EU Project 730843

CYbersecurity in the RAILway sector

D6.1 – Protection Profiles Specifications

Due date of deliverable: 2018-09-30

Leader of this Deliverable: atsec information security AB

Reviewed: AIRBUS

DOCUMENT STRUCTURE

This is a single PDF file containing the four different parts (documents) of the D6.1 deliverable:

- D6.1 – Introduction
- D6.1 – Base Protection Profile
- D6.1 – VLAN-Module
- D6.1 – VPN-Module

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

EU Project 730843

CYbersecurity in the RAILway sector

D6.1 – Introduction

Due date of deliverable: 2018-09-30

Leader of this Deliverable: atsec information security AB

Reviewed: AIRBUS

Document status		
Revision	Date	Description
001	2017-01-25	Staffan Persson, initial draft version for review
002	2018-03-01	Staffan Persson, second draft with more information added.
003	2018-03-18	Staffan Persson, completed chapter 1, 2 and 3, but not section 2.2, 3.4 and 3.5. Chapter 4 is partly done, but chapter 5 is not done.
004	2018-03-29	Markus Engqvist, performed review and minor revisions. Prepared for draft release to CYRail partners.
005	2018-05-17	Markus Engqvist, added to chapter 2, 3 and references. Finalized and prepare document ahead of final draft for internal review.
006	2018-06-18	Markus Engqvist, added related works and PP use cases.
007	2018-08-16	Christophe Ponchel, added “applicability in railway”-section
008	2018-09-04	Markus Engqvist, release version
009	2018-09-25	Markus Engqvist, address review comments
010	2019-02-14	Minor update due to EU review comments

Start date of project: 2016-10-01 Duration: 24 months

This project has received funding from the European Union’s Horizon2020 research and innovation programme under grant agreement No730843

Company	Details of contribution
atsec	This is an introduction and rationale explaining why, what and how the requirements were derived for the Protection Profile. It also explains how the security requirements of the Protection Profile fit in the requirements framework for the railway and how the Protection Profile is supposed to be used in the future.
AIRBUS	Performed review, analysed application in railway and added section 2.4.4.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

OBJECTIVES OF THE DELIVERABLE

In **D6.1 – Protection Profiles Specifications** a Common Criteria Protection Profile has been developed following Common Criteria (ISO/IEC 15408) and guides (ISO/IEC TR 15466). It is intended for components used in scenarios described in WP2 and used for components in an overall system security accreditation using a methodology described in WP3. The Protection Profile addresses threats and security objectives identified in WP4 and specifies requirements for security measures identified in WP5.

This introduction to the Protection Profiles should provide the context for the Protection Profiles. It should help the reader both to understand why we did this work, how we ended up with these requirements and how the Protection Profiles are supposed to be used.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

TABLE OF CONTENTS

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

LIST OF FIGURES

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

LIST OF TABLES

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

1. INTRODUCTION

This document is part of the deliverable D6.1 Protection Profile within the CYRail project.

It is an introduction and rationale explaining why, what and how security requirements were derived for the Protection Profile. It also explains how these security requirements fit into the requirements framework for the railway and how the Protection Profile is supposed to be used in the future.

The Protection Profile is a major deliverable from the CYRail project, building on the results of previous work packages. In general, a Protection Profile specifies the security requirements for a certain type of product. This Protection Profile specifies the requirements for the network components that shall ensure domain separation and protection of network traffic.

This introduction document is intended to improve the understanding for the CYRail project deliverable as well as making the Protection Profile both more accessible and easier to use.

The remainder of this document is structured as follows:

- **Overview** (chapter 2)
  An overview of the background to the CYRail project, explaining the security problem we see and how we are addressing it in the context of railway operations. It is also a summary of the specific approaches, methods and standards used by the CYRail project to analyse and meet these security problems. This chapter will also refer to what has been done in the different Work Packages and how it has contributed to WP6.
- **Protection Profiles Description** (chapter 3)
  A description of what an ISO/IEC 15408 Protection Profile is and how it can be used when evaluating products that are claiming compliance with the modular Protection Profile. How this Protection Profile and its Protection Profile modules will fit together with other Protection Profiles. It will also be explained how the security requirements have been derived for the Protection Profile and Protection Profile modules created within CYRail project.
- **Common Criteria and 62443** (chapter 4)
  How it is intended to be used in the context of system development and system accreditation, such as the ISA/IEC 62443.

The following Protection Profiles were developed as part of the CYRail-project under European Union's Horizon 2020 research and innovation programme (grant agreement no. 730843):

- Base Protection Profile for Network Separation Mechanisms
  Version 009, 2018-09-25;
- Protection Profile for Network Separation Mechanisms, VLAN Module
  Version 005, 2018-09-25; and
- Protection Profile for Network Separation Mechanisms, VPN Module
  Version 005, 2018-09-25.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

2. OVERVIEW

2.1 NEW SECURITY ISSUES

Traditionally IT systems were separated systems using proprietary protocols and components. Safety and reliability were key properties of these systems, but security largely relied on the fact that they were physically and logically isolated, composed of dedicated products using special protocols. This has now changed and is changing in the railway together with many other sectors. Since some years many industries have undergone a digital transformation that may be characterized as follows:

- **Connectivity**
  IT systems and components that used to be isolated are being connected with other IT systems and networks.
- **Shared resources**
  Shared resources, such as communication channels are no longer proprietary and exclusive used but shared with other services or types of users.
- **Standard components and protocols**
  Instead of using proprietary technology and protocols, commercial standard components and standard protocols are being used.

From a security point of view, this presents new risks. It gives attackers an advantage by enabling access to IT systems that are unprotected, or at least unable to protect themselves against active attacks. This also gives attackers the advantage of knowing the technology for which there are many publicly available exploits. Using standard components may also present larger attack surfaces for an attacker, as these components now provide more services than the previous dedicated IT components. Increased use of the IP protocols may also present the possibility for attackers to more easily traverse networks.

Using exposed standard components also puts a lot of constraint on the operators to patch and maintain such an environment. Processes that previously may not have been necessary.

The availability of standard commercial products will reduce the cost of components but may lead to unclear supply chains. Other businesses, such as telecom, the car industry, industrial processing systems, the energy sector, home automation, etc. are all experiencing this transition and are suffering from security and safety issues due to this.

To solve the new security issues, it is not realistic or even possible to completely replace or redesign existing IT systems and IT infrastructure. Nor is it possible to quickly change the management processes to what be required for such new IT infrastructure. What the CYRail project is aiming for is to help this transition through a methodical diagnosis and specification process. Starting with identifying the scenarios, followed by performing risk and threat analysis, identifying the mitigation strategies and security measures, and by pointing to international standards that have been developed for other industries, such as industrial systems. More specifically, we will identify how to minimize the attack surfaces and by isolation and separation of a system into security zones, and by using the concepts of the MILS architecture. We then turned the general need for separation into separation requirements for products by developing a number of Protection Profile modules for networks separation, and by pointing to Protection Profiles for host-based separation.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

CYRail project summary 1: Security issues

The security issues of the rail were further identified in the CYRail deliverables D2.1, D2.2, D3.2 and D4.1:

- D2.1 detailed the current safety and security requirements of current rail transport systems.
- D2.2 describes a realistic railway scenario that helps visualize the possible vulnerabilities or problems that may arise as a consequence of the digital developments within the railway.
- D3.2 works with the scenario to assess the risks and divide the scenario into security zones. This identifies the security problems that exist and their location. The deliverable builds upon an assessment methodology developed in D3.1
- In addition to the earlier deliverables, D4.1 identifies additional threats based on a study of previous security incidents in the railway together with other sectors.

Many security issues that the railway industry is facing are not unique. Therefore, many products used by the railway business are not going to be unique either. We have looked at other industries to see how they are identifying and addressing these issues, to see if similar solutions could be applicable also for rail.

Industrial Control Systems and SCADA

ENISA has in the report *Protecting Industrial Control Systems Recommendations for Europe and Member States* [1] identified that critical infrastructures, such as electricity generation plants, transportation systems, oil refineries, chemical factories and manufacturing facilities are large, distributed complexes. Plant operators must continuously monitor and control many different sections of the plant to ensure its proper operation.

During the last decades this remote command and control has been made feasible due to the development of networking technology and the advent of Industrial Control Systems (ICS). ICS are command and control networks and systems designed to support industrial processes. The largest subgroup of ICS is SCADA (Supervisory Control and Data Acquisition) systems.

ICS have passed through a significant transformation away from proprietary, isolated systems to open architectures and standard technologies highly interconnected with other corporate networks and the Internet. Today ICS products are mostly based on standard embedded systems platforms, applied in various devices, such as routers or cable modems, and they often use commercial off-the shelf software. All of this has resulted in reduction of costs, increased ease of use, and enabled remote monitoring and control. However, an important drawback derived from the connection to intranets and communication networks, is the increased vulnerability to computer network-based attacks.

The ENISA report [1] identifies in section 6.11.2 that legacy devices were often designed under some assumptions, such as that "devices are isolated", or "these systems are only understood by a small number of experts". After the previously mentioned transformation, these assumptions are no longer true. Built-in security is the best approach for protecting these systems, but for economic reasons a compensating, multi-layer approach is being implemented in most networks. The situation is worsened by the fact that ICS technologies lifecycle is much longer than the usual ICT lifecycles. As a result, many current ICS systems may remain vulnerable for longer.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

The CYRail project has identified and focused on these issues by separation and reduction of attack surfaces by using the MILS approach.

Automotive

The automotive industry is undergoing a structural change with connected drive and autonomous driving. The European Automobile Manufacturers Association (ACEA) recognizes that there are also security risks associated with these developments and have published "*six key principles to enhance the protection of connected and automated vehicles against cyber threats*" [2].

To stay ahead of cyber threats, in 2015 the automotive industry established an Automotive Information Sharing and Analysis Center (Auto-ISAC).

The Auto-ISAC Alliance has identified the following key cybersecurity functions as best practice [3] and refer to a number of relevant standards:

- **Governance**
  It leverages guidelines included in *ISO/IEC 27001—Information Security Management* and other cybersecurity management references.
- **Risk assessment and management**
  It leverages *NIST 800-30: Guide for Conducting Risk Assessments* and other established resources.
- **Security by design**
  It leverages *SAE J3061: Cybersecurity Guidebook for Cyber-Physical Vehicle Systems*, *NIST 800–64: Security Considerations in the Systems Development Lifecycle*, *NIST SP 800–121 Guide to Bluetooth Security*, *NIST SP–127: Guide to Securing WiMAX Wireless Communications*, *ISO 17799: Mobile Phone Security* and other established resources
- **Threat detection and protection**
  It leverages *NIST 800–137: Information Security Continuous Monitoring for Federal Information Systems and Organizations*, *ISO/IEC 30111: Vulnerability Handling Procedures* and other established resources
- **Incident response**
  It leverages *NIST SP 800–61: Computer Security Incident Handling Guide*, *ISO/IEC 27035:2011 Information security incident management* and other established resources.
- **Awareness and training**
  It leverages *NIST SP 800–50: Building an Information Technology Security Awareness and Training Program* and other established cybersecurity training resources
- **Collaboration and engagement with appropriate third parties**
  It leverages *NIST SP 800–150: Guide to Cyber Threat Information Sharing*, *ISO/IEC 27010:2012 - Information security management for inter-sector and inter-organizational communications*, and other established resources.

The automotive industry defines that best practices for security by design should consider:

1. Consider commensurate security risks early on and at key stages in the design process
2. Identify and address potential threats and attack targets in the design process
3. Consider and understand appropriate methods of attack surface reduction
4. Layer cybersecurity defences to achieve defence-in-depth
5. Identify trust boundaries and protect them using security controls
6. Include security design reviews in the development process
7. Emphasize secure connections to, from, and within the vehicle
8. Limit network interactions and help ensure appropriate separation of environments

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

9. Test hardware and software to evaluate product integrity and security as part of component testing
10. Perform software-level vulnerability testing, including software unit and integration testing
11. Test and validate security systems at the vehicle level
12. Authenticate and validate all software updates, regardless of the update method
13. Consider data privacy risks and requirements in accordance with the Consumer Privacy Protection Principles for Vehicle Technologies and Services

Several of them are principles that are supported by the MILS approach taken by CYRail project and described in WP5. Especially item 3 (attack surface reduction), item 4 (layered security and defence-in-depth), item 5 (identification and protection of trust boundaries) and item 8 (Limit network interactions and ensuring separation).

What we can see is that the automotive industry not only has the similar problems as the rail industry, but that they are taking a similar approach and to a large extent are relying on the same standards for doing this.

Aviation

The aviation industry is somewhat similar to the automotive and railway industry in that it used to have the security of legacy components and systems build upon the assumption that they are isolated. Now, these are connected to the other systems and networks, quite often also with the entertainment systems. At the same time, they must meet high safety and security standards.

In a report from Pete Cooper, Atlantic Council senior fellow, Cyber Statecraft Initiative [4], states that with increased digitization and connectivity, new levels of vulnerability arise. Moreover, he also sees similarities with other industries:

> *This study indicates that the aviation industry will likely experience cybersecurity challenges similar to other industries that have embraced the "digital revolution." As the industry moves forward, will it be able to maintain stakeholder trust by accurately perceiving the risks and opportunities as well as understanding adversary threats?*
>
> *Previously, aviation systems were relatively secure due to the bespoke nature of their design, isolation from other systems, and little in the way of communication protocols.*
>
> *[…]*
>
> *In addition, cyber adversaries and their capabilities evolve and adapt quickly. This may be particularly challenging for an industry where many of the systems have long design and development periods. As technology radically transforms design, production, operation, and maintenance of aircraft, models of safety and security must adapt.*

The report finishes with the conclusion that:

> *There is much the cybersecurity industry can learn from aviation. Managing safety in the face of complex risk has been culturally ingrained into aviation for many years. Achieving this has taken rigorous objectivity and both individual and shared responsibility and accountability. As organizations seek to exploit the opportunities of a connected aviation industry, they must retain the ability to be objective about both the benefits and risks. Innovative connected technologies, if sympathetically and securely integrated, can assist in efficiency and safety, but this must not be at the cost of unknown or unacceptable risk.*

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

ENISA has published a report on Securing Smart Airports [5]. Although most of the report is Airport specific, some information is relevant also for other industries. Section 9.6 provides a table of "Detailed security good practices" GP 01 to GP 44. Among them there are some good practices that are similar to what we in CYRail are adopting for defence in depth. One example is the good security practices GP 11:

> *GP 11 – Firewalls, network segmentation, and defence in depth:*
>
> *[…]*
>
> *A defence in depth approach should be taken to improve network security by further restricting traffic between network segments and hosts: for example, using VLANs for traffic separation, firewalled segmentation, and end-point controls. Separation of airport functions communications should be enforced. Defence in depth is an important security concept, as it can limit the impact of a breach in a specific control: additional layers of communication security, such as authenticated secure communications (such as, HTTPS) should be employed, combined with the multitude of best practices, including least privilege.*

From the aviation side, we can see that we not only have similar security issues, but also similar approaches for the security solutions. Even if the aviation industry cannot provide any direct solutions, we can confirm that the issues identified and the approach taken by CYRail is very similar to what the aviation industry is looking for.

2.2 Different Security Approaches

There are two different security approaches taken by CYRail project. The first one is the separating and containing legacy systems and components. This approach is necessary for the protection of legacy systems, that may otherwise have no way to mitigate threats.

The second approach is to move from legacy components by promoting an architecture that supports separation, monitoring and defence-in-depth. Applications and systems should be able to make full use of this architecture to facilitate effective management and monitoring within such a framework.

There are also other projects that, while sharing some similarities, are different and in turn yield different results than those of the CYRail project.

2.2.1 The MILS Approach

Multiple Independent Levels of Security (MILS) [6] [7] is a high-assurance security architecture based on the concepts of separation and controlled information flow. The cornerstone of the MILS-architecture is a separation mechanism that encapsulates trusted and untrusted applications in compartments that reduce mutual dependencies to communications over channels explicitly defined by policies. This key component has to be non-bypassable, evaluable, always invoked, and tamperproof (NEAT). This MILS concept can not only be applied at host level for separating application, but also be applied to the network communication by separating communication, either at physical, data-link, internet or application level by combining different technologies.

The principles of MILS go back to the concept of separation kernels, described over 30 years ago, such as [8]. At that time separation kernels were mainly an issue for the national security, i.e. red-black separation and controlled information flow (e.g., Bell-LaPadula) this later become relevant also in other areas [9], as well as in civilian and commercial sector [10].

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

This MILS approach is also used by the US program, Commercial Solutions for Classified (CSfC) that NSA has implemented [11]. Not only should the program provide multiple layers of defence, but also enables commercial products to be used in layered solutions to protect classified NSS information. This provides the ability to securely communicate, based on commercial standards, with a solution that can be fielded in months, versus years. For more information see https://www.nsa.gov/resources/everyone/csfc/.

This approach is implemented by specifying so called Capability Packages (CP) that describes how to implement this layered approach for specific type of solutions. An example given by the CSfC program is the Mobile Access CP [12] that describes how to protect classified transiting wired networks, domestic cellular networks and trusted wireless networks to include government private cellular networks and government private Wi-Fi networks.

> *This CP describes a general Mobile Access (MA) solution that protects classified information as it travels across either an untrusted network or a network consisting of multiple classification levels. This solution supports connecting end-user devices to a classified network via two layers of encryption terminated on the end-user devices provided that the end-user devices and the network operate at the same security level. The MA solution uses two nested, independent tunnels to protect the confidentiality and integrity of data (including voice and video) as it transits the untrusted network. The MA solution utilizes Internet Protocol Security (IPSec) as the outer tunnel and, depending on the solution design, IPsec or Transport Layer Security (TLS) as the inner layer of protection.*

Following this layered approach, we would achieve the following:

- Attack surface reduction – The attack surface will be reduced to specific layers and services visible at this layer. This means that the opportunities for an attacker will be reduced to what is visible at that layer.
- Layered security and defence-in-depth – Having multiple layers means not having to rely on a single layer for protection. If one layer becomes compromised we can still maintain the secure operation of the remaining system, which is protected by separate layers. By using monitoring and detection mechanisms we can also detect attacks before the whole system is at risk. This would allow for trusted recovery.
- Identification and protection of trust boundaries – The use of a layered approach offers the benefit of having clearly defined boundaries between the layers. This would provide a general protection against trust boundaries. In a contrasting single layer approach, each boundary would have to be defined to the whole system, and not only between two layers.
- Limit network interactions and ensuring separation – A layered approach also limits benign network interactions between components in a system. For critical infrastructure, unexpected network behaviour or congestion could pose operational issues. The separation ensures that services only communicate between each other as intended.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

CYRail project summary 2: MILS approach

Building upon the identified security issues of earlier deliverables, the MILS approach of the rail is specified in the CYRail deliverables D3.2, D5.1 and D5.2:

- D3.2 identifies the security zones and conduits together with their security levels. It also identifies the security requirements for each of these, describing different security levels which could be resolved through a layered approach.
- D5.1 identifies the MILS approach as the main mitigation strategy of large interconnected systems such as rail infrastructure.
- D5.2 describes how a layered approach can increase the resilience of systems in the event of a security incident.

The CYRail MILS approach is implemented for network communications. In critical infrastructure, there is a need for both host-based and network-based separation. CYRail deals with large distributed systems where critical communication between components is performed via computer networks. Untrusted services or users may also use these very same networks. Because of this, we have focused on MILS implementations for networks. Besides this document, the other half of deliverable will be the specification of Protection Profiles which can then be used when implementing this network MILS architecture. There is also current ongoing work being done regarding host-based separation in the form of separation kernels.

2.2.2 The Monitoring and Management Approach

CYRail defines conventional threats and implements countermeasures against them. However, no system can be guaranteed to be fully secure. For critical infrastructure we must anticipate that security issues will arise or that attacks will take place. Measures can then be defined that respond to such security events. CYRail adopts such a mindset and defines ways to both detect such events via monitoring, and to mitigate them through vulnerability management.

The monitoring refers to detecting vulnerabilities and attacks. CYRail studies the possible threats to the railway to accurately define attack and anomaly detection. The implementation of logging and Intrusion Detection Systems (IDS) are recommended, however also the use of ways to collect data about captured event and organize them.

The management refers to the ability to respond to incidents and manage the systems. When an issue is detected the system should respond accordingly. CYRail defines solutions that responds to events detected through the monitoring. Among other things CYRail presents ways to analyse and respond to any incidents. Most prominently through the specification of an alerting and incident management solution for the railway. Finally, resilience mechanisms are

CYRail project summary 3: Monitoring and management

The monitoring and management of the rail were further identified in the CYRail deliverables D4.2 and D4.3:

- D4.2 presents a study of state-of-the-art attack and anomaly detection which specifies techniques that would be applicable to railway infrastructure.
- D4.3 identifies the importance alerting and incident management. The design of a complete monitoring and incident response solution is presented for the rail scenario.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

defined to be able to recover from any incidents with minimal operational impact.

2.2.3 Related Works

There are also other approaches which could be considered to help mitigate these new security issues. These were also considered when deciding the scope of the Protection Profile, as we do not want multiple disparate Protection Profiles that could possible confuse and fragment the userbase. Below, we have compiled a brief study of some such projects and explained both similarities and differences between them and CYRail.

TAPPS – Trusted Apps for open CPSs

TAPPS is an EU-funded project in Horizon2020. The goal is summarized below:

> *"The main goal of the TAPPS project is to extend and customize CPS devices with new 3rd party services and features in an Apps platform in an efficient, secure and trusted way. TAPPS goes beyond traditional solutions for safety, security and reliability in the CPS domain and offers a new approach towards extensibility of CPS platforms."*

D-MILS – Distributed MILS

D-MILS is an EU-funded project in FP7. The goal is summarized below:

> *"The objective of the D-MILS is to provide an environment for the design, analysis, verification, compositional implementation and certification of scalable, interoperable, and affordable trustworthy architectures. D-MILS uses an advanced time-triggered network architecture for communication among its nodes, providing, predictable, deterministic behaviour for safety-, security-, and enterprise-critical operation."*

EURO-MILS

EURO-MILS is an EU-funded project in FP7. The mission is summarized below:

> *"To develop a solution for virtualisation of heterogeneous resources and provide strong guarantees for isolation of resources by means of Common Criteria certification with usage of formal methods."* [6]

Similarly, to CYRail, EURO-MILS mentions the increased interconnectivity of services within critical domains, such as the next generation of aviation and automotive. However, the focus of the project is not networks within larger infrastructures, but rather on virtualisation of embedded systems. EURO-MILS presents the need for secure isolation between virtual partitions, where Common Criteria is used to enable ways to validate the isolation.

As one of the results from EURO-MILS is a draft of a Protection Profile for separation kernels, the project is relevant to CYRail and WP6 which also result in a Protection Profile. However, the Protection Profile of CYRail is focused on separation of network traffic.

certMILS

certMILS is an EU-funded project in Horizon2020. The mission is summarized below:

> *"certMILS develops a security certification methodology for Cyber-physical systems (CPS). CPS are characterised by safety-critical nature, complexity, connectivity and open technology. certMILS aims to increase the economic efficiency and European competitiveness of CPS development, while demonstrating the effectiveness of safety & security certification of composable systems."* [7]

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

certMILS is based on the work in the EURO-MILS project. Providing secure isolation through virtualization to mitigate the new cyber threats within critical infrastructure. Transportation, including railway, is mentioned as one increasingly networked industry where the project will be applicable. Certification and evaluation are also a focus, and the project develops guidelines and methodologies for this.

The result of certMILS is the Protection Profile for separation kernels, which adopts a modular approach similar to CYRail where users are able to select their desired separation functionality.

2.3 Security Standards and Security Requirements

There are a number of different security standards. Most of them are not competing standards, but rather complementary standards covering different aspects of security and intended for different types of users.

The security standards mentioned in the CYRail project are the following:

- ISO/IEC 27000 series
- NIST SP-800 series
- ISA/IEC 62443 series
- ETSI standards, such as ETSI TS 102
- ISO/IEC 15408, also known as Common Criteria
- ISO/IEC 18045, also known as CEM

A short overview of these standards is provided below.

2.3.1 ISO/IEC 27000

ISO 27000 is a series of standards for Information Security Management Systems (ISMS). The series should provide best practice recommendations on the management of security risks through risk assessment, information security controls and continuous improvement, similar to the quality management systems in the ISO 9000 series. The ISO 27001 was developed out of the British Standard BSI 7799 and later on extended into a whole series of 27000 documents.

The management standard focused on information security to ensure secure operation of an organisation. Security controls are specified in ISO/IEC 27001:2013 [13], Annex A as *Reference control objectives and controls*, and they are mainly addressing the securing of an organisation and the information that it's processing. This means that when applying ISO 27001 to a developer's organisation, it would not contain any requirements or guidance on the secure architecture, design or implementation of products they are developing.

Summary

The CYRail project used the ISO/IEC 27000 series throughout the project. WP3 considers the use of ISO/IEC 27005 during the development of a security assessment methodology. The WP3 later extracts cyber threats and cyber vulnerabilities from the examples given in the standard for use in the security analysis. The standard is also used in the other work packages to help define terminology and concepts.

2.3.2 NIST SP-800

The Information Technology Laboratory (ITL) at the US National Institute of Standards (NIST) has developed a number of Special Publication 800 series on ITL's research, guidelines, and outreach efforts in information system security and its collaborative activities with industry, government and academic organizations. NIST is responsible for developing information

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

security standards and guidelines, including minimum requirements for federal systems that are outside of the national security systems. The NIST SP 800 publications have been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) and to help with managing cost effective programs to protect their information and information systems.

There is a range of publications covering different security areas from SP 800-12 *An Introduction to Information Security* [14], SP 800-30 *Guide for Conducting Risk Assessments* [15] to specific topics such as SP 800-179 *Guide to Securing Apple OS X 10.10 Systems for IT Professionals: A NIST Security Configuration Checklist*. The SP 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations* [16] provides a catalogue of security controls for all US federal information systems (except those related to national security). Appendix H of the SP document provides a mapping between SP 800-53 controls, the ISO/IEC 27001 controls, but also between SP 800-53 controls and the ISO/IEC 15408 (Common Criteria) security functional requirements.

Summary

The CYRail project used the NIST SP-800 series to define security terminology and concepts. WP3 incorporates SP-800-30 [15] the risk management. WP4 used it to define the current rail infrastructure situation, and the SP 800-61 [17] incident handling guide. WP5 used the SP 800-184 *Guide for Cyber Security Recovery* [18].

2.3.3 ISA/IEC 62443

The ISA/IEC 62443 [19] provides a general framework of requirements, including specific security requirements on components, systems, policies and procedures directed towards those responsible for specifying, designing, developing, implementing, or managing Industrial Automation and Control Systems (IACS).

Summary

The CYRail project used the ISA/IEC 62443 to define the methodology of WP3. The security levels of the standard were used to divide the original scenario from WP2 into different zones. WP4 and WP5 then reference these zones to connect their respective results to the scenario. The foundational requirements found in the ISA/IEC 62443 standard were first presented in WP2 and have then been used in both WP3 and WP5. The countermeasures of WP5 were mapped to the requirements in WP3, ensuring a common thread throughout the work.

The standard is also used in the other work packages to help define terminology and concepts. Being a well-established standard in security, it is often referenced throughout the CYRail project. E.g. WP4 to define the current rail infrastructure situation.

2.3.4 ETSI TS 102

The European Telecommunications Standards Institute (ETSI) is a by the European Standards Organization (ESO) recognized standards body, dealing with telecommunications, broadcasting and other electronic communications networks and services. ETSI works in close co-operation with CEN and CE NELEC, the other two ESOs, especially on matters which are the subject of an EC standardization mandate. Although the three ESOs deal with different sectors, they have common interests. With the convergence of IT and telecom, ETSI co-ordinates policies and work programmes to avoid overlapping activities and to increase efficiency.

