

TaSK – TLS-Testtool für die automatisierte Prüfung der Sicherheit des Kommunikationsprotokolls

Dr. Nico Klein (BSI) & Heinfried Cznottka (achelos GmbH)

Berlin, 24.05.2023

Digitalisierung

- Sichere und interoperable Kommunikationsverbindungen sind eine Grundvoraussetzung für die erfolgreiche Digitalisierung
 - Sicherheitsziele: Authentizität, Integrität und Vertraulichkeit



§3 BSI-Gesetz (Aufgaben des Bundesamtes)

- (1) Das Bundesamt fördert die Sicherheit in der Informationstechnik mit dem Ziel, die Verfügbarkeit, Integrität und Vertraulichkeit von Informationen und deren Verarbeitung zu gewährleisten. Hierzu nimmt es folgende wichtige im öffentlichen Interesse liegende Aufgaben wahr:

[...]

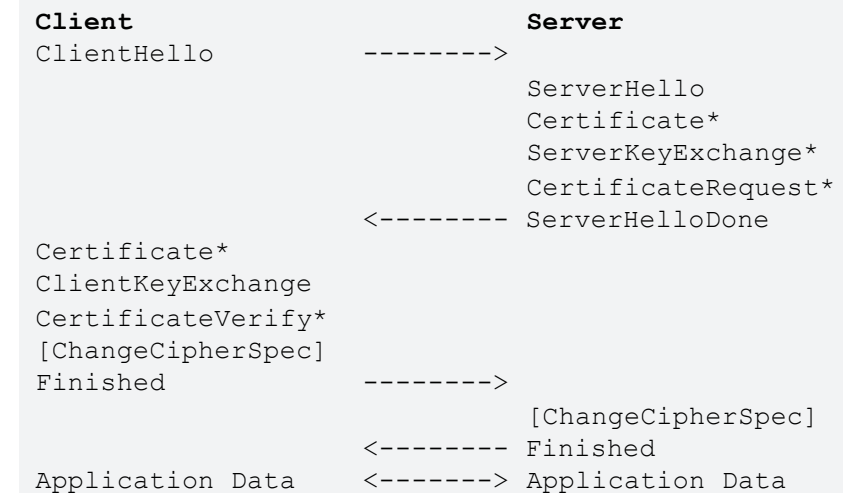
4. Entwicklung von Kriterien, Verfahren und Werkzeugen für die Prüfung und Bewertung der Sicherheit von informationstechnischen Systemen oder Komponenten und für die Prüfung und Bewertung der Konformität im Bereich der IT-Sicherheit;

[...]

- Verbindlichkeitscharakter ergibt sich aus zusätzlichen spezialgesetzlichen Vorgaben

TLS (Transport Layer Security)

- Client-Server-Modell
 - Einseitige oder beidseitige Authentifizierung
 - Viele Einstellmöglichkeiten
 - Welche TLS-Version wird gesprochen?
 - Welche Algorithmen werden unterstützt?
 - Welche Erweiterungen werden unterstützt?
- Welche Parameter sind sicher?
- Welche Parameter sind unsicher?
- Welche Parameter sind notwendig damit der Gegenpart mich versteht?



TLS 1.2 Handshake Protokoll

TLS-Vorgaben in Technischen Richtlinien

- Allgemeine Empfehlungen in TR 02102
- Fachanforderungen in TR 03116 Kryptographische Vorgaben für Projekte der Bundesregierung
- Anwendungsspezifische Anforderungen in Fach-TRn

Auszug aus der TR-02102

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	0x00,0x9E	[RFC5288]	2029+
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	0x00,0x9F	[RFC5288]	2029+
TLS_DHE_RSA_WITH_AES_128_CCM	0xC0,0x9E	[RFC6655]	2029+
TLS_DHE_RSA_WITH_AES_256_CCM	0xC0,0x9F	[RFC6655]	2029+

Tabelle 1: Empfohlene Cipher-Suiten für TLS 1.2 mit Perfect Forward Secrecy

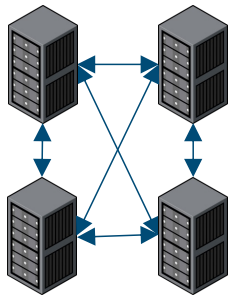
Auszug aus der TR-03116-4

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	2013	2026+
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	2013	2026+
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	2015	2026+
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	2015	2026+

Tabelle 1: Von TLS-Clients mindestens zu unterstützende Cipher Suites

Testen – aber wie?

