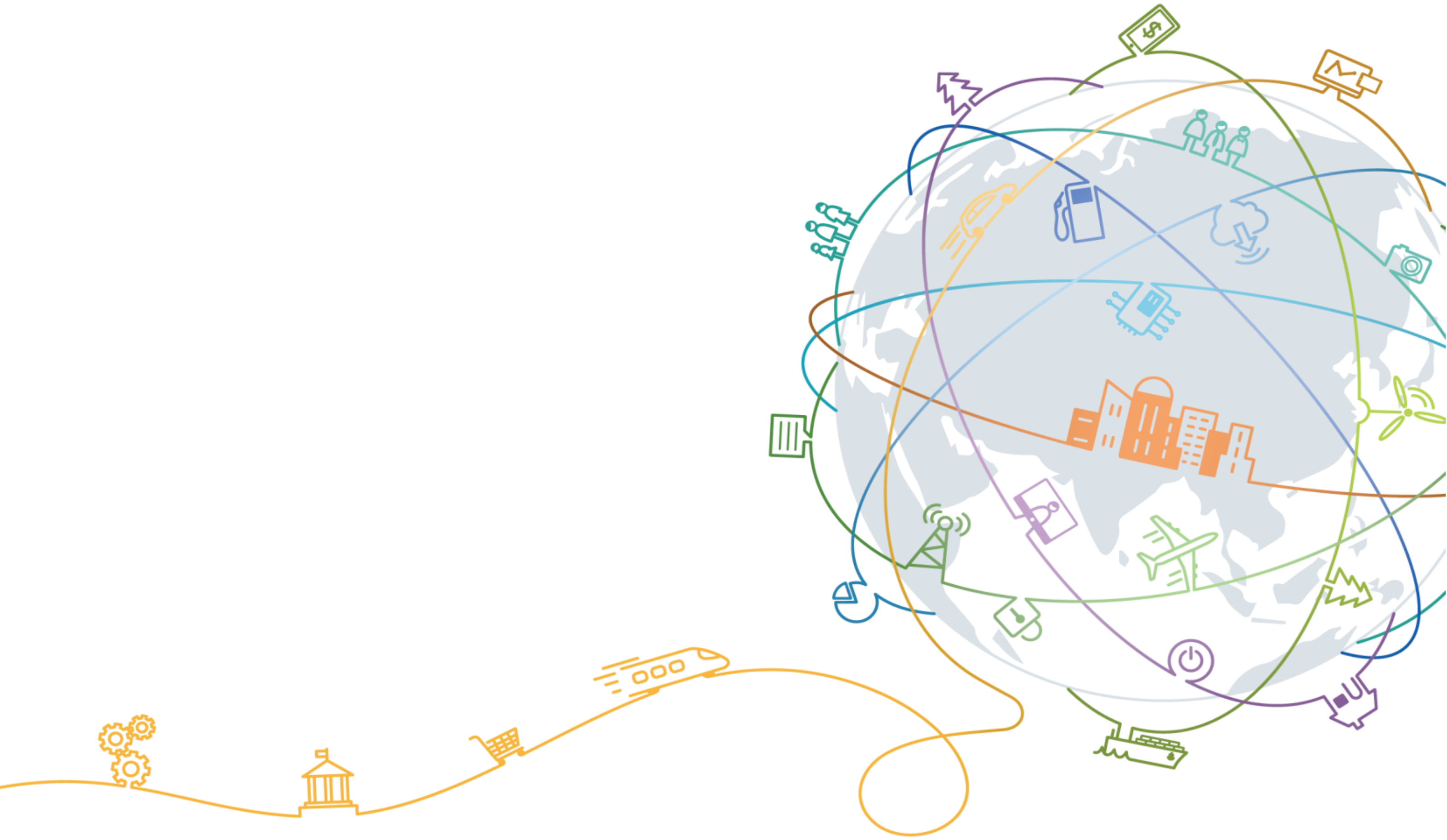
Baseboard Management Controller Protection Profile with Firmware update Module

Version	1.0
Date	2022-09-28



HUAWEI TECHNOLOGIES CO., LTD.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

About This Document

Purpose

This document provides a Protection Profile (PP) for devices used as Baseboard Management Controllers in general administrated servers (GS).

Change History

Changes between document issues are cumulative. The latest document issue contains all the changes made in earlier issues.

Date	Revision Version	Chapter Number	Change Description	Author
2022-09-28	1.0		Certified version	Trustworthiness Certification team, Huawei Computing Product Line

Contents

Figures

Tables

1 Introduction

1.1 Protection Profile Identification

Title	Baseboard Management Controller Protection Profile with Firmware update module
Authors:	Huawei Technologies Co. Ltd.
Version:	1.0
Date:	2022-09-28
CC Version:	3.1 Revision 5
Target EAL	EAL2 augmented with ALC_FLR.1

This PP uses the concept of modular Protection Profiles (PP), where the Base-PP defines the minimum and therewith mandatory set of security requirements, and where the Firmware Update (FWU) as PP-module covers the optional requirements for the conduct of a firmware update. The modularisation concept is described in [CPP1], chapter 9.

The Base-PP implements the core and must have respectively minimum set of functionalities of a Base Board Management Controller (BMC). This provides the fundament on which the ST writer can optionally and freely combine FWU PP-module, as there is no dependency between the PP-module parts. Consequently, following combinations result:

1. Base-PP only
2. Base-PP and FWU PP-module

The FWU PP-module implements a set of functionalities for the TOEs providing a firmware update mechanism. The FWU PP-module depends on the definitions provided by the Base-PP. The FWU PP-module cannot be used standalone and cannot be combined with another PP, as the requirements rely on the presence of security functionalities provided by the Base-PP.

1.2 TOE overview

1.2.1 Location of the TOE in a network

Nowadays it is a necessity and thus most servers used in various industries implement and operate a dedicated administration interface as the corresponding servers need configuration management and monitoring.

Such a server administration system is usually implemented by a so called out-of-band-management functionality realised with a Baseboard Management Controller (BMC) which is also the TOE of this PP. Generally, the TOE provides following management functionalities to its host server:

- Hardware monitoring (such as CPUs, fans, slots, etc)
- Fault diagnostics and management
- Energy management
- Firmware (e.g. BIOS) management and updating
- Storage management
- Server remote control

As an out-of-band system, the TOE is independent to all in-band components, so that it can provide following advantages:

- The service and management planes of a server are separated from each other, avoiding mutual interference.
- All Phase Manageability. A server can be managed without relying on the status of its CPUs, OS, and software.

As the TOE has a direct control to server, it's very critical to maintain its security to protect the integrity and availability of a server.

The TOE is usually integrated on the motherboard of a server, and provides physically or logically independent interface that should be used in a dedicated management network which is separated from other business networks. And this dedicated management network shall not be connected to the internet. Thus, the server management could be operated in a more secure network environment with trust communication path or channel.

Recommended good practices for an operational environment are the use of a dedicated management sub-network to manage the TOE and to not connect the TOE with the Internet. Generally, devices deployed within an IT network or domain, including servers, network devices, etc., provide a dedicated management port which is used to connect to the management sub-network, hence management traffic is separated from other service related traffic. At the boundary of this IT network, gateway and security devices shall be deployed appropriately to perform strictly access control policy and strong authentication mechanism for accessing management sub-network, and segregate incoming management traffic from remote users who may access via intranet or internet. These measurements are the first line of defence of operational environment at network level, they are out of scope of the TOE but recommended.

The networks outside the operational environment and before the gateway could be intranet or internet, which is regardless for our Base-PP, as we just assume proper network segregation of management network and other service network.

It is a commonly known fact that attackers adversely try to achieve access to servers in order to eavesdrop, tamper, control and abuse in any known or yet unknown way the conquered server for their own purposes, such as financial gain by blackmailing after encryption of essential files, illegally selling extracted secrets to other attackers, doing espionage or other adverse purposes.

For these reasons, a dedicated set of security functional and security assurance requirements shall be fulfilled to defence against these threats. This Base-PP provides a minimum and therefore mandatory set of security requirements to ensure the correct operation of the TOE first, which in turn provides critical management function to its hosting server.

1.2.2 The TOE Type and physical scope of the TOE

In a general sense, a general server (GS) may consist of a management plane and a service plane. The TOE constitutes thereby the management plane which is hosted by the server. As an autonomous computing system, the TOE can be operative while the service plane is off or in failure state.

The TOE accesses the service plane by internal interfaces of its host server such as PCIe, LPC and USB, so that the TOE can get the status of each hardware component of the host server and manage them. The TOE can even simulate or virtualises the peripheral devices such as mouse, keyboard and screen to enable the TOE user accessing the host server OS.

A general server architecture can be retrieved at [NIST-1], page 5. There is also a separation between the management plane, respectively the TOE, and the service plane carrying the primary operating system, the common user applications and the other not TOE relevant components of the GS.

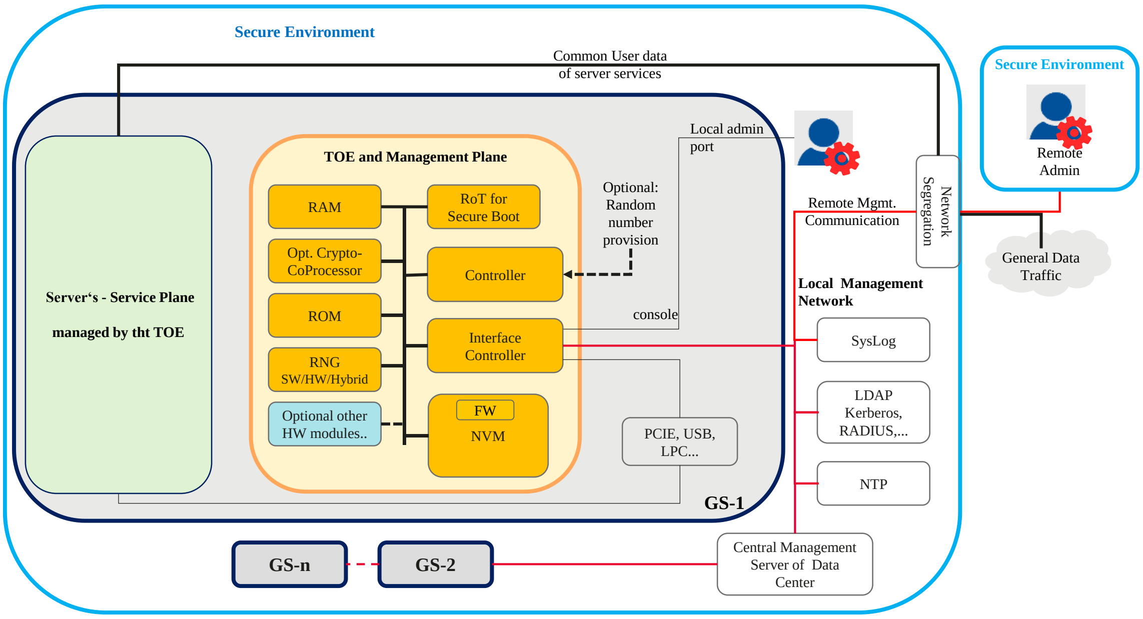
The physical scope of the TOE includes the HW, FW and the belonging user guidance. Only the TOE HW hosts and executes the TOE FW.