Among all the standards ETSI has published, there is one standard the ETSI TS 102 165 [20] [21] that is more relevant for the CYRail Project. This Technical Specification (TS) has been

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

produced by ETSI Technical Committee Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN). The standard consists of two parts:

- Part 1: *Method and proforma for Threat, Risk, Vulnerability Analysis*
- Part 2: *Protocol Framework Definition; Security Counter Measures*

The ETSI standard defines a method for use by ETSI standards developers to perform analysis of the threats, risks and vulnerabilities of a telecommunications system. The method builds from the ISO/IEC 15408 (Common Criteria) model for security assurance and evaluation and targets the means to build a Threat Vulnerability and Risk Analysis (TVRA). The TVRA forms part of the documentation set for the Target of Evaluation (TOE) as specified in the ETSI ES 202 382 [22] with its intended audience being the developer of standard based Protection Profiles. The document ES 202 382 *Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method and proforma for defining Protection Profiles* provides guidance how to write Protection Profiles.

The primary purpose for the ETSI TVRA was to support and rationalize security standardization and to support and rationalize system design decisions. Thereby complimenting the Common Criteria to prepare the justifications for security decisions that may as a result be referenced in a Protection Profile for the security feature.

Summary

The CYRail project used the ETSI standards for the TVRA methodology in WP3. Although the ISA/IEC 62443 was the main resource, the ETSI standards and the TVRA model were used to complement the steps which are not yet defined by ISA/IEC 62443.

2.3.5 ISO/IEC 15408 and ISO/IEC 18045

The ISO/IEC 15408, also known as Common Criteria, is used for specifying security requirements for IT security products and also for evaluating IT security products these requirements. IST/IEC 15408 is also used for specifying security requirements not only for a specific product, but also for specifying security requirements for certain types of products, such as operating systems, firewalls or databases. This is then done in a document called Protection Profile.

The ISO/IEC 18045 [23], known as the Common Methodology for Information Technology Security Evaluation (CEM). It is the evaluator guidance for evaluating IT security products according to the Common Criteria. The target audience for the CEM is primarily evaluators applying the CC and certifiers confirming evaluator actions. Although the CEM is relevant for evaluation of IT security products and Protection Profiles, is not directly relevant to the CYRail project.

Summary

The CYRail project used the ISO/IEC 15408 standard (Common Criteria) in for specifying the security requirements in the Protection Profiles. Part 1, *Annex B: Specification of Protection Profiles*, specifies the format for Protection Profiles, Part 2 provides a catalogue of security functional requirements (SFRs) and Part 3 provides a catalogue of security assurance requirements (SARs) that are packaged in Evaluation Assurance Levels (EALs). More specific the detailed requirements for Protection Profiles are specified in Part 3, chapter 10, *Class APE: Protection Profile evaluation.* It is expected that the Protection Profiles specifies the assurance requirements for a Protection Profile compliant product.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

2.4 PROTECTION PROFILE USE CASES

There exist different ways in how networks can be separated. Traffic flows through the device can be controlled and separated, or network traffic can be isolated within cryptographic tunnels as it travels over untrusted networks.

The Protection Profile specifies mechanisms for network separation at different layers of the network stack. The device described by this Protection Profile will then be able to support a MILS network architecture within critical infrastructure, i.e. the railway. The three different mechanisms are the following:

- Traffic flow control via Virtual LANs (VLAN)
- Cryptographic network channels via Internet Protocol Security (IPsec)
- Cryptographic application channels via Secure Shell (SSH) and Transport Layer Security (TLS).

Each of these mechanisms provides different security properties and therefore will apply to different situations. Below we will attempt to list a few use cases of the technology. Note that these are not how we're stating that these mechanisms are implemented, but rather examples to give a visual idea of their usage. The usage of the technologies will also depend upon their flexibility in regards to how they can be implemented, but also how they can be maintained to respond to changes in the environment.

There are also other possible uses for separation in the railway. For instance, separation kernels could be used to isolate different separation applications within a device running providing multiple separation mechanisms. This would protect the remaining separation functionality in the case that one mechanism was compromised.

2.4.1 VLAN

VLANs will be used to provide control over network traffic flow through the device. The technology works at a low level of the network stack and does not provide protection if an attacker has access to the network frames. It should be used in non-critical situations or in combination with another separation method. The separation provided by VLANs will also depend on the underlying physical infrastructure.

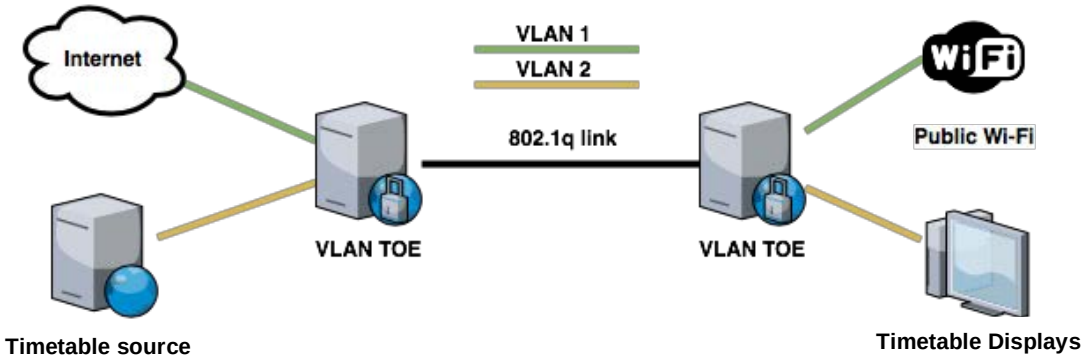

Figure 1 VLAN example

One example use case could be the segregation of exposed customer services, e.g. internet access and train schedule information. These are not critical to security or but could be separated to avoid interference.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

2.4.2 IPsec

IPsec is used to create VPNs, which forms a cryptographic channel between two networks. Compared to VLANs, this offers further separation of traffic inside and outside of a channel between two networks. As it only operates one layer above VLANs it poses less requirements of the physical infrastructure, but still also does not impact the operation of higher layer protocols.

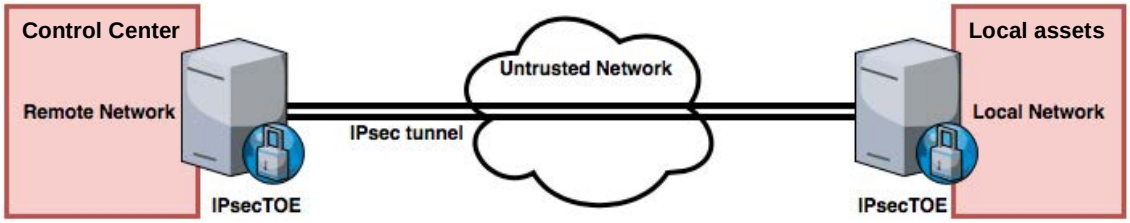

Figure 2 IPsec example: trusted channel

One example use case would be to secure two remote networks where traffic between these would otherwise transit via potentially untrusted paths, e.g. the internet. Using IPsec, trusted traffic would be encapsulated within a secure channel and inaccessible to a malicious intermediary.

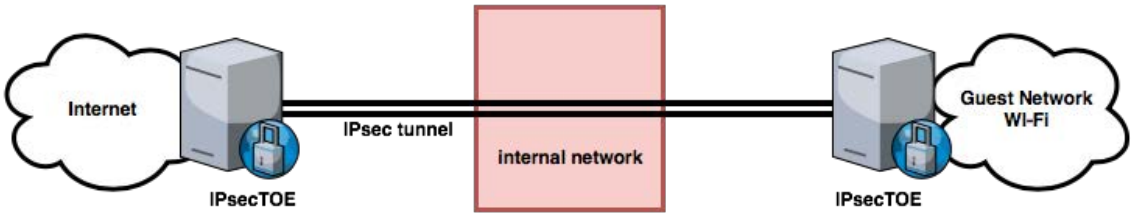

Figure 3 IPsec example: encapsulated traffic

The separation could also be used in a reverse situation: where untrusted traffic would have to transit over the physical infrastructure of an internal network. In this case, the untrusted traffic would be sealed inside the secure channel, unable to break out into the intermediary network.

2.4.3 SSH and TLS

SSH and TLS both operate on the application layer, which makes the protocols more flexible in how they can be used. The two protocols encrypt network traffic between server-client applications. While SSH is most often used for administration, the TLS is commonly used to protect many different types of network traffic and applications.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

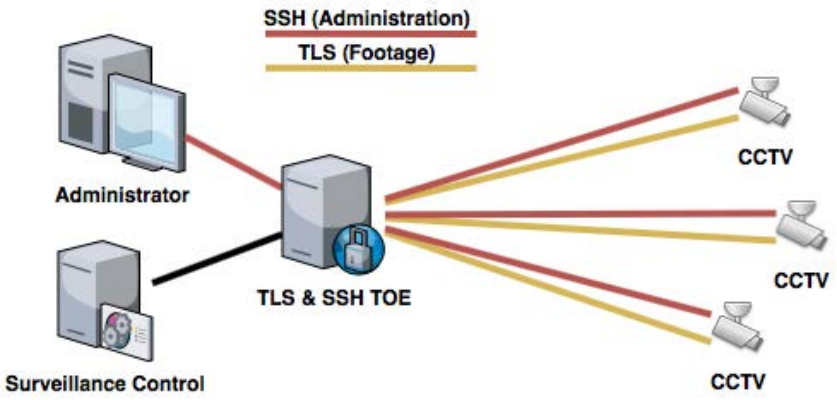

Figure 4 SSH and TLS example

The technologies will separate traffic between applications that travel over potentially exposed networks. One example would be a wireless network of CCTV cameras. SSH would here be used to manage the cameras, where each CCTV is an SSH server. TLS would be used to protect CCTV footage reported by the cameras to a control server. In this way, the integrity and confidentiality of traffic is protected despite an attacker being able to eavesdrop on the network.

2.4.4 Application in Railway

In this section are some examples of how the proposed PP (base and modules) can be used within the operational scenario and the security analysis described in WP2 and WP3.

VLAN Movement zone – Command-onboard zone

The network traffic within the Signalling conduit reflects the data flows between the different zones connected to it. As the Signalling conduit is also connected to the Internet, setting VLANs will be relevant to control network traffic flows, for example between the Movement zone and the Command-onboard zone: as stated in the CYRAIL security analysis report, the data that will get out of the movement zone consists of messages that will arrive at the onboard equipment through the BTS (or the balises) considering the restrictions the TSR Manager creates.

VPN (TLS) Command-onboard zone – Signal zone

Movement authorities created in the BTS are transmitted to the Signal devices to be further processed by the onboard ERTMS equipment. These communications have to be encrypted, for example using TLS.

VPN (IPSec) Maintain zone – OCC

In order to perform its tasks remotely, the Maintain zone needs to be connected to the OCC network, to access to the system through the Internet. Setting an IPSec VPN to grant the security requirements regarding communications appears as a relevant solution.

VPN (SSH) Administration workstation – Data server

As any server, the OCC's data server must be accessed by an administrator to perform administration tasks. This has to be done in a secure way, usually through an SSH tunnel. The data server must run an SSH server while the administration workstation runs an SSH client. Both are sharing their public keys. *(Note: this can be extended to any server managed by the administrator.)*

The figure below locates the TOE of each example given above.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

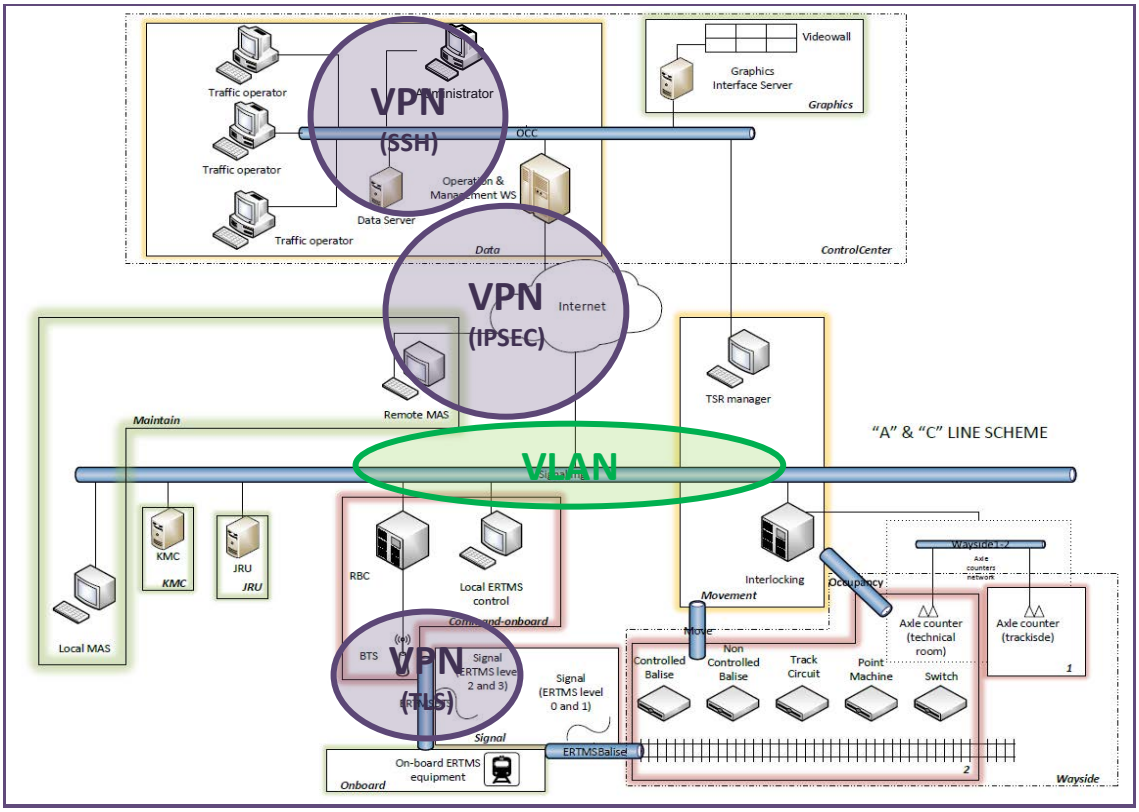

Figure 5 PP use cases applicable to the operational scenario

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

3. WHAT IS ISO 15408 AND PROTECTION PROFILES?

ISO/IEC 15408 (also known as Common Criteria or simply CC) is a standard for specifying security requirements and evaluating IT security products against these requirements.

The CC does so by providing a common set of requirements for the security functionality (ISO 15408 Part 2) of IT products and for assurance measures (ISO 15408 Part 3) applied to these IT products during a security evaluation. Evaluations of the assurance measures are performed according to IEC/ISO 18045 (also known as the Common Methodology or simply CEM).

The evaluation process establishes confidence that the security functionality of these IT products and the assurance measures applied to these IT products meet these requirements.

The CC is intentionally flexible, enabling a range of evaluation methods to be applied to a range of security properties of a range of IT products. Therefore, users of the standard are cautioned to exercise care that this flexibility is not misused.

The security claims of an IT product are specified by the developer in a document called the Security Target (ST). The mandatory content of a Security Target is specified by the Common Criteria, Part 1 Annex A. Each product and version of that product has its own ST, identifying the version and the configuration of the product as well as the scope that is evaluated.

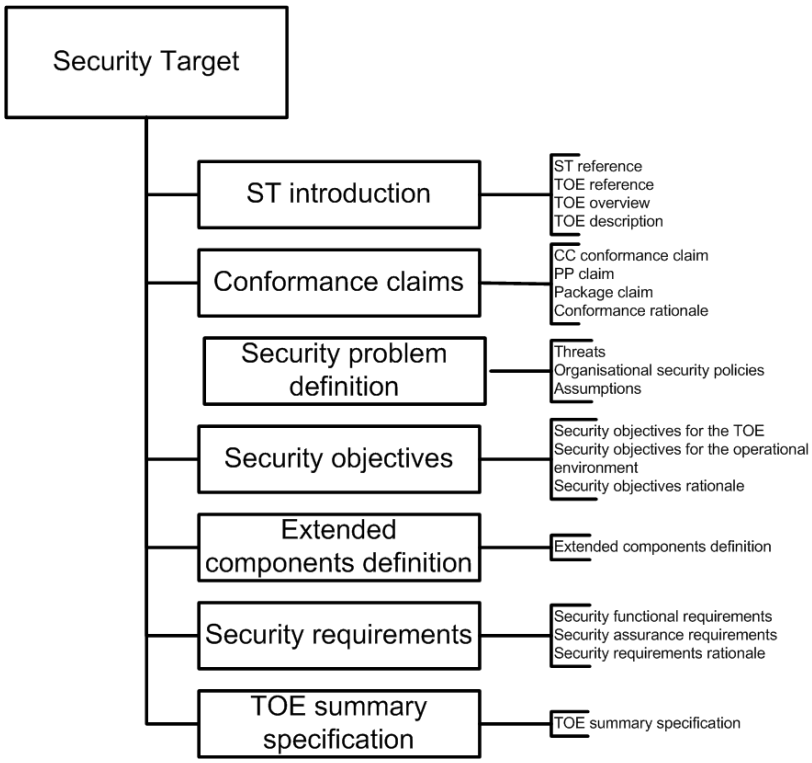

Figure 6, Security Target contents (Source: Common Criteria, Part 1)

The functional security requirements are usually taken from CC Part 2 and the assurance requirements are usually taken from CC Part 3, usually as a package defined as an evaluation assurance level (E.g., EAL4). The ST author may also define his own security requirements in the ST, usually only extended security functional requirements are defined in addition to part 2.

A Security Target is a developer document that may be defined freely by the developer. But it may also claim compliance to a set of security requirements that may have been be defined by the industry, such as minimum requirements for a certain type of product, such as network components. These general product type security requirements are defined in a document

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

called Protection Profile (PP). A Protection Profile is a concept defined in CC Part 1 and the mandatory content is specified by CC Part 1, Annex B.

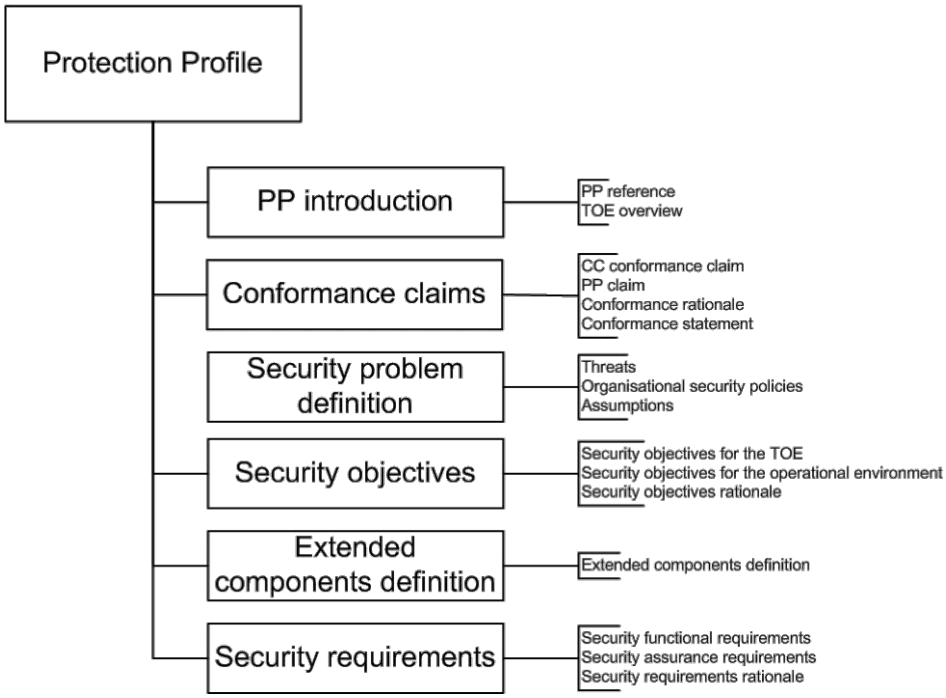

Figure 7, Protection Profile contents (Source: Common Criteria, Part 1)

The requirements of a Protection Profile should not be written to implementation specific, but for a type or class of products. Furthermore, a Protection Profile only specifies the minimum security requirements. The result of these differences in writing means that although Security Targets and Protection Profiles looks very similar, they are very different types of documents.

There are several reasons for this. First, we want as many products available as possible to choose from, so we don't want just one single vendor to meet these requirements. At least not if we are the customer. Second, we think that we as Protection Profiles authors are good in specifying the security requirements, but not necessary that we are good in designing security products, so we better leave that to the product developers. Third, we believe that we should only specify the *minimum* requirements and not all the "bells and whistles" since not all users may need them.

By having Protection Profiles, the customer knows that evaluated products that have claimed compliance to these Protection Profiles also meet the requirements. A Protection Profile is only useful if it can be accepted by the customers and met by several different vendors. Therefore, Protection Profiles shall only specify the minimum-security requirements for a type of product. A Protection Profile should be so generic so it could be used by many vendors and still so specific so we know that it contains the essential requirements.

Since it is difficult to write (good) Security Targets and Protection Profiles, ISO has developed Technical Report ISO TR15446 *Information technology — Security techniques — Guide for the production of Protection Profiles and Security Targets* [24] describing how to write Security Targets and Protection Profiles. It is strongly recommended if you want to learn more about STs and PPs.

3.1 What is a Modular Protection Profile?

A Protection Profile should specify the minimum set of security requirements for a certain type of product. However, what is minimum is not always very clear and sometimes it makes sense

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

to specify also optional security functionality in a Protection Profile. An example is firewalls that have a basic set of filtering and management functions, but also to specify optional packages that supports deep package inspection, application level filtering or even VPN functionality.

3.1.1 Modular Protection Profiles

The idea is to develop Protection Profiles that specify certain basic functionality and any optional functionality in extended packages or Protection Profile modules. This has been done for some years in different ways already but was formalized with the CC version 3.1 Release 5 with the concept of Base-PP, PP-Modules and PP-Configurations, as well as the way they can be used to evaluate compliant products.

A PP-Module is a consistent set of elements (threats, assumptions, organisational policies, objectives and security requirements) with a unique reference. Unlike Protection Profiles, PP-Modules address optional security features of a given type of TOE that cannot be required uniformly for all products of this kind.

Each PP-Module refers to at least one Base Protection Profile (or Base-PP) that provides the definition of the TOE type and the mandatory requirements to fulfil. The PP-Module specifies the modified TOE type, completes these requirements and has to be used with the Base-PP: a PP-Module may introduce new elements to the Base-PP and may also refine or interpret some of the elements of the Base-PP.

A PP-Module has to be evaluated as part of a PP-Configuration, at least with its mandatory Base-PPs since the evaluation of a PP-Module alone is meaningless.

A PP-Configuration is the combination of at least one PP-Module with its Base-PPs, without any additional content, so a PP-Configuration is much like a Protection Profile that would include all the elements from the Base-PPs and the PP-Modules. A PP-Configuration can select more PPs than the Base-PPs of the PP-Modules, but at least all of the Base-PPs of the referred PP-Modules must be included in the PP-Configuration. In case the PP-Module defines alternate sets of Base-PPs, only one of these sets must be used in the PP-Configuration.

A PP-Configuration must have unique reference and identifies all the PP components: selected Base-PPs and selected PP-Modules. A PP-Configuration can only combine certified Base-PPs to PP-Modules.

3.1.2 Using modular Protection Profiles

PP-Modules are supposed to be used in Security Targets only as part of well-identified PP-configurations. PP-Configurations are used like Protection Profiles. A Security Target can claim conformity to a PP-Configuration provided this PP-Configuration has been evaluated. The evaluation of the ST can rely on the results of the PP-Configuration evaluation results as usual.

Note that the evaluation of a PP-Configuration can arise in two situations, with no impact on the evaluation methodology:

- Independently of any product (a fortiori ST) evaluation, or
- As the first step of the evaluation of a Security Target that claims conformity with the PP-Configuration. Otherwise the conformance claim is meaningless and the ST evaluation would fail in this aspect.

In practice, a ST that claims conformance with a non-certified PP-Configuration can still be evaluated with a conformance claim against the Base-PP of the PP-Configuration; the elements of the ST that meet the PP-Modules of the PP-Configuration would be evaluated as standard additions to the Base-PP, proper to the TOE.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

3.2 How Protection Profiles are Used in Evaluations?

The Common Criteria works in the following way. A product, or actually a part or a combination of products in a certain configuration is evaluated. This is called the Target of the Evaluation (TOE). The specification of the TOE and what it should be good for, such as the security objectives and the environment in which it is intended to be used is specified in the Security Target. A Security Target for a specific TOE may claim compliance to one or more Protection Profiles.

The vendor makes the following claims [24]: My ST complies with your PP; My product complies with my ST; Therefore, my product complies with your PP and meets your requirements.

If the Security Target claim conformance to one or more Protection Profiles, we have to be sure that these Protection Profiles are also consistent, complete and technically sound base to be included into for an evaluation. This is usually done well before the development of the Security Target and the evaluation of the TOE. In the Common Criteria Part 1 is illustrated as follows:

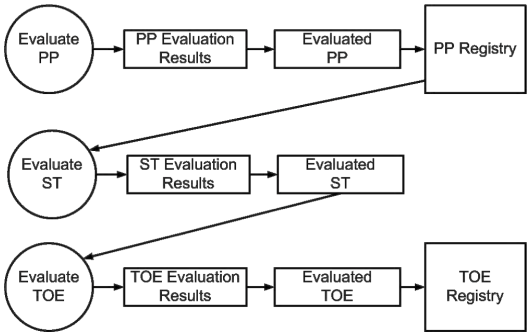

Figure 8, Evaluation chain (Source: Common Criteria, Part 1)

The assurance requirements specified in the Security Target are the ones that are evaluated. This means that for each assurance requirement there is also an associated evaluation activity. The assurance requirements are grouped into seven hierarchical evaluation assurance levels (EAL1-EAL7) that represent a consistent set of security assurance requirements. The assurance requirements for each EAL is shown in Figure 9 below.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		**1**	1	1	1	1	1
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**
	ADV_IMP				**1**	1	**2**	2
	ADV_INT					**2**	**3**	3
	ADV_SPM						**1**	1
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**
Guidance documents	AGD_OPE	**1**	1	1	1	1	1	1
	AGD_PRE	**1**	1	1	1	1	1	1
Life-cycle support	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5
	ALC_DEL		**1**	1	1	1	1	1
	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD			**1**	1	1	1	**2**
	ALC_TAT				**1**	**2**	**3**	3
Security Target evaluation	ASE_CCL	**1**	1	1	1	1	1	1
	ASE_ECD	**1**	1	1	1	1	1	1
	ASE_INT	**1**	1	1	1	1	1	1
	ASE_OBJ	**1**	**2**	2	2	2	2	2
	ASE_REQ	**1**	**2**	2	2	2	2	2
	ASE_SPD		**1**	1	1	1	1	1
	ASE_TSS	**1**	1	1	1	1	1	1
Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**3**	3	**4**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Vulnerability assessment	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5

Figure 9, Assurance Requirements for different EALs (Source: Common Criteria, Part 3)

The evaluation of a TOE (i.e. the product) defined by the Security Target and against the security assurance requirements specified in the Security Target always starts with the evaluation of the Security Target to ensure that it is a consistent, complete and technically sound base for an evaluation. This means that the Security Target evaluation (ASE class in the figure above) is the first step in the evaluation of a TOE. After that, the other security assurance requirements are verified, covering development (ADV), Guidance (AGD), Life-cycle support (ALC), Tests (ATE) and vulnerability assessment (AVA).

