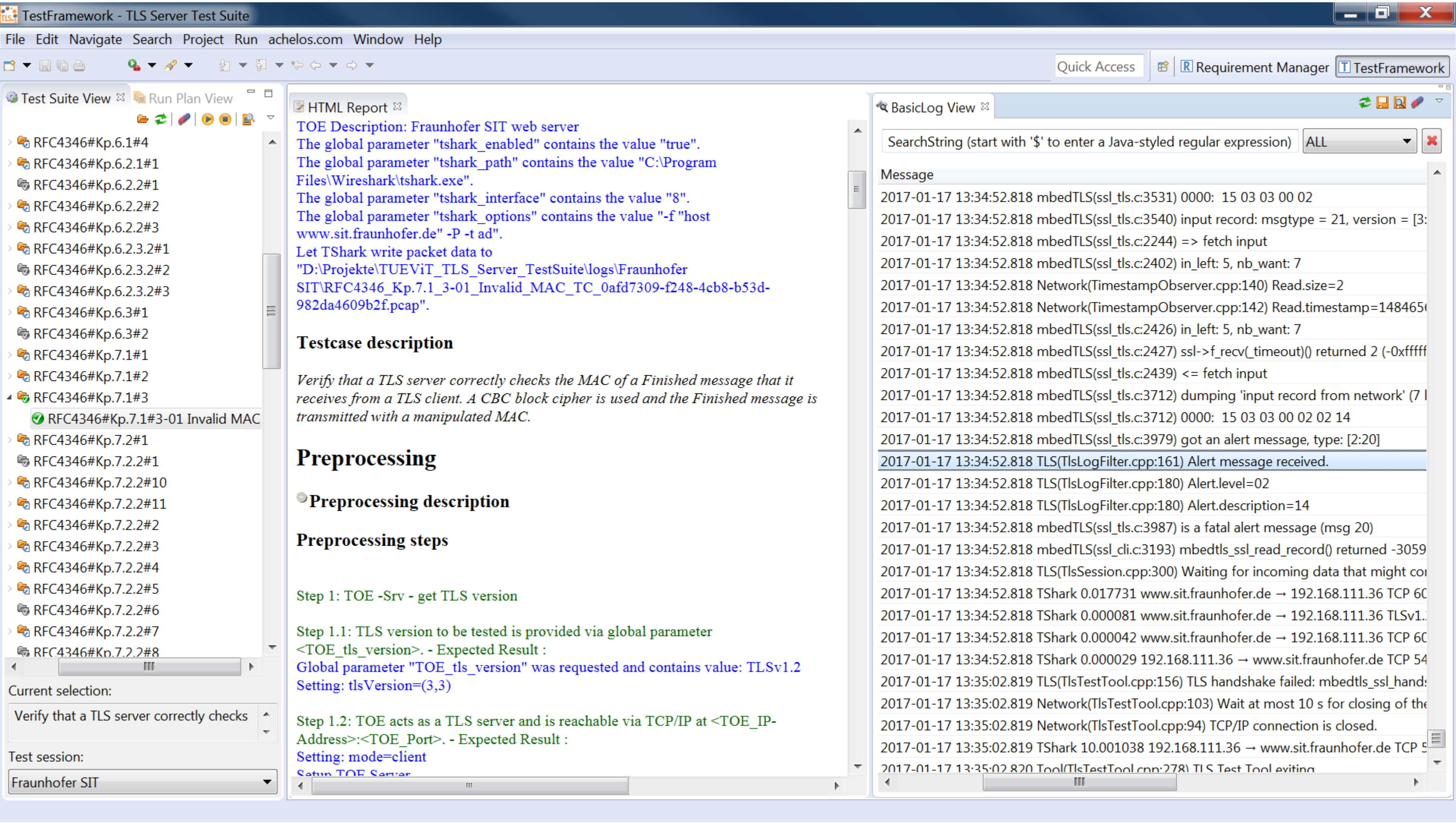
Step #	Opt...	Description

Edit Testcase Execution entry...