In order to provide a clear separation, the code and data executed or stored within the TOE is called FW. Other SW applications, code and data operated on the host or loaded after the TOE booting has been completed, is called SW. Such SW is not part of the TOE.

The design or chosen technology of the host defines also the TOE HW form factor which could be of any kind. For example, the TOE could be an integrated SoC on the motherboard of a GS, or a sub-PCB inserted in a GS slot. There is no limitation to the TOE´s form factor.

The location and outline of the TOE as well its main components within a GS and networks is illustrated below.

Figure 1 Location of the Base-PP TOE type



The TOE hardware architecture comprises the orange components in the yellow marked field, but can be extended on developer's decision with optional other HW modules as sketched with the light blue box connected with the dashed line.

The cryptographic services operated by the TOE require random numbers with appropriate entropy quality. For that reason, the TOE implements a random number generation (RNG) module, which need a seed of good entropy quality and the seed can be gathered from either inside or outside of the TOE. The ST writer shall define the source of entropy, and define the interface for it if it is gathered from outside of the TOE.

The interface component is a schematic summary of various interface functions. This TOE interface controller connects also to the local management network and to the PCIE, USB, LPC or similar components on the GS. Thus, the TOE accesses HW components of the host server directly to obtain their status and to provide server management functions to the TOE users through the local management network.

The general data traffic has no interface to the TOE as this traffic remains entirely on the service plane. This requires to segregate the so-called management traffic to the TOE from the general data traffic to the service plane. For that reason, a network segregation is operational precondition for this TOE.

The dark blue outline indicates the borders of the GS inside the secure operation environment. The secure operational environment is defined by the according objectives for the operational environment (OE) in chapter 4.3. The GS itself can be standalone or be part of a cloud or data centre with a centralised management server, also interacting with the TOE via the local management network.

The light blue outline indicates the secure operational environment which shall protect all ICT components from physical attacks.

The HW components of the TOE are the

1. Controller, providing the execution or processing environment for the FW as well as the management of the peripherals
2. Interface Controller, providing the local management network connectivity, connecting to the platform controller hub and provides the interfaces to the administrator
3. ROT, root of trust, an IC component containing the initial credentials and implementing the trust anchor for booting
4. ROM, an immutable memory containing the very initial FW package
5. RAM, is the fast and volatile memory required for the runtime operation of the controller
6. NVM, the non-volatile memory containing further FW packages, the log file and other non-TOE application SW
7. Cryptographic Co-Processor which is an optional HW based computation acceleration for cryptographic operations.
8. Random number generator module, if not implemented as pure FW-RNG

The FW components of the TOE are the

1. TOE booting programme
2. TOE underlying operating system (OS)
3. BMC application

The user guidance of the TOE are the

1. Preparative procedure
2. Operational user guidance

Some of the TOE TSF rely on the presence of services available on local management network. These services are provided by:

1. A Syslog server for collecting and managing audit logs
2. A NTP server for synchronizing system time
3. A LDAP[1] server for remote authentication
4. If present, a central management server for managing multiple TOEs

[1] Note that the LDAP server is just named as one typical example, it can be any other server type providing the comparable required functionality of a LDAP server.

1.2.3 The logical scope of the Base PP

The TOE provides following security features：

- ✓ User identification, authentication and authorization
- ✓ Cryptographic support
- ✓ Audit of events
- ✓ Security management
- ✓ TOE access control
- ✓ Trusted communication
- ✓ HW supported secure booting

1.2.3.1 User identification, authentication and authorization

The TOE provides user identification and authentication functionalities and supports role-based user access control. An identified and authenticated user can only access TOE resources and operations which are assigned to its role.

The TOE supports multiple authentication mechanisms including:

- Local authentication: the TOE performs user authentication by itself.
- Remote authentication: the TOE forward user authentication request to a remote entity which performs centralized authentication service based on standard protocols such as LDAP, Kerberos, etc. It is the remote entity performs authentication and returns result to the TOE.

For both mechanisms, multiple authentication methods such as password, biometric authentication, token, certificates, etc. could be implemented. The ST author shall specify methods in chapter 6.2.14 FIA_UAU.5. The methods performed by a remote entity is out of scope of the TOE, yet the communication between the TOE and the remote entity shall be secured by trusted channel.

For local authentication, methods based on cryptographic mechanism shall be implemented conform to a public reference standard, or to the SOG-IS recommendations [SOGIS]. And methods based on other mechanisms (e.g. password or biometric) shall meet a defined quality metric.

1.2.3.2 Cryptographic support

The TOE implements symmetric, asymmetric and hash-based cryptographic mechanisms for authentication, as well as for confidentiality and integrity protection. These cryptographic mechanisms could be implemented by HW, FW or hybrid cryptographic module, and shall conform to public reference standard, or to the SOG-IS recommendations [SOGIS].

Many cryptographic functionalities require the presence of random numbers with an appropriate entropy quality to prevent introducing vulnerabilities in cryptographic functions. For this, the TOE implements an RNG which is required to provide the random numbers with specified entropy quality whenever necessary.

The entropy source could be gathered from either inside or outside of the TOE, and the recommended entropy quality of the output random numbers shall be meet at least PTG.2, or DRG.3, or a higher quality metrics of [BSI-3].

The generated cryptographic key lengths as outcome of the key generation procedures - consuming the random numbers - should follow the protocol requirements.

1.2.3.3 Audit of events

The TOE provides audit function including audit log generation, reviewing audit logs, protecting audit logs storage and restricting access to audit logs.

1.2.3.4 Security management

The TOE provides management mechanism for security functionalities including management of:

1. User accounts and their attributes if applicable
2. Authentication failure policy
3. Security audit
4. TOE system time or the NTP configuration
5. Change default value(s) of credential(s) at first login
6. Restore default settings

1.2.3.5 TOE access control

The TOE provides user access session control functions including:

- Idle session management: the TOE terminates session which user is inactive for a period of time.
- Consecutive authentication failure process: for a given number of consecutive authentication failure within a period of time, the TOE locks the user for a specified period.
- Security banner: the TOE provides warning banner to a user at login.

1.2.3.6 Trusted communication

The TOE provides trusted communication with security protocols to secure any communication with external entities, including TOE user and all interacting devices deployed in the management network, such as Syslog, LDAP, or similar server types.

A recommendation of appropriate protocols implementing trusted communication is given in [BSI-1] and [SOGIS].

1.2.3.7 HW supported secure booting

The TOE provides secure booting function based on HW RoT (root of trust), which act as a trusted anchor to verify the FW package before executing it.

1.2.4 The Logical Scope of FWU PP-module

The FWU PP-module is a FW functionality, it provides following security feature:

1.2.4.1 HW supported secure FW updating

The TOE provides secure FW updating function by validating the FWU package based on HW RoT prior executing it. Only the FW stored in NVM can be updated, while the initial FW stored in ROM can't be updated.

1.2.5 The non-TOE Components

1. **All HW hosting and connected to the TOE components**
    - The service plane HW
    - Other GS components hosting the service plane
2. **All SW operated by the service plane**
    - Service plane OS
    - Service plane application SW

1.2.6 The TOE Lifecycle

The TOE underlies a device typical lifecycle, whereas the following discussion identifies certain aspects which have been considered and placed as requirements in this PP. A formal lifecycle description is not required for this TOE, this chapter has therefore an informational character.

The TOE lifecycle is built from following phases which can be seen as a sequence in lifetime:

Development and Production

During production of the server, the TOE is set into a default configuration. This default configuration shall ensure that no deliberately or inadvertently configuration setting can jeopardise the basic server operation at the time the server is set into its first operation. In addition, this secure default configuration protects the TOE also during the supply chain processes after production and prior delivery.

Especially, if parts of third parties are integrated the lifecycle model shall comprise the aspects of acceptance procedure and integration into the configuration management system and plan.
With respect to possible developer internal TOE part transports the lifecycle model shall cover also the aspects of internal transportation.

Delivery

While the TOE is subject of treatment in the supply chain, it is assumed that the TOE is protected from theft, physical tampering with, re-configuring, and any modification of its parts including its FW, for example by unauthorised user accesses.

The delivery procedure intents to ensure that each TOE product of the supply chain is delivered in the correct configuration to exactly the customer who ordered it and provides the description to achieve the acceptance of a delivered TOE by the correctly assigned recipient.

Start-Up

After powering up, the TOE HW provides the self-tested operational environment and delivers the initial credentials from the HW RoT. Those are prerequisites for the authenticity and integrity verification of the TOE FW packages loaded from immutable and mutable memories of the TOE.

During this loading procedure there shall be no other active connection from the TOE to the host, as this could endanger the TOE booting operation. This is considered in corresponding SFRs of chapter 6.

Also, the TOE is the very initial part of the GS being operative, and during the start-up sequence all host interfaces to the outside world shall be disabled.

First operation

When the TOE has reached its operational state the first time with the evaluated default setting, the administrator sets - as initial first step - new credentials for authentication and/or authorization. This, only once occurring step ensures a clear separation of responsibilities between the user on one hand, and the developer respectively manufacturer on the other hand. From that point in time onwards the

developer shall not be able to access the TOE without permission and support by the user.
Then the initial configuration by the user can continue, for example with the generation of other user accounts and other TOE and related server settings.

Normal operation

The TOE has conducted successfully secure booting and has proven that all TSF work correctly. The host provides the trusted management services to the GS environment.

Additional TOE life cycle for the FW PP-module

Depending on the use case and risk assessment it can be required to maintain the TOE on an up-to-date status of protection capabilities and functionality. Only in rare cases, for example closed isle-solution where the TOE is rather not exposed to any risk of adverse users, TOEs may come without update functionality. In most cases the following holds true:

During the lifetime it can occur that the TOE requires an update for several reasons.
Those could be a

- functional enhancement to meet new market needs,
- a correction of discovered faulty behaviour under previously unknown conditions,
- but also, security critical updates for the case new vulnerabilities have been discovered.

The TOE could support these updates by including protected FWUs or upgrade possibilities. Such FW renewal shall be conducted only by the appropriate administrator user - after successful authentication and authorization. The TOE TSF of the FWU PP-module ensures also that no erroneous and no obsolete, former FW version is loaded.

When the update or upgrade is successfully completed that TOE continues either with the phase first operation or normal operation.

Decommissioning

The TOE should consider also the state of decommissioning, reselling of whenever the TOE needs to leave the protecting operational environment. If the authorised user has decided that the TOE is to be finally set out of operation, the TOE FW should provide according functionality and/or guidance to set the TOE into a state where an adverse user cannot retrieve any harmful information. For example, such - also recommended - functionality could be the restoring of the initial setting as it was at the point in time of delivery. This restoring of defaults shall include also the deletion of any user stored secrets and credentials, or, at least procedures with similar effects are included and detailed in the user guidance of the TOE.
These means are required, as the TOE is not protected against invasive attacks. Therefore, attacks such as physically readout of memory contents could jeopardise user networks even the device is offline and off power. Or, it happens an undesired reactivation or even abuse of the TOE product in case it is resold or shipped for scrapping to an electronic recycling or disposal company.

2 Conformance Claims

2.1 Conformance claim to CC

This Base-PP and the FWU PP-module are conformant with the Common Criteria (CC) Version 3.1 in Revision 5 for CC part 1 [CCP1] and CC part 3 [CPP3].
No extended assurance components have been defined.

