TÜVIT

Welche Rolle spielt das Protection Profile bei Vertraulichkeit und Integrität?

Maximilian Wahner | TÜVIT - IT-Security | 30.11.2023

Motivation

Security Policy & Certificate Policy

To support the security requirements of confidentiality, integrity and availability […], C-ITS station operators shall operate C-ITS stations that have been assessed and certified using security assessment criteria against a certified protection profile as specified in the 'common criteria' / ISO 15408 and approved by the CPA. Due to the different features of the different types of C-ITS station and different location privacy requirements, different protection profiles may be defined.

[Security Policy, §25]

[…] All protection profiles and related documents applicable for the security certification of the C-ITS stations shall be evaluated, validated and certified according to ISO 15408, applying the Mutual Recognition Agreement of information technology security evaluation certificates of the Senior Officials Group on Information Systems Security (SOG-IS) , […].

[Security Policy, §26]

The cryptographic module shall be certified with one of the following protection profiles (PPs), with assurance level EAL-4 or higher: […]

[Certificate Policy, §322]

[…] All PPs and related documents applicable for the security certification of the cryptographic module shall be evaluated, validated and certified in accordance with ISO 15408, applying the Mutual recognition agreement of information technology security evaluation certificates of the Senior Officials Group on Information Systems Security (SOG-IS), […].

[Certificate Policy, §324]

Common Criteria

What‘s that?

- Standard for evaluation of IT Security Products

Common Criteria

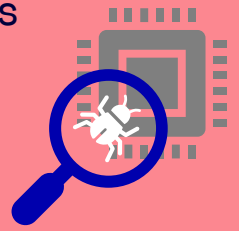
- ISO / IEC 15408

Why?

- State-of-the-Art Standard
- Flexibility
- Recognition

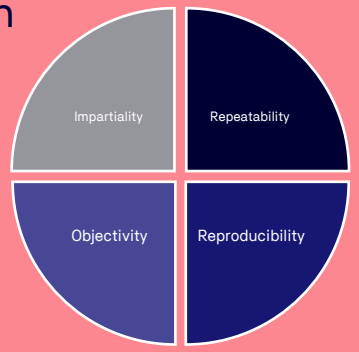
Objective

- Confidence in evaluated IT Products



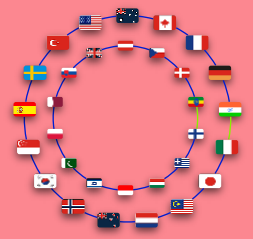
Achievement

- Independent & Overseen Evaluation



Properties

- IT Security capability evaluation of products
- Wide IT Security scope
- International recognition arrangement (CCRA) on government level



- Assurance Levelling
- Comparability of results

TÜVIT

Common Criteria

Common Criteria Recognition Arrangement (CCRA)

Objectives & Purpose

- High & consistent standards
- Confidence in certified IT security products & profiles
- Improve availability, efficiency & cost-effectiveness
- Eliminate the burden of duplicating evaluations

International Government Members & Agreement Mark

Status

- Last ratified arrangement status: July 2nd, 2014 (ICCC, 2014)
- Standard recognition up to EAL2+, iTC

Information Technology Security Mutual Recognition Agreement (SOGIS)

Objectives & Purpose

- In response to the EU Council Decision of March 31st 1992 (92/242/EEC) in the field of security of information systems, and the subsequent Council recommendation of April 7th (1995/144/EC) on common information technology security evaluation criteria

European Government Members & Agreement Mark

Status

- Last ratified arrangement status: January 10th, 2010
- Recognition up to EAL4 (& EAL7 for specific domains)

TÜVIT

Common Criteria

General Model

Assets

- Information/data stored, processed, and transmitted by IT products

Threats

- Threat agent (e.g. hacker) act adverse (e.g. remotely copying) on assets (e.g. data on HD)