Figure 10 below shows the area covered by each class of security assurance requirements.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

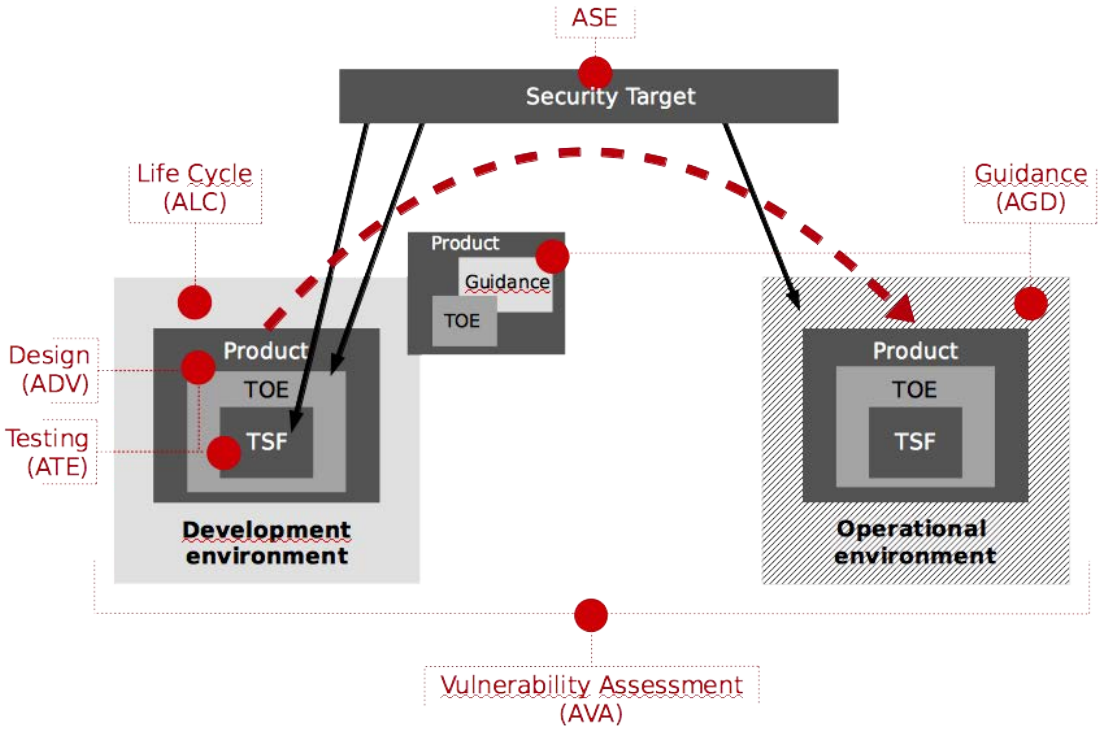

Figure 10, Evaluation assurance classes

In summary the TOE evaluation covers the following aspects, of course with different assurance levels depending on the EAL chosen in the Security Target, this is directly taken from the Common Criteria, Part 3 [25]:

- **ASE** – Evaluating an ST is required to demonstrate that the ST is sound and internally consistent, and, if the ST is based on one or more PPs or packages, that the ST is a correct instantiation of these PPs and packages. These properties are necessary for the ST to be suitable for use as the basis for a TOE evaluation.
- **ADV** – The requirements of the Development class provide information about the TOE. The knowledge obtained by this information is used as the basis for conducting vulnerability analysis and testing upon the TOE, as described in the AVA and ATE classes.
- **AGD** – The guidance documents class provides the requirements for guidance documentation for all user roles. For the secure preparation and operation of the TOE it is necessary to describe all relevant aspects for the secure handling of the TOE. The class also addresses the possibility of unintended incorrect configuration or handling of the TOE.
- **ALC** – Life-cycle support is an aspect of establishing discipline and control in the processes of refinement of the TOE during its development and maintenance. Confidence in the correspondence between the TOE security requirements and the TOE is greater if security analysis and the production of the evidence are done on a regular basis as an integral part of the development and maintenance activities.
- **ATE** – This encompasses four families: Test coverage, Test depth, Independent testing and Functional tests. Testing provides assurance that the TSF behaves as described (in the information provided by the developer).
  The emphasis in this class is on confirmation that the TSF operates according to its design descriptions.
- **AVA** – Vulnerability assessment class addresses the possibility of exploitable vulnerabilities introduced in the development or the operation of the TOE.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

It is important to say that the Common Criteria assessment focuses both on compliance verification of the security functionality (design review and functional testing) as well as analysis and active search for security vulnerabilities. The assessment covers both the analysis of the TOE (design and implementation) and assessment of the development environment. However, the Common Criteria does not provide you with any method for risk assessment nor does it focus on the developer maintenance or vulnerability of the TOE once the product has been completed.

3.3 How Have the Security Requirements Been Derived?

The work to derive the security requirements for our Protection Profile of Work Package (WP) 6 is based on the earlier deliverables in the CYRail project. The definition of a scenario (WP2) provided a realistic overview of the railway context, and the future challenges connected to increasingly open and digital rail infrastructure. The identification of vulnerabilities, threats and risks (WP3) led to a better understanding of what problem the Protection Profile should address. Having a well-defined scenario and risk assessment was necessary to ensure that the Protection Profile would be applicable to the railway and that the assumptions would be valid.

Early on the attack surface and interconnectivity of different services was identified as a main security issue, which presented a natural need for separation measures. Rail infrastructure may contain single-purpose or legacy components, whose security depends on isolation. Now these systems risks being vulnerable via interconnected networks. Separation and attack surface reduction were explicitly suggested by the MILS approach (WP5). The mitigation strategies and countermeasures defined by CYRail specifies the necessity of this approach. We identified the need for separation at both the host and the network level. As work on a Protection Profile addressing host-based separation is already ongoing in the certMILS project, our Protection Profile would focus on network separation. This is also an area where we did not identify much previous work.

To increase usability of the Protection Profile we looked towards the well-established Protection Profile for Network Devices [26] to draw inspiration from since our TOE would also be a network device. However, this Protection Profile was not sufficient for our requirements. To provide a variety of separation mechanisms we decided to adopt a modular approach and allow for the user to select the desired separation mechanism(s). This is also similar to the certMILS project and their modular Protection Profile.

3.4 What About the Future Use of this Protection Profile

The goal is for this Protection Profile to be (1) evaluated and certified; (2) provide input to the collaborative Protection Profile for Network Devices that is developed within the Common Criteria community. Of course, the goal is also that the Protection Profile will be used by the industry and that vendors will certify products claiming compliance to this Protection Profile. The more applicable the PP is the more users it will have which results in a wider selection of PP compliant products.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

4. ISA/IEC 62443 AND THE COMMON CRITERIA

The Common Criteria represent an established approach for the evaluation of the security of (parts of) IT products. While the CC framework is flexible and explicitly does not preclude its application in different areas, it was never intended to be effectivity used for the assessment of larger systems such as complete Industrial Automation and Control Systems.

4.1 OVERVIEW OF ISA/IEC 62443

The Instrumentation Systems and Automation Society (ISA), together with IEC, has developed the ISA/IEC 62443 standard which targets IACS. Its structure reflects the compositional architecture of industrial plants. As examples for IACS the first part of the IEC 62443 series mentions *control systems used in manufacturing and processing plants and facilities, building environmental control systems, geographically dispersed operations such as utilities (i.e., electricity, gas, and water), pipelines and petroleum production and distribution facilities, and other industries and applications such as transportation networks, that use automated or remotely controlled or monitored assets*.

The ISA/IEC-62443 series is directed towards those responsible for [19] specifying, designing, developing, implementing, or managing industrial automation and control systems. It consists of a number of documents organized in four different areas *General* (62443-1); *Policies and procedures* (62443-2); *System* (62443-3); and *Component level* (62443-4). Some documents have already been issued, while others are under revision or development. The standards are organized as shown in Figure 11 below:

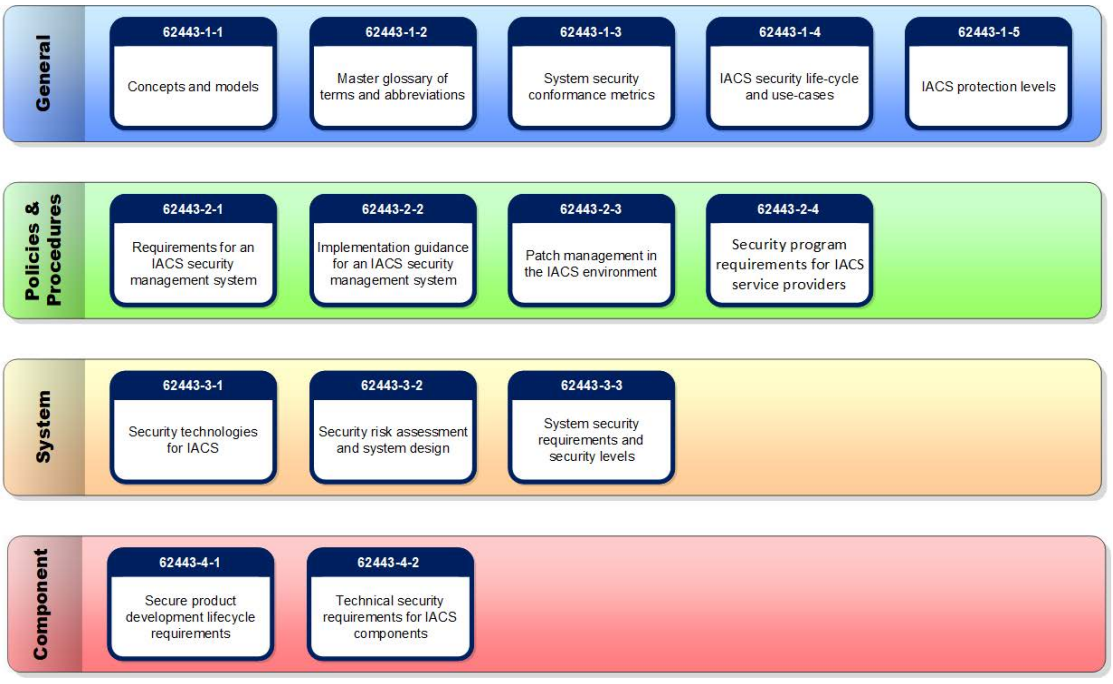

Figure 11: The IEC 62443 series. (Source: The 62443 Series of Standards [19])

The ISA/IEC 62443 overview provided by "*The 62443 Series of Standards Industrial Automation and Control Systems Security*" [19] give an excellent overview of the standard and the series of documents:

General – This group includes documents that address topics that are common to the entire series.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

- The 62443-1-1 standard introduces the concepts and models used throughout the series. The intended audience includes anyone wishing to become familiar with the fundamental concepts that form the basis for the series.
- The 62443-1-2 technical report contains a master glossary of terms and abbreviations used throughout the series.
- The 62443-1-3 document describes a series of quantitative metrics derived from the foundational requirements, system requirements and associated.
- The 62443-1-4 technical report provides a more detailed description of the underlying life cycle for IACS security, as well as several use cases that illustrate various applications.
- The 62443-1-5 document provides a methodology for evaluating of the level of protection provided by an operational IACS against cyber-security threats.

Policies and Procedures – Documents in this group focus on the policies and procedures associated with IACS security.

- The 62443-2-1 standard describes what is required to define and implement an effective IACS cyber security management system. The intended audience includes end users and asset owners who have responsibility for the design and implementation of such a program.
- The 62443-2-2 document provides guidance on what is required to operate an effective IACS cyber security management system. The intended audience includes end users and asset owners who have responsibility for the operation of such a program.
- The 62443-2-3 document provides guidance on the subject of patch management for IACS. The intended audience includes anyone who has responsibility for the design and implementation of a patch management discipline.
- The 62443-2-4 standard specifies requirements for suppliers of IACS. The principal audience include suppliers of control systems solutions. This standard was developed by IEC TC65 WG10.

System Requirements – The documents in the third group address requirements at the system level.

- The 62443-3-1 technical report describes the application of various security technologies to an IACS environment. The intended audience includes anyone who wishes to learn more about the applicability of specific technologies in a control systems environment.
- The 62443-3-2 standard addresses security risk assessment and system design for IACS. This standard is primarily directed at asset owners or end users.
- The 62443-3-3 standard describes the foundational system security requirements and security assurance levels.

Component Requirements – The fourth and final group includes documents that provide information about the more specific and detailed requirements associated with the development of IACS products.

- The 62443-4-1 standard describes the derived requirements that are applicable to the development of products. The principal audience include suppliers of control systems solutions.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

- The 62443-4-2 standard contains sets of derived requirements that provide a detailed mapping of the system requirements to subsystems and components of the system under consideration. The principal audience include suppliers of control systems solutions.

While the IEC 62443-3-1 to IEC 62443-3-3 target systems or industrial plants the IEC 62443-4-1 and the IEC 62443-4-2 targets individual components. Both IEC 62443-4-1 and IEC 62443-4-2 are still under development. However, ISA has already proposed and applied a certification scheme according to IEC 62443-4-1 and IEC 62443-4-2:

- Security Development Lifecycle Assurance Certification (SDLA) based on IEC 62443-4-1,
- Embedded Device Security Assurance (EDSA) based on IEC 62443-4-2.

In the section below, the relationships between IEC 62443 and the Common Criteria are pointed out and explained.

4.2 Similarities Between CC and 62443

The intention of the IEC 62443 standard series is to build extensions to enterprise security that adapt requirements for IT management systems and combine them with the unique requirements that embrace the strong availability needed by IACS.

The IEC 62443 provides a flexible framework to evaluate the security functions of such systems. This framework encompasses seven foundational requirement (FR) groups (IEC 62443-3-3) detailed below. These FRs are closely related to the security functional requirements (SFRs) defined in CC Part 2. That is CC SFRs could in principle be used to complement the FRs of IEC 62443-3-3.

IEC 62443 also defines requirements for security policies, procedures, and practices applicable to IACS solutions throughout their life cycle, describing what shall or should be provided during integration and maintenance activities (IEC 62443-2-4). Within the CC, the ALC class (live-cycle support) takes a similar point of view, rendering it a useful source to clarify or extend the IEC 62443 requirements.

There are already certified products meeting these IEC 62443 requirements, such as the station automation system SICAM PAS/PQS and SICAM AK3 by Siemens.

Since the ISA/IEC-62443 is targeted on system developer and integrator, and less on product developer, it does not provide much detail on the design and development of specific components, instead references are made from ISA/IEC-62443-4-2 to the ISO/IEC 15408 for components where high assurance is needed, such as crypto and key management components. In such cases it also refers to ISO 15408 assurance levels, such as EAL4 and EAL5 with augmentations of AVA_VAN.5. It also mentions appropriate Protection Profiles, but neither refers to any specific Protection Profiles or specific security functionality.

We believe that also other areas than crypto and key management would benefit from having more specific security requirements. By identifying and developing Protection Profiles for railway control and signalling systems we would be able to increase the level of security, but also nicely integrate into the existing framework of both ISA/IEC-62443 by building upon the ISO 15408 standard.

Please, note that ISA/IEC-62443 and ISO/IEC 15408 are not competing standards, but rather complementary standards with different focus, targeting different audiences (system developer and integrators vs product developers).

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

5. BIBLIOGRAPHY

[1] ENISA, “Securing Smart Airports,” December 2016. [Online]. Available: https://www.enisa.europa.eu/publications/securing-smart-airports/at_download/fullReport . [Accessed 17 May 2018].

[2] ACEA, “Principles of Automobile Cybersecurity,” September 2017. [Online]. Available: http://www.acea.be/uploads/publications/ACEA_Principles_of_Automobile_Cybersecurity.pdf. [Accessed 23 March 2018].

[3] Auto-ISAC, “Cybersecurity Best Practices,” July 2015. [Online]. Available: https://www.automotiveisac.com/best-practices/ . [Accessed 23 March 2018].

[4] C. Pete, “Aviation Cybersecurity, Finding Lift, Minimizing Drag. Atlantic Council Policy,” November 2017. [Online]. Available: http://www.atlanticcouncil.org/images/Aviation_Cybersecurity_web_1107.pdf. [Accessed 17 May 2018].

[5] ENISA, “Protecting Industrial Control Systems. Recommendations for Europe and Member States,” 14 December 2011. [Online]. Available: https://www.enisa.europa.eu/publications/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states/at_download/fullReport.

[6] EURO-MILS Consortium, “EURO-MILS,” [Online]. Available: http://www.euromils.eu. [Accessed 17 May 2018].

[7] certMILS consortium, “ certMILS,” [Online]. Available: https://certmils.eu/index.php. [Accessed 17 May 2018].

[8] J. Rushby, “Design and Verification of Secure Systems,” in *Proc. 8th ACM Symposium on Operating System Principles. pp. 12–21.*, 1981.

[9] W. S. Harrison, N. Hanebutte, P. Oman and J. Alves-Foss, “The MILS Architecture for a Secure Global Information Grid,” October 2005. [Online]. Available: http://static1.1.sqspcdn.com/static/f/702523/9277782/1288928922607/200510-Harrison.pdf?token=dZ1LQXgnZY58jFYPzJBpXsrJT14%3D. [Accessed 17 May 2018].

[10] W. S. H. P. O. a. C. T. Alves-Foss, “The MILS Architecture for High Assurance Embedded Systems,” International Journal of Embedded Systems. 2007. [Online]. Available: http://www.csds.uidaho.edu/papers/Alves-Foss06a.pdf.

[11] National Security Agency, “Commercial Solutions for Classified Hanbook,” November 2017. [Online]. Available: https://www.nsa.gov/resources/everyone/csfc/assets/files/csfc-customer-handbook.pdf. [Accessed 17 May 2018].

[12] National Security Agency, “Mobile Access Capability Package v2.0,” August 2017. [Online]. Available: https://www.nsa.gov/resources/everyone/csfc/capability-packages/assets/files/mobile-access-cp.pdf. [Accessed 23 March 2018].

This project has received funding from the European Union’s Horizon2020 research and innovation programme under grant agreement No730843

[13] ISO/IEC 27001:2013, “Information technology – Security techniques – Information security management systems – Requirements,” 2017. [Online]. Available: https://www.iso.org/standard/54534.html.

[14] NIST Special Publication 800-12, “An Introduction to Information Security, Revision 1,” June 2017. [Online]. Available: http://doi.org/10.6028/NIST.SP.800-12r1.

[15] NIST Special Publication 800-3, “Guide for Conducting Risk Assessments, Revision 1,” September 2012. [Online]. Available: http://doi.org/10.6028/NIST.SP.800-30 .

[16] NIST Special Publication SP 800-63, “Security and Privacy Controls for Federal Information Systems and Organizations, Revision 4,” April 2013. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-53r4.

[17] NIST Special Publication SP 800-61, “Computer Security Incident Handling Guide, Revision 2,” August 2012. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-61r2.

[18] NIST Special Publication 800-184, “Guide for Cybersecurity Event Recovery,” December 2016. [Online]. Available: https://doi.org/10.6028/NIST.SP.800-184 .

[19] ISA, “The 62443 Series of Standards, Industrial Automation and Control Systems Security,” February 2018. [Online]. Available: http://isa99.isa.org/Public/Information/The-62443-Series-Overview.pdf. [Accessed 17 May 2018].

[20] European Telecommunications Standards Institute, “Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis, V4.2.3, ETSI TS 102 165-1,” March 2011. [Online]. Available: http://www.etsi.org/deliver/etsi_ts/102100_102199/10216501/04.02.03_60/ts_10216501v040203p.pdf. [Accessed 17 May 2018].

[21] European Telecommunications Standards Institute, “Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 2: Protocol Framework Definition; Security Counter Measures, V4.2.1, ETSI TS 102 165-2,” Feburary 2007. [Online]. Available: http://www.etsi.org/deliver/etsi_ts/102100_102199/10216502/04.02.01_60/ts_10216502v040201p.pdf. [Accessed 17 May 2018].

[22] European Telecommunications Standards Institute, “Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method and proforma for defining Protection Profiles, V1.1.1, ETSI-TS-202-382,” April 2005. [Online]. Available: http://www.etsi.org/deliver/etsi_ES/202300_202399/202382/01.01.01_60/es_202382v010101p.pdf. [Accessed 17 May 2018].

[23] CCMB, “Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1 Revision 5,” April 2017. [Online]. Available: https://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R5.pdf. [Accessed 17 May 2018].

[24] Technical Report ISO/IEC TR 15446, “Information technology – Security techniques – Guide for the production of Protection Profiles and Security Targets, Second edition,” 01

This project has received funding from the European Union’s Horizon2020 research and innovation programme under grant agreement No730843

March 2009. [Online].

[25] CCMB, “Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model, April 2017, Version 3.1 Revision 5, CCMB-2017-04-001; Part 2: Security functional Components, April 2017, Version 3.1 Revision 5, CCMB-2017-04-002,” April 2017. [Online]. Available: https://www.commoncriteriaportal.org/cc/. [Accessed 17 May 2018].

[26] Network Device international Technical Community, “Collaborative Protection Profile for Network Devices (NDcPP), Version 2.0,” 05 May 2017. [Online]. Available: https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V2.0.pdf. [Accessed 17 May 2018].

[27] NIST Special Publication 800-64 Revision 2, “Security Considerations in the System Development Life Cycle,” October 2008. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-64r2.

[28] The PP/ST Guide, “Bundesamt für Sicherheit in der Informationstechnik, Version 2, Revision 0,” August 2010. [Online].

[29] ISO/IEC 27005:2010, “Information technology – Security techniques – Information security risk management,” 2011. [Online]. Available: https://www.iso.org/standard/56742.html .

[30] H. Kurth, G. Krummeck, C. Stüble and M. W. M. Weber, “HASK-PP – Protection profile for a high assurance security kernel,” June 2008. [Online].

[31] ENISA, “Proposal for a regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification("Cybersecurity Act").,” Brussels, 13 September 2017. [Online]. Available: https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-477-F1-EN-MAIN-PART-1.PDF. [Accessed 17 May 2018].

This project has received funding from the European Union’s Horizon2020 research and innovation programme under grant agreement No730843

EU Project 730843

CYbersecurity in the RAILway sector

D6.1 – Base Protection Profile for Network Separation Mechanisms

Due date of deliverable: 2018-09-30

Leader of this Deliverable: atsec information security AB

Reviewed: AIRBUS

Document status		
Revision	Date	Description
001	2017-07-18	Staffan Persson, initial draft version for review
002	2017-08-07	Staffan Persson, Caroline Holz auf der Heide, draft version for review
003	2018-01-22	Markus Engqvist, introduction, SPD and Objectives for base
004	2018-04-11	Markus Engqvist, adjustments of Base PP structure.
005	2018-05-18	Markus Engqvist, address internal comments, draft for external review
006	2018-06-06	Staffan Persson, added protection of key material FPT_SKP_EXT.1
007	2018-07-10	Staffan Persson, minor updates due to module consistency
008	2018-09-04	Markus Engqvist, release version
009	2018-09-25	Markus Engqvist, address review comments, update versions
010	2019-02-14	Minor update due to EU review comments

Start date of project: 2016-10-01 Duration: 24 months

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

REPORT CONTRIBUTION

Company	Details of contribution
atsec	Specification of the security requirements in a base Protection Profile
AIRBUS	Performed review

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

OBJECTIVES OF THE DELIVERABLE

In **D6.1 – Protection Profiles Specifications** a Common Criteria Protection Profile will be developed using existing standards and framework related to Protection Profiles. This includes the Common Criteria (ISO/IEC 15408) and guides (ISO/IEC TR 15466), as well as experience from existing Protection Profiles, standards and projects such as D-MILS, TAPPS and other related projects.

It will include the description of the operational environment (combination of threats, assumptions and policies that the components need to enforce) based on the operational scenario identified in WP2 and risk assessments in WP3 as well as identified threats in WP4. Security objectives for the systems and the operational environment will be derived based on mitigation strategies and countermeasures identified in WP5. Security functional requirements (SFRs) and security assurance requirements (SARs) will describe security functionality that need to be provided by specific system and evaluation activities to be performed to ensure that security mechanisms in these systems are sufficient and implemented correctly.

This part of the deliverable is the Base Protection Profile for Network Separation Mechanisms.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

TABLE OF CONTENTS

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

1. INTRODUCTION

With the new generation of infrastructure systems, we see an increased use of IP networks with interconnection of trusted and untrusted services. This presents a need for mechanisms to separate and isolate said networks to avoid conflicting services and reduce attack surface.

This Protection Profile has been developed as part of the CYRail-project under the European Union's Horizon 2020 research and innovation programme (grant agreement no. 730843).

1.1 BASE PROTECTION PROFILE REFERENCE

Title:	Base Protection Profile for Network Separation Mechanisms
PP Version:	009
Status:	Released
Date:	2018-09-25
Keywords:	Base PP, network device, network separation, PP Module, trusted channel, VLAN, VPN

This Protection Profile (PP) has been structured in accordance with [CC] Part 1. The main sections of the PP are the introduction, security problem definition, security objectives, security requirements and annexes.

1.2 TOE OVERVIEW

This PP describes the minimum security requirements of a network device that directs data transmitted over computer networks. This PP is intended to act as the Base PP of a PP Configuration. Together with the accompanying PP Modules, said PP Configuration will describe a network device that provides separation of networks and attack surface minimization.

The Base PP will specify requirements for the core functionality of the network device and the PP Modules will address different methods for network separation. The goal is to isolate network traffic that may be transferred over the same hardware.

1.2.1 TOE Type

The TOE is a network device used for aggregation and isolation of network traffic. It may be a stand-alone component or may be part of a boundary protection solution providing additional functionality.

1.2.2 Usage and Major Security Features of a TOE

The TOE is intended to be used where different network traffic must be separated and isolated, such as controlled safety and security critical network traffic from uncontrolled user traffic. The TOE should be possible to use as part of an implementation of Multiple Independent Levels of Security (MILS) for networks within critical infrastructure. MILS is a security architecture based on separation and controlled information flow.

Separation can be implemented in various ways, with different benefits and drawbacks. Therefore, the separation mechanisms are described within different PP Modules that specify separation on the link layer, the internet layer and the application layer. These are different layers of the Internet Protocol Suite. Users of the PP may select their desired separation mechanism(s) through the Modules. This means that the final TOE of a PP Configuration will provide more functionality than what is specified in this Base PP. The functionality of the Base PP should also support the separation mechanisms of the selected PP Modules.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

For a network device, other security functionality is required for management of the TOE and to ensure that it is in a secure state. A TOE compliant with this PP must provide the following security functionality:

- Management of security functionality, including identification and authentication of administrators, and management of security functionality.
- Trusted channel, providing confidentiality and integrity of remote management traffic between the TOE and an authenticated endpoint.
- Auditing of security relevant events, including failed authentication and configuration changes, along with transmitting the records securely to an auditing server.
- Self-tests and secure updates of the TOE.

1.2.3 Available non-TOE Hardware/Software/Firmware

The TOE itself may be software, hardware or a combination of both. For a TOE that is only software, there is obviously the need for hardware to run said software. Apart from this, there is a need for two devices to be located on the other end of secure channels provided by the TOE. These are an auditing server and a remote administrator's workstations.

There is no other need for any other non-TOE components made by this PP.

1.3 TOE Description

The TOE covered by this PP will be a network device that can support network separation mechanism(s). The separation of network traffic is essential when a common network is shared by services having different criticality or sensitivity. For example, the separation of an administrative network used by trusted and competent operators from a customer network that could be used by anyone. It may also be used to separate different types of services from each other, to prevent interference between the services.

This PP has been written in a generic way, so that the product is able to accommodate a wide variety of use cases. This means a larger userbase for the PP and is intended to increase the availability of PP compliant product.

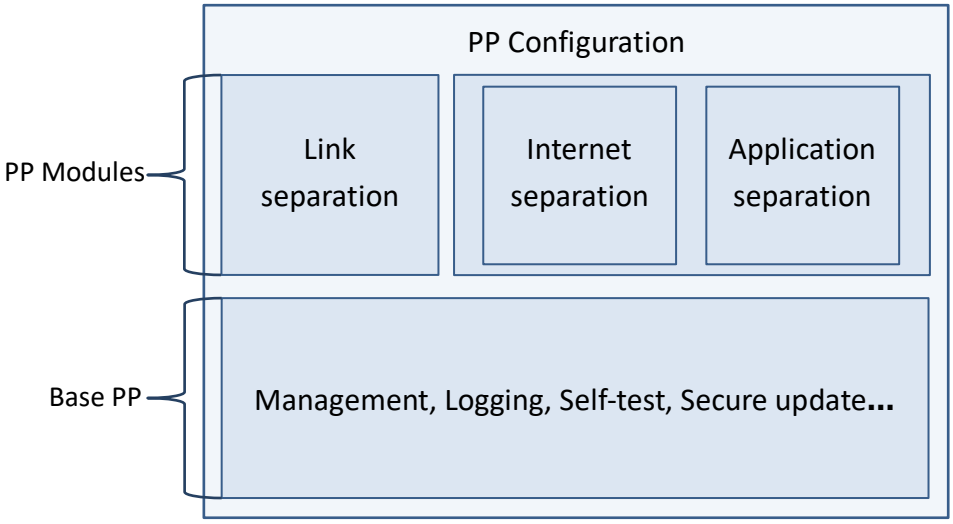

Figure 1 Example of intended PP Configuration

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

The TOE is a network device that is intended to be used in large systems within critical infrastructure. It therefore requires functionality that enable these systems to operate securely. This is the functionality specified in this Base PP. The separation mechanisms are specified separately as modules, of which at least one must be chosen. An example of an intended PP Configuration is visualized in Figure 1.