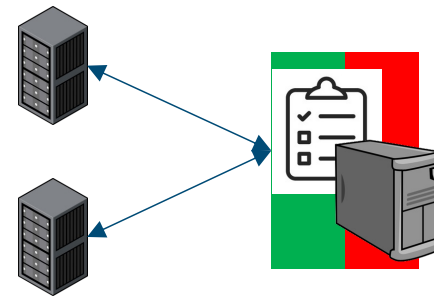
- Crossover-Testen



- Manuelles Testen



Konformitätsprüfung



Automatisiertes Testen

→ Automatisiertes Testtool für Konformitätsprüfung

TR 03116 – TS – eine generische Testspezifikation

- 12 Testfälle für das Implementation Conformance Statement
- 12 Testfälle für Zertifikate
- 30 Testfälle für TLS-Clients
- 26 Testfälle für TLS-Server
- Testfallbeschreibung als XML
- Positiv- und Negativtestfälle

ID	Purpose	Instruction	Profiles
TLS_B1_GP_01_T	This positive test evaluates the ability of the DUT to establish a TLS connection with valid parameters. The test is carried out for the TLS version [TLS_VERSION] and the cipher suite [CIPHERSUITE].	The test MUST be repeated for each combination of TLS version [TLS_VERSION] and non-ECC algorithm [CIPHERSUITE] supported by the DUT for incoming TLS connections.	TLS_SERVER, NO_CLIENT_CERT
TLS_B1_GP_02	This test verifies that the connection is not established if the client offers only cipher suites that are not listed in the ICS.		TLS_SERVER, NO_CLIENT_CERT

TR 03116 – Testspezifikation Annex

- Anwendungsspezifische Profile für Testfall-Mapping
 - TLS-Client
 - TLS-Server
 - eID-Client
 - eID-Server
 - Smart Metering
 - Email-Transport

Mandatory Profiles	Recommended Profiles
CHECK_CERTS ECC ENC_THEN_MAC INTERIM_SUITES_SRV OCSP_STAPLING SERVER_CERT SUPP_GROUPS TLS_1.2 TLS_SERVER	CERTIFIED_CA DURATION NO_COMPRESSION NO_HEARTBEAT NO_RENEGOTIATION NO_TRUNC_HMAC PFS SESSION_ID SESSION_TICKET

Table 2: General TLS server profiles

Projekt TaSK - Testtool für die automatisierte Prüfung der Sicherheit von Kommunikationsprotokollen

- Von der Testspezifikation (www.bsi.bund.de/tr) zum Testtool
 - Projektpartner: achelos GmbH
 - OpenSource (<https://github.com/BSI-Bund/TaSK/>)
-
- Umsetzung der Testspezifikation TR 03116-TS
 - Modulares Testtool
 - Kommandozeilen-Steuerung und REST-API
 - Motivator für das automatisierte Ansprechen von Clients

Architektur und Demo

- Architektur
- Profilierung für vorgegebene und eigene Testobjekte
- Open Source & Schnittstellen
- Community & Services

Wie werden die richtigen Testfälle ausgewählt?

- Implementation Conformance Statement
 - Deklariert die vom DUT unterstützten Funktionalitäten
 - Wird benutzt, um die auszuführenden Testfälle auszuwählen
 - Bestimmt die erforderlichen Parameter für den Test

Implementation Conformance Statement (ICS)