Countermeasures

- Security mechanisms to protect assets & supportive environmental conditions

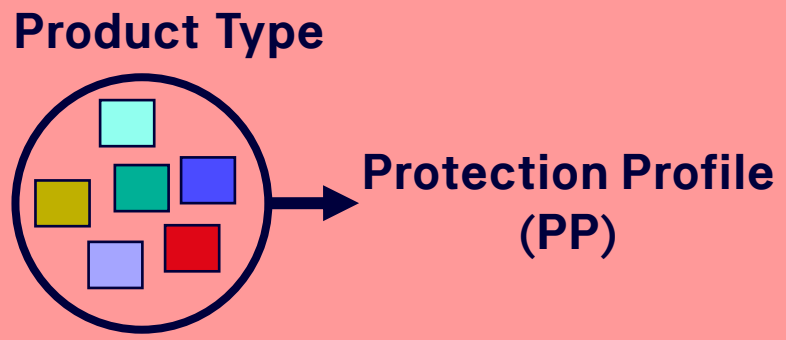
Assurance

- Confidence in Sufficiency & Correctness of countermeasures

Common Criteria

Protection Profile (**PP**)

- **implementation-independent** statement of security needs for a **Target Of Evaluation** (TOE) **type**



- Written by **interest group**
- **Generic** set of security requirements

- Examples (PP) https://www.commoncriteriaportal.org/pps/

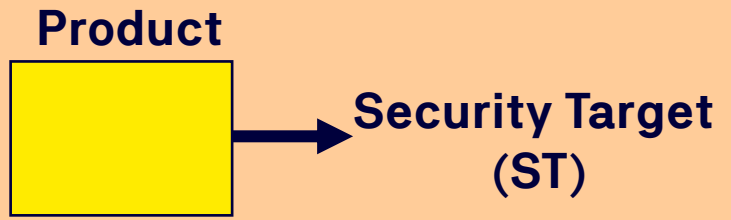
vs.

vs.

vs.

Security Target (**ST**)

- implementation-dependent statement of security needs for a **specific** identified **Target Of Evaluation** (TOE)



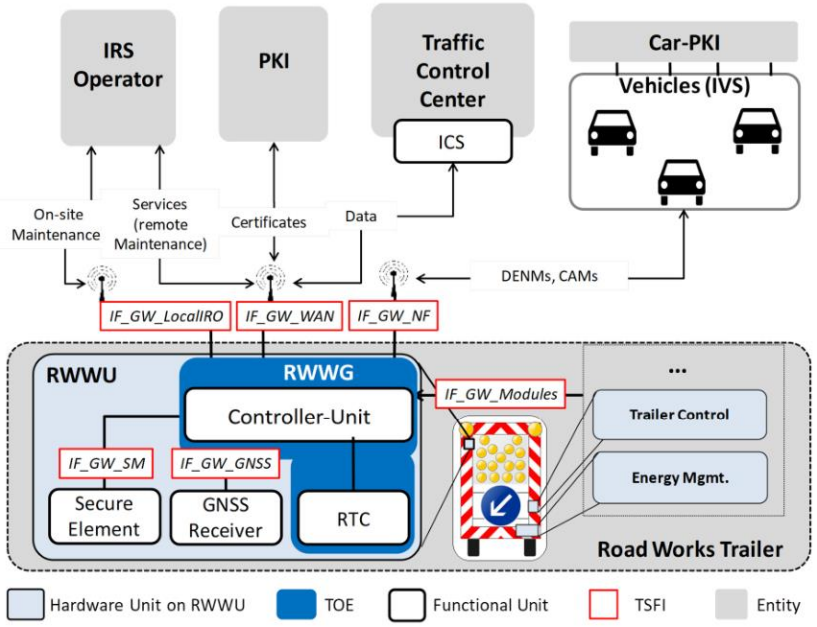
- Written by **product developer**
- **Specific** security requirements