The Base-PP is extended to CC part 2 [CCP2] with following extensions:

- SFR FPT_FPV.1 Firmware Package Validation
- SFR FPT_HWROT.1 Root of Trust Based on HW
- SFR FPT_ROTSB.1 Root of Trust Secure Booting HW support
- SFR FCS_RNG.1 Random Number Generation

The optional FWU PP-module extends CC part 2 [CCP2] as follows, and reuses selected extensions from the Base-PP. and defines additional extensions:

- SFR FPT_FWU.1 FW Update – HW support

Neither the Base-PP nor the FWU PP-module claim conformance to another PP.

The CC evaluation methodology [CEM] applies completely as well as the evaluator action elements given in this PP.

2.2 PP claims

The Base-PP with the optional FWU PP-module allows to select one of the following combinations:

1. Base-PP only
2. Base-PP and FWU PP-module

PP configuration, Base-PP and the FWU PP-module require **strict** conformance of the ST or PP claiming conformance to the Base-PP, and if used, to the selected PP-module.

2.3 Consistency Rationale for the FWU PP-module

The FWU PP-module can only be used together with the Base-PP, as it completes the Base-PP with the protected updates functionality for the TOE FW. Consequently, if a firmware update mechanism is present and provided by the TOE, the FWU PP-module ensures that a comprehensive package, consisting of a defined list of SFRs as given in chapter 6.3, shall be fulfilled to protect the FW update. The defined package of SFRs provides the correct and protected conduct of the FW update process.

Many of the authentication, authorization, integrity, and confidentiality requirements are already covered by the Base-PP, but FPT_FWU.1 is necessary to conduct a secure update with the TOE hardware support and implementing a version control.

The FW update process and how the TOE protection is maintained, is detailed in chapter 6.3.

The FWU PP-module provides an additional threat, forms an objective, and adds a policy, an assumption and an objective for the environment.

This add-on, and the according provisions from the Base-PP do not conflict or contradict to the Base-PP, but the FWU PP-module forms an optional complementation to the Base-PP.

The FWU-PP depends on the provisions of the Base-PP and cannot be combined with any other PP.

2.4 Assurance Level Claim

The minimum assurance level claim of the TOE using the Base-PP is:

EAL2 augmented with ALC_FLR.1

This conformance claim applies for the Base-PP and also for the optional combination with the FWU PP-module.

3 Security Problem Definition

3.1 Asset Definitions

3.1.1 Base-PP

The assets in the TOE that need to be protected are classified into the following types:

- TOE’s FW
- Any data stored, processed or generated
- TSF data
  - audit records
  - account information with administrator and user credentials
  - ephemeral keys and random values used for the trusted communication
  - configuration data of the TOE
- TSF protected operation.
  Thereby it is meant that TOE services offered to the GS are available in correct and protected manner.
- Random numbers

3.1.2 FWU PP-module

If the TOE implements a FW update mechanism which adds the following asset requiring according protection:

- Remote data:
  Any data and/or code stored outside the TOE and deemed to be uploaded to the TOE.

3.2 Threats

3.2.1 Base-PP

The assets for the Base-PP of this TOE type are threatened by following threat agents:

Table 1 Threats against the Assets of the Base-PP

Threat	Asset	Exploit result
T.Unauthenticated An adverse user connected and authenticated successfully from outside to the server.	TSF data	• The adverse user can access the TOE functions and is thus enabled to read, tamper or even destruct the TOE or sever configuration settings and/or audit logs. This comprises also attacks on the local management network interface, its servers and the connection to the central management server of the cloud or data centre. • The destruction of audit logs could make it even undetectable for the administrator that an unauthenticated access was conducted. • If the TSF data are not deleted after decommissioning or reselling of the TOE, the attacker can physically retrieve those and abuse the TSF data at other user devices being active. • If the developer default password and/or other default credentials present after delivery are not immediately changed by the authorised user, the developer and attacker knowing the default values could access the TOE without knowledge of the user and abuse the TOE.
T.Unauthorised An adverse user could authorise and achieves then the rights of the administrator role.	TSF data	• The administrator could in the worse completely abuse the TOE with administrator rights. Such scenario would comprise also attacks local management network interface, its servers and the connection to the central management server of the cloud or data centre. • This includes also adversely reconfiguration of the TOE; for example, grant access to further attackers and/or abuse the entire server for eavesdropping, tampering of TOE, host, common user

		data, construct DoS/DDoS, of other servers, or similar network-based scenarios in a larger attack scenario.
T.Intercept An adverse user able to intercept the communication between TOE, administrator, or servers on the local management network. This comprises also the machine-to-machine connection to the central management server of the cloud or data centre.	TSF data	• The adverse user can reuse TSF data for replay or tampering of the before eavesdropped security relevant information interchanged between the entities, in order to gain access and the role of an authorised administrator. • Tampered TSF data could lead to adversely reconfiguration of the TOE. This could include for example granting access to further attackers and/or abuse the entire server in a larger attack scenario.
T.AccessData An adverse user able to access, read or tamper any data stored, communicated and operated by the TOE.	Data	• Disclosed, deleted, or tampered data could lead to uncontrollable damage and loss of availability. • Eavesdropped credentials can lead to unauthenticated and unauthorised access and exploits of TOE functionalities.
T.FaultyFW A loss of FW integrity caused by natural, other physical, or induced errors during internal loading procedures of the FW.	TOE’s FW TSF-protected operation	• The induction of errors into the FW by other physical, e.g. voltage glitches, or nature, e.g. radiation events, can lead to loss of FW integrity, faulty behaviour, vulnerabilities and unavailability of service. The danger of fault induction by physical reasons is mainly given during initial FW loading, i.e. at booting time and when FW parts are loaded from the TOE’s NVM on the bus. • Another threat appears if the FW would be loaded and executed without authenticity and integrity check. Here, the loading from a memory module inside the TOE is in focus. A fault during conduct could lead to loading and execution of maliciously formed FW packages, where an attacker could exploit resulting erroneous behaviour, take over control of the TOE in the worse, or achieve full stop of operation and services. All of that can harm the TOE operation and could lead to full stop of operation and services.

T.BadRandomNumbers	Random numbers	This threat applies in case of a bad or not operating RNG. This RNG shortcoming can occur due to environmental conditions outside the specified limits, any other physical event disturbing the RNG and HW failure. Physical attacks are excluded from this threat due to the protected operational environment. • All that can lead to an RNG output of none, trivial numbers such as constants, repetition of previously generated random numbers, or illicit formed random values with biased entropy statistics. If those bad numbers are used by the TSF or the TSF protection, the entire TOE and its services, most cryptography but also communication protection, are in danger to fail or being compromised. • Also, since random numbers can be and usually are in use as input for cryptographic key generation and derivation procedures, their compromise would compromise also the resulting key or enable for later cryptographic analysis. A compromised key implements a long-lasting threat. All of the above could enable an attacker to remove the confidentiality protection of stored and transmitted data, to attack the TSF directly, and to exchange or manipulate data or FW/SW packages on the TOE. All that can lead to the compromise and loss of all other TOE assets as well.

3.2.2 FWU PP-module

This threat is generated only if the TOE implements a FW update mechanism.

Table 2 Threats against the Assets of the FWU PP-module

Threat	Asset	Exploit result
T.FaultyFWU	Remote data	• This threat is generated in cases where the FW would be loaded and executed without authenticity and integrity check or version validation. Loading refers here to a remotely conducted FW package update. An induced fault during conduct could lead to loading and execution of maliciously formed FW packages where an attacker could exploit resulting vulnerabilities, take over control of the TOE in the worse, or achieve full stop of operation and services. • This threat is generated when an attacker is able to observe and tamper the remote communication of the TOE FWU mechanism. This could lead to abuse of the update mechanism by exchange or compromising of the FW package with a malicious code package, or the attacker is able to manipulate the FWU mechanism in a way exceeding the desired FWU mechanism, so that other code is overwritten. • Or the threat is given, if an obsolete FW package, in worse coming with publicly known vulnerabilities, is presented for download and updated. All of that can harm the TOE operation and could lead to full stop of operation and services.

3.3 Organizational Security Policies

3.3.1 OSP for the Base-PP

Following policies are assumed to be effectively implemented or in place reducing the related threats to the assets:

3.3.1.1 Policy P.ChangeForced

At the point in time the TOE is produced the TOE can be equipped with a default set of initial authentication credentials. These credentials are deemed to protect the TOE and therewith the GS during delivery and storage.

For this reason, the cryptographic quality of these credentials matters and in consequence, if the developer generates these default credentials outside the TOE, and imports them during the production phase, the developer should use appropriate equipment, for example a HW Security Module (HSM).

In addition, the developer is required to protect the default credentials from tampering and disclosure as long the legitimate user has not changed the default credentials into his individually defined credentials.

The TOE shall force the first administrator operating initially the TOE the first time to change the default into user individual credentials.

This provides a separation of responsibilities and preserves that even if developer´s premises would have been compromised or an inside attacker disclosing initial credentials was discovered, the operated TOE remains authentication protected.

3.3.2 OSP for the FWU PP-module

3.3.2.1 Policy P.Ctrl_FWU

The user organization should deploy an organizational policy to keep all operated BMC FW packages up to date with the latest FW package release.

The policy should include the procedure to come to an update decision, the testing of the FW update, the user roles and other rules of the conduct.
The policy should also stipulate rules to maintain the data protection of the FW packages handled and should ensure that only by the user organization authorised and trained personnel operates the update following the user guidance of the TOE.

3.4 Assumption for the Base-PP

The following assumptions are defined in order that the TOE can meet the targeted EAL:

3.4.1 A.PhysicalProtection

- The TOE and its host as well as the GS are protected against physical access from unauthorised users and attackers.
- The servers Sys Log, NTP and LDAP or similar servers on the local management network are part of the equal physical protection means in the equally protected environment as used for the GS hosting the TOE.
- RMTs, PCs or other ICT devices operated by the authorised users and connected to the local management network run in a comparable physical protected environment.

3.4.2 A.ManagementNetwork

- All instances on the local management network, especially the servers Sys Log, NTP and LDAP or similar, in the physical protected environment operate correctly and their services are available anytime.

Specifically, this assumption holds true for the local management network interfaces and the connection to the central management server of the cloud or data centre.

3.4.3 A.InternalConnections

- The host internal connections on bus and network level between TOE and host, respectively between the management plane and the service plane, are available and work correctly.

3.4.4 A.NetworkSegregation

- The local management network, carrying the management traffic of administrators and connected servers, and the general data traffic of the common users are segregated within the physically protected environment.
- The traffic segregation into different networks is immediately and automatically conducted as soon traffic from administrators has been detected.

3.4.5 A.TrustedPersonnel

- It is assumed, that personnel working as authorised administrators have been carefully selected for trustworthiness and trained for proper use of the TOE. These administrative users shall be technical competent, act thoroughly, do not act deliberately in a jeopardizing way, obey and maintain instructions provided by the TOE documentation.
- As this TOE defines a management platform with which a GS is operated and maintained, administrator users are assumed to connect and use the TOE in short time frames or even on a regular basis. It is assumed that administrators are required to maintain:
  - that the objectives for the operational environment, see chapter 4.3 are fulfilled
  - check for the availability of security relevant SW, FW updates or patches, and
  - conduct such check either on regular basis or immediately in case of vulnerabilities as soon such update is provided

3.4.6 A.RNG-Seed

Regardless of the random seed source, the following is assumed to be available for the TOE’s RNG:

- Random seed of sufficient entropy quality is present whenever requested by the RNG.
- The random seed is neither disclosed to any, nor gets reused by any other component outside the TOE.
- Random numbers as output from the RNG are neither biased nor manipulated in any way.