Step # 5 □ Optional

Description: Send Finished message with wrong MAC.
The MAC is invalidated by flipping the bits of the first byte.

Expected Result: Receive Alert message from TOE with level = fatal and description = bad_record_mac.
Connection is closed by TOE.



- RFC4346#Kp.6.1#4
- RFC4346#Kp.6.2.1#1
- RFC4346#Kp.6.2.2#1
- RFC4346#Kp.6.2.2#2
- RFC4346#Kp.6.2.2#3
- RFC4346#Kp.6.2.3.2#1
- RFC4346#Kp.6.2.3.2#2
- RFC4346#Kp.6.2.3.2#3
- RFC4346#Kp.6.3#1
- RFC4346#Kp.6.3#2
- RFC4346#Kp.7.1#1
- RFC4346#Kp.7.1#2
- RFC4346#Kp.7.1#3
  - ✓ RFC4346#Kp.7.1#3-01 Invalid MAC
- RFC4346#Kp.7.2#1
- RFC4346#Kp.7.2.2#1
- RFC4346#Kp.7.2.2#10
- RFC4346#Kp.7.2.2#11
- RFC4346#Kp.7.2.2#2
- RFC4346#Kp.7.2.2#3
- RFC4346#Kp.7.2.2#4
- RFC4346#Kp.7.2.2#5
- RFC4346#Kp.7.2.2#6
- RFC4346#Kp.7.2.2#7
- RFC4346#Kp.7.2.2#8

Current selection:

Verify that a TLS server correctly checks

Test session:

Fraunhofer SIT

TOE Description: Fraunhofer SIT web server
The global parameter "tshark_enabled" contains the value "true".
The global parameter "tshark_path" contains the value "C:\Program Files\Wireshark\tshark.exe".
The global parameter "tshark_interface" contains the value "8".
The global parameter "tshark_options" contains the value "-f "host www.sit.fraunhofer.de" -P -t ad".
Let TShark write packet data to "D:\Projekte\TUEViT_TLS_Server_TestSuite\logs\Fraunhofer SIT\RFC4346_Kp.7.1_3-01_Invalid_MAC_TC_0afd7309-f248-4cb8-b53d-982da4609b2f.pcap".

Testcase description

Verify that a TLS server correctly checks the MAC of a Finished message that it receives from a TLS client. A CBC block cipher is used and the Finished message is transmitted with a manipulated MAC.