1.3.1 Base PP Functionality

The TOE must enable remote management for administrators in possession of valid credentials. This management interface must enable management of the security functionality and important security updates or self-tests. The interface must also be locked down to prevent unauthorised access, as this would compromise the security of the TOE. Any remote session must also be protected. The TOE must protect itself from remote tampering of the management interface as it may have an Internet Protocol Suite Layer 1 or Layer 2 connection to untrusted users/attackers. Within larger infrastructures there may exist different roles, e.g. operational administrators and security administrators. Other roles than an administrator may need to access TSF data, but not modify it. In the case that such roles exist, the TOE must be able to restrict access to data and functionality according to these roles.

The TOE must also be able to generate audit data from security related events. This involves possible attacks such as authentication attempts or channels going down, but also the actions of administrators for accountability purposes. The TOE should offer the possibility to securely send this data to an audit server/service, where logs from the whole system can be aggregated.

The TOE should be able to perform self-tests that ensure that it is in a secure state. To allow for flexible use of this PP the exact procedures of the self-tests are not defined. The ST author should implement the tests that are most applicable or effective for their product. Tests could for example verify the integrity of the software or the operation of the underlying hardware.

It should be possible to update the software of the TOE. The update mechanism is essentially a way to replace the software of the TOE. In the case that this functionality is compromised, an attacker could take complete control of all the device's functionality. To mitigate this, the TOE should be able to verify any updates and ensure that they are legitimate.

While this Base PP only describes a network device and no separation mechanisms, the security functionality of the TOE must still support the separation mechanisms of the chosen PP Module(s). The security requirements of the Base PP should also cover, where applicable, to each selected separation mechanism. This means that the functionality in this PP should be extended to also apply to the separation functionality. I.e. the management functionality must also allow management of the separation mechanisms and security related events of the separation mechanisms must generate audit logs.

1.3.2 PP Configurations and Use of PP Modules

Due to the differences between the described separation mechanisms, both in terms of how they can be applied and what results the provide, this PP will allow the ST author to choose the required functionality. This is to increase the flexibility and applicability of the PP. The different separation mechanisms are structured into the following PP Modules:

PP Module	Description
Link layer separation	The module specifies the logical isolation of low level network traffic through the use of Virtual LANs (VLAN) for ethernet frames.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

Internet layer separation	The module specifies the logical isolation of network traffic through the use of IPsec VPN tunnels for IP packets.
Application layer separation	The module specifies the logical isolation of high level network traffic through cryptographic TLS or SSH channels.

Table 1 PP Module list

This PP is meant to act as the Base PP in a PP Configuration that incorporates one or more of the separation mechanisms listed above. Such a PP Configuration is mandatory to include **at least one** (1) of the above listed PP Modules for separation.

The PP Modules will specify additional requirements that may impact the functionality of the Base PP. In these cases, it will be clearly labelled in the Modules. This is especially true for SFRs where the goal is not to iterate the whole requirement but to extend the necessary additions to an assignment or selection, e.g. auditable events. For these SFRs the intent is that the ST author would merge the SFRs of the PP Module(s) and the Base PP.

The available modules are:

- Protection Profile for Network Separation Mechanisms, VLAN Module Version 005, 2018-09-25 [VLAN]; and
- Protection Profile for Network Separation Mechanisms, VPN Module Version 005, 2018-09-25 [VPN].

1.3.3 Separation Use Cases

Below follow examples of how and when the separation mechanisms of the PP Modules can be applied. This is intended to help readers identify which mechanisms would meet their requirements.

Background

For systems which include components of different security criticalities, best practice is to compartmentalize such components into secluded groups. However, for sectors that require large and geographically distributed systems, this solution is not as simple. The networks that connect such systems may depend upon complex physical infrastructure. To alter or add new services to the system, while still maintaining the compartmentalization, could result in expensive and time-consuming endeavours. Especially as modern services will often require interconnectivity between system components.

As a result, compartmentalization by traditional physical separation is not viable. This poses new issues to security of the systems. The threat is an increase to both the attack surface and also the potential that an attack escalates throughout the system. Large interconnected networks can also suffer from decreased performance due to congestion or undesired interference between different services.

Link layer separation

VLANs are used to logically isolated networks at a low level. This permits networks to make use of the same underlying physical infrastructure, while maintaining the benefits of separation. As the separation is performed on a low level (link layer), the impact to a system's protocols and services are negligible. Any service will simply perceive the network as physically separated. It should also be noted that while more flexible than physically altering networks, secure implementation of VLANs will require a structured approach so that it is configured correctly, and requires awareness of the possible ways VLANs could be bypassed (e.g. through higher level protocols or physical access to the broadcast domain).

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

Internet layer separation

IPsec is used to create Virtual Private Networks (VPN). This enables the creation of a logical connection between two otherwise remote networks. While previously the networks would be able to communicate through a potentially untrusted network, this connection would be direct via the use of IPsec. Any services located on the higher levels of the stack (above the internet layer) could communicate with each other securely. Also, as the connection is perceived as direct between the networks, an IPsec VPN can also encapsulate untrusted traffic travelling through the connections of an internal or trusted network. The encapsulated traffic would not be able to control the route and therefore be unable to in any way affect the traversed network, apart from perhaps increasing the traffic load.

Application layer separation

SSH and TLS create cryptographic channels between devices or applications. This allows for a trusted channel that could even traverse networks, and thus separating the traffic from the rest of the network(s). This is a flexible approach and can mostly be implemented without any requirements on the underlying network infrastructure.

Most commonly SSH is used for administration, providing a relatively simple way to access remote systems for management purposes. For TLS the applications are more varied. It is commonly used to provide security for otherwise unencrypted protocols. As such it can also be used to add security to any other data that need to be sent over a network.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

2. CONFORMANCE CLAIM

This PP claims conformance to

- Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. Version 3.1, Revision 5. April 2017. CCMB-2017-04-001
- Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components. Version 3.1, Revision 5. April 2017. CCMB-2017-04-002
- Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components. Version 3.1, Revision 5. April 2017. CCMB-2017-04-003

as follows

- Part 2 extended,
- Part 3 conformant.

2.1 PP CLAIM

This PP does not claim any conformance to other Protection Profiles.

2.2 PACKAGE CLAIM

This PP claims conformance to the EAL4 package of security assurance requirements, augmented with ALC_FLR.2.

2.3 CONFORMANCE RATIONALE

Since this PP does not claim conformance to any PP, this section is not applicable.

2.4 CONFORMANCE STATEMENT

This PP requires demonstrable conformance of any ST or PP claiming conformance to this PP.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

3. SECURITY PROBLEM DEFINITION

The security problem definition defines the security problem that is addressed by the TOE as well as the assumptions on the operational environment necessary for the TOE to be able to address the security problem.

3.1 THREATS

This section of the security problem definition describes the threats that are countered by the TOE, its operational environment, or a combination of the two.

The assets to be protected consist of:

- TSF data – software, configuration files, audit records, authentication information and keys that are controlling the behaviour of the TSFs or is the result of a TSF and relevant to determine if the TOE is in a secure state.
- User data – Any other data of users that is stored on the TOE.

Attackers are unauthorised persons or IT entities that may have unlimited network access to the TOE.

Threat	Description
T.REMOTE	An attacker may be able to intercept traffic between the TOE and a trusted remote system, such as an administrator workstation.
T.UPDATE	An attacker may provide malicious TOE updates or old versions of the TOE software to introduce back doors or known exploitable weaknesses into the TOE.
T.TAMPER	An attacker may access TOE management functions and read, modify or destroy security critical system data or tamper with the security functions.

3.2 ORGANISATIONAL SECURITY POLICIES

The following organisational security policies are to be enforced by the TOE and the TOE environment.

OSP	Description
P.ACCOUNT	Administrators shall be accountable for the actions they conduct by generating sufficient audit records for the actions.
P.AUDIT	The TOE shall be able to record all of its security relevant events and transmit them securely to a remote audit server.
P.MANAGE	The TOE shall provide the means for authorised administrators to manage the security functions of the TOE.
P.SELFTEST	The TOE shall be able to verify the correctness of security functionality during start-up or operation.

3.3 ASSUMPTIONS

This section specifies the assumptions on the TOE environment that are necessary for the TOE to meet its security objectives.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

Assumption	Description
A.ADMIN	Authorised administrators are competent, non-hostile and follow all their guidance; however, they are capable of error.
A.AUDIT	The environment is able to receive, store and protect the audit records generated by the TOE and provides the means for analysis of the audit records.
A.PHYSICAL	The TOE is physically secure, i.e. no unauthorised persons have physical access to the TOE or its underlying platform.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

4. SECURITY OBJECTIVES

The security objectives provide a concise statement of the intended response to the security problem. It will describe which security needs will be addressed by the TOE and which will be addressed by the TOE environment, in the form of a statement of security objectives.

4.1 SECURITY OBJECTIVES FOR THE TOE

The following security objectives are to be met by the TOE.

Objective	Description
O.REMOTE	The TOE must be able to provide a trusted path between the TOE and other trusted IT systems ensuring authenticity, confidentiality and integrity of transmitted data.
O.UPDATE	The TOE must only accept updates that are newer than the currently running version and where the origin and integrity of the update can be trusted.
O.TAMPER	The TOE must protect itself against attempts by attackers to gain unauthorised access to management functionality.
O.AUDIT	The TOE must be able to provide an audit trail of security relevant events as well as for accountability of administrative actions and transmit them securely to a remote audit server.
O.MANAGE	The TOE must provide the means for an authorised administrator to configure and manage the TOE security functions. The management must be performed locally or through a secure communications channel.
O.SELFTEST	The TOE must be able to perform self-tests to verify correct operation of security functionality.

4.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

The following security objectives are to be met by the TOE environment.

Objective	Description
OE.ADMIN	Authorised administrators given privileges are competent, non-hostile and follow all their guidance; however, they are capable of error.
OE.AUDIT	The environment is able to receive, store and protect the audit records generated by the TOE and provides the means for analysis of the audit records.
OE.PHYSICAL	The TOE is physically secure, i.e. no unauthorised persons have physical access to the TOE and its underlying system.

4.3 SECURITY OBJECTIVES RATIONALE

4.3.1 Coverage

The following tables provide a mapping of security objectives both for the TOE and the TOE environment to the environment defined by the threats, policies and assumptions, illustrating that each security objective for the TOE covers at least one threat or policy, and that each security objective for the TOE environment covers at least one policy, threat or assumption.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

	T.REMOTE	T.UPDATE	T.TAMPER	P.ACCOUNT	P.AUDIT	P.MANAGE	P.SELFTEST	A.ADMIN	A.AUDIT	A.PHYSICAL
O.REMOTE	X									
O.UPDATE		X								
O.TAMPER			X							
O.AUDIT				X	X					
O.MANAGE						X				
O.SELFTEST							X			
OE.ADMIN								X		
OE.AUDIT									X	
OE.PHYSICAL										X

4.3.2 Sufficiency

The following rationale provides justification that the security objectives are suitable to counter each individual threat and that each security objective tracing back to a threat actually contributes to the mitigation of that threat.

Threat	Rationale for the security objectives
T.REMOTE	This threat is addressed by O.REMOTE which ensures that the trusted channels implemented by the TOE for administration maintains confidentiality and integrity of the traffic.
T.UPDATE	This threat is addressed by O.UPDATE that ensures the TOE will only accept legitimate updates.
T.TAMPER	This threat is addressed in part by O.TAMPER that ensures external attackers cannot bypass, deactivate or tamper with the TOE.

The following rationale provides justification that the security objectives of the TOE and the TOE environment are suitable to address each individual OSP and that each security objective tracing back to an OSP actually contributes in addressing the OSP

OSP	Rationale for the security objectives
P.ACCOUNT	This OSP is addressed by O.AUDIT that ensures that all authorised use of security functionality is recorded.
P.AUDIT	This OSP is addressed by O.AUDIT that ensures the TOE will provide an audit trail of security relevant events and that this trail can be securely transmitted to a remote audit server.
P.MANAGE	This OSP is addressed by O.MANAGE that ensures the TOE will provide management functionality to authorised administrators.
P.SELFTEST	This OSP is addressed by O.SELFTEST that ensures the TOE can and will perform self-tests to verify correct operation.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

The following rationale provides justification that the security objectives of the TOE environment are suitable to address each individual assumption and that each security objective tracing back to an assumption actually contributes in addressing the assumption.

Assumption	Rationale for the security objectives
A.ADMIN	Addressed by OE.ADMIN, which is identical to the assumption.
A.AUDIT	Addressed by OE.AUDIT, which is identical to the assumption.
A.PHYSICAL	Addressed by OE.PHYSICAL, which is identical to the assumption.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

5. EXTENDED COMPONENTS DEFINITION

The extended components in this Protection Profile for SFRs FTP_TST_EXT.1 and FTP_TUD_EXT.1 have been taken directly from the collaborative Protection Profile for Network Devices, Version 2.0, 5-May-2017 [cPPND].

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

6. SECURITY REQUIREMENTS

The conventions used in descriptions of the SFRs are as follows:

- Unaltered SFRs are stated in the form used in [CC] or their extended component definition;
- Assignment and Selections wholly or partially complete in the PP: indicated with **bold text**;

6.1 SECURITY FUNCTIONAL REQUIREMENTS

6.1.1 FAU_GEN.1 – Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

- Start-up and shutdown of the audit functions;
- All auditable events for the **not specified** level of audit; and
- **All administrative actions**
- **Self-test (automatic and administrator initiated)**
- **Trusted update (automatic and administrator initiated)**
- **[assignment: *other specifically defined auditable events*].**

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the ST/PP: **none**

Application note: All administrative actions means all administrative functions defined in FMT_SMF.1.

Application note: If the ST specifies security functionality in addition to the one specified in this PP, additional audit events might have to be added to meet the security objective O.AUDIT.

6.1.2 FIA_UAU.1 – Timing of authentication

FIA_UAU.1.1 The TSF shall allow [assignment: *list of TSF mediated actions*] on behalf of the user to be performed before the user is authenticated.

FIA_UAU.1.2 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.3 FIA_UID.1 – Timing of identification

FIA_UID.1.1 The TSF shall allow [assignment: *list of TSF-mediated actions*] on behalf of the user to be performed before the user is identified.

FIA_UID.1.2 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.4 FMT_MOF.1 – Management of functions in TSF

FMT_MOF.1.1 The TSF shall restrict the ability to [selection*: determine the behaviour of, disable, enable, modify the behaviour of*] the functions [assignment: *list of*

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

functions] to **administrators, [assignment: *the authorised identified roles*].**

Application note: The ST author should use FMT_MTD.1 to define the limitations of the roles defined in FMT_SMR.1.

6.1.5 FMT_MTD.1 – Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear, [*assignment*: other operations]*] the [assignment: *list of TSF data*] to **administrators, [assignment: *the authorised identified roles*].**

Application note: The ST author should use FMT_MTD.1 to define the limitations of the roles defined in FMT_SMR.1.

6.1.6 FMT_SMF.1 – Specification of management functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

- **Query software version**
- **Initiate update of the TOE software**
- **Initiate TOE self-test**
- **[assignment: *list of additional management functions to be provided by the TSF*].**

6.1.7 FMT_SMR.1 – Security management roles

FMT_SMR.1.1 The TSF shall maintain the roles **administrator, [assignment: *the authorised identified roles*].**

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

Application note: In the case that more roles or different types of administrators exists for the TOE the ST author should use FMT_SMR.1.1 to specify these roles.

6.1.8 FPT_STM.1 – Time stamps

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps.

Application note: In the case that a TOE depends on an external source for time information the ST author should specify this in the form of an objective for the TOE Operational Environment.

6.1.9 FPT_TST_EXT.1 – TSF Testing

FPT_TST_EXT.1.1 The TSF shall run a suite of the following self-tests **during initial start-up (on power on) and [selection:** *periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self-tests should occur]*] to demonstrate the correct operation of the TSF: [assignment: *list of self-tests run by the TSF*].

Application note: If because of the nature of the TOE such a start-up process does hardly ever take place, and if the TOE does not perform tests periodically, then the possibility for an administrator to initiate self-tests should exist, together with guidance on how.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

6.1.10 FPT_SKP_EXT.1 – Protection of TSF Data (for reading of all pre-shared, symmetric and private keys)

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric keys, and private keys.

Application note: This requirement is for the protection keys, key material, and authentication credentials from unauthorized disclosure. This data should only be accessed for the purposes of their assigned security functionality, and there is no need for them to be displayed/accessed at any other time. It applies to the credentials for administrator access, but may also apply to any other key material maintained for any other PP modules providing trusted channels.

6.1.11 FPT_TUD_EXT.1 – Trusted Update

FPT_TUD_EXT.1.1 The TSF shall provide Security Administrators the ability to query the currently executing version of the TOE firmware/software as well as the most recently installed version of the TOE firmware/software.

FPT_TUD_EXT.1.2 The TSF shall provide Security Administrators the ability to manually initiate updates to TOE firmware/software and [selection: *support automatic checking for updates, support automatic updates, no other update mechanism*].

Application note: The selection in FPT_TUD_EXT.1.2 distinguishes the support of automatic checking for updates and support of automatic updates. The first option refers to a TOE that checks whether a new update is available, communicates this to the administrator (e.g. through a message during an administrator session, through log files) but requires some action by the administrator to actually perform the update. The second option refers to a TOE that checks for updates and automatically installs them upon availability.

FPT_TUD_EXT.1.3 The TSF shall provide means to authenticate firmware/software updates to the TOE using a [selection: *digital signature mechanism, published hash*] prior to installing those updates.

Application note: The authentication method referenced in the selection of FPT_TUD_EXT.1.3 should be further detailed in FCS_COP.1. The ST author should choose the mechanism implemented by the TOE; it is of course acceptable to implement both mechanisms.

6.1.12 FCS_COP.1 – Cryptographic operation

FCS_COP.1.1 The TSF shall perform [**selection: *digital signature verification, cryptographic hashing***] in accordance with a specified cryptographic algorithm [assignment: *cryptographic algorithm*] and cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*]

Application note: This SFR is required for authentication of updates and should detail the authentication method referenced in FPT_TUD_EXT.1.3.

6.1.13 FTP_TRP.1 – Trusted path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and **remote** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from **modification, disclosure**, **[assignment*: other types of integrity or confidentiality violation***]**.

Application note: Should cryptography be used to fulfil the protection requirements the ST author must define SFRs for the functionality related to cryptography. If the cryptographic

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

mechanism is identical to that of a selected PP Module, the TOE does not require separate functionality for its trusted path.

FTP_TRP.1.2 The TSF shall permit **remote users** to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for **initial user authentication, remote administration, [assignment: *other services for which trusted path is required*]**.

Application note: The remote user(s) of this SFR should cover the administrator, as to satisfy the security objective O.REMOTE. Local administration is covered by the assumption A.PHYSICAL.

6.1.14 FTP_ITC.1 – Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall provide a communication channel between itself and another trusted IT product that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification and disclosure.

Application note: Should cryptography be used to fulfil the protection requirements the ST author must define SFRs for the functionality related to cryptography. If the cryptographic mechanism is identical to that of a selected PP Module, the TOE does not require separate functionality for its trusted path.

FTP_ITC.1.2 The TSF shall permit [selection: *the TSF, another trusted IT product*] initiate communication via the trusted channel.

Application note: The selection in FTP_ITC.1.2 will depend on how the audit reporting to a central server happens. For example, an administrator could access the records remotely, a central audit server could initiate the load, or the TOE itself can transmit the records automatically to the central server.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **transfer of audit data, [assignment*: list of functions for which a trusted channel is required*].**

Application note: FTP_ITC.1 should cover the connection to a remote audit server to fulfil the requirement O.AUDIT.

6.2 Security Functional Requirements Rationale

6.2.1 Coverage

The following table provides a mapping of SFR to the security objectives, showing that each security functional requirement addresses at least one security objective and that all security objectives are addressed by one or more SFRs.

	O.REMOTE	O.UPDATE	O.TAMPER	O.AUDIT	O.MANAGE	O.SELFTEST
FAU_GEN.1				X		
FIA_UAU.1			X			
FIA_UID.1			X			

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

FMT_MOF.1			X			
FMT_MTD.1			X			
FMT_SMF.1					X	
FMT_SMR.1					X	
FPT_STM.1				X		
FPT_TST_EXT.1						X
FTP_TUD_EXT.1		X				
FPT_SKP_EXT.1	X					
FTP_TRP.1	X					
FTP_ITC.1				X		
FCS_COP.1		X				

6.2.2 Sufficiency

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives.

Security objective	Rationale how the SFRs are meeting the security objective
O.REMOTE	The objective: • The TOE must be able to provide a trusted path between the TOE and other trusted IT systems ensuring authenticity, confidentiality and integrity of transmitted data. is met by: • FTP_TRP.1 which ensures that remote authentication and administration take place over a secure channel.
O.UPDATE	The objective: • The TOE must only accept updates that are newer than the currently running version and where the origin and integrity of the update can be trusted. is met by: • FTP_TUD_EXT.1 which ensures that updates are performed on a regular basis or can be imitated by administrators, and that the TOE is able to verify the updates. • FCS_COP.1 provides the TOE with the required cryptographic operation to authenticate the updates.
O.TAMPER	The objective: • The TOE must protect itself against attempts by attackers to gain unauthorised access to management functionality. is met by: • FIA_UAU.1 ensures that administrators have to authenticate before performing any actions. • FIA_UID.1 ensures that administrators have to identify before performing any actions. • FMT_MOF.1 ensures that management of security functions is restricted to authorised users.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

	• FMT_MTD.1 Ensures that ensures that management of TSF data is restricted to authorised users.
O.AUDIT	The objective: • The TOE must be able to provide an audit trail of security relevant events as well as for accountability of administrative actions and transmit them securely to a remote audit server. is met by: • FAU_GEN.1 ensures that audit records can be generated for security-relevant events. • FPT_STM.1 ensures that the audit records are accompanied by accurate time stamps. • FTP_ITC.1 ensures that audit records can be transferred securely to an audit server.
O.MANAGE	The objective: • The TOE must provide the means for an authorised administrator to configure and manage the TOE security functions. The management must be performed locally or through a secure communications channel. is met by: • FMT_SMF.1 ensures that the security functions can be managed. • FMT_SMR.1 ensures that there are roles authorised for management.
O.SELFTEST	The objective: • The TOE must be able to perform self-tests to verify correct operation of security functionality. is met by: • FTP_TST_EXT.1 ensures that the TOE can perform self-tests to verify its secure operation.

6.2.3 Security Functional Requirements Dependency Analysis

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives.

SFR	Dependencies	Resolved
FAU_GEN.1	FPT_STM.1	Resolved
FIA_UAU.1	FIA_UID.1	Resolved
FIA_UID.1	No dependencies	–
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	Resolved
FMT_MTD.1	FMT_SMR.1 FMT_SMF.1	Resolved
FMT_SMF.1	No dependencies	–
FMT_SMR.1	FIA_UID.1	Resolved
FPT_STM.1	No dependencies	–

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

FPT_TST_EXT.1	No dependencies	–
FPT_TUD_EXT.1	FCS_COP.1	Resolved
FPT_SKP_EXT.1	No dependencies	–
FTP_TRP.1	No dependencies	–
FTP_ITC.1	No dependencies	–
FCS_COP.1	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Not resolved. Importing, generation and deletion of keys are not required for the authentication of updates specified in FTP_TUD_EXT.1.

6.3 Security Assurance Requirements

The security assurance requirements of this Security are those defined for the assurance level EAL4 augmented with ALC_FLR.2.

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
	ALC_FLR.2 Flaw reporting procedures (augmentation)
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: basic design
	ATE_FUN.1 Functional testing

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

	ATE_IND.2 Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis

6.4 Security Assurance Requirements Rationale

In general, assurance requirements must be commensurate with the exposure of systems to untrustworthy and unauthorised entities, but also the risk and value of the assets it protects.

Since the architecture addressed by the type of TOE specified in this PP includes systems where both factors are likely to be high, a sufficient level of assurance must be selected to provide system users with appropriate assurance that the system will be able to withstand such threats.

The TOE is expected to provide sufficient assurance to reliably support mechanisms for separating network traffic and requires a level of assurance that includes the evaluation of possible interference between different types of traffic.

The EAL4 level was also deemed as the minimum level of assurance because it shall support separation of security and safety critical communication where leakage and interference must be prevented. EAL4 is also the lowest assurance package which includes source-code analysis. The source code analysis is necessary to assess the implementation quality and ensure that the TOE is correctly implemented and does not contain any malicious code.

EAL4 is augmented by ALC_FLR.2 as during operations new vulnerabilities may be discovered, either through developer actions (e.g., developer testing) or those discovered by others. It requires the developer to have procedures addressing these vulnerabilities. The process used by the developer corrects any discovered vulnerabilities and performs an analysis to ensure that no new vulnerabilities are created when fixing the discovered ones.

Dependencies within the EAL package selected (EAL4) for the security assurance requirements have been considered by the authors of CC Part 3 and are not analysed here again. The augmentation by flaw remediation, ALC_FLR.2, has no dependencies on other requirements. The security functional requirements in this Protection Profile do not introduce dependencies on any security assurance requirement; neither do the security assurance requirements in this Protection Profile introduce dependencies on any security functional requirement.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

7. REFERENCES

[CC] Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model, April 2017, Version 3.1 Revision 5, CCMB-2017-04-001; Part 2: Security functional Components, April 2017, Version 3.1 Revision 5, CCMB-2017-04-002; Part 3: Security Assurance Components, April 2017, Version 3.1 Revision 5, CCMB-2017-04-003.

[CEM] Common Methodology for Information Technology Security Evaluation. Evaluation Methodology. April 2017, Version 3.1, Revision 5, CCMB-2017-04-004.

[cPPND] collaborative Protection Profile for Network Devices, Version 2.0 (5 May 2017).

[ISO15446] Technical Report ISO/IEC TR 15446, Information technology – Security techniques – Guide for the production of Protection Profiles and Security Targets, Second edition 2009-03-01.

[PPST-Guide] The PP/ST Guide, August 2010, Version 2, Revision 0, Bundesamt für Sicherheit in der Informationstechnik.

[VLAN] Protection Profile for Network Separation Mechanisms, VLAN Module, Version 005, 2018-09-25. The Protection Profile module developed as part of the CYRail-project under European Union's Horizon 2020 research and innovation programme (grant agreement no. 730843).

[VPN] Protection Profile for Network Separation Mechanisms, VPN Module, Version 005, 2018-09-25. The Protection Profile module developed as part of the CYRail-project under European Union's Horizon 2020 research and innovation programme (grant agreement no. 730843).

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

EU Project 730843

CYbersecurity in the RAILway sector

D6.1 – Protection Profile for Network Separation Mechanisms, VLAN Module

Due date of deliverable: 2018-09-30

Leader of this Deliverable: atsec information security AB

Reviewed: AIRBUS

Document status		
Revision	Date	Description
001	2018-01-22	Initial draft version
002	2018-04-11	Adjustments of PP Module structure for consistency with Base PP
003	2018-08-06	Final draft for internal review
004	2018-09-04	Release version
005	2018-09-25	Address review comments
006	2019-02-14	Minor update due to EU review comments

Start date of project: 2016-10-01 Duration: 24 months

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

Company	Details of contribution
atsec	Specification of the security requirements in a Protection Profile Module
AIRBUS	Performed review

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

OBJECTIVES OF THE DELIVERABLE

In **D6.1 – Protection Profiles Specifications** a Common Criteria Protection Profile will be developed using existing standards and framework related to Protection Profiles. This includes the Common Criteria (ISO/IEC 15408) and guides (ISO/IEC TR 15466), as well as experience from existing Protection Profiles, standards and projects such as D-MILS, TAPPS and other related projects.