Application Note

The quality and confidentiality of random numbers is crucial for the TOE TSF. The seed is the essential fundament for the random number generation. Therefore, the ST writer should clarify whether the random seed is part of TOE’s RNG or received from the host. In the latter case, the ST writer must confirm that the entropy source is conducted in an appropriately protected environment. As an example, the environment could be conformant to the requirements given by the MSSR catalogue, [MSSR].

End of application note.

3.5 Assumption for the FWU PP-module

The FWU PP-module does not add an assumption to those from Base PP.

Application Note

Since no assumption are added, it is of specific importance that the OSP P.Ctrl_FWU is fulfilled by the user organization. The ST writer should provide a statement on this.

End of application note.

4 Security Objectives for the TOE

4.1 Security Objectives for the Base-PP

With respect to threats and assets, following objectives are required that the TOE meets the targeted EAL.

4.1.1 O.Authentication

The TOE shall identify and authenticate TOE user before any action. And the TOE shall provide multiple authentication mechanisms including:

- Local authentication: the TOE performs user authentication by itself.
- Remote authentication: the TOE forward user authentication request to a remote entity which performs centralized authentication service based on standard protocols such as LDAP, Kerberos, etc. It is the remote entity performs authentication and returns result to the TOE.

For both mechanisms, multiple authentication methods such as password, biometric authentication, token, certificates, etc. could be implemented. The ST author shall specify methods in chapter 6.2.14 FIA_UAU.5. The methods performed by a remote entity is out of scope of the TOE, yet the communication between the TOE and the remote entity shall be secured by trusted channel.

For local authentication, methods based on cryptographic mechanism shall be implemented conform to a public reference standard, or to the SOG-IS recommendations [SOGIS]. And methods based on other mechanisms (e.g. password or biometric) shall meet a defined quality metric.

4.1.2 O.Authorization

The TOE shall perform a role-based authorization mechanism which assigns to each role a dedicated predefined set of accessible and executable functions. Functions outside the assigned set shall not be accessible.

For this PP role definition, the administrator role has full access to all TOE functionalities. Deviations in form of establishing an administrator hierarchy are allowed.

4.1.3 O.FWValidation

The TOE shall validate both authenticity and integrity of FW packages taken from mutable memories before executing them. The authenticity validation must ensure that the FW packages are issued by an authenticated manufacturer and the integrity validation ensures that the FW packages are not tampered or modified illegally.

4.1.4 O.Communication

The TOE shall secure communications between the TOE and external entities including user and other external devices deployed in the management network. The security communication protocols shall conform to [SOGIS], [BSI-1], or a public standard.

The TOE shall control user access session by:

- Idle session management: the TOE terminates session which user is inactive for a period of time.
- Consecutive authentication failure process: for a given number of consecutive authentication failure within a period of time, the TOE locks the user for a specified period.
- Security banner: the TOE provides warning banner to a user at login.

4.1.5 O.Audit

The TOE shall generate logs from security related events. Only authorized user is able to configure the audit function or review the audit log. The TOE shall protect audit log storage from loss.

4.1.6 O.SecurityManagement

The TOE shall provide authenticated and authorised user with security management respectively security configuration functions. The basic management function including management of:

- User accounts and their attributes if applicable
- Authentication failure policy
- Security audit
- TOE system time or the NTP configuration
- Change default value(s) of credential(s) at first login
- Restore default settings

4.1.7 O.LifeCycle

The TOE shall support following lifecycle aspects:

1. Set into operation:

At the point in time the TOE is produced a set of default credentials protects the TOE from false identification, authentication and authorization. This set of default credentials protects the TOE during delivery, storage and during the installation phases, until the first legitimated administrator sets the TOE into operation and configures the TOE.

Since the default credentials can be generated by the developer environment the developer is in charge for their generation, storage and import. This is out of the scope of this TOE.

But, at the point in time of the first TOE configuration, the responsibility for the protected handling of the default credentials is removed from the developer and put to the legitimate administrator. This is an important step in the lifecycle, as the TOE is from that point on accessible by the legitimate administrator and the manufacturer access without administrator’s permission is removed. Aside from this lifecycle aspect, the operation to change the default credentials, is a security management function and therefore it is assigned to O.SecurityManagement.

The TOE must provide means that the first user, setting the TOE into operation after delivery, is required to login with developer default credentials, but then to change those into user defined credentials. This change marks the point in time, where the legal responsibility for the credential´s ownership is moved from the manufacturer to the user. This is a security management functionality.

The administrator is from that point in time on in responsibility for all possible harm caused by disclosed credentials.

2. Decommissioning:

At the point in time the administrator conducts decommissioning of the TOE, or the TOE is subject of reselling, or the TOE is moved outside the protected operational environment for other reason, the TOE should first either be physical securely destructed by the owner, or the host, or, second, the TOE provides functionality to securely delete all user defined credentials and put it back in the original delivery condition with its default credentials.
In the first case, the user guidance should obligate the user and provide some guidance so that a decommissioned TOE cannot be reactivated and abused. For the second case, the related functionality has been implemented as function and the restoration of the original default settings comprise the deletion of all user defined credentials.
In both cases there should be information given in the operational user guidance.

4.1.8 O.GoodEntropy

- The statistical entropy quality of the random numbers remains in sound conditions and fulfils the stated entropy quality requirements throughout the specified operational conditions and ranges.
- Whenever, random numbers are generated while being within the specified operational conditions and range the statistical entropy remains unbiased.
- The random numbers are considered having sufficient entropy quality, if the requirements of PTG.2 or DRG.3 as defined in [BSI-3], or of an alternative comparable standardised and public metric are met. Other quality metrics with comparable statistical requirements are accepted as well.

4.2 Security Objectives for the FWU PP-module

4.2.1 O.FWUValidation

Each loaded FW package shall be validated prior execution. The validation comprises the correctness of the version, and its authenticity and integrity verification.
This combination, in either sequence, ensures that no manipulated FW package and no outdated FW package (version control) can be executed.

4.2.2 O.Ctrl_FWU

If the TOE provides update functionality, then the FWU mechanism shall only be conducted over a trusted communication channel with an authenticated and authorised user, respectively communication entity.
This can also include a trusted non-human user connected on the local management network. On top of the given trusted path, when using the FWU mechanism, the FWU mechanism shall support data authentication, confidentiality and integrity protection of the transmitted user data, as well as its validation and logging of the event.

The trusted channel shall protect the data in transmission from manipulation and disclosure.

4.3 Security Objectives for the Operational Environment (OE)

4.3.1 OEs for the Base-PP

Following security objectives shall be met by the operational environment in order to assure the required protection for the correct operation of the TOE:

4.3.1.1 OE.ExclusiveProtHost

As the host, respectively the GS’s service plane, usually conducts other services and interfaces with other components out of scope of the TOE, it is essential to define that no other management functionality or application shall be operated on the host´s management plane, as long the TOE conducts its administration and management operation. A possible other server management instance could lead to interference and conflicts with the TOE and unpredictable behaviour of the service plane if management operations from different management instances are conducted at the same time.
This results in following objectives:

- As long the TOE conducts booting and any management operation on the host, no other application or SW shall by default be able to interact, to interfere, to inject other code, or conduct administrative or other management functions on the GS's management plane respectively the TOE.

- The TOE host, the GS's service plane and its operational environment provides physical protection of the management traffic on the local management network, as well as physical and logical segregation from common user traffic inside the server, i.e. separation of management from service plane.
- The booting integrity verification sequence shall be an offline, autonomous and inside-only procedure of the TOE without involving external services, except the option for reception of random numbers from the host. If the TOE implements an RNG from the list, given in chapter 1.2.2, the TOE operates entirely autonomous.

4.3.1.2 OE.CorrectHost

- The host respectively the GS's service plane is out of control of the TOE and for this reason it is essential that the host provides its functionalities in the correct way which include the essential provisions of power, possibly clock frequencies and other essential physical interfaces.
- During operation the TOE host, respectively the GS's service plane, does in no way jeopardise the correct operation of the TOE, meaning interfere the correct TOE operation.
- The host respectively the GS's service plane interacting with the TOE shall be available and work correctly as specified.
- The host respectively the GS's service plane provides isolation from any external connection for the time the TOE conducts the booting. This is given at each powering-up or after a reset of the host.

4.3.1.3 OE.PhysicalProtection

- The TOE and its host as well as its local peripherals are protected against physical access from unauthorised users and attackers.
- The servers Sys Log, NTP and LDAP or similar servers on the local management network are part of the equal physical protection means in the same environment as used for the GS hosting the TOE.
- As the central management server of the cloud or data centre operates also on the local management network, the equal physical protection means in the same, or comparable equal or even better protecting environment as used for the GS must be given.
- The local and remote locations of the RMTs, PCs or other ICT devices used by administrators are at least physically protected on a comparable level as the GS location hosting the TOE.

4.3.1.4 OE.ManagementNetwork

All instances on the local management network, especially the servers Sys Log, NTP and LDAP or similar servers, in the physical protected environment operate correctly and their services are available for the TOE anytime requested.

This comprises also the availability of the non-human-initiated connection to the central management server of the cloud or data centre.

Aside of the availability of the non-human-initiated connection to the central management server of the cloud or data centre, it is essential that the operational policy of the central management server does not conduct any management operation conflicting with the management operation of the TOE.

Such seamless and non-conflicting operational policy is out of scope of the TOE and belongs to the administrator of the cloud or data centre.

4.3.1.5 OE.NetworkSegregation

- The operational environment provides a segregation of traffic coming from remote administrators on one hand and from other common user traffic on the other hand.
- The operational environment provides a segregation of traffic coming from the non-human-initiated communication of the central management server of the cloud or data centre. However, this central administration traffic shall use the same local management network bearing the human administrator traffic.
- The segregation shall be implemented as soon the traffic's data type can be assigned. Administrator user traffic are routed via the local management network to the TOE.

4.3.1.6 OE.TrustedPersonnel

Personnel working as authorised administrators shall be carefully selected for trustworthiness and trained for correct use of the TOE. Administrators shall be technical competent, act thoroughly, do not interact deliberately in a jeopardizing way with the host and the TOE, and obey and maintain instructions provided by the TOE documentation.

4.3.1.7 OE.CredentialProtection

It occurs at the point in time the TOE is produced that default, initial or other secret keys and other credential data are generated by the operational environment. If those are then imported into the host deemed for the use by the TOE' TSF, the following shall apply for the operational environment:

- Appropriate cryptographic methods respectively generation devices are applied
- and/or, if provided with the user guidance, the user is obligated to conduct the secret generation conformant to the user guidance, and
- these external generated data are either securely destroyed after import to the TOE or
- kept access controlled, integrity and confidentiality protected at all times the TOE is not finally decommissioned.

The equal objectives apply when the first administration user, respectively the device owner or, in other words, the customer overwrites the default credentials with customer individual credentials. This preserves also the final legal domain separation between developer and user. From that point on the developer cannot be made reliable if the user generated credentials become disclosed, or are trivial values, or have characteristics enabling for being abused in other ways.