Supported TLS Versions

Table 4: Supported TLS versions

TLS Versions	Supported cipher suites

Table 5: Supported cipher suites

TLS Versions	Supported Elliptic Curves / DH Groups

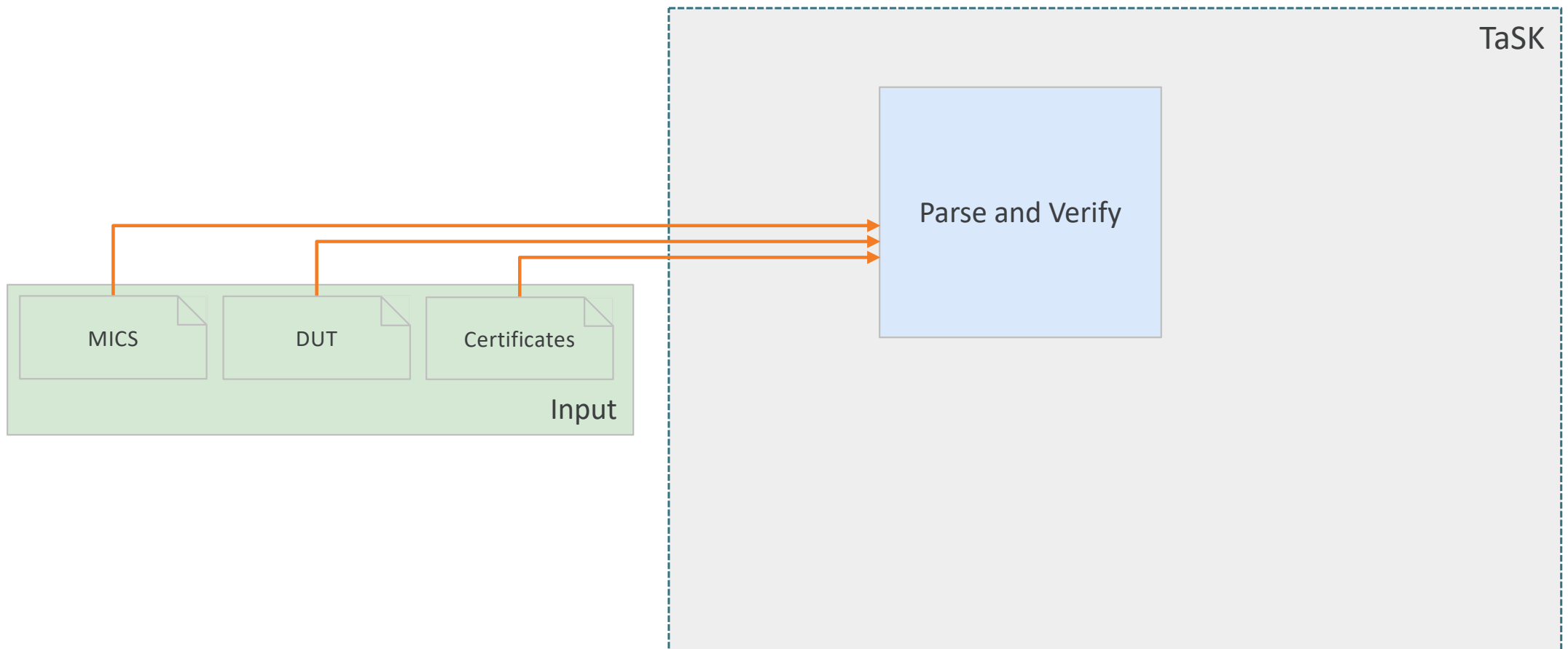
Table 7: Supported Elliptic Curves / DH Groups