It will include the description of the operational environment (combination of threats, assumptions and policies that the components need to enforce) based on the operational scenario identified in WP2 and risk assessments in WP3 as well as identified threats in WP4. Security objectives for the systems and the operational environment will be derived based on mitigation strategies and countermeasures identified in WP5. Security functional requirements (SFRs) and security assurance requirements (SARs) will describe security functionality that need to be provided by specific system and evaluation activities to be performed to ensure that security mechanisms in these systems are sufficient and implemented correctly.

This part of the deliverable is the VLAN Module of the Base Protection Profile for Network Separation Mechanisms.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

TABLE OF CONTENTS

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

1. INTRODUCTION

This Protection Profile Module is intended to be used in conjunction with the Base Protection Profile for Network Separation Mechanisms.

It was developed as part of the CYRail-project under European Union's Horizon 2020 research and innovation programme (grant agreement no. 730843).

1.1 PROTECTION PROFILE MODULE REFERENCE

Title:	Protection Profile for Network Separation Mechanisms, VLAN Module
PP Version:	005
Status:	Released
Date:	2018-09-25
Keywords:	Network device, Network separation, Virtual LAN, VLAN, PP Module, Base PP

This Protection Profile (PP) has been structured in accordance with [CC] Part 1. The main sections of the PP are the introduction, security problem definition, security objectives, security requirements and annexes.

1.2 BASE PP IDENTIFICATION

Base Protection Profile for Network Separation Mechanisms, Version: 009, 2018-09-25

1.3 TOE OVERVIEW

This PP Module defines the minimum security requirements for Virtual Local Area Network (VLAN) separation. It must be used together with the Base PP, as it only describes additional functionality for separation in contrast to all the necessary functionality of a TOE. The VLAN separation works at the link layer to create logical broadcast domains to partition and isolate computer networks. This PP Module is one of multiple that each describe a different mechanism to separate network traffic.

1.3.1 TOE Type

The TOE is a network device used for aggregation and isolation of network traffic. It may be a stand-alone component or may be part of a boundary protection solution providing additional functionality.

1.3.2 Usage and Major Security Features of a TOE

The TOE is intended to be used where computer networks need to be separated and isolated, such as controlled security critical traffic from untrusted user traffic. The separation will be provided at the link layer for networks that may otherwise be physically connected through the TOE. The link layer is the lowest level of the Internet Protocol Suite.

VLANs will be used to partition and isolate the flow of network traffic into different logical broadcast domains. Ethernet frames will be associated with a specific VLAN and only be forwarded to their intended destinations, regardless of any higher-level protocols used. The result of the separation is to reduce the attack surface of a computer network.

VLANs will only protect the traffic flow through the TOE at the link layer. This means that the TOE cannot be used to guarantee confidentiality or integrity of the network traffic. In the case that an attacker would gain physical access a link or endpoint of a different broadcast domain, the TOE cannot provide any protection. Neither can this PP control access to the network through higher levels protocols that route network traffic between the broadcast domains.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

A TOE compliant with this PP Module must provide the following security functionality:

- VLAN Information flow control – Controlling network traffic sent through the TOE to only allow traffic to be forwarded within its respective broadcast domain.
- Management of VLAN functionality
- Recording of auditable events related to VLAN management.

1.3.3 Available non-TOE Hardware/Software/Firmware

Should the TOE implement aggregation of VLAN traffic through VLAN tagging, there is a need for a secure device on the other side of this link that supports the tagging of the TOE.

This Module has no need for any other specific non-TOE components, other than what is stated in the Base PP.

1.4 TOE Description

The TOE is a network device that provides partitioning of physical LANs into logically isolated broadcast domains. The separation is done at the link layer for ethernet frames on the same physical LAN, but creates the appearance and functionality of multiple different networks. These Virtual LANs (VLANs) can ensure that network applications and traffic is separated, despite using the same physical infrastructure. It reduces the need for multiple sets of cabling and networking device to be deployed. Also, the use of VLANs offer flexibility as changes are done to device configurations rather than physical cables and network infrastructure.

1.4.1 VLAN Separation

The protocol most commonly used today to configure VLANs is IEEE 802.1Q. The IEEE committee defined this method of multiplexing VLANs in an effort to provide multivendor VLAN support on Ethernet networks. The standard defines a system of VLAN tagging for Ethernet frames and the accompanying procedures to be used by bridges and switches in handling such frames. The standard also contains provisions for a quality-of-service prioritization scheme commonly known as IEEE 802.1p and defines the Generic Attribute Registration Protocol.

Since VLANs separates the communication at the link layer, the separation is done by network devices operating at link layer. The level of security depends on the ability of the network device to ensure this separation. This will reduce the attack surface as it will not be visible at for the IP traffic. The configuration of VLANs is less flexible since the VLAN tagging must be consistently managed at the network device level and not by applications or services using the network. This means that VLAN should be used for types of services or services that are expected to be static, such as the separation of administrative communication from customer services.

For an attacker with access to the frames, VLANs will not provide any confidentiality, only separation. So, if confidentiality is an issue, payload encryption is necessary, maybe by using IPsec or TLS, which also is providing additional isolation at internet or application layers.

1.4.2 VLAN Attacks

There exists a number of common security issues related to VLANs. One type of attack is known as VLAN hopping, meaning unauthorised access between VLANs. Spoofed traffic could make the device believe that the attacker is located on another VLAN. Other attacks can manipulate the underlying forwarding functionality of a device providing VLANs. Should it be possible to affect such functionality, any above flow control such as VLANs would no longer have any effect. An example is to spoof Address Resolution Protocol (ARP) messages.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

2. CONSISTENCY RATIONALE

The TOE of the Base PP is a network device that provides network separation. However, the Base PP only specifies core requirements for a generic network device. Network separation can be implemented in various ways, with different benefits and drawbacks. Therefore, the separation requirements are specified in PP Modules, such as this one, to allow for selection of the desired separation mechanism(s). It is guaranteed that the Base PP provides network separation as it is mandatory to use it together with at least one separation Module.

This PP Module does not describe functionality of a network device but specifies the requirements for isolation of network traffic on the link layer through the use of VLANs. Properly implemented VLAN separation can guarantee that traffic within logical broadcast domains transmitted through the TOE is isolated.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

3. CONFORMANCE CLAIM

This PP Module claims conformance to [CC]

- Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. Version 3.1, Revision 5. April 2017. CCMB-2017-04-001
- Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components. Version 3.1, Revision 5. April 2017. CCMB-2017-04-002
- Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components. Version 3.1, Revision 5. April 2017. CCMB-2017-04-003

as follows

- Part 2 extended,
- Part 3 conformant.

3.1 PP CLAIM

Since a PP Module cannot not claim any conformance to other Protection Profiles, this section is not applicable.

3.2 PACKAGE CLAIM

This PP Module inherits the conformance claim to the EAL4 package of security assurance requirements, augmented with ACL_FLR.2, from its Base PP.

3.3 CONFORMANCE RATIONALE

Since this PP Module does not claim conformance to any PP, this section is not applicable.

3.4 CONFORMANCE STATEMENT

This PP Module inherits the demonstrable conformance statement of its Base PP.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

4. SECURITY PROBLEM DEFINITION

The security problem definition defines the security problem that is addressed by the TOE as well as the assumptions on the operational environment necessary for the TOE to be able to address the security problem.

4.1 THREATS

This section of the security problem definition describes the threats that are countered by the TOE, its operational environment, or a combination of the two.

The assets to be protected consist of:

- User data – Network traffic transmitted through the TOE within a specific broadcast domain.

Attackers are unauthorized persons or IT entities located on networks that are connected through the TOE. Attackers could, but are not guaranteed to, be located within a logical broadcast domain.

Threat	Description
T.FLOW-VLAN	An attacker is able to unauthorizedly access the network traffic of a broadcast domain through the TOE which is different from the one the attacker is located on.

4.2 ORGANISATIONAL SECURITY POLICIES

The following organisational security policies are to be enforced by the TOE and the TOE environment.

OSP	Description
P.AUDIT-VLAN	The TOE must be able to provide an audit trail of security relevant events as well as accountability for authorised use of security functions.
P.MANAGE-VLAN	The TOE shall provide the means for authorised administrators to manage the security functionality of the TOE.

Note: This PP Module requires additional management and audit functionality than what is specified in the Base PP. To emphasise this, the policies P.AUDIT and P.MANAGE are also present in this PP Module. The additional OSPs are covered by additional security objectives and (when addressed by the TOE) security functional requirements.

4.3 ASSUMPTIONS

This section specifies the assumptions on the TOE environment that are necessary for the TOE to meet its security objectives.

Assumption	Description
A.PEER-VLAN	It is assumed that, for interfaces of the TOE that are configured to accept tagged frames, the endpoint(s) connected to that interface will behave as expected and not send maliciously tagged frames to the TOE.
A.LINKS	It is assumed that the physical links between the TOE and its endpoints of one broadcast domain are not accessible to unauthorised attackers of a

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

	different broadcast domain.
A.ROUTING	It is assumed that any external routing on the between the broadcast domains of the TOE does not represent any problems to the security objectives, as the data link separation cannot counteract this.

Note: All assumptions of the Base PP also apply to an ST claiming compliance to this PP Module. For this reason, they are not repeated here.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

5. SECURITY OBJECTIVES

The security objectives provide a concise statement of the intended response to the security problem. It will describe which security needs will be addressed by the TOE and which will be addressed by the TOE environment, in the form of a statement of security objectives.

5.1 SECURITY OBJECTIVES FOR THE TOE

The following security objectives are to be met by the TOE.

Objective	Description
O.FLOW-VLAN	The TOE must provide a means for separation of VLANs to ensure that network traffic transmitted through the TOE is restricted to its respective broadcast domains.
O.AUDIT-VLAN	The TOE must be able to generate security relevant events as well as events related to authorised use of security functions.
O.MANAGE-VLAN	The TOE must provide the means for an authorised administrator to configure and manage the TOE security functionality.

5.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

The following security objectives are to be met by the TOE environment.

Objective	Description
OE.PEER-VLAN	It is assumed that, for interfaces of the TOE that are configured to accept tagged frames, the endpoint connected to that interface will behave as expected and not send maliciously tagged frames to the TOE.
OE.LINKS	It is assumed that the physical links between the TOE and its endpoints of one broadcast domain are not accessible to unauthorised attackers of a different broadcast domain.
OE.ROUTING	It is assumed that any external routing on the between the broadcast domains of the TOE does not represent any problems to the security objectives, as the data link separation cannot counteract this.

5.3 SECURITY OBJECTIVES RATIONALE

5.3.1 Coverage

The following tables provide a mapping of security objectives both for the TOE and the TOE environment to the environment defined by the threats, policies and assumptions, illustrating that each security objective for the TOE covers at least one threat or policy, and that each security objective for the TOE environment covers at least one policy, threat or assumption.

	T. FLOW-VLAN	O:AUDIT-VLAN	O.MANAGE-VLAN	A.PEER-VLAN	A.LINKS	A.ROUTING

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

O.FLOW-VLAN	X					
O.AUDIT-VLAN		X				
O.MANAGE-VLAN			X			
OE.PEER-VLAN				X		
OE.LINKS					X	
OE.ROUTING						X

5.3.2 Sufficiency

The following rationale provides justification that the security objectives are suitable to counter each individual threat and that each security objective tracing back to a threat actually contributes to the mitigation of that threat.

Threat	Rationale for the security objectives
T.FLOW-VLAN	This threat is addressed by O.FLOW-VLAN, which ensures that the TOE will provide proper separation of traffic via VLANs. OE. PEER-VLAN, OE.LINKS and OE.ROUTING also ensure that the separation cannot be bypassed through ways which VLANs are incapable of addressing.

The following rationale provides justification that the security objectives of the TOE and the TOE environment are suitable to address each individual OSP and that each security objective tracing back to an OSP actually contributes in addressing the OSP

OSP	Rationale for the security objectives
P.AUDIT-VLAN	This OSP is addressed by O.AUDIT-VLAN, which ensures that all security related events are recorded. In addition, it is supported by the OE.AUDIT from the Base PP for the collection, storage and protection the audit records, as well as for providing the means for analysis of the audit records.
P.MANAGE-VLAN	This OSP is addressed by O.MANAGE-VLAN that ensures the TOE will provide management functionality to authorised administrators.

The following rationale provides justification that the security objectives of the TOE environment are suitable to address each individual assumption and that each security objective tracing back to an assumption actually contributes in addressing the assumption.

Assumption	Rationale for the security objectives
A.PEER-VLAN	Addressed by OE.PEER-VLAN, which is identical to the assumption.
A.LINKS	Addressed by OE.LINKS, which is identical to the assumption.
A.ROUTING	Addressed by OE.ROUTING, which is identical to the assumption.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

6. EXTENDED COMPONENTS DEFINITION

This module does not define any extended components.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

7. SECURITY REQUIREMENTS

The conventions used in descriptions of the SFRs are as follows:

- Unaltered SFRs are stated in the form used in [CC] or their extended component definition;
- Assignment and Selections wholly or partially complete in the PP: indicated with **bold text**;

7.1 SECURITY FUNCTIONAL POLICIES

7.1.1 VLAN Flow Control Policy

The TOE must implement an information flow control SFP called “VLAN Flow Control Policy” ensuring the separation of link layer network traffic. The policy must separate network traffic flowing through the TOE via the use of VLANs to create virtual broadcast domains.

7.2 SECURITY FUNCTIONAL REQUIREMENTS

7.2.1 FAU_GEN.1 – Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

- Start-up and shutdown of the audit functions;
- All auditable events for the **not specified** level of audit; and
- **Configuration of VLAN functionality;**
- **[assignment: *other specifically defined auditable events*].**

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the ST/PP: **none**

Application note: As VLANs require specific auditable events, this SFR is present in both this PP Module and the Base PP. In the ST it is expected that this SFR is merged with the equivalent SFR (FAU_GEN.1) of the Base PP and not iterated as if they were two different SFRs.

7.2.2 FDP_IFC.1 – Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the **VLAN Flow Control Policy** on

subjects: interfaces;

information: ethernet frames;

operations:

- **permit or deny link layer network traffic**
- **tag or untag ethernet frames**

This project has received funding from the European Union’s Horizon2020 research and innovation programme under grant agreement No730843

7.2.3 FDP_IFF.1 – Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the **VLAN Flow Control Policy** based on the following types of subject and information security attributes:

subject security attributes:

- **interface identifier**
- **VLAN identifier assigned to interface**

information security attributes:

- **VLAN tag (IEEE 802.1Q)**
- **destination MAC address**

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold:

- **The receiving and transmitting interfaces (subjects) are configured to be in the same VLAN.**

FDP_IFF.1.3 The TSF shall enforce the

- **Tagging and untagging of frame headers as per IEEE 802.1Q, for packets received or transmitted via interfaces assigned with multiple VLANs.**

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules:

- **none**

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules:

- **The receiving and transmitting interfaces (subjects) are not configured to be in the same VLAN.**
- **An ethernet frame has erroneous or unexpected VLAN tag(s).**

7.2.4 FMT_MSA.1 – Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the **VLAN Flow Control Policy** to restrict the ability to [selection: *change_default, query, modify, delete, [assignment: other operations]*] the security attributes:

- **VLAN identifier assigned to interface**
- **[assignment: *list of security attributes*]**

to **administrators, [assignment: *the authorised identified roles*]**.

Application note: The authorised roles may be the ones defined in FMT_SMR.1 of the Base PP, but may also be separate roles in case the management of the trusted channel is separate from the management of the functionality of the Base PP.

7.2.5 FMT_MSA.3 – Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the **VLAN Flow Control Policy** to provide **restrictive** default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the **administrators, [assignment: *the authorised identified roles*]** to specify alternative initial values to override the default values when an object or information is created.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

7.2.6 FMT_MOF.1 – Management of functions in TSF

FMT_MOF.1.1 The TSF shall restrict the ability to [selection*: determine the behaviour of, disable, enable, modify the behaviour of*] the functions [assignment: *list of functions*] to [assignment: *the authorised identified roles*].

Application note: See the application note for FMT_MSA.1.

7.2.7 FMT_MTD.1 – Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear, [*assignment*: other operations]*] the [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*].

Application note: See the application note for FMT_MSA.1.

7.2.8 FMT_SMF.1 – Specification of management functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions:

- **Assignment of VLANs to interfaces**
- **[assignment: *list of additional VLAN management functions to be provided by the TSF*].**

Application note: As VLANs presents additional management functionality, this SFR is present in both this PP Module and the Base PP. In the ST it is expected that this SFR is merged with the equivalent SFR (FMT_SMF.1) of the Base PP and not iterated as if they were two different SFRs.

7.3 Security Functional Requirements Rationale

7.3.1 Coverage

The following table provides a mapping of SFR to the security objectives, showing that each security functional requirement addresses at least one security objective and that all security objectives are addressed by one or more SFRs.

	O.FLOW-VLAN	O.AUDIT-VLAN	O.MANAGE-VLAN
FAU_GEN.1		X	
FDP_IFC.1	X		
FDP_IFF.1	X		
FMT_MSA.1			X
FMT_MSA.3			X
FMT_MOF.1			X
FMT_MTD.1			X
FMT_SMF.1			X

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

7.3.2 Sufficiency

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives.

Security Objective	Rationale how the SFRs are meeting the security objective
O.FLOW-VLAN	The objective: • The TOE must provide a means for separation of VLANs to ensure that network traffic transmitted through the TOE is restricted to its respective broadcast domains. is met by: • FDP_IFC.1 and FDP_IFF.1 ensures that the TOE enforces the VLAN Flow Control Policy by providing separation of network traffic.
O.AUDIT-VLAN	The objective: • The TOE must be able to provide an audit trail of security relevant events. is met by: • FAU_GEN.1 ensures that audit records can be generated for security relevant events and authorised use of security functionality. • FPT_STM.1 in the Base PP ensures that audit records are accompanied by accurate time stamps.
O.MANAGE-VLAN	The objective: • The TOE must provide the means for an authorised administrator to configure and manage the TOE security functionality. is met by: • FMT_MOF.1 then restricts the ability to modify the behaviour of functions to identified authorized roles. • FMT_MTD.1 restrict the changes to TSF data associated with the security functions to identified authorized roles. • FMT_MSA.1 and FMT_MSA.3 ensures that initialization and management of VLAN security attributes is protected. • FMT_SMF.1 ensures that the TOE provides the ability to configure security functionality of the VLAN.

7.3.3 Security Functional Requirements Dependency Analysis

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives.

SFR	Dependencies	Resolved
FAU_GEN.1	FPT_STM.1	Resolved, as FPT_STM.1 is part of the Base PP.
FDP_IFC.1	FDP_IFF.1	Resolved
FDP_IFF.1	FPD_IFC.1	Resolved
FMT_MSA.3	FMT_MSA.1	Resolved

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

	FMT_SMR.1	Resolved
FMT_MSA.1	[FDP_IFC.1 or FDP_ACC.1] FMT_SMF.1 FMT_SMR.1	Resolved by FDP_IFC.1 Resolved Resolved, as FMT_SMR.1 is part of the Base PP. If any management functions such as assignment of VLAN interfaces are done it must be restricted to a role defined in the Base PP.
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	Resolved Resolved by the Base PP. If any change of functions is possible it must be restricted to a role defined in FMT_SMR.1 of the Base PP.
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	Resolved Resolved by the Base PP. If any change to TSF data is possible it must be restricted to a role defined in FMT_SMR.1 of the Base PP.
FMT_SMF.1	No dependencies	–

7.4 Security Assurance Requirements

The security assurance requirements of this Security are those defined for the assurance level EAL4 augmented with ALC_FLR.2, as specified in the Base PP.

7.5 Security Assurance Requirements Rationale

The assurance requirements are inherited from the Base PP.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

8. REFERENCES

[Base] Base Protection Profile for Network Separation Mechanisms, Version 009, 2018-09-25. The Base Protection Profile developed as part of the CYRail-project under European Union's Horizon 2020 research and innovation programme (grant agreement no. 730843).

[CC] Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model, April 2017, Version 3.1 Revision 5, CCMB-2017-04-001; Part 2: Security functional Components, April 2017, Version 3.1 Revision 5, CCMB-2017-04-002; Part 3: Security Assurance Components, April 2017, Version 3.1 Revision 5, CCMB-2017-04-003.

[CEM] Common Methodology for Information Technology Security Evaluation. Evaluation Methodology. April 2017, Version 3.1, Revision 5, CCMB-2017-04-004.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

EU Project 730843

CYbersecurity in the RAILway sector

D6.1 – Protection Profile for Network Separation Mechanisms, VPN Module

Due date of deliverable: 2018-09-30

Leader of this Deliverable: atsec information security AB

Reviewed: AIRBUS

Document status		
Revision	Date	Description
001	2018-01-22	Initial draft version
002	2018-04-11	Adjustments of PP Module structure for consistency with Base PP
003	2018-08-11	Final draft for internal review
004	2018-09-04	Release version
005	2018-09-25	Address review comments
006	2019-02-14	Minor update due to EU review comments

Start date of project: 2016-10-01 Duration: 24 months

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

REPORT CONTRIBUTION

Company	Details of contribution
atsec	Specification of the security requirements in a Protection Profile Module
AIRBUS	Performed review

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

OBJECTIVES OF THE DELIVERABLE

In **D6.1 – Protection Profiles Specifications** a Common Criteria Protection Profile will be developed using existing standards and framework related to Protection Profiles. This includes the Common Criteria (ISO/IEC 15408) and guides (ISO/IEC TR 15466), as well as experience from existing Protection Profiles, standards and projects such as D-MILS, TAPPS and other related projects.

It will include the description of the operational environment (combination of threats, assumptions and policies that the components need to enforce) based on the operational scenario identified in WP2 and risk assessments in WP3 as well as identified threats in WP4. Security objectives for the systems and the operational environment will be derived based on mitigation strategies and countermeasures identified in WP5. Security functional requirements (SFRs) and security assurance requirements (SARs) will describe security functionality that need to be provided by specific system and evaluation activities to be performed to ensure that security mechanisms in these systems are sufficient and implemented correctly.

This part of the deliverable is the VPN Module of the Base Protection Profile for Network Separation Mechanisms.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

TABLE OF CONTENTS

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

1. INTRODUCTION

This Protection Profile Module is intended to be used in conjunction with the Base Protection Profile for Network Separation Mechanisms.

It was developed as part of the CYRail-project under European Union's Horizon 2020 research and innovation programme (grant agreement no. 730843).

1.1 PROTECTION PROFILE MODULE REFERENCE

Title:	Protection Profile for Network Separation Mechanisms, VPN Module
PP Version:	005
Status:	Released
Date:	2018-09-25
Keywords:	Network device, Network separation, Virtual Private Network, VPN, IPsec, TLS, SSH, HTTPS, PP Module, Base PP

This Protection Profile (PP) has been structured in accordance with [CC] Part 1. The main sections of the PP are the introduction, security problem definition, security objectives, security requirements and annexes.

1.2 BASE PP IDENTIFICATION

Base Protection Profile for Network Separation Mechanisms, Version: 009, 2018-09-25

1.3 TOE OVERVIEW

This PP Module defines the minimum security requirements for a TOE providing Virtual Private Networks (VPNs) and/or secure communication channels over computer networks. Through these methods, the TOE provides separation of traffic within and outside of said channels. It must be used together with the Base PP, as it only describes the additional functionality for separation, in contrast to all the necessary functionality of a TOE.

VPNs are established using IPsec, an end-to-end security scheme operating at the internet layer of the Internet Protocol Suite. The secure channels are established using SSH or TLS, two cryptographic protocols operating at the application layer of the Internet Protocol Suite. This PP Module is one of multiple that each describe a different mechanism to separate network traffic.

1.3.1 TOE Type

The TOE is a network device that provides isolation of network traffic through the use of a trusted channel between itself and another trusted component. It may be a stand-alone component or may be part of a boundary protection solution providing additional functionality.

1.3.2 Usage and Major Security Features of a TOE

The TOE is intended to be used where traffic between computer networks, or between components within such a network, need to be isolated and separated from entities that reside within networks that the traffic is transmitted over. The separation will be provided at the Internet and/or application layer, depending on the choices made while using this PP Module.

IPsec will be used to establish a logical direct connection between two networks, so that it would appear they are directly connected. Traffic that would need to traverse intermediary carrier networks would now travel through a cryptographic tunnel, where the contents of the

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

tunnel is isolated from entities outside of it. Operating at the network level, any services or protocols operating at the application layer will perceive the tunnel as a normal direct link.

SSH and TLS will be used to establish a trusted channel between two or more applications, such as client and server applications. While it will not create any virtual direct link, it will provide any traffic transmitted between the applications with a layer of encryption. This means that the traffic transmitted within this channel will be isolated from the network which it traverses.

A TOE compliant with this PP Module must provide the following security functionality:

- Provide a trusted channel between the TOE and another network device. The protocol used for the trusted channel are at least one of IPsec, TLS or SSH, but also multiple protocols may be supported by the TOE.
- Directing network traffic to ensure that only certain traffic is flowing through the channel.
- Management related to the trusted channel.
- Auditing of security critical events related to the trusted channel and its management.

1.3.3 Available non-TOE Hardware/Software/Firmware

To establish a trusted channel, there is a need for a secure device on the other side of this link that supports the cryptographic protocols of the TOE. In the case of TLS and SSH,

This Module has no need for any other specific non-TOE components, other than what is stated in the Base PP.

1.4 TOE Description

The TOE is a network device providing a trusted channel. The security functionality of the network device is the one of Base PP and the security functionality of this PP module. The specific security functionality of the PP module is to provide a trusted channel between the TOE and another trusted component, it could be a VPN connection connecting two networks over a carrier network (e.g., using IPsec) or it may be a trusted channel between two or more applications such as client server applications (e.g., using TLS or SSH).

Each of the different separation mechanisms of this PP module are described below.

1.4.1 Trusted channel using IPsec

Internet Protocol Security (IPsec) is a network protocol that authenticates and encrypts the packets of data sent over an IP network and is specified in RFC2406. IPsec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to use during the session.

IPsec can protect data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host).

IPsec uses cryptographic security services to protect communications over Internet Protocol (IP) networks. IPsec supports network-level peer authentication, data-origin authentication, data integrity, data confidentiality (encryption), and replay protection. For authentication certificates are typically used and for session key establishment IKEv2 [RFC 7296] is used.

IPsec provides separation in that it provides confidentiality and integrity by using a secure channel. Each application using the IPsec channel will then benefit from the security of the

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

channel. However, both the authentication and the key exchange protocols are exposed to other IP network traffic is part of the attack surface of IPsec.

IPsec is an end-to-end security scheme operating in the internet layer of the Internet Protocol Suite, while some other Internet security systems in widespread use, such as Transport Layer Security (TLS) and Secure Shell (SSH), operate in the upper layers at the Transport Layer (TLS) and the application layer (SSH). Hence, only IPsec protects all application traffic over an IP network. IPsec can automatically secure applications at the internet layer.

Using an IPsec network is easier and more flexible that VLANs. However, managing a larger number of IPsec networks is only possible using certificates (for authentication). That in turn requires some sort of PKI, which is not part of the TOE or the TOE of the Base PP.

1.4.2 Trusted Channel Using TLS

Transport Layer Security (TLS) is a network protocol that provides communications security over computer networks between TLS client-server applications. The current latest protocol version is 1.3, which is specified in RFC 8446. However, that version of the protocol was released only recently (august 2018). The most commonly used and mature version of the protocol is still TLS 1.2, as specified in RFC 5246.

In applications design, TLS is often implemented on top of transport layer protocols, encrypting the protocol-related data of protocols such as HTTP, FTP, SMTP, NNTP, XMPP and others. For this reason, TLS is often built into the client-server application directly and, unlike IPsec, not part of the underlying network infrastructure. Therefore, it is not unlikely that client-server applications use TLS on networks that partly are IPsec encrypted.