Application Note:

The developer may follow the NCCA or CB endorsed recommendations as given [SOGIS] and [BSI-1]. If appropriate, the user guidance should be extended with examples and/or references to public documents, standards including the CB-endorsed.

The notification in the user guidance is important to separate the responsibility for the credentials, secrets between the TOE developer and TOE user.

End of the application note.

4.3.1.8 OE.AuditStorage

The TOE is required to fulfil the objective O.Audit and provides procedures for the logging of security events and the backup of the audit log-file.

The host and/or the operational environment shall preserve sufficient integrity protected memory space and the capability for unlimited backup of the log-files on the Sys Log server connected on the management network.

The treatment of log-files on the Sys Log server should be part of an organization policy which is outside the TOE. In any case the TOE shall be able to conduct the backup of log-files without limitation in size and intervals, or backup-blocking by unavailability by the environment.

The Sys Log server shall be available all time.

4.3.1.9 OE.RNG-Services

The random seed generation is crucial for the entropy quality of the random numbers as the RNG itself. Consequently, the environment where the seed is generated and the RNG is operated shall ensure that:

- The seed generation is operated in an environment which can be trusted from TOE perspective. If the random seed is part of the TOE’s RNG then this is proven in itself.
- The random seed is neither disclosed to any, nor gets reused, biased or manipulated in other ways by any other component outside the TOE.
- The random seed comes with appropriate entropy quality.
- The random seed shall be available all times the TOE requires its availability.

Application Note

The quality and confidentiality of random numbers is crucial for the TOE TSF. The seed is the essential fundament for the random number generation. Therefore, if the entropy source is operated outside the TOE, the ST writer should confirm by a statement that the entropy source is conducted in an appropriately protected environment. As an example, the environment could be conformant to the requirements given by the MSSR catalogue, [MSSR].

End of application note.

4.3.2 OEs for the FWU PP-module

4.3.2.1 OE.FWU_Usage

If the TOE provides update functionality it is essential that, when accessing the TOE, the authorised user at his premises shall support the trusted communication channel. The channel is protected by means of authentication and confidentiality requiring interaction with the user.

Additionally, and if the TOE operates an FWU mechanism, administrator users have means in place to either receive developer notifications or check regularly check at developer provided sources or receive information in other ways upon developer provided TOE FWU packages.

The administrator user is capable to decide in responsible manner whether an FWU package needs to be installed and conducts the required action.

4.4 Security Objectives Rationale for the Base-PP

Table 3 Security Objective Rational for the Base-PP

Threats, Assumptions, Policies	Objectives	Rationale
T.Unauthenticated	O.Authentication O.Communication O.SecurityManagement O.Audit O.Lifecycle	O.Authentication The threat of uncontrolled users accessing the TOE functionality is countered by the requirement to implement at least one of the recommended authentication methods. The authentication is also in place for any operational status when a user tries accessing the TOE and this holds true for the entire lifecycle. Thus, this threat is countered anytime. O.Communication The application of one of the protocols, conformant to either a public referenced standard, or to the SOG-IS recommendations [SOGIS], ensures that communication between TOE and a remote entity is only established after successful identification and authentication of each entity. By that it is not practical that attacker can capture such protected communication channel. O.SecurityManagement The security management defines the threshold of allowed failed access attempts and provides an appropriate reaction policy if the threshold is achieved or exceeded. This preserves that attackers cannot brute force or conduct unlimited analysis of authentication credentials. The TOE forces the user to change the default password and/or other developer default credentials after initial powerup to achieve a separation between developer and user. Else, the developer or attackers knowing the default values could access the TOE without knowledge of the user. O.Audit

Threats, Assumptions, Policies	Objectives	Rationale
		Any login and failed login attempt are documented in the log. This enables administrators to identify misbehaviour of users and tracing back attack attempts to the root cause or individual account. Such audit logs enable administrators to take appropriate action and defence against adverse users. O.LifeCycle The TOE shall protect itself from being tampered or modified even during delivery, storage and installation phases of its hosts. For that reason, the TOE provides initial protection with a secure deemed default configuration including set of default credentials requiring identification, authentication and authorization even at the first time the TOE is set into operation. The initial change of default credentials at first set into operation is an important step in the lifecycle, but its conduct is a security management function and thus it is an assigned matter of O.SecurityManagement. Even after decommissioning the TOE shall not provide the condition for being reactivated and abused. This is prevented with functionality to wipe all user credentials securely and put it into the original delivery conditions with respect to default credentials and default configuration.

Threats, Assumptions, Policies	**Objectives**	**Rationale**
T.Unauthorised	O.Authorization O.SecurityManagement O.Audit	O.Authorization Unauthorised execution of functionalities is rendered not practical as each authenticated user has assigned a dedicated role which is equipped with defined set of functionalities accessible and executable. Functions outside the defined set are not accessible as those belong to a different user role. Thus, only authorised functions can be executed. O.SecurityManagement Administrators define and configure with the security management the allowed functionality for each user role. As an option the security management can require another authentication step prior the set of functions is made accessible. The presence of a dedicated security management protects against adverse role extension or privilege level elevation, and prevents from the use of not allowed functions for an identified role. O.Audit Administrative actions are logged with sufficient detailed information and enable by that to trace back to malicious events and identify adverse users. The audit process shall ensure that even no administrator can tamper or delete the log file.

Threats, Assumptions, Policies	Objectives	Rationale
T.Intercept	O.Communication O.SecurityManagement	O.Communication The threat of interception is countered by using protocols conformant to either a public referenced standard, or to the SOG-IS recommendations [SOGIS]. Such a protocol preserves that it is not practical for an attacker to exploit identification and authentication of the entities establishing a secured communication, even the attacker eavesdrops or tampers the communication. O.SecurityManagement The administrator configures with the security management the communication with remote users that only the appropriate secure protocols with predefined entities having the correct credentials can be established. The security management prevents the establishment of communication channels using inappropriate protocols for administrator management tasks.

Threats, Assumptions, Policies	**Objectives**	**Rationale**
T.AccessData	O.Communication O.SecurityManagement	O.Communication The use of a protocol, conformant to either a public referenced standard, or to the SOG-IS recommendations [SOGIS], preserves that data transferred via this protocol is authenticated as well as integrity and confidentiality protected. Even deletion of data during transfer can be detected. As data content of administrator´s management traffic can contain user and personal data, the protection of those from disclosure is crucial in technical sense but also for following the GDPR. O.SecurityManagement The administrator configures with the security management the communication with remote users. This configuration comprises that only the appropriate protocol, conformant to either a public referenced standard, or to the SOG-IS recommendations [SOGIS] with integrity and confidentiality protection are applied. The security management prevents the establishment of communication channels using vulnerable and cryptographic weak protocols for administrator management tasks.
T.FaultyFW	O.FWValidation	O.FWValidation The authenticity and integrity of each FW package loaded from a mutable memory shall be verified after loading but before execution. This prevents from undefined TOE behaviour by the undetected induction of faults during the booting sequence.

Threats, Assumptions, Policies	**Objectives**	**Rationale**
T.BadRandomNumbers	O.GoodEntropy	O.GoodEntropy The TSFs rely on the availability of random numbers of the specified quality. The RNG is in charge to provide those anytime and as long the specified operational conditions for the integrated RNG are met. This objective provides the presence of random numbers as specified and ensures that the TSF conduct protection and results are based on random numbers of appropriate entropy quality.
A.PhysicalProtection	OE.PhysicalProtection	The host and the TOE, both do not claim protection against direct physical attacks. For that reason, it is essential to operate both in a protected environment, to sward physical tampering, penetration and abuse of the TOE (and host). In addition, the physical protection of remote connected administrators is covered as well, as these working places could be abused to attack TOE and host. The objective OE.PhysicalProtection meets the assumption A.PhysicalProtection.
A.ManagementNetwork	OE.ManagementNetwork	The justification of A.ManagementNetwork is that the TOE acts as a distant client and cannot verify the correctness of operation of the connected servers on the management network. However, dedicated security functionality with respect to audit, time synchronization, time stamps and authentication relies on the correct operation of the servers on the management network. For that reason, the means of OE.ManagementNetwork shall cover the aspects of the assumption A.ManagementNetwork.

Threats, Assumptions, Policies	**Objectives**	**Rationale**
A.InternalConnections	OE.ExclusiveProtHost	As the TOE is operated in a host operating other applications, an interfering, eavesdropping or abuse of internal communication inside the host cannot be detected by the TOE. For that reason, the assumption is justified that the host is exclusively operated for the TOE only as long the booting takes place until the TOE has achieved its correct full functionality, and during the times the TOE conducts the desired management operation on the host. And, it is also required that the host provides segregation from other user traffic and protection of the communication between TOE and host as long the TOE executes its management functions for the host. Both is covered with OE.ExclusiveProtHost and the assumption A.InternalConnections is met by this.
A.NetworkSegregation	OE.NetworkSegregation	As soon administrator management traffic enters the operational environment the traffic is to be separated and protected from other user traffic in order to avoid adverse redirection, analysis of meta-data, DoS/DDoS or similar. For that reason, this kind of traffic is to be protected and separated by the means given in OE.NetworkSegregation. These means meet the assumption A.NetworkSegregation.
A.TrustedPersonnel	OE.TrustedPersonnel	Correct configuration and operation of the TOE is crucial for the trustworthy operation of the host and therewith to the entire general administrated server. For that reason, the users conducting the management functions shall be able to deploy the operations correctly and the users shall not implement vulnerabilities by deliberate or erroneous configurations. The OE.TrustedPersonnel meets the assumption A.TrustedPersonnel.

Threats, Assumptions, Policies	Objectives	Rationale
T.Unauthenticated	OE.CredentialProtection OE.AuditStorage	At the point in time the TOE is produced, the cryptographic means for authentication and authorization are equipped with default credentials. Disclosure of these credentials from developer´s premises or just using trivial values could compromise the TOE and in consequence the entire general administrated server, as an adverse user could access then the administrator role. For this reason, the cryptographic quality of these credentials matters. Thus OE.CredentialProtection contributes in the defence against T.Unauthenticated. In the event of unauthenticated access, for example with tampering, adverse modification or even destruction of the host and therewith destruction also of the host-stored log-file, it would be essential to exploit the backup of log-file. For that reason, the operational environment provides always sufficient and integrity protected memory space to conduct these backups. Thus, the environmental objective OE.AuditStorage and the OE.CredentialProtection, both together contribute to the protection against T.Unauthenticated.
P.ChangeForced	OE.CredentialProtection	At the point in time the TOE is produced, the cryptographic means for authentication and authorization could be equipped with default credentials. These credentials are deemed to protect the TOE and therewith the GS during storage and delivery. For this reason, the cryptographic quality of these credentials matters. In addition, the legitimate administrator user shall ensure that also no remotely connected adverse user from developer´s personnel having knowledge of and abusing the default credentials can compromise the general administrated server. The first administrator user shall either be forced or obligated by the user guidance to import self-created credentials to replace the developer default credentials. In all cases, the cryptographic quality of these credentials matters. OE.CredentialProtection takes care of these requirements and fulfils P.ChangeForced.

Threats, Assumptions, Policies	**Objectives**	**Rationale**
A.RNG-Seed	OE.RNG-Services	The TOE operation requires in any case the anytime availability of random numbers in good quality and uncompromised condition. The random seed is input to this operation and shall be available on request of the RNG. Regardless, where the random seed is generated, inside or outside the TOE, it must come from a trusted environment. OE.RNG-Services takes care of this and meets the assumption A.RNG-Services.