Preprocessing

Preprocessing description

Preprocessing steps

Step 1: TOE -Srv - get TLS version

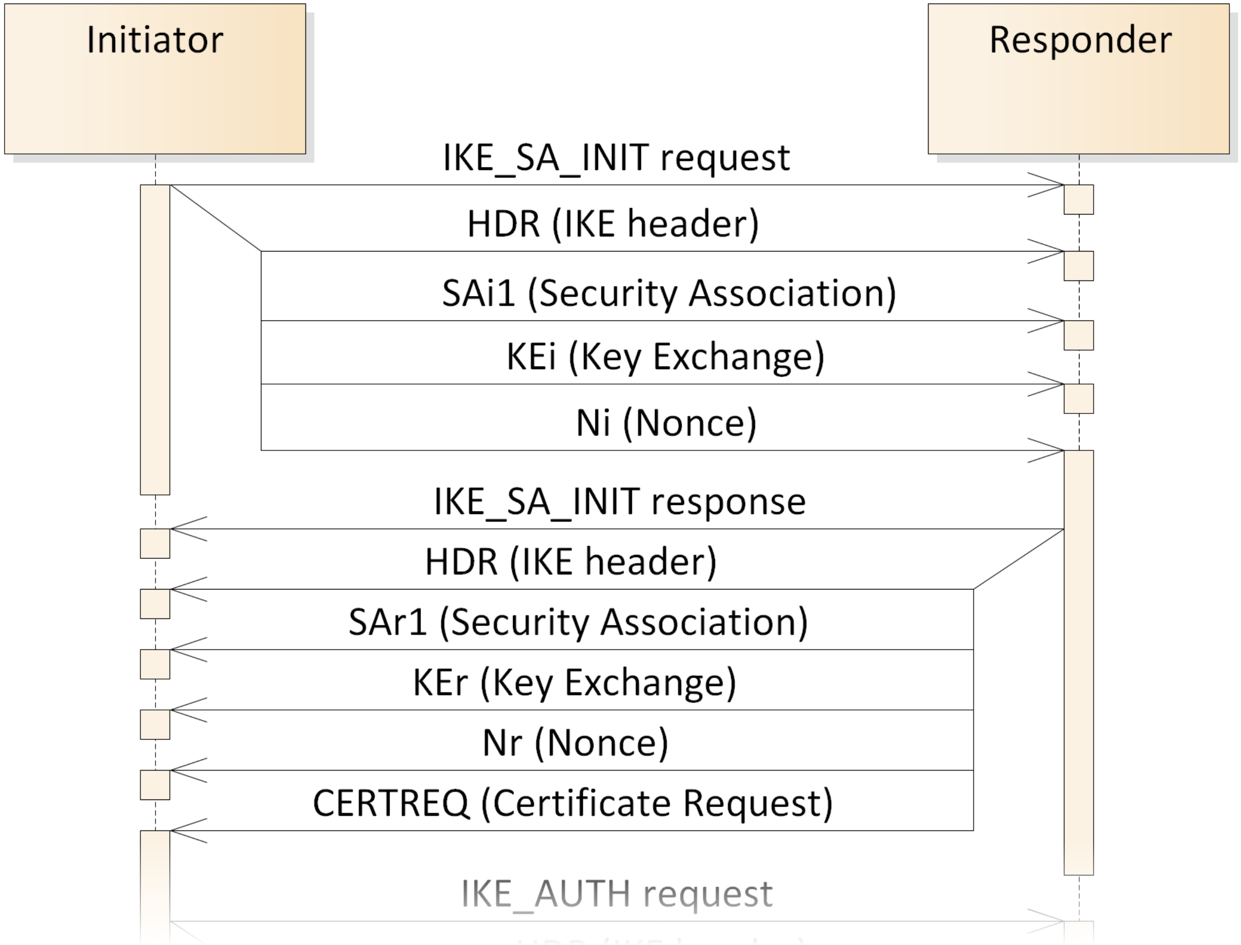
Step 1.1: TLS version to be tested is provided via global parameter <TOE_tls_version>. - Expected Result :
Global parameter "TOE_tls_version" was requested and contains value: TLSv1.2
Setting: tlsVersion=(3,3)

Step 1.2: TOE acts as a TLS server and is reachable via TCP/IP at <TOE_IP-Address>:<TOE_Port>. - Expected Result :
Setting: mode=client
Setup TOE Server