Asymmetric encryption is used during the TLS handshake to imitate a session, and then protects traffic with symmetric encryption and hashing algorithms. TLS can be used with several different cipher suites that specify the cryptographic algorithms. For authentication, TLS makes use of X.509 certificates. By default, the client authenticates the server, but mutual authentication can be added. Due to the certificates used in TLS, there is also the need to manage these certificates. In larger networks, this could require a Public Key Infrastructure (PKI) to simplify management.

1.4.3 Trusted Channel Using SSH

Secure Shell (SSH) is, similarly to TLS, a network protocol that provides communications security over computer networks between SSH client-server applications. The current version is SSH2 and the protocol is specified in RFC 4251.

Asymmetric encryption is used when initiating a session, and then protects traffic with symmetric encryption and hashing algorithms. Public-key cryptography is used to authenticate the server, while the client can authenticate themselves within the encrypted channel. SSH can be used with several different cipher suites that specify the cryptographic algorithms.

SSH is most commonly used between two applications for remote management, such as executing commands or transferring files. These two use cases are common for SSH because, in contrast to TLS, SSH more specifically defines the connections inside an established tunnel.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

2. CONSISTENCY RATIONALE

The TOE of the Base PP is a network device that provides a trusted channel. However, the Base PP only specifies core requirements for a generic network device. Since network separation can be implemented in various ways, the separation requirements are specified in PP Modules, such as this one, to allow for selection of the desired separation mechanism(s). It is guaranteed that the Base PP provides network separation as it is mandatory to use it together with at least one separation Module.

This PP Module does not describe functionality of a network device, but specifies the requirements for isolation and protection of network traffic on through the use of a trusted channel.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

3. CONFORMANCE CLAIM

This PP Module claims conformance to [CC]

- Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. Version 3.1, Revision 5. April 2017. CCMB-2017-04-001
- Common Criteria for Information Technology Security Evaluation. Part 2: Security Functional Components. Version 3.1, Revision 5. April 2017. CCMB-2017-04-002
- Common Criteria for Information Technology Security Evaluation. Part 3: Security Assurance Components. Version 3.1, Revision 5. April 2017. CCMB-2017-04-003

as follows

- Part 2 extended,
- Part 3 conformant.

3.1 PP CLAIM

Since a PP Module cannot claim any conformance to other Protection Profiles, this section is not applicable.

3.2 PACKAGE CLAIM

This PP Module inherits the conformance claim to the EAL4 package of security assurance requirements, augmented with ACL_FLR.2, from its Base PP.

3.3 CONFORMANCE RATIONALE

Since this PP Module does not claim conformance to any PP, this section is not applicable.

3.4 CONFORMANCE STATEMENT

This PP Module inherits the demonstrable conformance statement of its Base PP.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

4. SECURITY PROBLEM DEFINITION

The security problem definition defines the security problem that is addressed by the TOE as well as the assumptions on the operational environment necessary for the TOE to be able to address the security problem.

4.1 THREATS

This section of the security problem definition describes the threats that are countered by the TOE, its operational environment, or a combination of the two.

The assets to be protected consist of:

- User data – Network traffic transmitted through the TOE within a specific broadcast domain.

Attackers are persons or IT entities with access to network traffic on either side of a cryptographic channel established by the TOE. I.e. trying to either break into; or out of the channel.

Threat	Description
T.DISCLOSE	An external attacker gains unauthorised access to information transmitted between the TOE and its remote peer endpoint.
T.MODIFY	The attempts of an external attacker to modify data transmitted between the TOE and a remote peer endpoint goes undetected.
T.TUNNEL	An external attacker using the trusted channel gain unauthorized access to information or resources by breaking out of the tunnel provided by the secure channel.

Note: The threats T.DISCLOSE and T.MODIFY applies to the use-case tunnels where trusted traffic is tunnelled of untrusted networks, whereas the T.TUNNEL applies to the use-case when untrusted traffic is tunnelled of trusted networks.

4.2 ORGANISATIONAL SECURITY POLICIES

The following organisational security policies are to be enforced by the TOE and the TOE environment.

OSP	Description
P.AUDIT-VPN	The TOE must be able to provide an audit trail of security relevant events as well as accountability for authorised use of security functions.
P.FLOW-VPN	The TOE must ensure that network traffic is mediated by the TOE to ensure that all network traffic on the trusted channel interface is only passed through the trusted channel to prevent information leakage.
P.MANAGE-VPN	The TOE shall provide the means to authorised administrators to manage the security functions of the TOE.

Note: This PP Module requires additional management and audit functionality than what is specified in the Base PP. To emphasise this, the policies P.AUDIT and P.MANAGE are also

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

present in this PP Module. The additional OSPs are covered by additional security objectives and (when addressed by the TOE) security functional requirements.

4.3 ASSUMPTIONS

This section specifies the assumptions on the TOE environment that are necessary for the TOE to meet its security objectives.

Assumption	Description
A.PEER-VPN	It is assumed that peer TOE entities for the trusted channels are able to protect the integrity and confidentiality of data transmitted to the TOE via encryption and provide authentication for such data. Upon receipt of data from the TOE, the peer external IT entity must be able to decrypt the data and verify that the received data accurately represents the data that was originally transmitted.

Note: All assumptions of the Base PP also apply to an ST claiming compliance to this PP Module. For this reason, they are not repeated here.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

5. SECURITY OBJECTIVES

The security objectives provide a concise statement of the intended response to the security problem. It will describe which security needs will be addressed by the TOE and which will be addressed by the TOE environment, in the form of a statement of security objectives.

5.1 SECURITY OBJECTIVES FOR THE TOE

The following security objectives are to be met by the TOE.

Security Objective	Description
O.AUDIT-VPN	The TOE must be able to generate security relevant events as well as events related to authorised use of security functions.
O.CHANNEL	The TOE must be able to provide trusted channels to remote trusted networks and protect information transmitted to and received from such networks against unauthorised disclosure and to detect any modification of incoming information transmitted from such networks, and to provide the means for the remote network to verify the integrity of information transmitted out of the TOE to such networks.
O.MANAGE-VPN	The TOE must provide the means for an authorised administrator to configure and manage the TOE security functions.
O.FLOW-VPN	The TOE must mediate the flow of network traffic to ensure that network traffic intended to be passed through the trusted channel only leaves the TOE through the trusted channel in accordance to the security policy.

5.2 SECURITY OBJECTIVES FOR THE OPERATIONAL ENVIRONMENT

The following security objectives are to be met by the TOE environment.

Security Objective	Description
OE.PEER-VPN	It is assumed that peer TOE entities for the trusted channels are able to protect the integrity and confidentiality of data transmitted to the TOE via encryption and provide authentication for such data. Upon receipt of data from the TOE, the peer external IT entity must be able to decrypt the data and verify that the received data accurately represents the data that was originally transmitted.

5.3 SECURITY OBJECTIVES RATIONALE

5.3.1 Coverage

The following tables provide a mapping of security objectives both for the TOE and the TOE environment to the environment defined by the threats, policies and assumptions, illustrating that each security objective for the TOE covers at least one threat or policy, and that each security objective for the TOE environment covers at least one policy, threat or assumption.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

	T.DISCLOSE	T.MODIFY	T.TUNNEL	P.AUDIT-VPN	P.FLOW-VPN	P.MANAGE-VPN	A.PEER
O.AUDIT-VPN				X			
O.CHANNEL	X	X	X				
O.MANAGE-VPN						X	
O.FLOW-VPN					X		
OE.PEER-VPN							X

5.3.2 Sufficiency

The following rationale provides justification that the security objectives are suitable to counter each individual threat and that each security objective tracing back to a threat actually contributes to the mitigation of that threat.

Threat	Rationale for the security objectives
T.TUNNEL	The threat of an external attacker breaking out of the secure channel to gain unauthorized access to information is addressed by the security objectives of establishing a cryptographically secure trusted channel (O.CHANNEL). In addition, it is supported by the OE.PEER.
T.DISCLOSE	The threat of an external attacker gaining unauthorised access to information transmitted between the TOE and its remote peer endpoint is addressed by the security objectives of establishing a cryptographically secure trusted channel (O.CHANNEL). In addition, it is supported by the OE.PEER for the other end of the trusted channel, i.e. encryption and decryption of data.
T.MODIFY	The threat of an external attacker to modify data transmitted between the TOE and a remote peer endpoint going undetected is addressed by the security objectives of establishing a cryptographically secure trusted channel (O.CHANNEL). In addition, it is supported by the OE.PEER for the other end of the trusted channel, i.e. for the integrity protection.

The following rationale provides justification that the security objectives of the TOE and the TOE environment are suitable to address each individual OSP and that each security objective tracing back to an OSP actually contributes in addressing the OSP

OSP	Rationale for the security objectives
P.FLOW-VPN	The OSP that the TOE must ensure that network traffic is mediated by the TOE to ensure that network traffic intended for the trusted channel is only passed through the trusted channel is addressed by TOE mediation (O.FLOW-VPN).
P.AUDIT-VPN	This OSP is addressed by O.AUDIT-VPN, which ensures that all security related events are recorded.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

P.MANAGE-VPN	This OSP is addressed by O.MANAGE-VPN that ensures the TOE will provide management functionality to authorised administrators.

The following rationale provides justification that the security objectives of the TOE environment are suitable to address each individual assumption and that each security objective tracing back to an assumption actually contributes in addressing the assumption.

Assumption	**Rationale for the security objectives**
A.PEER	Addressed by OE. PEER, which is identical to the assumption.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

6. EXTENDED COMPONENTS DEFINITION

All extended components for SFRs describing IPsec and TLS have been based on SFRs from [cPPND], the collaborative Protection Profile for Network Devices, Version 2.0, 5-May-2017.

The extended components defined here in this Protection Profile as well as the ones taken from [cPPND] can easily be identified by the extension keyword EXT.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

7. SECURITY REQUIREMENTS

The conventions used in descriptions of the SFRs are as follows:

- Unaltered SFRs are stated in the form used in [CC] or their extended component definition;
- Assignment and selections wholly or partially complete in the PP: indicated with **bold text**;
- Refinement made in the PP: the refinement text is indicated with ~~strikethroughs~~ when removed or underlined when added;
- Iteration: indicated by adding a string starting with "/" (e.g. "FCS_COP.1/Hash").

7.1 SECURITY FUNCTIONAL POLICIES

7.1.1 Network information flow control SFP

The TOE must implement an information flow control (SFP) called "Network Information Flow Control SFP" ensuring the separation of network traffic. A trusted channel may be either a virtual private network (VPN) using IPsec, an SSH connection, a TLS connection or an HTTPS connection. We may have different Network Information Flow Control SFPs depending on the policy the TOE should implement as well as depending on the protocols used. The policy should ensure that traffic only flows in the trusted between the foreseen endpoints and not in any other way. This is to ensure that traffic that needs to be protected only flows to the authenticated parties in any case the trusted channel is protected by cryptographic means.

7.2 BASIC SECURITY FUNCTIONAL REQUIREMENTS

7.2.1 FAU_GEN.1 – Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

- Start-up and shutdown of the audit functions;
- All auditable events for the **not specified** level of audit; and
- **All administrative actions:**
  - *Generating/import of, changing, or deleting of cryptographic keys (in addition to the action itself a unique key name or key reference shall be logged)* ***{IPsec, SSH, TLS, HTTPS}***
- [assignment: *other specifically defined auditable events*].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

- Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
- For each audit event type, based on the auditable event definitions of the functional components included in the ST/PP: **none**

Application note: In the ST it is expected that this SFR is merged with the equivalent SFR of the Base PP and not iterated as if they were two different SFRs. If the ST specifies any security functionality in addition to the one specified in this PP, additional audit events might have to be added to meet the security objective O.AUDIT-VPN.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

7.2.2 FMT_MSA.1 – Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the [assignment: *access control SFP(s), information flow control SFP(s)*] to restrict the ability to [selection: *change_default, query, modify, delete, [assignment: other operations]*] the security attributes [assignment: *list of security attributes*] to [assignment: *the authorised identified roles*].

Application note: The authorised roles may be the ones defined in FMT_SMR.1 of the Base PP, but may also be separate roles in case the management of the trusted channel is separate from the management of the functionality of the Base PP.

7.2.3 FMT_MSA.3 – Static attribute initialisation

FMT_MSA.3.1 The TSF shall enforce the [assignment: *access control SFP, information flow control SFP*] to provide [*restrictive*] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [assignment: *the authorised identified roles*] to specify alternative initial values to override the default values when an object or information is created.

Application note: See the application note for FMT_MSA.1.

7.2.4 FMT_MOF.1 – Management of functions in TSF

FMT_MOF.1.1 The TSF shall restrict the ability to [selection*: determine the behaviour of, disable, enable, modify the behaviour of*] the functions [assignment: *list of functions*] to [assignment: *the authorised identified roles*].

Application note: See the application note for FMT_MSA.1.

7.2.5 FMT_MTD.1 – Management of TSF data

FMT_MTD.1.1 The TSF shall restrict the ability to [selection: *change_default, query, modify, delete, clear, [*assignment*: other operations]*] the [assignment: *list of TSF data*] to [assignment: *the authorised identified roles*].

Application note: See the application note for FMT_MSA.1.

7.2.6 FMT_SMF.1 – Specification of management functions

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: [assignment: *list of management functions to be provided by the TSF,* [selection:

- *Ability to configure the cryptographic functionality;*
- *Ability to configure thresholds for SSH rekeying;*
- *Ability to configure the lifetime for IPsec Security Associations;*
-].

Application note: Please, note that the configuration of the cryptographic functionality for IPsec includes but is not limited to the specification of permitted cipher suites, key management protocols and authentication methods.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

7.3 GENERIC CRYPTOGRAPHIC SFRS

The generic cryptographic security functional requirements are those that are common and used by the trusted channels, without being specific to a certain type of trusted channels. Not all selections are possible of needed all trusted channel protocols. These selections have been marked by the tags {IPSEC}, {TLS} or SSH} to indicate when they should be considered.

7.3.1 FCS_CKM.1/Symmetric – Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm

- **as needed in the TLS 1.2 standard (RFC5246) and in the DTLS 1.2 standard (RFC 6347) for [selection:**
  - ***AES-128 in the* [selection: *Cipher Block Chaining Mode (CBC), Galois/Counter Mode (GCM)*] *and specified cryptographic key size 128 bit*;**
  - ***AES-256 in the* [selection*: Cipher Block Chaining Mode (CBC), Galois/Counter Mode (GCM)*] *and specified cryptographic key size 256 bit*]**

  that meet the following: [FIPS197] and [NIST SP 800-38D].
  {TLS, DTLS}
- **as needed in the SSH protocol for [selection:**
  - ***AES-128 in the* [selection: *Cipher Block Chaining Mode (CBC), Counter Mode (CTR), Galois/Counter Mode (GCM)] and specified cryptographic key size 128 bit*,**
  - ***AES-192 in the* [selection: *Cipher Block Chaining Mode (CBC), Counter Mode (CTR), Galois/Counter Mode (GCM)] and specified cryptographic key size 192 bit*,**
  - ***AES-256 in the* [selection: *Cipher Block Chaining Mode (CBC), Counter Mode (CTR), Galois/Counter Mode (GCM)] and specified cryptographic key size 256 bit*]**

  that meet the following: [FIPS197] and [NIST SP 800-38D].
  {SSH}

~~and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*]~~.

Application note: This SFR covers the generation of AES keys for the TLS, DTLS, and SSH connections. The selection must be made by the ST author depending on the choice of the protocol in FTP_ITC.1 and the chosen cipher suites for TLS and DTLS and/or the chosen encryption algorithms for SSH. Recommendations for key generation are in [NIST SP 800-133].

7.3.2 FCS_CKM.1/Asymmetric – Cryptographic key generation

FCS_CKM.1.1 The TSF shall generate **asymmetric** cryptographic keys in accordance with a specified cryptographic key generation algorithm: **[selection:**

- ***RSA schemes using cryptographic key sizes of at least 2000-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.3;***

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

- ***ECC schemes using [*selection: *nistp256, nistp384, nistp521, brainpoolP256r1, brainpoolP384r1, brainpoolP512r1] that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4;***
- ***FFC schemes using cryptographic key sizes of at least 2000-bit or greater that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.1.]***

~~and specified cryptographic key sizes [assignment: *cryptographic key sizes*] that meet the following: [assignment: *list of standards*].~~

Application note: The ST author selects all key generation schemes used for key establishment and device authentication. When key generation is used for key establishment, the schemes in FCS_CKM.2.1 and selected cryptographic protocols must match the selection. When key generation is used for device authentication, other than ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, pgp-sign-rsa, pgp-sign-dss, the public key is expected to be associated with an X.509v3 certificate. Recommendations for key generations are in [NIST SP 800-133].

7.3.3 FCS_CKM.2 – Cryptographic Key Establishment

FCS_CKM.2.1 The TSF shall **perform** cryptographic **key establishment** in accordance with a specified cryptographic key **establishment** method **[selection:**

- **RSA-based key establishment schemes that meet the following: NIST Special Publication 800-56B Revision 1, "Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography";**
- **Elliptic curve-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography";**
- **Finite field-based key establishment schemes that meet the following: NIST Special Publication 800-56A Revision 2, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"]**

~~that meets the following: [assignment: *list of standards*].~~

Application note: This is a refinement of the SFR FCS_CKM.2 to deal with key establishment rather than key distribution. The ST author selects all key establishment schemes used for the selected cryptographic protocols. For Diffie-Hellman groups, ST authors should make the corresponding selection from the SFR instead of using the Finite field-based key establishment selection. The RSA-based key establishment schemes are described in Section 9 of NIST SP 800-56B Revision 1; however, Section 9 relies on implementation of other sections in SP 800-56B Revision 1.

The elliptic curves used for the key establishment scheme correlate with the curves specified in FCS_CKM.1.1.

The domain parameters used for the finite field-based key establishment scheme are specified by the key generation according to FCS_CKM.1.1.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

7.3.4 FCS_CKM.4 – Cryptographic key destruction

FCS_CKM.4.1 The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [assignment*:*

- *For* plaintext *keys in volatile storage, the destruction shall be executed by a [*selection*: single overwrite consisting of [selection: a pseudo-random pattern using the TSF's RBG, zeroes, ones, a new value of the key, [*assignment: *a static or dynamic value that does not contain any CSP]], destruction of reference to the key directly followed by a request for garbage collection];*
- *For plaintext keys in non-volatile storage, the destruction shall be executed by the invocation of an interface provided by a part of the TSF that [*selection:
    - *logically addresses the storage location of the key and performs a [*selection: *single, [*assignment: *number of passes]-pass] overwrite consisting of [*selection: *a pseudo-random pattern using the TSF's RBG, zeroes, ones, a new value of the key, [*assignment: *a static or dynamic value that does not contain any CSP]];*
    - *instructs a part of the TSF to destroy the abstraction that represents the key]]*

that meets the following: *No Standard*.

Application note: In parts of the selections where keys are identified as being destroyed by "a part of the TSF", the TSS identifies the relevant part and the interface involved. The interface referenced in the requirement could take different forms for different TOEs, the most likely of which is an application-programming interface to an OS kernel. There may be various levels of abstraction visible. For instance, in a given implementation the application may have access to the file system details and may be able to logically address specific memory locations. In another implementation the application may simply have a handle to a resource and can only ask another part of the TSF such as the interpreter or OS to delete the resource.

Where different key destruction methods are used for different keys and/or different destruction situations then the different methods and the keys/situations they apply to are described in the TSS (and the ST may use separate iterations of the SFR to aid clarity). The TSS describes all relevant keys used in the implementation of SFRs, including cases where the keys are stored in a non-plaintext form. In the case of non-plaintext storage, the encryption method and relevant encrypting-key are identified in the TSS.

Some selections allow assignment of "a value that does not contain any CSP". This means that the TOE uses some specified data not drawn from an RBG meeting FCS_RBG_EXT requirements, and not being any of the particular values listed as other selection options. The point of the phrase "does not contain any CSP" is to ensure that the overwritten data is carefully selected, and not taken from a general pool that might contain current or residual data that itself requires confidentiality protection.

For the avoidance of doubt: the "cryptographic keys" in this SFR include session keys. Key destruction does not apply to the public component of asymmetric key pairs.

7.3.5 FCS_COP.1/AES – Cryptographic operation

FCS_COP.1.1 The TSF shall perform **encryption/decryption** in accordance with a specified cryptographic algorithm [assignment*: AES used in [*selection: *CBC, CTR,*

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

GCM] mode] and cryptographic key sizes *[*assignment: *128 bits, 192 bits, 256 bits*] that meet the following: [assignment*: AES as specified in ISO 18033-3 with [*selection: *CBC as specified in ISO 10116, CTR as specified in ISO 10116, GCM as specified in ISO 19772]*].

Application note: For the first selection of FCS_COP.1.1/AES, the ST author chooses the mode or modes in which AES operates. For the second selection, the ST author chooses the key sizes that are supported by this functionality. The modes and key sizes selected here correspond to the cipher suite selections made in the trusted channel requirements.

7.3.6 FCS_COP.1/Signature – Cryptographic operation

FCS_COP.1.1/Signature The TSF shall perform **cryptographic signature services (generation and verification)** in accordance with a specified cryptographic algorithm [selection:

- *RSA Digital Signature Algorithm and cryptographic key sizes **(modulus)** [assignment: at least 2000 bits or greater],*
- *Elliptic Curve Digital Signature Algorithm and cryptographic key sizes [assignment: at least 250 bits or greater]*

] that meet the following: [selection:

- *For RSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 5.5, using PKCS #1 v2.1 Signature Schemes RSASSA-PSS,*
- *For ECDSA and ECGDSA schemes: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Section 6 and Appendix D, Implementing "NIST curves" [*selection*: P-256, P-384, P-521]; ISO/IEC 14888-3, Section 6.4, and/or RFC 5639, „Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation" [*selection*: brainpoolP256r1, brainpoolP384r1, brainpoolP512r1]*

].

Application note: The ST author chooses the algorithm(s) implemented to perform digital signatures. For the algorithm(s) chosen, the ST author makes the appropriate assignments/selections to specify the parameters that are implemented for that algorithm. The ST author ensures that the assignments and selections for this SFR include all the parameter values necessary for the cipher suites selected for the protocol SFRs (see Section 6.5) that are included in the ST. The ST author checks for consistency of selections with other FCS requirements, especially when supporting elliptic curves.

7.3.7 FCS_COP.1/Hash – Cryptographic operation

FCS_COP.1.1/Hash The TSF shall perform **cryptographic hashing services** in accordance with a specified cryptographic algorithm [selection: *SHA-256, SHA-384, SHA-512*] ~~and cryptographic key sizes [*assignment: cryptographic key sizes*]~~ and message digest sizes [selection: *256, 384, 512*] bits that meet the following: [assignment: *ISO/IEC 10118- 3:2004]*.

Application note: The hash selection should be consistent with the overall strength of the algorithm used for FCS_COP.1/AES and FCS_COP.1/Signature (for example, SHA 256 for 128-bit keys).

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

7.3.8 FCS_COP.1/KeyedHash Cryptographic operation

FCS_COP.1.1/KeyedHash The TSF shall perform **keyed-hash message authentication** in accordance with a specified cryptographic algorithm *[*selection: *HMAC-SHA-1-96, HMAC-SHA-256, HMAC-SHA-384, HMAC-SHA-512]* and cryptographic key sizes [assignment: *key size (in bits) used in HMAC*] **and message digest sizes [selection: 160, 256, 384, 512] bits** that meet the following: [assignment*: ISO/IEC 9797-2:2011, Section 7 "MAC Algorithm 2"]*.

Application note: The key size [k] in the assignment falls into a range between L1 and L2 (defined in ISO/IEC 10118 for the appropriate hash function). For example, for SHA-256, L1=512, L2=256, where L2 ≤ k ≤ L1.

7.3.9 FCS_COP.1/MAC Cryptographic operation (MAC)

FCS_COP.1.1/MAC The TSF shall perform **message authentication** in accordance with a specified cryptographic algorithm [selection:

- *AES-XCBC-MAC-96 (as specified in RFC3566, 7296) and cryptographic key size 128 bit, AES-CMAC (as specified in RFC 4493) and cryptographic key size 128 bit, AEAD_AES_128_GCM (as specified in RFC 5647 Section 6.1) and cryptographic key size 128 bit*, **{IPsec}**
- *AEAD_AES_256_GCM (as specified in RFC 5647 Section 6.2) and cryptographic key sizes 256 bit*] **{SSH}**

~~and cryptographic key sizes~~ ~~that meet the following: .~~

Application note: AES-XCB-MAC-96 is used as message authentication for the IKEv2 messages and the ESP packages in the IPsec protocol. For IKEv2 RFC 7296 shall be applied, whereas for the IPsec protocol RFC 3566.

7.3.10 FCS_RGB_EXT.1 Random Bit generation

FCS_RBG_EXT.1.1 The TSF shall provide a **deterministic** random number generator that implements: [selection: *capability list of class DRG.3, capability list of class DRG.4 (both specified in AIS20/31)*].

Application note: The ST author shall make use of [KS2011] and [AIS 20/31] for determining the random number.

FCS_RBG_EXT.1.2 The deterministic RNG shall be seeded by using [selection: *PTRNG of the class PTG.3 as random source, NPTRNG of the class NTG.1 as random source (as specified in AIS20/31)*].

Application note: The ST author shall make use of [KS2011] and [AIS 20/30] for the decision about the seeding.

7.4 SFRs Specific for IPsec, SSH, TLS, HTTPS

A compliant TOE will provide encryption for the communication paths between itself and the endpoint to protect the transmission of sensitive data to and from the TOE. These channels are implemented using one (or more) of the following standard protocols: IPsec, SSH, TLS and HTTPS. These protocols are defined by RFCs that offer some flexibility in the choice of the implementation.

This PP does not specify the ciphersuites, but recommendations for cipher suites can be found in [NDcPP] as well as in ([BSI-TR-02102-2], [BSI-TR-02102-3], [BSI-TR-02102-4], and [BSI-TR-03116-4].

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

7.4.1 FDP_IFC.1 – Subset information flow control

FDP_IFC.1.1 The TSF shall enforce the [assignment: *information flow control SFP*] on [assignment: *list of subjects, information, and operations that cause controlled information to flow to and from controlled subjects covered by the SFP*].

7.4.2 FDP_IFF.1 – Simple security attributes

FDP_IFF.1.1 The TSF shall enforce the [assignment: *information flow control SFP*] based on the following types of subject and information security attributes: [assignment: *list of subjects and information controlled under the indicated SFP, and for each, the security attributes*].

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [assignment: *for each operation, the security attribute-based relationship that must hold between subject and information security attributes*].

FDP_IFF.1.3 The TSF shall enforce the [assignment: *additional information flow control SFP rules*].

FDP_IFF.1.4 The TSF shall explicitly authorise an information flow based on the following rules: [assignment: *rules, based on security attributes, that explicitly authorise information flows*].

FDP_IFF.1.5 The TSF shall explicitly deny an information flow based on the following rules: [assignment: *rules, based on security attributes, that explicitly deny information flows*].

Application note: It is expected that for each trusted channel protocol used there will be at least one information flow control SFP for FDP_IFC.1 and FDP_IFF.1 that ensures which information that flows through the trusted channel. This means that these SFRs may have to be iterated.

7.4.3 FTP_ITC.1 – Inter-TSF trusted channel

FTP_ITC.1.1 The TSF shall be capable of using [selection: *IPsec, SSH, TLS, HTTPS*] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: audit server, [selection*: authentication server, [assignment: [other capabilities], no other capabilities*] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification and disclosure.

FTP_ITC.1.2 The TSF shall permit **the TSF or the authorized IT entities** to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [assignment*: list of **services for which the TSF is able to initiate communications***].

Application note: The other trusted IT product is for IPsec expected to be a network device meeting the same requirements as a product claiming compliance to this Protection Profile. For SSH and TLS it could also be an application or any other network product.