4.5 Security Objectives Rationale for the FWU PP-module

Table 4 Security Objective Rational for the FWU PP-module

Threats, Assumptions, Policies	Objectives	Rationale
T.FaultyFWU	O.FWUValidation O.Ctrl_FWU	O.FWUValidation This objective preserve, that a remotely loaded FW package has been proven for its authenticity and integrity and that the package was subject of a version control check. By that it is ensured that a FW update is only conducted with correct and verified FW package. If this objective would not be fulfilled, an adverse user could be able to update with a vulnerable or even attack optimised FW package. O.Ctrl_FWU FW packages in transmission can be eavesdropped and tampered with as this is out of control of the TOE and exposed to attackers. If this objective would not be fulfilled, an adverse user could be able to intermit, induce other code packages, manipulate contents and similar. For that reason, FW packages in transmission shall be appropriately protected with authentication, authorization, as well as integrity and confidentiality protection. This objective preserves this protection.
A.PhysicalProtection	OE.PhysicalProtection OE.CorrectHost	Since the TOE is not enabled to implement physical protection means against invasive or non-invasive attacks at local premises, the host is required to implement means of the OE.PhysicalProtection to cover this assumption. For the equal reasons, meaning the TOE has not implement checking means to verify the correctness of the host when operating other applications or even the host HW, the OE.CorrectHost must fulfil the assumption A.PhysicalProtection.

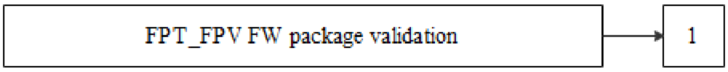
Threats, Assumptions, Policies	**Objectives**	**Rationale**
A.TrustedPersonnel	OE.TrustedPersonnel	In case the TOE provides an FWU mechanism the administrator user shall take care for FWU packages provided by the developer in order to keep the TOE up-to-date with the most recent FWU packages. The operational environment provides the required information and the means to receive TOE FWU packages by the responsible administrator user. The administrator user is also capable to decide in responsible manner upon the conduct of the FWU. The OE.TrustedPersonnel meets the assumption A.TrustedPersonnel.
P.Ctrl_FWU	OE.FWU_Usage	The TOE provides (optional) remote FW update functionality initiated and conducted by an authorised, but distant user. Distant means that the user environment, out of which the update is conducted, is out of control of the TOE. Thus, a working place can be operated by different users, the authenticated and authorised, and the not-authenticated and not-authorised. For that reason, the user environment is required to support the identification, authentication and authorisation means for the trusted communication channel.

5 Extended Components Definitions

5.1 For the Base-PP

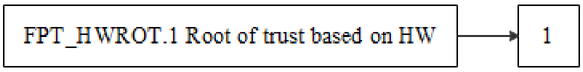
- SFR FPT_FPV.1 Firmware Package Validation
- SFR FPT_HWROT.1 Root of Trust Based on HW
- SFR FPT_ROTSB.1 Root of Trust Secure Booting HW support
- SFR FCS_RNG.1 Random Number Generation

5.1.1 FPT_FPV.1 Firmware Package Validation

Family behaviour:	This family defines the requirements for the authenticity and integrity verification of FW packages by means of digital signature.
Component levelling:	 This family consists of one component.
Hierarchical to:	No other components.
Management:	There are no management activities foreseen.
Dependencies:	FPT_HWROT.1 Root of trust based on HW FCS_COP.1 Cryptographic operation
Audit:	There are no actions defined to be auditable.

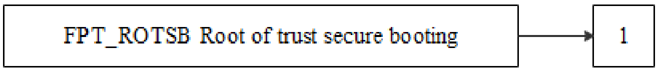
FPT_FPV.1 FW package validation	
FPT_FPV.1.1	The digital signature verification shall be based on following credential data: ***[selection , choose one of:*** • ***public key,*** • ***pubic key taken from a certificate,*** • ***hash value of a public key,*** • ***hash value of a certificate*** ***]*** which have to be retrieved from the HW ROT as defined with FPT_HWROT.1.
FPT_FPV.1.2	The TSF shall conduct following verification to each FW package taken from mutable memories: Verify the digital signature of each FW package with the credential data defined by FPT_FPV.1.1, or, with the public key extracted from a FW package, of which the belonging digital signature was successfully verified before using the credential data as defined with FPT_FPV.1.1 according to the cryptographic operations defined with FCS_COP.1.

5.1.2 FPT_HWROT.1 Root of Trust based on HW

Family behaviour:	This family defines the requirement for the presence of a root of trust implemented as immutable HW based module for hosting certificates, public keys, other credentials and integrity verification reference values as initial credentials.
Component levelling:	 This family consists of one component only.
Hierarchical to:	No other components.
Management:	There are no management activities foreseen.
Dependencies:	This family has no dependencies.
Audit:	There are no actions defined to be auditable.

FPT_HWROT.1 Root of Trust	
FPT_HWROT.1.1	The TSF shall contain an immutable root of trust that contains trusted data [***selection, choose one of: certificate, public key, hash of public key/s, hash of certificates,*** **[assignment: other credential values**]], which are preserved in [***selection:*** • ***a one-time-programmable (OTP) memory,*** • ***a dedicated security component,*** • **[assignment: other HW components**]].

5.1.3 FPT_ROTSB.1 Root of trust secure booting

Family behaviour:	This family defines the requirements for the conduct of booting the TOE so that as a result the TSF operate correctly and the desired TOE services can be provided in the protected way.
Component levelling:	 This family consists of one component.
Hierarchical to:	No other components.
Management:	There are no management activities foreseen.
Dependencies:	FPT_FPV.1 FW package validation FPT_FLS.1 Failure with preservation of secure state
Audit:	There are no actions defined to be auditable.

FPT_ROTSB.1 Root of trust secure booting HW support	
FPT_ROTSB.1.1	The first FW package shall be taken from the immutable TOE memory and shall be executed as initial step of the booting sequence.
FPT_ROTSB.1.2	All other FW packages, i.e. all taken from mutable memories such as the NVM, shall be successfully verified before execution, following the requirements of FPT_FPV.1 Firmware package validation.
FPT_ROTSB.1.3	The booting procedure shall be atomic, **[assignment: other properties if needed]**.

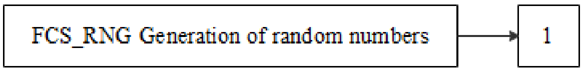
Application Note for ROTSB.1.3:

The meaning of atomic is that the whole booting procedure shall be either completely performed in one step without any break or interrupt, or the booting shall be considered as a fail.

The ST author should assign a list of other relevant properties (non-interruptible, autonomous, exclusive ways) for the booting procedure. The assignment may comprise also “none”.

End of the application note.

5.1.4 FCS_RNG Random Number Generation

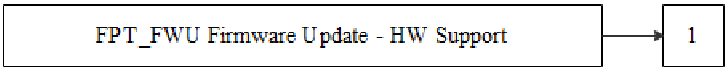
Family behavior:	This family defines quality requirements for the generation of random numbers which are intended to be used for cryptographic purposes.
Component leveling:	 This family consists of one component.
Hierarchical to:	No other components.
Management:	There are no management activities foreseen.
Dependencies:	This family has no dependencies.
Audit:	There are no actions defined to be auditable.

FCS_RNG.1 Random Number Generation	
FCS_RNG.1.1	The TSF shall provide a ***[selection: physical, non-physical true, deterministic, hybrid physical, hybrid deterministic]*** random number generator that implements: **[assignment: list of security capabilities]**.
FCS_RNG.1.2	The TSF shall provide ***[selection: bits, octets of bits, numbers [assignment: format of the numbers]]*** that meet **[assignment: a defined quality metric]**.

5.2 For the FWU-PP module

The FWU PP-module defines only one new SFR.

5.2.1 FPT_FWU.1 FW Update – HW Support

Family behaviour:	This family defines the requirements for secure firmware update based on hardware RoT.
Component levelling:	 This family consists of one component.
Management:	There are no management activities foreseen.
Dependencies	FPT_FPV.1 Firmware package validation FPT_RCV.3 Automated recovery without undue loss FMT_SMF.1 Specification of management functions
Audit:	The update of the TOE FW requires to enter the new update data generated by the its conduct following the definition of: • SFR FAU_GEN.1 Audit Data Generation

FPT_FWU.1 – FW Update – HW support	
FPT_FWU.1.1	The TOE FW update procedure comprises following: • The TSF shall check the version validity of FWU packages by [**assignment: mechanism to verify validity of FWU version]** to prevent updating to a revoked version. • The TSF shall verify the FW update package following the requirements defined in FPT_FPV.1 Firmware package validation and **[assignment: none, other checking]** prior to the execution of the package.
FPT_FWU.1.2	The FW update procedure shall be atomic.

Application note for FPT_FWU.1.2

The meaning of atomic is that the whole FW update procedure shall be either completely performed in one step without any break or interrupt, or the FW update shall be considered as a fail.

End of application note.

6 Security Functional Requirements

6.1 Notation conventions

Following conventions apply for the Security Functional Requirement claims:

- ~~Strikethrough~~ indicates text replaced with alternative text as a refinement.
- [Underlined text in brackets] indicates additional text provided as a refinement.
- If not being the headline of the SFR itself, **bold** text indicates the completion of an assignment.
- ***Italicised and bold*** text indicates the completion of a selection.
- Iteration/Identifier indicates an element of the iteration, whereas the identifier distinguishes the different iterations.
- Normal text applies unchanged from the SFR definition in [CCP2]

New defined SFRs are discussed in chapter 5.

6.2 Security Functional Requirements for the Base-PP

The subchapters are sorted in alphabetical order and not according their priority.

6.2.1 FAU_GEN.1 Audit Data Generation

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: a) Start-up and shutdown of the audit functions; b) All auditable events for the ***minimum*** level of audit; and c) following auditable events: 1. **User login and logout** 2. **Power on, power off and restart of the TOE** 3. **Operate system management functions as defined in FMT_SMF.1 Specification of management functions** 4. **[assignment: other specifically defined auditable events.]**
FAU_GEN.1.2	The TSF shall record within each audit record at least the following information: a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **[assignment: other audit information]**

Application Note:

With respect to FAU_GEN.1.1:
The TOE may implement the audit functions in a way that those are active instantly after start-up and remain active all time, without management function to activate or inactivate them. By this way the audit functions cannot be bypassed and thus the presence of audit functions constitutes no auditable event. Otherwise, the recording of start-up and shutdown of audit functions shall be applicable.

End of the application note.

6.2.2 FAU_GEN.2 User Identity Association

FAU_GEN.2 User Identity Association	
FAU_GEN.2.1	For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused the event.

6.2.3 FAU_SAR.1 Audit review

FAU_SAR.1 Audit Review	
FAU_SAR.1.1	The TSF shall provide **administrators, and [assignment: other role defined by FMT_SMR.1]** with the capability to read **entirely all information** from the audit records.
FAU_SAR.1.2	The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.2.4 FAU_SAR.2 Restricted Audit Review

FAU_SAR.2 Restricted audit review	
FAU_SAR.2.1	The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.2.5 FAU_STG.1 Protected Audit Trail Storage

FAU_STG.1 Protected Audit Trail Storage	
FAU_STG.1.1	The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.
FAU_STG.1.2	The TSF shall be able to ***prevent*** unauthorised modifications to the stored audit records in the audit trail.