SearchString (start with '$' to enter a Java-styled regular expression) ALL

```
Message
2017-01-17 13:34:52.818 mbedTLS(ssl_tls.c:3531) 0000:  15 03 03 00 02
2017-01-17 13:34:52.818 mbedTLS(ssl_tls.c:3540) input record: msgtype = 21, version = [3:
2017-01-17 13:34:52.818 mbedTLS(ssl_tls.c:2244) => fetch input
2017-01-17 13:34:52.818 mbedTLS(ssl_tls.c:2402) in_left: 5, nb_want: 7
2017-01-17 13:34:52.818 Network(TimestampObserver.cpp:140) Read.size=2
2017-01-17 13:34:52.818 Network(TimestampObserver.cpp:142) Read.timestamp=148465
2017-01-17 13:34:52.818 mbedTLS(ssl_tls.c:2426) in_left: 5, nb_want: 7
2017-01-17 13:34:52.818 mbedTLS(ssl_tls.c:2427) ssl->f_recv(_timeout)() returned 2 (-0xffff
2017-01-17 13:34:52.818 mbedTLS(ssl_tls.c:2439) <= fetch input
2017-01-17 13:34:52.818 mbedTLS(ssl_tls.c:3712) dumping 'input record from network' (7 
2017-01-17 13:34:52.818 mbedTLS(ssl_tls.c:3712) 0000:  15 03 03 00 02 02 14
2017-01-17 13:34:52.818 mbedTLS(ssl_tls.c:3979) got an alert message, type: [2:20]
2017-01-17 13:34:52.818 TLS(TlsLogFilter.cpp:161) Alert message received.
2017-01-17 13:34:52.818 TLS(TlsLogFilter.cpp:180) Alert.level=02
2017-01-17 13:34:52.818 TLS(TlsLogFilter.cpp:180) Alert.description=14
2017-01-17 13:34:52.818 mbedTLS(ssl_tls.c:3987) is a fatal alert message (msg 20)
2017-01-17 13:34:52.818 mbedTLS(ssl_cli.c:3193) mbedtls_ssl_read_record() returned -3059
2017-01-17 13:34:52.818 TLS(TlsSession.cpp:300) Waiting for incoming data that might co
2017-01-17 13:34:52.818 TShark 0.017731 www.sit.fraunhofer.de → 192.168.111.36 TCP 60
2017-01-17 13:34:52.818 TShark 0.000081 www.sit.fraunhofer.de → 192.168.111.36 TLSv1.
2017-01-17 13:34:52.818 TShark 0.000042 www.sit.fraunhofer.de → 192.168.111.36 TCP 60
2017-01-17 13:34:52.818 TShark 0.000029 192.168.111.36 → www.sit.fraunhofer.de TCP 54
2017-01-17 13:35:02.819 TLS(TlsTestTool.cpp:156) TLS handshake failed: mbedtls_ssl_hand
2017-01-17 13:35:02.819 Network(TlsTestTool.cpp:103) Wait at most 10 s for closing of the
2017-01-17 13:35:02.819 Network(TlsTestTool.cpp:94) TCP/IP connection is closed.
2017-01-17 13:35:02.819 TShark 10.001038 192.168.111.36 → www.sit.fraunhofer.de TCP 5
2017-01-17 13:35:02.820 Tool(TlsTestTool.cpp:278) TLS Test Tool exiting
```

Protocols – IKE handshake 1



Initiator

Responder

IKE_SA_INIT request

HDR (IKE header)

SAi1 (Security Association)

KEi (Key Exchange)

Ni (Nonce)

IKE_SA_INIT response

HDR (IKE header)

SAr1 (Security Association)

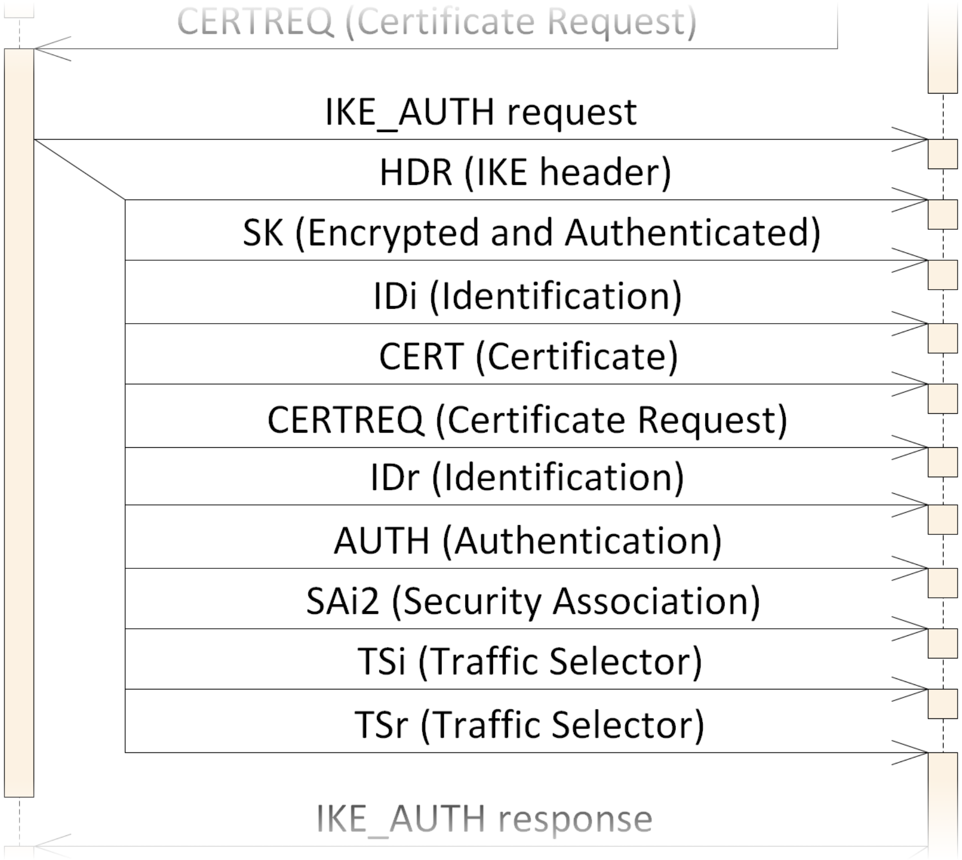
KEr (Key Exchange)