TLS Versions	Supported Signature Algorithms

Table 8: Supported Signature Algorithms

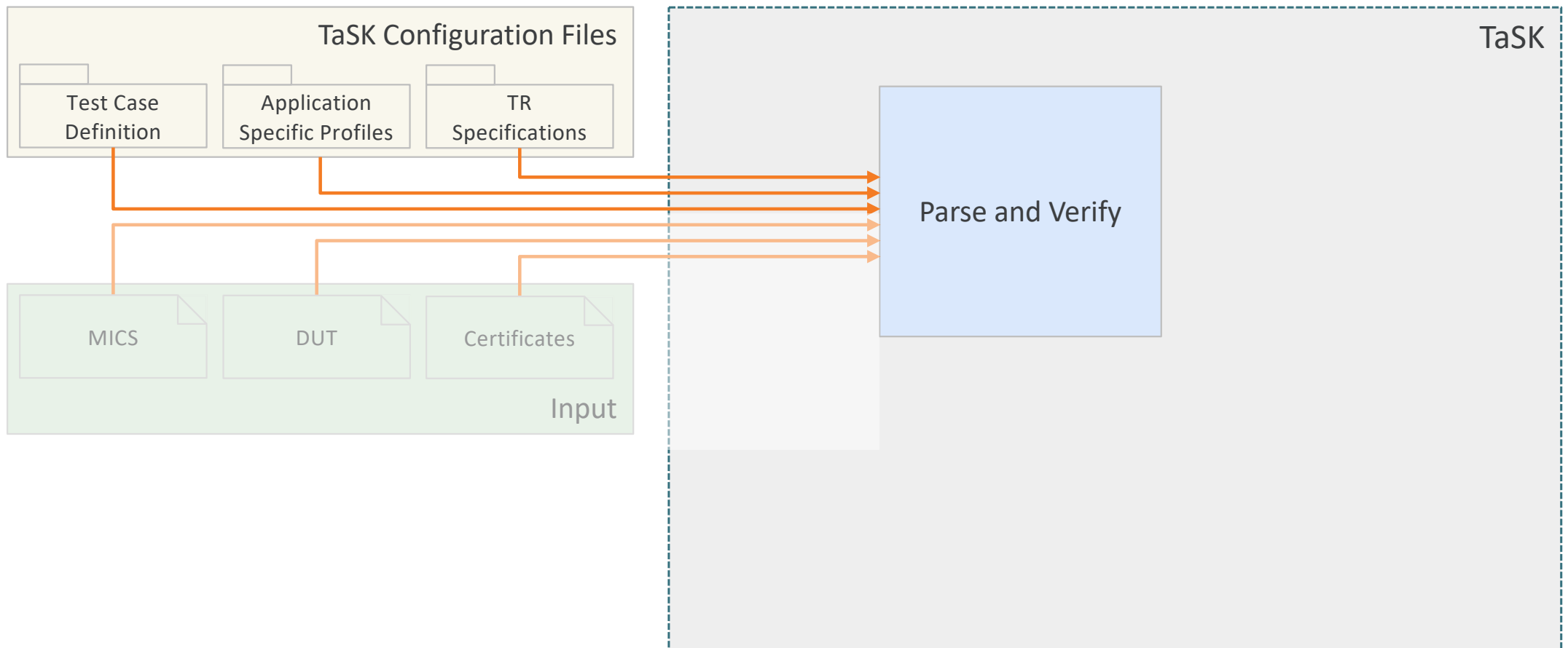
Modulare Architektur

Input Verarbeitung