- Examples (ST) https://www.commoncriteriaportal.org/products/##

TÜVIT

Released Protection Profiles

Road Works Warning Gateway – RWWG-PP



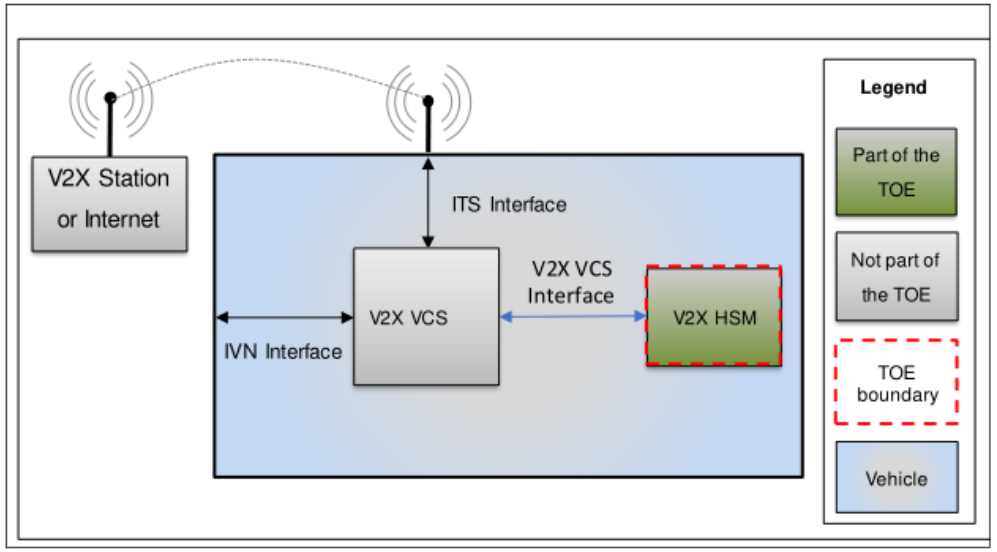
TOE and its Environment

ID	BSI-CC-PP-0106
Issuer	Bundesministerium für Verkehr und digitale Infrastruktur
Release	31.07.2019
TOE	Road Works Warning Unit
EAL	EAL3

Properties	• Specific Context
	• Need of a Secure Element for specific Cryptographic Operations
	• Security Features:
	  • TLS Communication to IRS Operator or TCC
	  • Digital Signature Verification
	  • Secure Firmware Update
	  • Self-Test Possibilities
	  • Audit Generation
	  • Authentication and Identification Mechanisms
	  • Management Functionalities
	  • ...

Released Protection Profiles

V2X HSM – PP



TOE System Overview, External V2X HSM

ID	BSI-CC-PP-0114
Issuer	Car 2 Car Communication Consortium
Release	20.12.2021
TOE	V2X Hardware Security Module
EAL	EAL4+

Properties	• Secure Cryptographic Operations:
	  • Random Number Generation
	  • V2X Key Management
	  • Digital Signature Generation
	  • (User Data) ECIES Encryption/Decryption
	• Self Protection (Physical Attacks)
	• Communication Interface (VCS – V2X HSM)

Not (Yet) Released Protection Profiles

V-ITS-S - PP

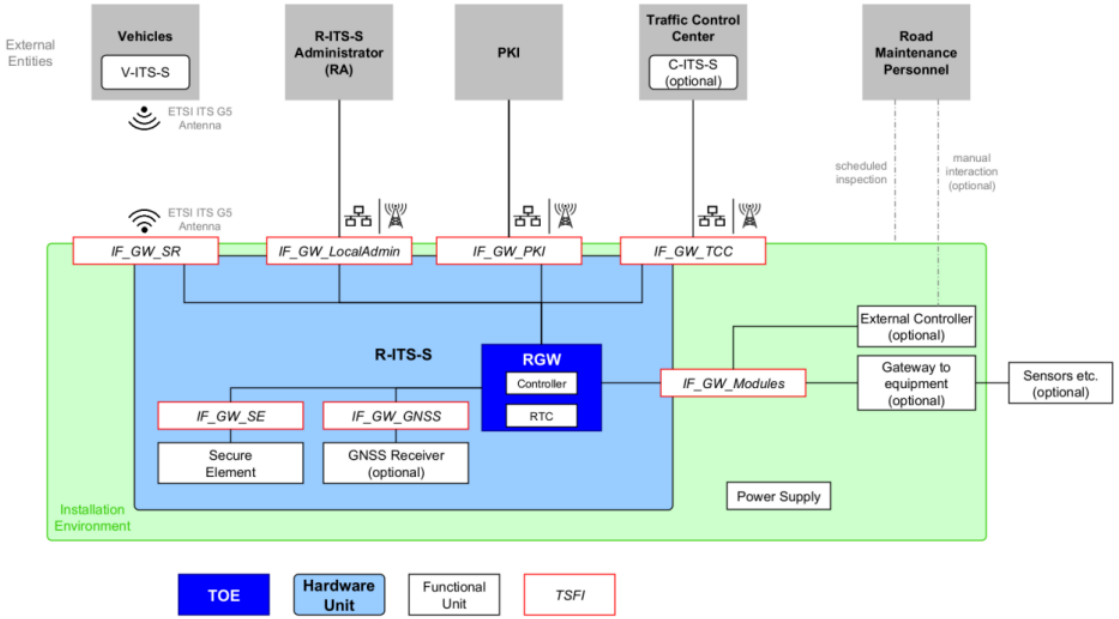
Example of a TOE Overview

ID	???-CC-PP-????
Issuer	Car 2 Car Communication Consortium
Release	TBD (probably end of 2024 or in 2025)
TOE	V2X ITS Station
EAL	TBD (probably EAL3 / EAL3+)