Nr (Nonce)

CERTREQ (Certificate Request)

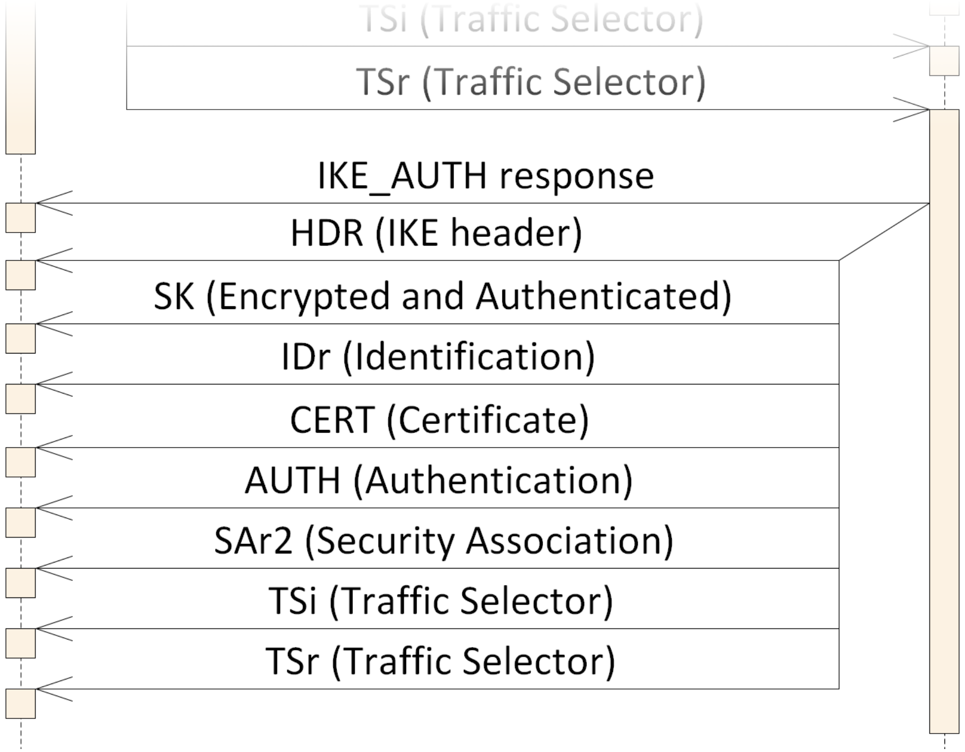
IKE_AUTH request

Protocols – IKE handshake 2



© 2018 achelos

Protocols – IKE handshake 3



© 2018 achelos