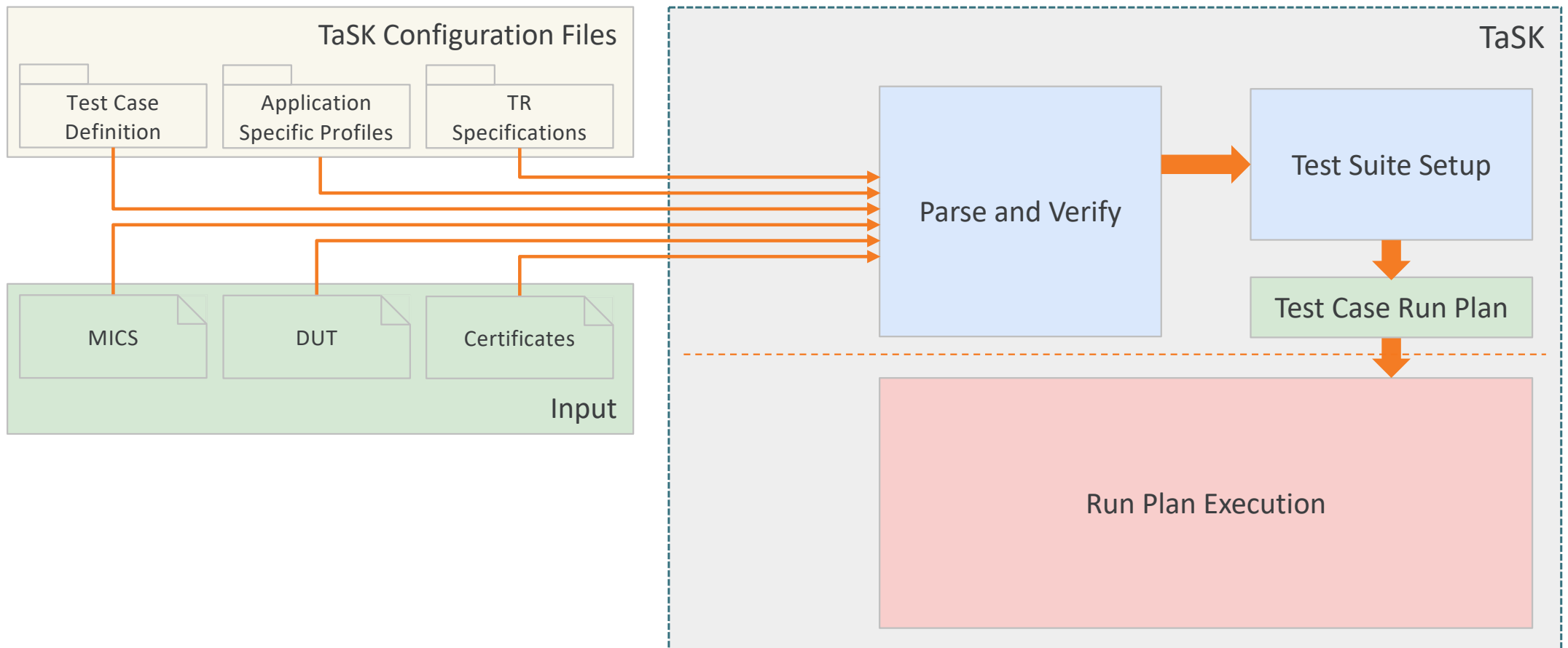
Modulare Architektur

Verarbeitung Spezifikationen



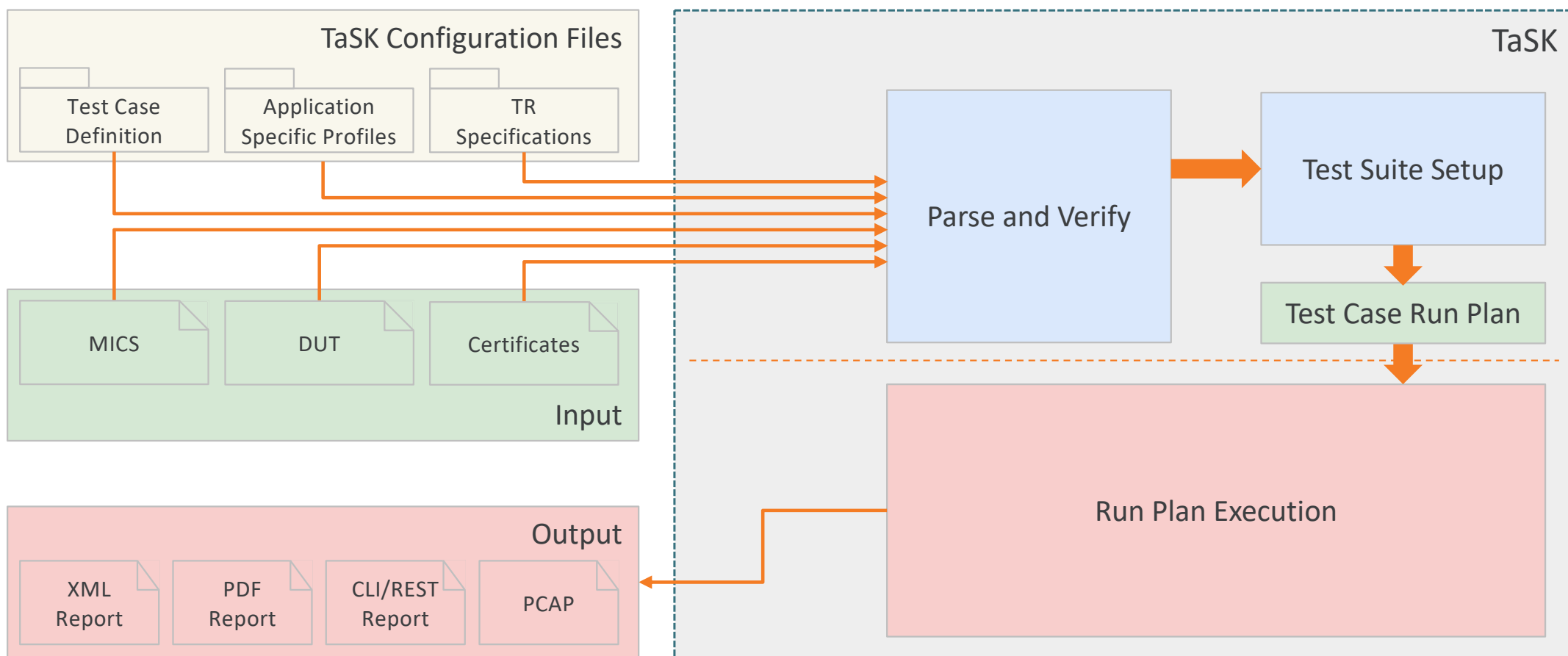
Modulare Architektur

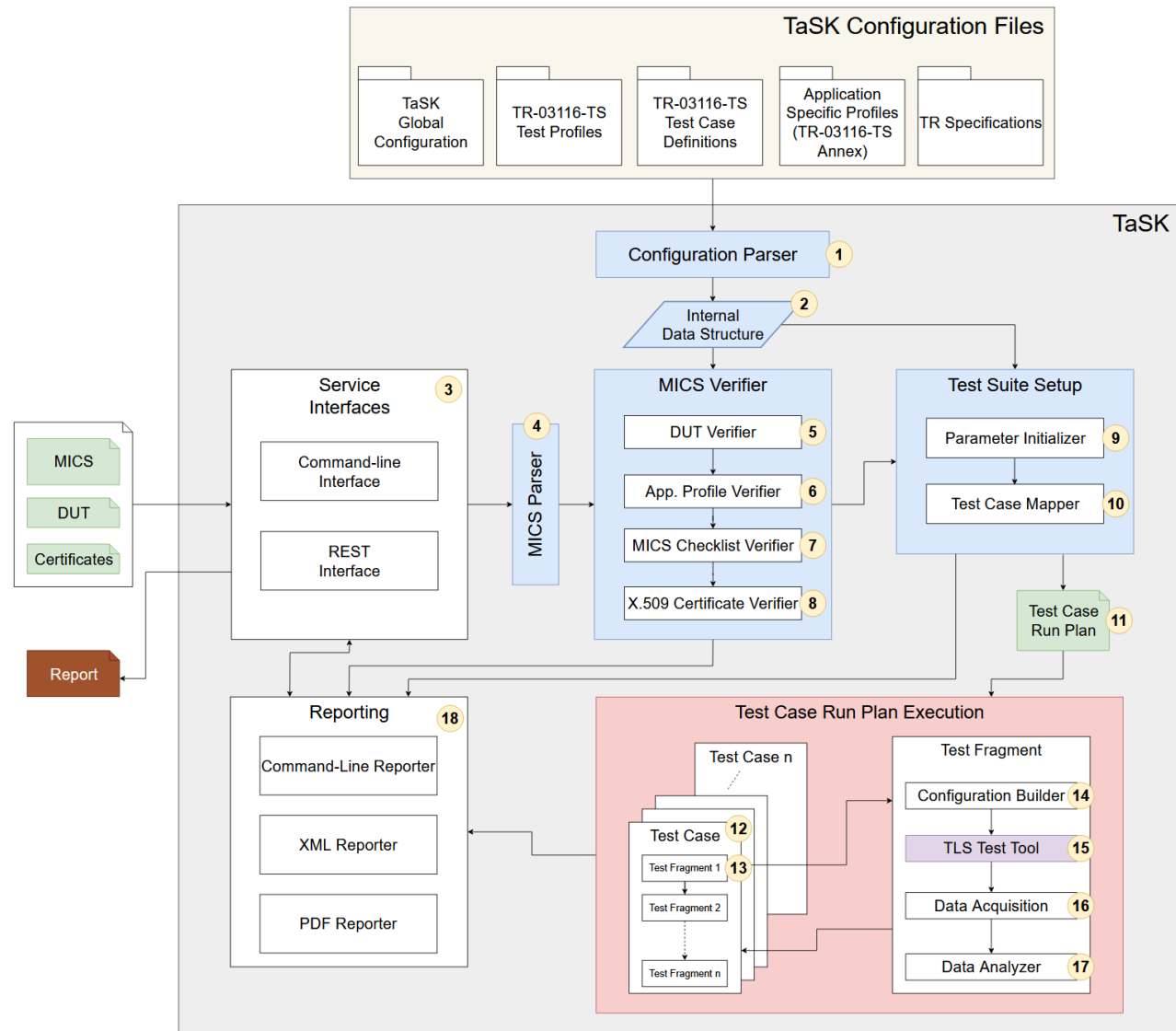