7.5 SELECTION-BASED SFRS

The dependencies corresponding to the specific SFRs in this section are shown in the following table for a better overview. Which SFR has to be selected here is dependent on the selection in

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

FTP_ITC.1. Since a TOE claiming compliance to the PP module must provide a trusted channel at least one of the protocols IPsec, TLS or SSH must be provided by a TOE.

SFR	Dependencies to
FCS_IPSEC_EXT.1	FCS_CKM.1/Symmetric Cryptographic Key Generation FCS_CKM.1/Asymmetric Cryptographic Key Generation FCS_CKM.2 Cryptographic Key Establishment FCS_COP.1/AES Cryptographic Operation FCS_COP.1/Signature Cryptographic Operation FCS_COP.1/Hash Cryptographic Operation FCS_COP.1/KeyedHash Cryptographic Operation FCS_COP.1/MAC Cryptographic Operation FCS_RBG_EXT.1 Random Bit Generation
FCS_SSHC_EXT.1	FCS_CKM.1/Symmetric Cryptographic Key Generation FCS_CKM.1/Asymmetric Cryptographic Key Generation FCS_CKM.2 Cryptographic Key Establishment FCS_COP.1/AES Cryptographic Operation FCS_COP.1/Signature Cryptographic Operation FCS_COP.1/Hash Cryptographic Operation FCS_COP.1/KeyedHash Cryptographic Operation FCS_COP.1/MAC Cryptographic Operation FCS_RBG_EXT.1 Random Bit Generation FIA_X509_EXT SFRs (if selected as authentication)
FCS_SSHS_EXT.1	FCS_CKM.1/Symmetric Cryptographic Key Generation FCS_CKM.1/Asymmetric Cryptographic Key Generation FCS_CKM.2 Cryptographic Key Establishment FCS_COP.1/AES Cryptographic Operation FCS_COP.1/Signature Cryptographic Operation FCS_COP.1/Hash Cryptographic Operation FCS_COP.1/KeyedHash Cryptographic Operation FCS_COP.1/MAC Cryptographic Operation FCS_RBG_EXT.1 Random Bit Generation FIA_X509_EXT SFRs (if selected as authentication)
FCS_TLSC_EXT.1	FCS_CKM.1/Symmetric Cryptographic Key Generation FCS_CKM.1/Asymmetric Cryptographic Key Generation FCS_CKM.2 Cryptographic Key Establishment FCS_COP.1/AES Cryptographic Operation FCS_COP.1/Signature Cryptographic Operation FCS_COP.1/Hash Cryptographic Operation FCS_COP.1/KeyedHash Cryptographic Operation FCS_RBG_EXT.1 Random Bit Generation FIA_X509_EXT.2 Certificate Authentication
FCS_TLSS_EXT.1	FCS_CKM.1/Symmetric Cryptographic Key Generation FCS_CKM.1/Asymmetric Cryptographic Key Generation FCS_CKM.1 Cryptographic Key Generation

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

	FCS_CKM.2 Cryptographic Key Establishment FCS_COP.1/AES Cryptographic Operation FCS_COP.1/Signature Cryptographic Operation FCS_COP.1/Hash Cryptographic Operation FCS_COP.1/KeyedHash Cryptographic Operation FCS_RBG_EXT.1 Random Bit Generation FIA_X509_EXT.2 Certificate Authentication
FCS_HTTPS_EXT.1	FCS_TLSC_EXT.1 TLS Client Protocol, or FCS_TLSS_EXT.1 TLS Server Protocol
FIA_X509_EXT.1	FIA_X509_EXT.2 Certificate Authentication FIA_X509_EXT.3 Certificate Requests
FIA_X509_EXT.2	FIA_X509_EXT.1 Certificate Validation FIA_X509_EXT.3 Certificate Requests
FIA_X509_EXT.3	FCS_CKM.1/Asymmetric Cryptographic Key Generation FIA_X509_EXT.1 Certificate Validation FIA_X509_EXT.2 Certificate Authentication

FCS_IPSEC_EXT IPsec protocol

If a TOE implements IPsec, a corresponding selection in FTP_ITC.1 should have been made that defines what the IPsec protocol is implemented to protect. IPsec is a peer-to-peer protocol and as such does not need to be separated into client and server requirements.

7.5.1 FCS_IPSEC_EXT.1 IPsec Protocol

FCS_IPSEC_EXT.1.1 The TSF shall implement the IPsec architecture as specified in RFC4301.

Application note: RFC 4301 Section 4.4.1 requests an IPsec implementation to protect IP traffic through the use of a Security Policy Database (SPD). The SPD contains rules that determine how ingoing and outgoing packets are processed by IPsec. All packets (also non-IPsec packets) are handled with these rules.

FCS_IPSEC_EXT.1.2 The TSF shall have a nominal, final entry in the SPD that matches anything that is otherwise unmatched, and discards it.

FCS_IPSEC_EXT.1.3 The TSF shall implement [selection: transport mode, tunnel mode].

Application note: The ST author selects the supported modes of operation for IPsec.

FCS_IPSEC_EXT.1.4 The TSF shall implement the IPsec protocol ESP as defined by RFC 4303 using the cryptographic algorithms [selection: *AES-CBC-128, AES-CBC-192, AES-CBC-256 (specified in RFC 3602), AES-CTR-128, AES-CTR-192, AES-CTR-256 (specified in RFC 3686), no other algorithm*] together with a Secure Hash Algorithm (SHA)-based HMAC [selection: *HMAC-SHA-1-96 (specified in RFC 2404), HMAC-SHA2-256-128, HMAC-SHA2-384-192, HMAC-SHA2-512-256 (specified in RFC 4868), AES-XCBC-MAC-96 (specified in RFC 3566), AES-CMAC-96 (specified in RFC 4494), no other algorithm*] and [selection: *AES-GCM-128, AES-GCM-192, AES-GCM-256 (all specified in RFC 4106), no other algorithm*].

Application note: When an AES-CBC or AES-CTR algorithm is selected, at least one SHA-based HMAC or AES-XCBC-MAC or AES-CMAC must also be chosen. If only an AES-GCM algorithm is selected, then an additional integrity protection is not required, since AES-GCM

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

satisfies both confidentiality and integrity functions. IPsec may utilize a truncated version of the SHA-based HMAC functions contained in the selections. Where a truncated output is utilized, it shall be highlighted in the TSS.

FCS_IPSEC_EXT.1.5 The TSF shall implement the protocol IKEv2 as defined in RFCs 5996, 7296 and [selection: *with no support for NAT traversal, with mandatory support for NAT traversal as specified in RFC 5996 or RFC 7296, Section 2.23)*], and [selection: *no other RFCs for hash functions, HMAC-SHA1-96, AES-XCBC-96 (defined in RFC 7296), RFC 4868 for hash functions*].

Application note: If the TOE implements SHA-2 hash algorithms for IKEv2, the ST author selects RFC 4868. If the TOE implements the use of truncated SHA-based HMACs as described in RFC 4868, they shall be highlighted in the TSS. If HMAC-SHA1-96 or AES-XCBC-96 is implemented, the ST author has to use RFC 7296.

FCS_IPSEC_EXT.1.6 The TSF shall ensure the encrypted payload in the IKEv2 protocol uses the cryptographic algorithms [selection: *AES-CBC-128 (specified in RFC 7296), AES-CTR-128 (specified in RFC 5930), AES-GCM-128, AES-GCM-256 (specified in RFC 5282)*].

FCS_IPSEC_EXT.1.7 The TSF shall ensure that IKEv2 SA lifetimes can be configured by a Security Administrator based on [selection: *number of bytes; length of time, where the time values can be configured within [*assignment*: integer range including 24] hours*].

Application note: The ST author chooses either volume-based lifetimes or time-based lifetimes (or a combination). This requirement must be accomplished by providing Security Administrator-configurable lifetimes (with appropriate instructions in documents mandated by AGD_OPE). Hardcoded limits do not meet this requirement. In general, instructions for setting the parameters of the implementation, including lifetime of the SAs, should be included in the guidance documentation generated for AGD_OPE.

FCS_IPSEC_EXT.1.8 The TSF shall ensure that IKEv2 Child SA lifetimes can be configured by a Security Administrator based on [selection: *number of bytes; length of time, where the time values can be configured within [*assignment: *integer range including 8] hours*].

Application note: The ST author chooses either volume-based lifetimes or time-based lifetimes (or a combination). This requirement must be accomplished by providing Security Administrator-configurable lifetimes (with appropriate instructions in documents mandated by AGD_OPE). Hardcoded limits do not meet this requirement. In general, instructions for setting the parameters of the implementation, including lifetime of the SAs, should be included in the guidance documentation generated for AGD_OPE.

FCS_IPSEC_EXT.1.9 The TSF shall generate the secret value x used in the IKE Diffie-Hellman key exchange ("x" in g^x mod p) using the random bit generator specified in FCS_RBG_EXT.1, and having a length of at least [assignment*: (one or more) number(s) of bits that is at least twice the security strength of the negotiated Diffie-Hellman group*] bits.

Application note: For DH groups 19, 20, 21, 28, 29, and 30, the "x" value is the point multiplier for the generator point G.

Since the implementation may allow different Diffie-Hellman groups to be negotiated for use in forming the SAs, the assignment in FCS_IPSEC_EXT.1.9 may contain multiple values. For each DH group supported, the ST author consults Table 2 in NIST SP 800-57 "Recommendation for Key Management –Part 1: General" to determine the security strength

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

("bits of security") associated with the DH group. Each unique value is then used to fill in the assignment for this element. For example, suppose the implementation supports DH group 14 (2048-bit MODP) and group 20 (ECDH using NIST curve P-384). From Table 2, the bits of security value for group 14 is 112, and for group 20 is 192.

Because nonces may be exchanged before the DH group is negotiated, the nonce used should be large enough to support all TOE-chosen proposals in the exchange.

FCS_IPSEC_EXT.1.11 The TSF shall ensure that IKE protocols implement DH Group(s) [selection: *14 (2048-bit MODP), 15 (3072-bit MODP), 16 (4096-bit MODP), 19 (256-bit Random ECP), 20 (384-bit Random ECP), 21 (512-bit Random ECP) 24 (2048-bit MODP with 256-bit POS), 28 (brainpoolP256r1), 29 (brainpoolP384r1), 20 (brainpoolP512r1)*].

Application note: The selection is used to specify additional DH groups supported. This applies IKEv2 exchanges.

FCS_IPSEC_EXT.1.12 The TSF shall be able to ensure by default that the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the IKEv2 IKE_SA connection is greater than or equal to the strength of the symmetric algorithm (in terms of the number of bits in the key) negotiated to protect the IKEv2 CHILD_SA connection.

Application note: While it is acceptable for this capability to be configurable, the default configuration in the evaluated configuration (either "out of the box" or by configuration guidance in the AGD documentation) must enable this functionality.

FCS_IPSEC_EXT.1.13 The TSF shall ensure that the IKE protocol perform peer authentication using [selection:

- *RSASSA-PSS with SHA-256 (2048 bit),*
- *RSASSA-PSS with SHA-384 (4096 bit)*
- *ECDSA-256 with curve secp256r1 or brainpoolP256r1,*
- *ECDSA-384 with curve secp384r1 or brainpoolP384r1,*
- *ECDSA-512 with curve secp512r1 or brainpoolP512r1*
- *ECGDSA-256 with curve brainpoolP256r1,*
- *ECGDSA-384 with curve brainpoolP384r1,*
- *ECGDSA-512 with curve brainpoolP512r1*]

that use X.509v3 certificates that conform to RFC 4945 and [selection: *Pre-shared Keys, no other method*].

Application note: At least one public-key-based Peer Authentication method is required in order to conform to this PP; one or more of the public key schemes is chosen by the ST author to reflect what is implemented. The ST author also ensures that appropriate FCS requirements reflecting the algorithms used (and key generation capabilities, if provided) are listed to support those methods. Note that the TSS will elaborate on the way in which these algorithms are to be used (for example, RFC 2409 specifies three authentication methods using public keys; each one supported will be described in the TSS).

FCS_IPSEC_EXT.1.14 The TSF shall only establish a trusted channel if the presented identifier in the received certificate matches the configured reference identifier, where the presented and reference identifiers are of the following types: [selection: *IP address, Fully Qualified Domain Name (FQDN), user FQDN, Distinguished Name (DN)*] and [selection: *no other reference identifier type*, [assignment: *other supported reference identifier types*]].

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

Application note: When using RSA or ECDSA certificates for peer authentication, the reference and presented identifiers take the form of either a DN, IP address, FQDN or user FQDN. The reference identifier is the identifier the TOE expects to receive from the peer during IKE authentication. The presented identifier is the identifier that is contained within the peer certificate body. The ST author shall select the presented and reference identifier types supported and may optionally assign additional supported identifier types in the second selection. Excluding the DN identifier type (which is necessarily the Subject DN in the peer certificate), the TOE may support the identifier in either the Common Name or Subject Alternative Name (SAN) or both.

The preferred method for verification is the Subject Alternative Name using DNS names, URI names, or Service Names. Verification using the Common Name is required for the purposes of backwards compatibility. Additionally, support for use of IP addresses in the Subject Name or Subject Alternative name is discouraged as against best practices but may be implemented

Supported peer certificate algorithms are the same as FCS_IPSEC_EXT.1.13.

FCS_SSHC_EXT and FCS_SSHS_EXT SSH protocol

If a TOE implements SSH, a corresponding selection in FTP_ITC.1 and/or FTP_TRP.1 should have been made that defines what the SSH protocol is implemented to protect.

A TOE may act as the client or the server in an SSH session. The requirement has been separated into SSH Client (FCS_SSHC_EXT) and SSH Server (FCS_SSHS_EXT) requirements to allow for these differences.

7.5.2 FCS_SSHC_EXT.1 SSH Client Protocol

FCS_SSHC_EXT.1.1 The TSF shall implement the SSH-2 protocol that complies with RFC(s) [selection: *4250, 4251, 4252, 4253, 4254, 4256, 4335, 4344*] and make use of [selection: *RFC 4255, 4419, 4432, 4462, 4716, 4818, 5656, 6187, 6239, 6594, 6668, none of these extensions*].

Application note: The ST author selects which of the RFCs to which conformance is being claimed. As in some of these specification methods are used which are obsolete or possibly no longer secure, the ST author shall combine the specifications and the algorithms which are defined in the later components such that these algorithms are used with high priority and (the possibly weak or obsolete) algorithms of the specification with low priority or, as far as possible, never.

FCS_SSHC_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, [selection: *password-based, host-based, no other method*].

FCS_SSHC_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [assignment: *number of bytes*] bytes in an SSH transport connection are dropped.

Application note: RFC 4253 provides for the acceptance of “large packets” with the caveat that the packets should be of “reasonable length” or dropped. The assignment should be filled in by the ST author with the maximum packet size accepted, thus defining “reasonable length” for the TOE.

FCS_SSHC_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms:

This project has received funding from the European Union’s Horizon2020 research and innovation programme under grant agreement No730843

[selection: *aes128-cbc, aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr, aes256-ctr, AEAD_AES_128_GCM, AEAD_AES_256_GCM*].

Application note: RFC 5647 specifies the use of the AEAD_AES_128_GCM and AEAD_AES_256_GCM algorithms in SSH. As described in RFC 5647, AEAD_AES_128_GCM and AEAD_AES_256_GCM can only be chosen as encryption algorithms when the same algorithm is being used as the MAC algorithm. Corresponding FCS_COP entries are included in the ST for the algorithms selected here.

FCS_SSHC_EXT.1.5 The TSF shall ensure that the SSH public-key based authentication implementation uses [selection: *pgp-sign-rsa (2000 bit), pgp-sign-dss (2000 bit/ 250 bit)*] and [selection: *ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp521, x509v3-rsa2048-sha256, no other public key algorithms*] as its public key algorithm(s) and rejects all other public key algorithms.

Application note: pgp-sign-rsa and pgp-sign-dss has to be used together with a SHA-2- hash function corresponding to the key length. If x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384 or x509v3-ecdsa-sha2-nistp521 are selected, then the list of trusted certification authorities must be selected in FCS_SSHC_EXT.1.9 and the FIA_X509_EXT SFRs are applicable.

FCS_SSHC_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses [selection: hmac-sha1, hmac-sha2-256, hmac-sha2-512] and [selection: AEAD_AES_128_GCM, AEAD_AES_256_GCM, no other MAC algorithms] as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).

Application note: RFC 5647 specifies the use of the AEAD_AES_128_GCM and AEAD_AES_256_GCM algorithms in SSH. As described in RFC 5647, AEAD_AES_128_GCM and AEAD_AES_256_GCM can only be chosen as MAC algorithms when the same algorithm is being used as the encryption algorithm. RFC 6668 specifies the use of the sha2 algorithms in SSH.

FCS_SSHC_EXT.1.7 The TSF shall ensure that [selection: *diffie-hellman-group-exchange-sha256, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, rsa2048-sha256, no other methods*] are the only allowed key exchange methods used for the SSH protocol.

FCS_SSHC_EXT.1.8 The TSF shall ensure that within SSH connections the same session keys are used for a threshold of no longer than one hour, and no more than one gigabyte of transmitted data as specified in RFC 4253. After either of the thresholds is reached, a rekey needs to be performed.

Application note: This SFR defines two thresholds - one for the maximum time span the same session keys can be used and the other one for the maximum amount of data that can be transmitted using the same session keys. Both thresholds need to be implemented and a rekey needs to be performed on whichever threshold is reached first. For the maximum transmitted data threshold, the total incoming and outgoing data needs to be counted. The rekey applies to all session keys (encryption, integrity protection) for incoming and outgoing traffic.

It is acceptable for a TOE to implement lower thresholds than the maximum values defined in the SFR.

For any configurable threshold related to this requirement the guidance documentation needs to specify how the threshold can be configured. The allowed values must either be specified in the

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

guidance documentation and must be lower or equal to the thresholds specified in this SFR or the TOE must not accept values beyond the thresholds specified in this SFR.

FCS_SSHC_EXT.1.9 The TSF shall ensure that the SSH client authenticates the identity of the SSH server using a local database associating each host name with its corresponding public key or [selection: *a list of trusted certification authorities, no other methods*] as described in RFC 4251 section 4.1.

Application note: The list of trusted certification authorities can only be selected if x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp521 or x509v3-rsa2048-sha256 are selected in FCS_SSHC_EXT.1.5.

7.5.3 FCS_SSHS_EXT.1 SSH Server Protocol

FCS_SSHS_EXT.1.1 The TSF shall implement the SSH-2 protocol that complies with RFC(s) [selection*: 4250, 4251, 4252, 4253, 4254, 4256, 4335, 4344*] and make use of [selection: *RFC 4255, 4419, 4432, 4462, 4716, 4818, 5656, 6187, 6239, 6594, 6668, none of these extensions*].

Application note: The ST author selects which of the RFCs to which conformance is being claimed. As in some of these specification methods are used which are obsolete or possibly no longer secure, the ST author shall combine the specifications and the algorithms which are defined in the later components such that these algorithms are used with high priority and (the possibly weak or obsolete) algorithms of the specification with low priority or, as far as possible, never.

FCS_SSHS_EXT.1.2 The TSF shall ensure that the SSH protocol implementation supports the following authentication methods as described in RFC 4252: public key-based, password-based.

FCS_SSHS_EXT.1.3 The TSF shall ensure that, as described in RFC 4253, packets greater than [assignment: *number of bytes*] bytes in an SSH transport connection are dropped.

Application note: RFC 4253 provides for the acceptance of “large packets” with the caveat that the packets should be of “reasonable length” or dropped. The assignment should be filled in by the ST author with the maximum packet size accepted, thus defining “reasonable length” for the TOE.

FCS_SSHS_EXT.1.4 The TSF shall ensure that the SSH transport implementation uses the following encryption algorithms and rejects all other encryption algorithms: [selection: *aes128-cbc, aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr, aes256-ctr, AEAD_AES_128_GCM, AEAD_AES_256_GCM*].

Application note: RFC 5647 specifies the use of the AEAD_AES_128_GCM and AEAD_AES_256_GCM algorithms in SSH. As described in RFC 5647, AEAD_AES_128_GCM and AEAD_AES_256_GCM can only be chosen as encryption algorithms when the same algorithm is being used as the MAC algorithm. Corresponding FCS_COP entries are included in the ST for the algorithms selected here.

FCS_SSHS_EXT.1.5 The TSF shall ensure that the SSH public-key based authentication implementation uses [selection: *pgp-sign-rsa (2000 bit), pgp-sign-dss (2000 bit/ 250 bit)*] and [selection: *ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384, x509v3-ecdsa-sha2-nistp521, x509v3-rsa2048-sha256, no other public key algorithms*] as its public key algorithm(s) and rejects all other public key algorithms.

This project has received funding from the European Union’s Horizon2020 research and innovation programme under grant agreement No730843

Application note: pgp-sign-rsa and pgp-sign-dss has to be used together with a SHA-2- hash function corresponding to the key length. If x509v3-ecdsa-sha2-nistp256, x509v3-ecdsa-sha2-nistp384 or x509v3-ecdsa-sha2-nistp521 are selected, then the list of trusted certification authorities must be selected in FCS_SSHS_EXT.1.9 and the FIA_X509_EXT SFRs are applicable. For the *-sha2-* implementations the sha-2 hash function has to be selected depending on the bit length of the curve in accordance with RFC 5656, Section 6.2.1.

FCS_SSHS_EXT.1.6 The TSF shall ensure that the SSH transport implementation uses [selection: *hmac-sha1, hmac-sha2-256, hmac-sha2-512*] and [selection: *AEAD_AES_128_GCM, AEAD_AES_256_GCM, no other MAC algorithms*] as its data integrity MAC algorithm(s) and rejects all other MAC algorithm(s).

Application note: RFC 5647 specifies the use of the AEAD_AES_128_GCM and AEAD_AES_256_GCM algorithms in SSH. As described in RFC 5647, AEAD_AES_128_GCM and AEAD_AES_256_GCM can only be chosen as MAC algorithms when the same algorithm is being used as the encryption algorithm. RFC 6668 specifies the use of the sha2 algorithms in SSH.

FCS_SSHC_EXT.1.7 The TSF shall ensure that [selection: *diffie-hellman-group-exchange-sha256, ecdh-sha2-nistp256, ecdh-sha2-nistp384, ecdh-sha2-nistp521, rsa2048-sha256, no other methods*] are the only allowed key exchange methods used for the SSH protocol.

FCS_SSHC_EXT.1.8 The TSF shall ensure that within SSH connections the same session keys are used for a threshold of no longer than one hour, and no more than one gigabyte of transmitted data as specified in RFC 4253. After either of the thresholds is reached a rekey needs to be performed.

Application note: This SFR defines two thresholds - one for the maximum time span the same session keys can be used and the other one for the maximum amount of data that can be transmitted using the same session keys. Both thresholds need to be implemented and a rekey needs to be performed on whichever threshold is reached first. For the maximum transmitted data threshold, the total incoming and outgoing data needs to be counted. The rekey applies to all session keys (encryption, integrity protection) for incoming and outgoing traffic.

It is acceptable for a TOE to implement lower thresholds than the maximum values defined in the SFR.

For any configurable threshold related to this requirement the guidance documentation needs to specify how the threshold can be configured. The allowed values must either be specified in the guidance documentation and must be lower or equal to the thresholds specified in this SFR or the TOE must not accept values beyond the thresholds specified in this SFR.

FCS_TLSC_EXT and FCS_TLSS_EXT TLS protocol

If a TOE implements TLS, a corresponding selection in FTP_ITC.1 or FTP_TRP.1 should be made to define what the TLS protocol is implemented to protect.

A TOE may act as the client, the server, or both in TLS sessions. The requirement has been separated into TLS Client (FCS_TLSC_EXT) and TLS Server (FCS_TLSS_EXT) requirements to allow for these differences. If the TOE acts as the client during the claimed TLS sessions, the ST author should claim one of the FCS_TLSC_EXT requirements. If the TOE acts as the server during the claimed TLS sessions, the ST author should claim one of the FCS_TLSS_EXT requirements. If the TOE acts as both a client and server during the claimed TLS sessions, the ST author should claim one of the FCS_TLSC_EXT and FCS_TLSS_EXT requirements.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

TLS may be performed with client authentication.

7.5.4 FCS_TLSC_EXT.1 – TLS Client Protocol (Authenticated)

FCS_TLSC_EXT.1.1 The TSF shall implement **TLS 1.2 (RFC 5246)** and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:

[selection:

- *TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 3268*
- *TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288*
- *TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 3268*
- *TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288*
- *TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289*
- *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*
- *TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 as defined in RFC 3268*
- *TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 as defined in RFC 5288*
- *TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 as defined in RFC 3268*
- *TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 as defined in RFC 5288*
- *TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289*
- *TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289*
- *TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289*

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

- *TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*
- *TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289*
- *TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289*
- *TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289*
- *TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*
- *TLS_DH_DSS_WITH_AES_128_CBC_SHA256 as defined in RFC 3268*
- *TLS_DH_DSS_WITH_AES_128_GCM_SHA256 as defined in RFC 5288*
- *TLS_DH_DSS_WITH_AES_256_CBC_SHA256 as defined in RFC 3268*
- *TLS_DH_DSS_WITH_AES_256_GCM_SHA384 as defined in RFC 5288*
- *TLS_DH_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 3268*
- *TLS_DH_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288*
- *TLS_DH_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 3268*
- *TLS_DH_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288*
- *TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256 as defined in RFC 5489*
- *TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384 as defined in RFC 5489*
- *TLS_DHE_PSK_WITH_AES_128_CBC_SHA256 as defined in RFC 5487*
- *TLS_DHE_PSK_WITH_AES_128_GCM_SHA256 as defined in RFC 5487*
- *TLS_DHE_PSK_WITH_AES_256_CBC_SHA384 as defined in RFC 5487*
- *TLS_DHE_PSK_WITH_AES_256_GCM_ SHA384 as defined in RFC 5487*
- *TLS_RSA_PSK_WITH_AES_128_CBC_SHA256 as defined in RFC 5487*
- *TLS_RSA_PSK_WITH_AES_128_GCM_SHA256 as defined in RFC 5487*
- *TLS_RSA_PSK_WITH_AES_256_CBC_SHA384 as defined in RFC 5487*

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

- *TLS_RSA_PSK_WITH_AES_256_GCM_ SHA384 as defined in RFC 5487*

].

Application note: Some current available implementation of DH(E) in TLS only support 1024 bit. These cipher suites are only recommended if they make use of at least 2000 bit.

The cipher suites TLS_ECDHA_ECDSA_*, TLS_ECDHE_RSA_*, TLS_DHE_DSS_*, and TLS_DHE_RSA_* provide Perfect Forward Secrecy. If the use of a cipher suite with Perfect Forward Secrecy is not possible, TLS_ECDH_ECDSA_*, TLS_ECDH_RSA_*, TLS_DH_DSS_*, and TLS_DH_RSA_* are recommended. The cipher suites TLS_ECDHE_PSK_* and TLS_DHE_PSK_* provide Perfect Forward Secrecy, whereas TLS_RSA_PSK_* does not provide it.

The cipher suites to be tested in the evaluated configuration are limited by this requirement. The ST author should select the cipher suites that are supported. It is necessary to limit the cipher suites that can be used in an evaluated configuration administratively on the server in the test environment.

FCS_TLSC_EXT.1.2 The TSF shall verify that the presented identifier matches the reference identifier per RFC 6125, Section 6.

Application note: The rules for verification of identify are described in Section 6 of RFC 6125. The reference identifier is established by the Administrator (e.g. entering a URL into a web browser or clicking a link), by configuration (e.g. configuring the name of a mail server or authentication server), or by an application (e.g. a parameter of an API) depending on the application service. Based on a singular reference identifier's source domain and application service type (e.g. HTTP, SIP, LDAP), the client establishes all reference identifiers which are acceptable, such as a Common Name for the Subject Name field of the certificate and a (case-insensitive) DNS name, URI name, and Service Name for the Subject Alternative Name field. The client then compares this list of all acceptable reference identifiers to the presented identifiers in the TLS server's certificate.