Properties	• Need of a Secure Element for specific Cryptographic Operations
	• Planned Functionality (Draft Status):
	  • Digital Signature Verification
	  • Symmetric Encryption / Encryption
	  • Plausibility Validation
	  • Security Association Management
	  • Enrolment
	  • Authorization
	  • Identity Management
	  • …

Not (Yet) Released Protection Profiles

R-ITS-S - PP



TOE and its Environment

ID	BSI-CC-PP-0122
Issuer	Bundesanstalt für Straßenwesen (BASt)
Release	Early 2024
TOE	Roadsite ITS Station
EAL	EAL3

Properties	• Need of a Secure Element for specific Cryptographic Operations
	• Security Features:
	  • Encrypted Communication to RA, TCC, PKI
	  • Trusted Communication Establishment with the RA, TCC, PKI
	  • Digital Signature Verification
	  • Secure Firmware Update
	  • Self-Test Possibilities
	  • Audit Generation
	  • Authentication and Identification Mechanisms
	  • Management Functionalities
	  • ...

Common Criteria

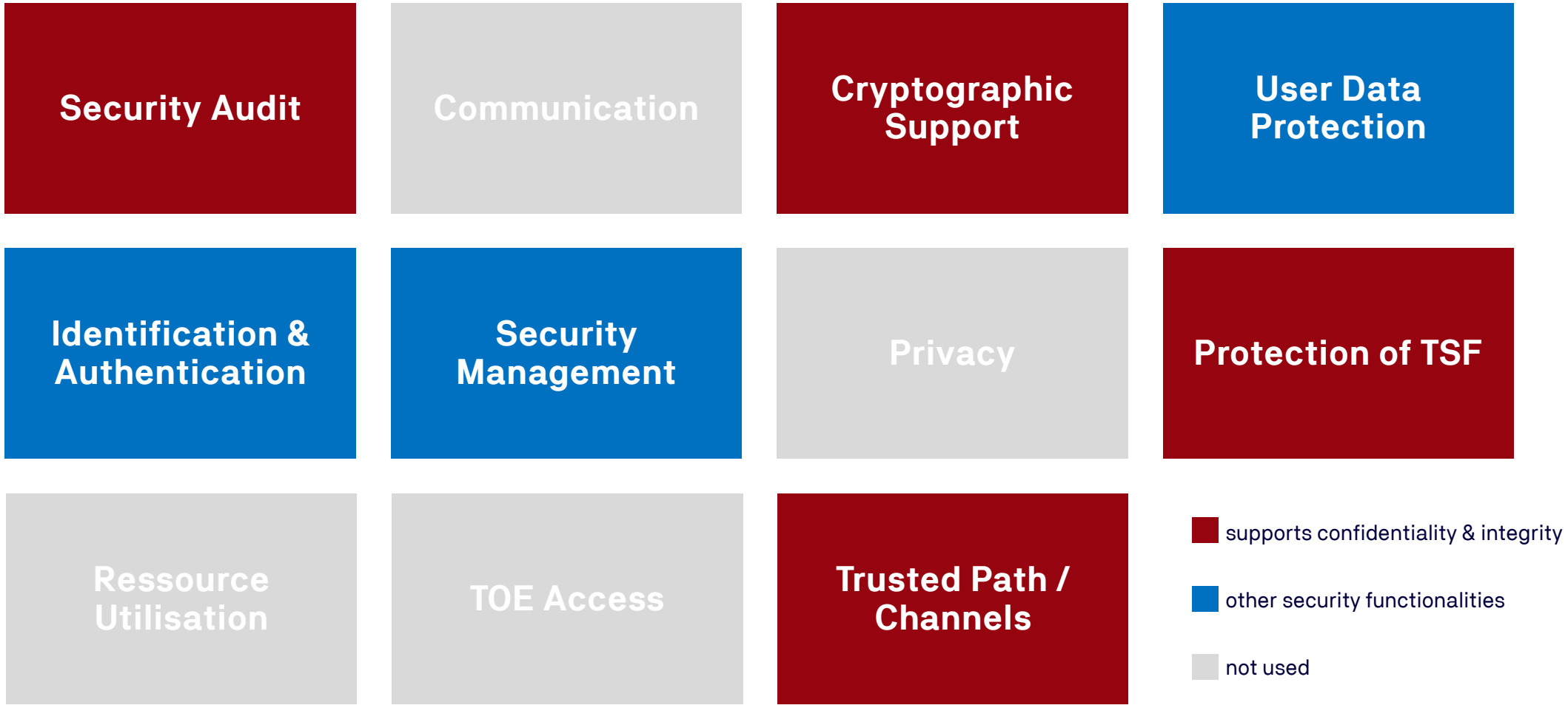
Security Functionality Requirements - Classes