Trennung ICS & Testausführung



Modulare Architektur

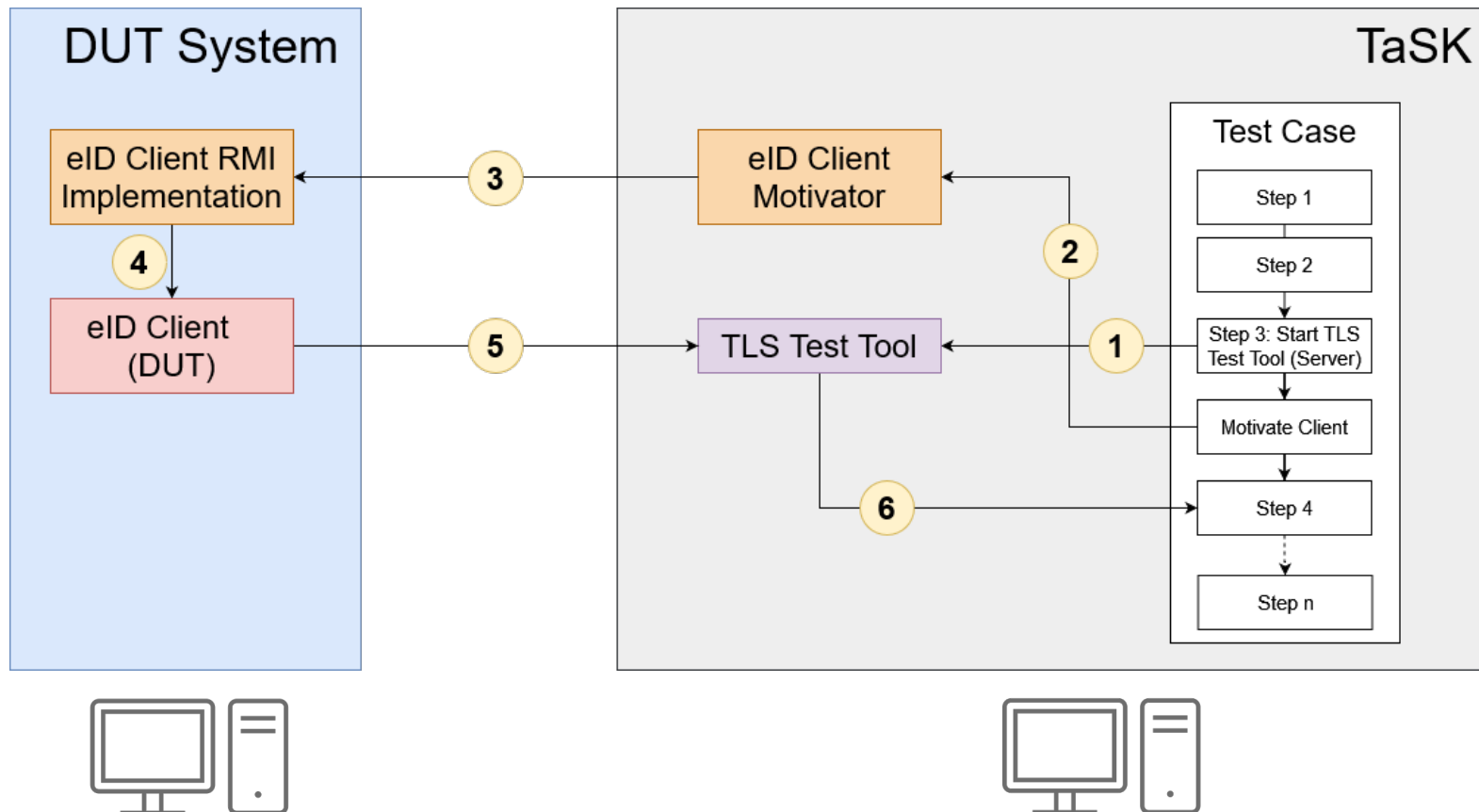
Reports und Logging





Design Entscheidung

RMI Komponenten



Zusammenfassung

- Optimiert auf BSI TR Anforderungen
- Freie Verfügbarkeit als Open Source
- Flexible Nutzung und Integration
- Detaillierte Dokumentation
- Hoher Automatisierungsgrad