The preferred method for verification is the Subject Alternative Name using DNS names, URI names, or Service Names. Verification using the Common Name is required for the purposes of backwards compatibility. Additionally, support for use of IP addresses in the Subject Name or Subject Alternative name is discouraged as against best practices but may be implemented. Finally, the client should avoid constructing reference identifiers using wildcards. However, if the presented identifiers include wildcards, the client must follow the best practices regarding matching; these best practices are captured in the evaluation activity.

FCS_TLSC_EXT.1.3 The TSF shall only establish a trusted channel if the server certificate is valid. If the server certificate is deemed invalid, then the TSF shall [selection: *not establish the connection, request authorization to establish the connection, [assignment: other action]*].

Application note: If TLS is selected in FTP_ITC or FTP_TRP.1, then validity is determined by the identifier verification, certificate path, the expiration date, and the revocation status in accordance with RFC 5280.

FCS_TLSC_EXT.1.4 The TSF shall [selection: *not present the Supported Elliptic Curves Extension, present the Supported Elliptic Curves Extension with the following curves:* [selection: *secp256r1, secp384r1, brainpoolP256r1, brainpoolP384r1, brainpoolP512r1, and no other curves*]] in the Client Hello.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

Application note: If ciphersuites with elliptic curves were selected in FCS_TLSC_EXT.1.1, a selection of one or more curves is required. If no cipher suites with elliptic curves were selected in FCS_TLSC_EXT.1.1, then “none” should be selected.

This requirement limits the elliptic curves allowed for authentication and key agreement to the curves from FCS_COP.1/Signature and FCS_CKM.1/Asymmetric and FCS_CKM.2. This extension is required for clients supporting Elliptic Curve cipher suites.

Note that the curves secp256r1 or secp384r1 are equivalent to nistp256 or nistp384, respectively.

FCS_TLSC_EXT.1.5 The TSF shall support mutual authentication using X.509v3 certificates.

Application note: The use of X.509v3 certificates for TLS is addressed in FIA_X509_EXT.2.1. This requirement adds that the client must be capable of presenting a certificate to a TLS server for TLS mutual authentication.

7.5.5 FCS_TLSS_EXT.1 TLS Server Protocol with mutual authentication

FCS_TLSS_EXT.1.1 The TSF shall implement **TLS 1.2 (RFC 5246)** and reject all other TLS and SSL versions. The TLS implementation will support the following ciphersuites:

[selection:

- *TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 3268*
- *TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288*
- *TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 3268*
- *TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288*
- *TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289*
- *TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289*
- *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*
- *TLS_DHE_DSS_WITH_AES_128_CBC_SHA256 as defined in RFC 3268*
- *TLS_DHE_DSS_WITH_AES_128_GCM_SHA256 as defined in RFC 5288*

This project has received funding from the European Union’s Horizon2020 research and innovation programme under grant agreement No730843

- *TLS_DHE_DSS_WITH_AES_256_CBC_SHA256 as defined in RFC 3268*
- *TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 as defined in RFC 5288*
- *TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289*
- *TLS_ECDH_ECDSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289*
- *TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289*
- *TLS_ECDH_ECDSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*
- *TLS_ECDH_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 5289*
- *TLS_ECDH_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289*
- *TLS_ECDH_RSA_WITH_AES_256_CBC_SHA384 as defined in RFC 5289*
- *TLS_ECDH_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289*
- *TLS_DH_DSS_WITH_AES_128_CBC_SHA256 as defined in RFC 3268*
- *TLS_DH_DSS_WITH_AES_128_GCM_SHA256 as defined in RFC 5288*
- *TLS_DH_DSS_WITH_AES_256_CBC_SHA256 as defined in RFC 3268*
- *TLS_DH_DSS_WITH_AES_256_GCM_SHA384 as defined in RFC 5288*
- *TLS_DH_RSA_WITH_AES_128_CBC_SHA256 as defined in RFC 3268*
- *TLS_DH_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5288*
- *TLS_DH_RSA_WITH_AES_256_CBC_SHA256 as defined in RFC 3268*
- *TLS_DH_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288*
- *TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256 as defined in RFC 5489*
- *TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384 as defined in RFC 5489*
- *TLS_DHE_PSK_WITH_AES_128_CBC_SHA256 as defined in RFC 5487*
- *TLS_DHE_PSK_WITH_AES_128_GCM_SHA256 as defined in RFC 5487*
- *TLS_DHE_PSK_WITH_AES_256_CBC_SHA384 as defined in RFC 5487*

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

- *TLS_DHE_PSK_WITH_AES_256_GCM_ SHA384 as defined in RFC 5487*
- *TLS_RSA_PSK_WITH_AES_128_CBC_SHA256 as defined in RFC 5487*
- *TLS_RSA_PSK_WITH_AES_128_GCM_SHA256 as defined in RFC 5487*
- *TLS_RSA_PSK_WITH_AES_256_CBC_SHA384 as defined in RFC 5487*
- *TLS_RSA_PSK_WITH_AES_256_GCM_ SHA384 as defined in RFC 5487*

].

Application note: The cipher suites to be tested in the evaluated configuration are limited by this requirement. The ST author should select the optional cipher suites that are supported. It is necessary to limit the cipher suites that can be used in an evaluated configuration administratively on the server in the test environment.

FCS_TLSS_EXT.1.2 The TSF shall deny connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0, and TLS 1.1.

Application note: All SSL versions, TLS 1.0, and TLS 1.1 are denied.

FCS_TLSS_EXT.1.3 The TSF shall [selection: *perform RSA key establishment with key size* [selection: *2048 bits, 3072 bits, 4096 bits*]; *generate EC Diffie-Hellman parameters over the curves* [selection: *secp256r1, secp384r1, brainpoolP256r1, brainpoolP384r1, brainpoolP512r1*] *and no other curves; generate Diffie-Hellman parameters of size 2048 bits and* [selection: *3072 bits, no other size]*].

Application note: If the ST lists a DHE or ECDHE cipher suite in FCS_TLSS_EXT.1.1, the ST must include the Diffie-Hellman or the curves selection in the requirement. FMT_SMF.1 requires the configuration of the key agreement parameters to establish the security strength of the TLS connection.

FCS_TLSS_EXT.1.4 The TSF shall support mutual authentication of TLS clients using X.509v3 certificates.

FCS_TLSS_EXT.1.5 The TSF shall not establish a trusted channel if the client certificate is invalid. If the client certificate is deemed invalid, then the TSF shall [selection: *not establish the connection, request authorization to establish the connection,* [assignment: *other action*]].

Application note: The use of X.509v3 certificates for TLS is addressed in FIA_X509_EXT.2.1. This requirement adds that this use must include support for client-side certificates for TLS mutual authentication.

If TLS is selected for FTP_ITC, then validity is determined by the certificate path, the expiration date, and the revocation status in accordance with RFC 5280. Certificate validity shall be tested in accordance with testing performed for FIA_X509_EXT.1.

FCS_TLSS_EXT.1.6 The TSF shall not establish a trusted channel if the distinguished name (DN) or Subject Alternative Name (SAN) contained in a certificate does not match the expected identifier for the client.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

Application note: The client identifier may be in the Subject field or the Subject Alternative Name extension of the certificate. The expected identifier may either be configured, may be compared to the Domain Name, IP address, username, or email address used by the client, or may be passed to a directory server for comparison.

FCS_EXT HTTPS Protocol

If a TOE implements HTTPS, a corresponding selection in FTP_ITC.1 and/or FTP_TRP.1 should have been made that defines what the HTTPS protocol is implemented to protect.

7.5.6 FCS_HTTPS_EXT.1 HTTPS Protocol

FCS_HTTPS_EXT.1.1 The TSF shall implement the HTTPS protocol that complies with RFC 2818.

Application note: The ST author must provide enough detail to determine how the implementation is complying with the standard(s) identified; this can be done by additional detail in the TSS.

FCS_HTTPS_EXT.1.2 The TSF shall implement HTTPS using TLS.

FCS_HTTPS_EXT.1.3 If a peer certificate is presented, the TSF shall [selection: *not require client authentication, not establish the connection, request authorization to establish the connection,* [assignment: *other action*]] if the peer certificate is deemed invalid.

Application note: If HTTPS is selected in FTP_TRP.1 or FTP_ITC.1, then validity is determined by the identifier verification, certificate path, the expiration date, and the revocation status in accordance with RFC 5280. Certificate validity is tested in accordance with testing performed for FIA_X509_EXT.1.

Authentication using X.509 certificates (FIA_X.509_EXT)

This family defines the behaviour, management, and use of X.509v3 certificates for functions to be performed by the TSF. Components in this family require validation of certificates according to a specified set of rules, use of certificates for authentication for protocols and integrity verification, and the generation of certificate requests.

FIA_X509_EXT.1 X509 Certificate Validation requires the TSF to check and validate certificates in accordance with the RFCs and rules specified in the component.

FIA_X509_EXT.2 X509 Certificate Authentication requires the TSF to use certificates to authenticate peers in protocols that support certificates, as well as for integrity verification and potentially other functions that require certificates.

FIA_X509_EXT.3 X509 Certificate Requests requires the TSF to be able to generate Certificate Request Messages and validate responses.

7.5.7 FIA_X.509_EXT.1 X.509 Certificate Validation

FIA_X509_EXT.1.1 The TSF shall validate certificates in accordance with the following rules:

- RFC 5280 certificate validation and certificate path validation.
- The certificate path must terminate with a trusted CA certificate.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

- The TSF shall validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates.
- The TSF shall validate the revocation status of the certificate using [selection: *the Online Certificate Status Protocol (OCSP) as specified in RFC 6960, a Certificate Revocation List (CRL) as specified in RFC 5280 Section 6.3, Certificate Revocation List (CRL) as specified in RFC 5759 Section 5, no revocation method*].
- The TSF shall validate the extendedKeyUsage field according to the following rules: [assignment: *rules that govern contents of the extendedKeyUsage field that need to be verified*].

Application note: FIA_X509_EXT.1.1 lists the rules for validating certificates. The ST author selects whether revocation status is verified using OCSP or CRLs. The ST author fills in the assignment with rules that may apply to other requirements in the ST. For instance, if a protocol such as TLS that uses certificates is specified in the ST, then certain values for the extendedKeyUsage field (e.g., “Server Authentication Purpose”) could be specified.

FIA_X509_EXT.1.2 The TSF shall only treat a certificate as a CA certificate if the basicConstraints extension is present and the CA flag is set to TRUE.

Application note: This requirement applies to certificates that are used and processed by the TSF and restricts the certificates that may be added as trusted CA certificates.

7.5.8 FIA_X509_EXT.2 X509 Certificate Authentication

FIA_X509_EXT.2.1 The TSF shall use X.509v3 certificates as defined by RFC 5280 to support authentication for [selection*: HTTPS, IPsec, TLS, SSH, [*assignment: *other protocols], no protocols*], and [selection: *code signing for system software updates, code signing for integrity verification, [*assignment: *other uses*], no additional uses].

Application note: If the TOE specifies the implementation of communications protocols that perform peer authentication using certificates, the ST author either selects or assigns the protocols that are specified; otherwise, they select “no protocols”. Protocols that do not use X.509 based peer authentication include SSH, where than ecdsa-sha2-nistp256, ecdsa-sha2-nistp384, ecdsa-sha2-nistp521, pgp-sign-rsa, pgp-sign-dss are selected. The TOE may also use certificates for other purposes; the second selection and assignment are used to specify these cases.

FIA_X509_EXT.2.2 When the TSF cannot establish a connection to determine the validity of a certificate, the TSF shall [selection: *allow the Administrator to choose whether to accept the certificate in these cases, accept the certificate, not accept the certificate*].

Application note: Often a connection must be established to check the revocation status of a certificate - either to download a CRL or to perform a lookup using OCSP. The selection is used to describe the behaviour in the event that such a connection cannot be established (for example, due to a network error). If the TOE has determined the certificate valid according to all other rules in FIA_X509_EXT.1, the behaviour indicated in the selection determines the validity. The TOE must not accept the certificate if it fails any of the other validation rules in FIA_X509_EXT.1. If the Administrator-configured option is selected by the ST author, the ST author also selects the corresponding function in FMT_SMF.1.

This project has received funding from the European Union’s Horizon2020 research and innovation programme under grant agreement No730843

7.5.9 FIA_X509_EXT.3 X.509 Certificate Requests

FIA_X509_EXT.3.1 The TSF shall generate a Certificate Request Message as specified by RFC 2986 and be able to provide the following information in the request: public key and [selection: *device-specific information, Common Name, Organization, Organizational Unit, Country, [*assignment: *other information]*].

FIA_X509_EXT.3.2 The TSF shall validate the chain of certificates from the Root CA upon receiving the CA Certificate Response.

7.6 Security Functional Requirements Rationale

7.6.1 Coverage

The following table provides a mapping of SFR to the security objectives, showing that each security functional requirement addresses at least one security objective and that all security objectives are addressed by one or more SFRs.

	O.CHANNEL	O.MANAGE-VPN	O.FLOW-VPN	O.AUDIT-VPN
FAU_GEN.1				X
FMT_MSA.1			X	
FMT_MSA.3			X	
FMT_MOF.1		X		
FMT_MTD.1		X		
FMT_SMF.1		X		
FCS_CKM.1/Symmetric	X			
FCS_CKM.1/Asymmetric	X			
FCS_CKM.2	X			
FCS_CKM.4	X			
FCS_COP.1/AES	X			
FCS_COP.1/Signature	X			
FCS_COP.1/Hash	X			
FCS_COP.1/KeyedHash	X			
FCS_COP.1/MAC	X			
FCS_RGB_EXT.1	X			
FDP_IFC.1			X	
FDP_IFF.1			X	
FTP_ITC.1	X			
FCS_IPSEC_EXT.1	X			
FCS_SSHC_EXT.1	X			

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

FCS_SSHS_EXT.1	X			
FCS_TLSC_EXT.1	X			
FCS_TLSS_EXT.1	X			
FCS_HTTPS_EXT.1	X			
FIA_X.509_EXT.1	X			
FIA_X509_EXT.2	X			
FIA_X509_EXT.3	X			

Application note: Only one trusted channel protocol is required to meet the security objective O.CHANNEL and not all. The protocol(s) implemented are specified by FPT_ITC.1 as IPsec, SSH, TLS or HTTPS and they require either: FCS_IPSEC_EXT.1; FCS_SSHC_EXT.1, FCS_SSHS_EXT.1; FCS_TLSC_EXT.1, FCS_TLSS_EXT.1; or FCS_HTTPS_EXT.1 is required.

7.6.2 Sufficiency

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives.

Security Objective	Rationale how the SFRs are meeting the security objective
O.AUDIT-VPN	The objective: • The TOE must be able to generate security relevant events as well as events related to authorised use of security functions. is met by: • FAU_GEN.1 ensures that audit records can be generated for security relevant events and authorised use of security functionality. • FPT_STM.1 in the Base PP ensures that audit records are accompanied by accurate time stamps.
O.CHANNEL	The objective: • The TOE must be able to provide trusted channels to remote trusted networks and protect information transmitted to and received from such networks against unauthorised disclosure and to detect any modification of incoming information transmitted from such networks, and to provide the means for the remote network to verify the integrity of information transmitted out of the TOE to such networks is met by: • FPT_ITC.1 ensuing that there is a trusted channel. It selects one or more of the trusted channel protocols: IPsec, SSH, TLS or HTTPS. Depending on the selection the following SFR will also satisfy the security objective O.CHANNEL For IPsec it is met by: • FCS_IPSEC_EXT.1 for the IPsec protocol • FCS_CKM.1/Symmetric Cryptographic Key Generation

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

	• FCS_CKM.1/Asymmetric Cryptographic Key Generation • FCS_CKM.2 Cryptographic Key Establishment • FCS_COP.1/AES Cryptographic Operation • FCS_COP.1/Signature Cryptographic Operation • FCS_COP.1/Hash Cryptographic Operation • FCS_COP.1/KeyedHash Cryptographic Operation • FCS_COP.1/MAC Cryptographic Operation • FCS_RBG_EXT.1 Random Bit Generation If X.509 has been selected as authentication method, also: • FIA_X509_EXT.1 for the X.509 Certificate Validation, FIA_X509_EXT.2 for the X.509 Certificate Authentication, FIA_X509_EXT.3 for the X.509 Certificate Requests. For SSH client support it is met by: • FCS_SSHC_EXT.1 for the SSH client protocol • FCS_CKM.1/Symmetric Cryptographic Key Generation • FCS_CKM.1/Asymmetric Cryptographic Key Generation • FCS_CKM.2 Cryptographic Key Establishment • FCS_COP.1/AES Cryptographic Operation • FCS_COP.1/Signature Cryptographic Operation • FCS_COP.1/Hash Cryptographic Operation • FCS_COP.1/KeyedHash Cryptographic Operation • FCS_COP.1/MAC Cryptographic Operation • FCS_RBG_EXT.1 Random Bit Generation If X.509 has been selected as authentication method, also: • FIA_X.509_EXT.1 for the X.509 Certificate Validation, FIA_X509_EXT.2 for the X.509 Certificate Authentication, FIA_X509_EXT.3 for the X.509 Certificate Requests. and for SSH server support it is met by: • FCS_SSHS_EXT.1 for the SSH server protocol • FCS_CKM.1/Symmetric Cryptographic Key Generation • FCS_CKM.1/Asymmetric Cryptographic Key Generation • FCS_CKM.2 Cryptographic Key Establishment • FCS_COP.1/AES Cryptographic Operation • FCS_COP.1/Signature Cryptographic Operation • FCS_COP.1/Hash Cryptographic Operation • FCS_COP.1/KeyedHash Cryptographic Operation • FCS_COP.1/MAC Cryptographic Operation • FCS_RBG_EXT.1 Random Bit Generation If X.509 has been selected as authentication method, also: • FIA_X509_EXT.1 for the X.509 Certificate Validation, FIA_X509_EXT.2 for the X.509 Certificate Authentication, FIA_X509_EXT.3 for the X.509 Certificate Requests. For TLS client support it is met by: • FPT_ITC.1 ensuing that there is a trusted TLS channel

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

	• FCS_TLSC_EXT.1 • FCS_CKM.1/Symmetric Cryptographic Key Generation • FCS_CKM.1/Asymmetric Cryptographic Key Generation • FCS_CKM.2 Cryptographic Key Establishment • FCS_COP.1/AES Cryptographic Operation • FCS_COP.1/Signature Cryptographic Operation • FCS_COP.1/Hash Cryptographic Operation • FCS_COP.1/KeyedHash Cryptographic Operation • FCS_RBG_EXT.1 Random Bit Generation • FIA_X509_EXT.2 Certificate Authentication If X.509 has been selected as authentication method, also: • FIA_X.509_EXT.1 for the X.509 Certificate Validation, FIA_X509_EXT.2 for the X.509 Certificate Authentication, FIA_X509_EXT.3 for the X.509 Certificate Requests. and for TLS server support it is met by: • FPT_ITC.1 ensuing that there is a trusted TLS channel • FCS_TLSS_EXT.1 • FCS_CKM.1/Symmetric Cryptographic Key Generation • FCS_CKM.1/Asymmetric Cryptographic Key Generation • FCS_CKM.1 Cryptographic Key Generation • FCS_CKM.2 Cryptographic Key Establishment • FCS_COP.1/AES Cryptographic Operation • FCS_COP.1/Signature Cryptographic Operation • FCS_COP.1/Hash Cryptographic Operation • FCS_COP.1/KeyedHash Cryptographic Operation • FCS_RBG_EXT.1 Random Bit Generation If X.509 has been selected as authentication method, also: • FIA_X509_EXT.1 for the X.509 Certificate Validation, FIA_X509_EXT.2 for the X.509 Certificate Authentication, FIA_X509_EXT.3 for the X.509 Certificate Requests. For HTTPS it is met by: • FPT_ITC.1 ensuing that there is a trusted HTTPS channel • FCS_HTTPS_EXT.1 for the HTTPS protocol • FCS_TLSC_EXT.1 TLS Client Protocol • FCS_TLSS_EXT.1 TLS Server Protocol • Depending on the TLS client or server selection, also all the SFR that are specified above for the TLS client and server respectively. If X.509 has been selected as authentication method, also the corresponding FIA_X509_EXT SFRs.
O.MANAGE-VPN	The objective: • The TOE must provide the means for an authorised administrator to configure and manage the TOE security functions. is met by: • FMT_MOF.1 then restricts the ability to modify the behaviour of functions to identified authorized roles.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

	• FMT_MTD.1 restrict the changes to TSF data associated with the trusted channel also to identified authorized roles. • FMT_MSA.1 and FMT_MSA.3 ensures that initialization and management of the security attributes associated with the trusted channel is protected. • FMT_SMF.1 ensure the authorized administrators with the ability to configure the security properties of the trusted channel.
O.FLOW-VPN	The objective: • The TOE must mediate the flow of network traffic to ensure that network traffic intended to be passed through the trusted channel only leaves the TOE through the trusted channel in accordance to the security policy. is met by: • FDP_IFC.1 and FDP_IFF.1 ensures that the TOE enforces the Network Information Flow Control SFP for the network traffic using the trusted channel.

7.6.3 Security Functional Requirements Dependency Analysis

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives.

SFR	Dependencies	Resolved
FAU_GEN.1	FPT_STM.1	Resolved, as FPT_STM.1 is part of the Base PP.
FMT_MSA.1	[FDP_IFC.1 or FDP_ACC.1] FMT_SMF.1 FMT_SMR.1	Resolved by FDP_IFC.1 Resolved Resolved by the Base PP. If operations on security attributes are possible it must be done by a role defined in FMT_SMR.1 of the Base PP.
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	Resolved Resolved by the Base PP. If any override of restrictive default values is possible it must be restricted to a role defined in FMT_SMR.1 of the Base PP.
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	Resolved Resolved by the Base PP. If any change of functions is possible it must be restricted to a role defined in FMT_SMR.1 of the Base PP.
FMT_MTD.1	FMT_SMF.1 FMT_SMR.1	Resolved Resolved by the Base PP. If any change to TSF data is possible it must be restricted to a role

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

		defined in FMT_SMR.1 of the Base PP.
FMT_SMF.1	No dependencies	–
Generic Cryptographic SFRs		
FCS_CKM.1/Symmetric	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	Resolved by FCS_CKM.2 Resolved
FCS_CKM.1/Asymmetric	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	Resolved by FCS_CKM.2 Resolved
FCS_CKM.2	[FTP_ITC.1 or FTP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Resolved by FCS_CKM.1 (also FTP_ITC.1 could be used for import as a secure channel) Resolved
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Resolved by FCS_CKM.1 (also FTP_ITC.1 could be used for import as a secure channel)
FCS_COP.1/AES	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Resolved by FCS_CKM.1 (also FTP_ITC.1 could be used for import as a secure channel) Resolved
FCS_COP.1/Signature	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Resolved by FCS_CKM.1 (also FTP_ITC.1 could be used for import as a secure channel) Resolved
FCS_COP.1/Hash	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Not resolved Not resolved FCS_COP.1/Hash specifies keyless hashing operations, so initialisation and destruction of keys are not relevant
FCS_COP.1/KeyedHash	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Resolved by FCS_CKM.1 (also FTP_ITC.1 could be used for import as a secure channel) Resolved
FCS_COP.1/MAC	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1] FCS_CKM.4	Resolved by FCS_CKM.1 (also FTP_ITC.1 could be used for import as a secure channel) Resolved
FCS_RGB_EXT.1	No dependencies	–
SFRs for IPsec, SSH, TLS and HTTPS		
FDP_IFC.1	FDP_IFF.1	Resolved
FDP_IFF.1	FDP_IFC.1 FMT_MSA.3	Resolved Resolved

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

FTP_ITC.1	No dependencies	–
FCS_HTTPS_EXT.1 (HTTPS Protocol)	[FCS_TLSC_EXT.1 or FCS_TLSS_EXT.1]	FCS_TLSC_EXT.1 and FCS_TLSS_EXT.1
FCS_IPSEC_EXT.1 (IPsec Protocol)	FCS_CKM.1 FCS_CKM.2 FCS_COP.1/DataEncryption FCS_COP.1/SigGen FCS_COP.1/Hash FCS_COP.1/KeyedHash FCS_RBG_EXT.1	Resolved Resolved Resolved Resolved Resolved Resolved Resolved
FCS_SSHC_EXT.1 (SSH Client Protocol)	FCS_CKM.1 FCS_CKM.2 FCS_COP.1/DataEncryption FCS_COP.1/SigGen FCS_COP.1/Hash FCS_COP.1/KeyedHash FCS_RBG_EXT.1	Resolved Resolved Resolved Resolved Resolved Resolved Resolved
FCS_SSHS_EXT.1 (SSH Server Protocol)	FCS_CKM.1 FCS_CKM.2 FCS_COP.1/DataEncryption FCS_COP.1/SigGen FCS_COP.1/Hash FCS_COP.1/KeyedHash FCS_RBG_EXT.1	Resolved Resolved Resolved Resolved Resolved Resolved Resolved
FCS_TLSC_EXT.1 (TLS Client Protocol)	FCS_CKM.1 FCS_CKM.2 FCS_COP.1/DataEncryption FCS_COP.1/SigGen FCS_COP.1/Hash FCS_COP.1/KeyedHash FCS_RBG_EXT.1	Resolved Resolved Resolved Resolved Resolved Resolved Resolved
FCS_TLSC_EXT.2 (TLS Client Protocol with authentication)	FCS_CKM.1 FCS_CKM.2 FCS_COP.1/DataEncryption FCS_COP.1/SigGen FCS_COP.1/Hash FCS_COP.1/KeyedHash FCS_RBG_EXT.1	Resolved Resolved Resolved Resolved Resolved Resolved Resolved
FCS_TLSS_EXT.1 (TLS Server Protocol)	FCS_CKM.1 FCS_CKM.2 FCS_COP.1/DataEncryption FCS_COP.1/SigGen FCS_COP.1/Hash FCS_COP.1/KeyedHash FCS_RBG_EXT.1	Resolved Resolved Resolved Resolved Resolved Resolved Resolved

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

FCS_TLSS_EXT.2 (TLS Server Protocol w. mutual authentication)	FCS_CKM.1 FCS_CKM.2 FCS_COP.1/DataEncryption FCS_COP.1/SigGen FCS_COP.1/Hash FCS_COP.1/KeyedHash FCS_RBG_EXT.1	Resolved Resolved Resolved Resolved Resolved Resolved Resolved
FIA_X509_EXT.1 (X.509 Certificate Validation)	None	–
FIA_X509_EXT.2 (X.509 Certificate Authentication)	None	–
FIA_X509_EXT.3 (X.509 Certificate Requests)	FCS_CKM.1	Resolved

7.7 Security Assurance Requirements

The security assurance requirements of this Security are those defined for the assurance level EAL4 augmented with ALC_FLR.2, as specified in the Base PP.

7.8 Security Assurance Requirements Rationale

The assurance requirements are inherited from the Base PP.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843

8. REFERENCES

[Base] Base Protection Profile for Network Separation Mechanisms, Version 005, 2018-09-25. The Base Protection Profile developed as part of the CYRail-project under European Union's Horizon 2020 research and innovation programme (grant agreement no. 730843).

[CC] Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model, April 2017, Version 3.1 Revision 5, CCMB-2017-04-001; Part 2: Security functional Components, April 2017, Version 3.1 Revision 5, CCMB-2017-04-002; Part 3: Security Assurance Components, April 2017, Version 3.1 Revision 5, CCMB-2017-04-003.

[CEM] Common Methodology for Information Technology Security Evaluation. Evaluation Methodology. April 2017, Version 3.1, Revision 5, CCMB-2017-04-004.

[cPPND] collaborative Protection Profile for Network Devices, Version 2.0 (5 May 2017).

[ISO15446] Technical Report ISO/IEC TR 15446, Information technology – Security techniques – Guide for the production of Protection Profiles and Security Targets, Second edition 2009-03-01.

[PPST-Guide] The PP/ST Guide, August 2010, Version 2, Revision 0, Bundesamt für Sicherheit in der Informationstechnik.

This project has received funding from the European Union's Horizon2020 research and innovation programme under grant agreement No730843