Application Note:

The selection “prevent” relies on the fulfilment of the assumption of A.TrustedPersonnel and the objective for the environment OE.TrustedPersonnel and OE.PhysicalProtection, as the audit records underlie a backup procedure which means storage outside the GS. This backup place of audit records and logging file is out of scope of the TOE.

End of the application note.

6.2.6 FAU_STG.3 Action in Case of Possible Audit Data Loss

FAU_STG.3 Action in Case of Possible Audit Data Loss	
FAU_STG.3.1	The TSF shall **overwrite the oldest stored audit records,** if the audit trail exceeds **the maximum size of the log files**.

Application Note:

The audit trail is recorded into the log file present in the mutable memory of the TOE. The developer shall confirm that the size of the log file, the backup intervals and the storage location for the backup outside the TOE are subject of administrator settings.

End of the application note.

6.2.7 FCS_CKM.1 Cryptographic key generation

FCS_CKM.1 Cryptographic key generation	
FCS_CKM.1.1	The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm **[assignment: cryptographic key generation algorithm]** and specified cryptographic key sizes **[assignment: cryptographic key sizes]** that meet the following: **[assignment: list of standards]**.

Application Note:

It is recommended that the developer follows the recommendations as given in [SOGIS] and/or [BSI-1], since these cryptographic mechanisms are publicly discussed and well understood with respect to their cryptographic or mathematic characteristics.

If the developer decides to choose one or more proprietary cryptographic mechanisms, then the cryptographic or mathematic characteristics shall be additional part of the security evaluation. However, implementation of proprietary cryptography is not recommended, instead the developer should follow either a public referenced standard, or the recommendations of [SOGIS].

End of the application note.

6.2.8 FCS_CKM.4 Cryptographic key destruction

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: cryptographic key destruction method]** that meets the following: **[assignment: list of standards]**.

Application Note:

The key destruction methods shall be applied to all ephemeral keys generated and used for the secured protocols and communication. The equal methods shall be applied once the TOE-FW achieves a decommission status. This ensures that also a decommissioned GS cannot be reactivated and abused.

End of application note.

6.2.9 FCS_COP.1 Cryptographic operation

FCS_COP.1 Cryptographic Operation	
FCS_COP.1.1	The TSF shall perform **[assignment: list of cryptographic operations]** 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:

- The ST writer is reminded to extent the FCS_COP.1 SFR with an iteration to define the individually chosen cryptographic algorithm. The method of iteration allows the definition of several cryptographic algorithms associated with the security objectives. If only one cryptographic algorithm is added in the Security Target, the iteration identifier is not required.
- The ST writer shall provide the cryptographic operations, algorithms and key lengths used for:
  - Verifying the authenticity and integrity of the FW packages using the HW ROT
  - Integrity verification of public keys and certificates using the HW ROT
  - Protecting the integrity and confidentiality of data stored and in transmission
- The cryptographic operations shall comprise symmetric, asymmetric, authentication and integrity protection mechanism respectively algorithms. All implemented algorithms with its key lengths should have a remaining acceptable lifetime which should correspond with the expected lifetime of the general administrated server.
- It is strongly recommended that the developer follows the recommendations as given in [SOGIS] and/or [BSI-1], since these cryptographic mechanisms are publicly discussed and well understood with respect to their cryptographic or mathematic characteristics.
- If the developer decides to choose one or more proprietary cryptographic mechanisms, then the cryptographic or mathematic characteristics shall be additional part of the security evaluation. However, implementation of proprietary cryptography is not recommended instead the developer should follow either a public referenced standard, or the recommendations of [SOGIS].

End of the application note.

6.2.10 FCS_RNG.1 Random number generation

For this TOE the random seed used as input to the RNG of the TOE can come either from TOE internal source or is provided by the host. In both cases the RNGs must provide its output with the appropriate entropy quality. The trustworthiness on the seed if coming from the host is covered by A.RNG-Seed and OE.RNG-Services.

FCS_RNG.1 Random Number Generation	
FCS_RNG.1.1	The TSF shall provide a ***[selection: physical, non-physical true, deterministic, hybrid physical, hybrid deterministic]*** random number generator that implements: **[assignment: list of security capabilities]**.
FCS_RNG.1.2	The TSF shall provide ***[selection: bits, octets of bits, numbers [assignment: format of the numbers]]*** that meet **[assignment: a defined quality metric]**.

Application Note:

The ST author is required to clarify the origin of the entropy source providing the seed. Specifically, if the seed source is integrated part of the RNG or provided from external.
If the seed is generated outside the TOE, the ST writer must confirm that the TOE receives a seed that meets the specified quality metric.

The application note 10, as given in [PP0084] applies:
A physical random number generator (RNG) produces the random number by a noise source based on physical random processes. A non-physical true RNG uses a noise source based on non-physical random processes like human interaction (key strokes, mouse movement). A deterministic RNG uses an random seed to produce a pseudorandom output. A hybrid RNG combines the principles of physical and deterministic RNGs where a hybrid physical RNG produces at least the amount of entropy the RNG output may contain and the internal state of a hybrid deterministic RNG output contains fresh entropy but less than the output of RNG may contain.

End of application note.

6.2.11 FIA_AFL.1 Authentication Failure Handling

FIA_AFL.1 Authentication Failure Handling	
FIA_AFL.1.1	The TSF shall detect when ***an administrator configurable positive integer within*** **[assignment: range of acceptable values]** unsuccessful authentication attempts occur related to **[assignment: list of authentication events]**.
FIA_AFL.1.2	When the defined number of unsuccessful authentication attempts has been ***[selection: met, surpassed]***, the TSF shall **[assignment: list of actions]**.

6.2.12 FIA_SOS.1 Verification of secrets

FIA_SOS.1 Verification of secrets	
FIA_SOS.1.1	The TSF shall provide a mechanism to verify that secrets meet [**assignment: a defined quality metric**]

6.2.13 FIA_UAU.2 User authentication before any action

FIA_UAU.2 User authentication before any action	
FIA_UAU.2.1	The TSF shall require each user being successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

Application note:

For the case that a symmetric authentication scheme based on password methods is used, the evaluator is specifically required to evaluate the means to ensure an appropriate password characteristic. The evaluator is required to verify the implementation against its specification and conduct a vulnerability assessment.

Since the term user comprises human and non-human users, the evaluation shall specifically evaluate and confirm that the authentication and authorization measures, applied for the non-human user connected on the local management network, are appropriate. This comprises evaluation of the means on the TOE and a documentation with confirmation of the local management network operator with respect to the connected server.

End of application note.

6.2.14 FIA_UAU.5 Multiple authentication mechanisms

FIA_UAU.5 Multiple authentication mechanisms	
FIA_UAU.5.1	The TSF shall provide • local authentication: the TOE shall perform authentication autonomously based on **[assignment: authentication mechanisms]** • remote authentication: the TOE shall forward an authentication request to a remote entity based on **[assignment: authentication mechanism]** to support user authentication.
FIA_UAU.5.2	The TSF shall authenticate any user's claimed identity according to the **[assignment: rules describing how the multiple authentication mechanisms provide authentication]**.

6.2.15 FIA_UAU.7 Protected authentication feedback

FIA_UAU.7 Protected authentication feedback	
FIA_UAU.7.1	The TSF shall provide only **non-information-disclosing signs** to the user while the authentication is in progress.

Application Note:

Example for non-information disclosing signs output to the user are signs "•, *, -" or similar.

For the case the user is a server, the authentication feedback does not leak any information about the used credential. In that case, the non-information-disclosing signs are pass or fail information for the server.

End of the application note.

6.2.16 FIA_UID.2 User identification before any action

FIA_UID.2 User identification before any action	
FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

Application Note:

An enabled user can be identified by the credentials he has including user name and password, if no token-based method is applied.

For the case that a symmetric authentication scheme based on password methods is used, the evaluator is specifically required to evaluate the means to ensure an appropriate password characteristic. The evaluator is required to verify the implementation against its specification and conduct a vulnerability assessment.

End of application note.

6.2.17 FMT_MOF.1 Management of Security Functions Behaviour

FMT_MOF.1 Management of Security Functions Behaviour	
FMT_MOF.1.1	The TSF shall restrict the ability to ***[selection: determine the behaviour of, disable, enable and modify the behaviour of]*** the functions **defined in FMT_SMF.1** to **[assignment: the authorised role defined in FMT_SMR.1].**

Application Note:

Any user identified receives a role and scope assignment which constitutes the authentication. User roles are used to control the set of commands that can be executed, and scopes are used to control the set of operating objects.

A command execution on the behaviour of the security functions shall only be possible if the user role matches the permission for the specific command. And, an operating object shall only be accessed, if the object resources are within the permitted user scope.

The correct configuration of user roles and scopes depend on the identification, authentication and authorization mechanism is crucial for FMT_MOF.1.

End of the application note.

6.2.18 FMT_SMF.1 Specification of management functions

FMT_SMF.1 Specification of management functions	
FMT_SMF.1.1	The TSF shall be capable of performing the following management functions: **Management of the:** **1. user accounts and their attributes if applicable** **2. authentication failure policy** **3. security audit** **4. TOE system time or the NTP configuration** **5. change default value(s) of credential(s) at first login** **6. restore default settings** **7. *[selection: none, session policy, [assignment: other management functions]]***

Application Note:

Security audit: This addresses the recording and logging of events.

Session policy: Established sessions with inactive users must be terminated in order to avoid abuse of the session, for example by another user accessing the working place of the initial user.
It includes also setting the threshold of consecutive access attempts.

Default settings: This means restoration of the settings as it was at delivery point in time. That includes removal of stored user secrets and credentials. Typical cases would be TOE decommissioning, reselling or generally, moving the TOE out of the protected environment.

End of application note.

6.2.19 FMT_SMR.1 Security roles

<table>
<tr><th colspan="2">FMT_SMR.1 Security Roles</th></tr>
<tr><td>FMT_SMR.1.1</td><td>The TSF shall maintain the roles
<table>
<tr><th>Role name</th><th>Privileges</th></tr>
<tr><td><b>Administrator</b></td><td><b>The accounts of this group are used for security management and are authorised to perform all functions defined by FMT_SMF.1.</b></td></tr>
<tr><td><b>[Assignment: Other roles]</b></td><td><b>[Assigned privileges of the other roles]</b></td></tr>
</table></td></tr>
<tr><td>FMR_SMR1.2</td><td>The TSF shall be able to associate users with roles.</td></tr>
</table>

Application Note:

The Base-PP defines the administrator role only, but it is up to the developer to add and define further user roles and assign their privileges. However, added role definitions shall not conflict with each other and the here fined administrator role.

End of the application note.

6.2.20 FPT_FLS.1 Failure with preservation of secure state

FPT_FLS.1 Failure with preservation of secure state	
FPT_FLS.1.1	The TSF shall preserve a secure state when the following types of failures occur: • **FW package failure** • **non-availability of the cryptographic coprocessor or other HW shortcomings,** • **[assignment: list of types of failures in the TSF].**

Application Note:

The FW package failure can basically be an authenticity or integrity error, and can be a version control mismatch, if a FW update mechanism is implemented.

End of the application note.