Demo

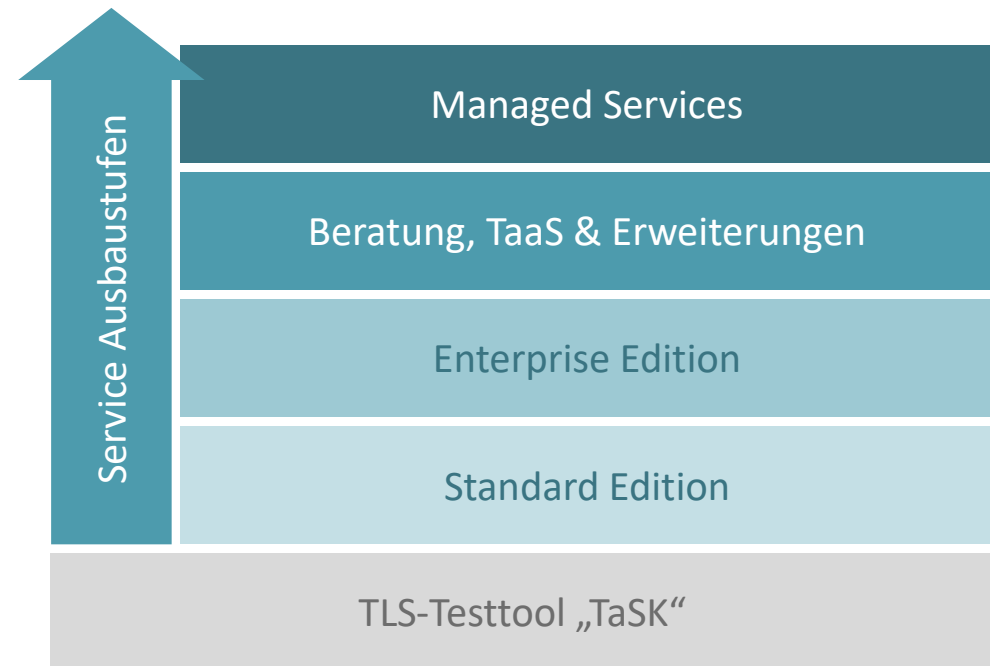


Firmensitz	achelos GmbH Vattmannstraße 1 33100 Paderborn Germany
Geschäftsführung	Kathrin Asmuth, Thomas Freitag
Unternehmen	Herstellerunabhängiges Softwareentwicklungs- und Beratungshaus in Paderborn, gegründet im Mai 2008
Kompetenz	Expertenwissen in verschiedensten Kompetenzen in Kryptographie und Sicherheitstechnologie
Zielmärkte	Security, Health, Industry, Public, Payment, Connect
Angebot	Produkte, Services (Consulting, Security Engineering, Entwicklung, Testen), Produktentwicklungspartner für Embedded Security
Fokus	Übergreifende IT-Sicherheitsthemen und Industrielösungen für den internationalen Markt
Kunden Partner	Staatliche Institutionen, private Unternehmen und Organisationen mit Bedarf an Lösungen für sicherheitskritische Anwendungsfelder

OSS Business Modell / Serviceangebot durch achelos



- Flexibles Serviceangebot
- Unterstützung für
 - individuelle Erweiterungen
 - Bereitstellung neuer Releases
 - Anpassung auf neue Profile
 - Fehlerbehebungen
 - Allgemeiner Support
- Managed Service/
Testing as a Service



Q & A

Dr. Nico Klein (BSI)

Telefon: +49 (0)228 99 9582-6544

E-Mail: nico.klein@bsi.bund.de

Heinfried Cznottka (achelos GmbH)

Telefon: +49 175 2929 021

E-Mail: heinfried.cznottka@achelos.de