- Security Audit
- Communication
- Cryptographic Support
- User Data Protection
- Identification & Authentication
- Security Management
- Privacy
- Protection of TSF
- Ressource Utilisation
- TOE Access
- Trusted Path / Channels

TÜVIT

Roadsite-ITS-Station – Protection Profile

Security Functionality Requirements - Classes

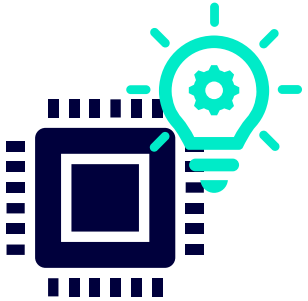


TÜVIT

Confidence in IT Security Products

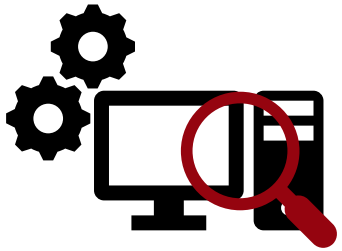
Specification & Documentation Analysis
(ASE / ADV / AGD)

Developer

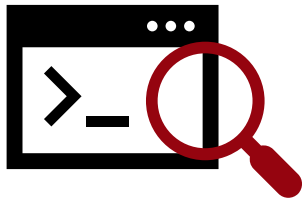


IT Security Product
(Target of Evaluation - TOE)

Life Cycle Support - Audits
(ALC)



Testing
(ATE)



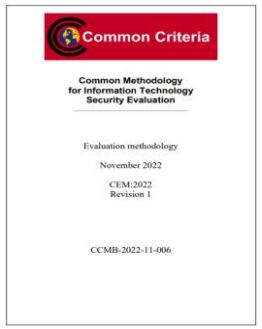
Code Inspection (ADV_IMP)

Vulnerability Analysis
(AVA)

TÜVIT

Common Criteria

Evaluation and Certification

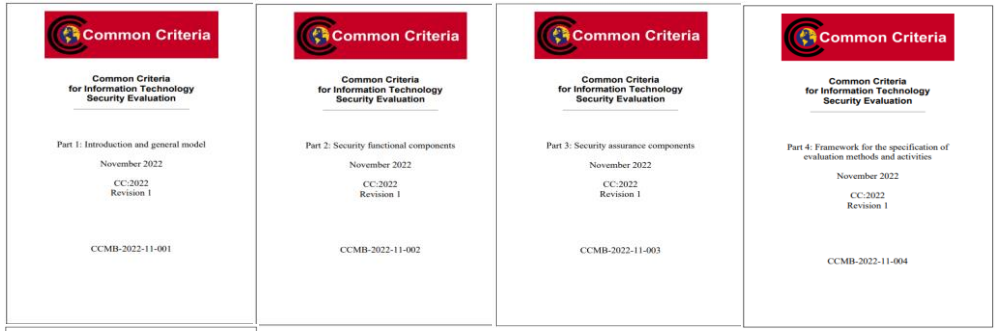


CC **Evaluation Criteria**

CEM **Evaluation Methodology**

Scheme **National Certification Scheme**

PP **Protection Profile**



Evaluation → Evaluation Results → Certification → Certificate

TÜVIT

TÜVIT

Haben Sie Fragen?

Maximilian Wahner

Mail: m.wahner@tuevit.de