6.2.21 FPT_FPV.1 Firmware package validation

FPT_FPV.1 FW package validation	
FPT_FPV.1.1	The digital signature verification shall be based on following credential data: ***[selection , choose one of:*** • ***public key,*** • ***pubic key taken from a certificate,*** • ***hash value of a public key,*** • ***hash value of a certificate*** ***]*** which have to be retrieved from the HW ROT as defined with FPT_HWROT.1.
FPT_FPV.1.2	The TSF shall conduct following verification to each FW package taken from mutable memories: Verify the digital signature of each FW package with the credential data defined by FPT_FPV.1.1, or, with the public key extracted from a FW package, of which the belonging digital signature was successfully verified before using the credential data as defined with FPT_FPV.1.1 according to the cryptographic operations defined with FCS_COP.1.

6.2.22 FPT_HWROT.1 Root of Trust based on HW

FPT_HWROT.1 Root of Trust	
FPT_HWROT.1.1	The TSF shall contain an immutable root of trust that contains trusted data [***selection, choose one of: certificate, public key, hash of public key/s, hash of certificates,*** **[assignment: other credential values**]], which are preserved in [***selection:*** • ***a one-time-programmable (OTP) memory,*** • ***a dedicated security component,*** • **[assignment: other HW components**]].

6.2.23 FPT_RCV.3 Automated recovery without undue loss

FPT_RCV.3 Automated recovery without undue loss	
FPT_RCV.3.1	When automated recovery from **[assignment: list of failures or service discontinuations as specified in FPT_FLS.1]** is not possible, the TSF shall enter a maintenance mode where the ability to return to a secure state is provided.
FPT_RCV.3.2	For **[assignment: list of failures or service discontinuations as specified in FPT_FLS.1]** the TSF shall ensure the return of the TOE to a secure state using automated procedures.
FPT_RCV.3.3	The functions provided by the TSF to recover from failure or service discontinuity shall ensure that the secure initial state is restored without exceeding [**assignment: quantification**] for loss of TSF data or objects under the control of the TSF.
FPT_RCV.3.4	The TSF shall provide the capability to determine the objects that were or were not capable of being recovered.

Application Note:

The FW package failure can have different sources, an authenticity or integrity error and a version control mismatch. The version control is typically deployed, if a FW update mechanism is implemented.

End of the application note.

6.2.24 FPT_ROTSB.1 Root of Trust secure booting HW support

FPT_ROTSB.1 Root of trust secure booting HW support	
FPT_ROTSB.1.1	The first FW package shall be taken from the immutable TOE memory and shall be executed as initial step of the booting sequence.
FPT_ROTSB.1.2	All other FW packages, i.e. all taken from mutable memories such as the NVM, shall be successfully verified before execution, following the requirements of FPT_FPV.1 Firmware package validation.
FPT_ROTSB.1.3	The booting procedure shall be atomic, **[assignment: other properties if needed]**.

Application Note:

The meaning of atomic is that the whole booting procedure shall be either completely performed in one step without any break or interrupt, or the booting shall be considered as a fail.

The ST author should assign a list of other relevant properties (non-interruptible, autonomous, exclusive ways) for the booting procedure. The assignment may comprise also “none”.

End of the application note.

6.2.25 FPT_STM.1 Reliable time stamps

Reliable time stamps are essential for the TOE TSF including for example also the entries of auditable events into the log file following the SFR audit requirements.

FPT_STM.1 Reliable time stamps	
FPT_STM.1.1	The TSF shall be able to provide reliable time stamps.

Application Note:

Following the OE.ManagementNetwork the TOE should retrieve its time stamp or synchronization information from the NTP server connected to the local management network.

End of application note.

6.2.26 FPT_TST.1 TSF testing

FPT_TST.1 TSF testing	
FPT_TST.1.1	The TSF shall run a suite of self-tests ***[selection:*** ***during initial start-up,*** ***periodically during normal operation,*** ***at the conditions [assignment: conditions under which self-test should occur]*** ***]*** to demonstrate the correct operation of ***[selection: [assignment: parts of TSF], the TSF].***
FPT_TST.1.2	The TSF shall provide authorised users with the capability to verify the integrity of ***no data***.
FPT_TST.1.3	The TSF shall provide authorised users with the capability to verify the integrity of ***none***.

Application Note

FPT_TST 1.1 specifies when the TSF will perform the self-test but does not allow user triggered TSF testing (“***at the request of the authorised user”*** is not in the selection list as original FPT_TST). Therefore, FPT_TST_1.2 and 1.3 are assigned with “no data” and “none” to express that TSF does not provide any TSF (or part of TSF) integrity verification capability to authorized users [CPP2, annex J.14].

End of application note.

End of application note.

6.2.27 FTA_SSL.3 TSF-initiated termination

FTA_SSL.3 TSF-initiated termination	
FTA_SSL.3.1	The TSF shall terminate an interactive session after a **time interval of user inactivity.**

Application Note:

If a session is inactive for a defined time frame the TSF shall terminate the session automatically. This is because there could in the worse be a capturing of the inactive connection by an adverse user on the remote side which is out control of the TOE.
The ST writer should confirm that the TOE is delivered with an appropriate default configuration than can be modified by the administrator. This holds for GUI sessions with human user as well as for any other server session operated.

End of the application note.

6.2.28 FTA_TAB.1 Default TOE access banners

FTA_TAB.1 Default TOE access banners	
FTA_TAB.1.1	Before establishing a user session, the TSF shall display an advisory warning message regarding unauthorised use of the TOE.

6.2.29 FTA_TSE.1 TOE session establishment

FTA_TSE.1 TOE session establishment	
FTA_TSE.1.1	The TSF shall be able to deny session establishment based on • **Authentication failure** • **User is already disabled or locked**

6.2.30 FTP_ITC.1 Inter-TSF trusted channel

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 or disclosure.
FTP_ITC.1.2	The TSF shall permit ***[selection: the TSF, another trusted IT product*]** to initiate communication via the trusted channel.
FTP_ITC.1.3	The TSF shall initiate communication via the trusted channel for **[assignment: list of functions for which a trusted channel is required].**

6.2.31 FTP_TRP.1 Trusted path

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 and replay***.
FTP_TRP.1.2	The TSF shall permit ***remote users following FMT_SMR.1*** to initiate communication via the trusted path.
FTP_TRP.1.3	The TSF shall require the use of the trusted path for ***[selection: initial user authentication, [assignment: other services for which trusted path is required]].***

Application Note:

The ST writer should specifically confirm that the TOE operates appropriate public recommended protocols for communication with remote users as these users manage and administrate the general application server. And, that the common user is not enabled to establish a trusted path to the TOE.

End of the application note.

6.3 Security Functional Requirements for the FWU PP-module

For the case, the FWU PP-module has been claimed, the following forms the required SFR package definition.

It is fact that analysis methods and attack technologies evolve over the time. However, it depends on the individual use case and recommended risk assessment, whether the TOE requires update functionality to maintain the level of resistance against attackers.
For example, the TOE could also be operated in closed isle-network never exposed to higher risk.

For that reason, the FWU PP-module is made optional.

Application Note:

It is essential for the ST writer to clarify and confirm the use case scenario and feasibly also the environment, whether a TOE requires update functionality or not. It is to be noted that a once-for-ever BMC solution can implement a high risk for immediate vulnerability exploitation, if there is any future risk that the TOE use case and its environment could change. Therefore, the ST writer shall make clear and confirm that it is a dedicated decision not to apply update mechanisms.

End of the application note.

The optional FW update mechanism is a function of the TOE FW which is supported by HW means.

This update functionality shall only be accessible, after a trusted and cryptographic protected session, between the TOE and the user, has been established. Using such protected communication path and due to its operation in secure environments only, one focus of the evaluation of the FW update is on verification and confirmation of the fulfilment of previously defined SFRs of the Base-PP, while the other is on the new defined SFRs of the FWU PP-module to protect the conduct of the update procedure.

The following set of SFRs forms a dedicated shall have, completely to be fulfilled, set of SFRs, where it is marked which additional and optional SFRs form the FWU PP-module.
The evaluator shall explicitly confirm the fulfilment of the entire set in context with FW update. This forms a new evaluator action element.

The ST writer is recommended to take the defined set of SFRs as guidance to check whether the fulfilment of the selected Base-PP SFRs is given in any case, also for the conduct of the FW update.

6.3.1 Iterated FMT_SMF.1/ FWU.1 Specification of management functions – update

FMT_SMF.1/ FWU.1 Specification of management functions - update	
FMT_SMF.1/ FWU.1.1	The TSF shall be capable of performing the following management functions: **configuration of the TOE FW Update.**

Application Note

The authentication, authorization and role definitions from the Base-PP apply to this iteration, meaning that only the authorised user as required by FMT_MOF.1 is allowed to configure the FW update of the TOE.

End of application note.

6.3.2 FPT_FWU.1 FW Update – HW support

FPT_FWU.1 – FW Update – HW support	
FPT_FWU.1.1	The TOE FW update procedure comprises following: • The TSF shall check the version validity of FWU packages by [**assignment: mechanism to verify validity of FWU version]** to prevent updating to a revoked version. • The TSF shall verify the FW update package following the requirements defined in FPT_FPV.1 Firmware package validation and **[assignment: none, other checking]** prior to the execution of the package.
FPT_FWU.1.2	The FW update procedure shall be atomic.

Application note for FPT_FWU.1.2

The meaning of atomic is that the whole FW update procedure shall be either completely performed in one step without any break or interrupt, or the FW update shall be considered as a fail.

End of application note.

6.3.3 Overview of the SFR package for the FWU PP-module

The following table maps the SFRs required for the FW update functionality to the fundamental and essential security functionalities. All of them are mandatory.

Table 5 the SFRs and components comprising the SFR package for the FWU PP-module

Authentication	
FIA_UAU.2 User Authentication before any action	Base-PP
FIA_UAU.5 Multiple authentication mechanism	Base-PP
FIA_UAU.7 Protected authentication feedback	Base-PP
FIA_UID.2 User identification before any action	Base-PP
Authorisation	
FMT_SMF.1 Specification of management functions	Base-PP
FMT_MOF.1 Management of security functions behaviour	Base-PP
Protected Communication	
FTP_ITC.1 Inter-TSF trusted channel	Base-PP
FTP_TRP.1 Trusted Path	Base-PP
FTA_SSL.3 TSF initiated termination	Base-PP
Signature verification	
FCS_COP.1 Cryptographic operation	Base-PP
FPT_FPV.1 Firmware package validation	Base-PP
Conduct of FWU operation	
FMT_SMF.1/ FWU.1 Specification of management functions – update	FWU PP-module
FPT_FWU.1 FW-Update – HW support	FWU PP-module
Failure Handling during FWU operation	

FPT_FLS.1 Failure with preservation of secure state	Base-PP
Finalization of the FWU by TSF testing	
FPT_TST.1 TSF testing	Base-PP
Documentation and Logging	
FAU_GEN.1 Audit data generation	Base-PP
FAU_GEN.2 User identity association	Base-PP
FPT_STM.1 Reliable time stamps	Base-PP

7 Security Functional Requirements Rationale

7.1 Objectives and Security Functional Requirements

Following table provides an overview of the assignment of SFRs to the individual objectives in order to cover those. The justification follows after the overview table.

Table 6 The SFR to objectives mapping to the Base-PP and to the FWU-PP

Objectives	SFR
Base-PP	
O.Authentication	FIA_AFL.1; FIA_SOS.1; FIA_UAU.2; FIA_UAU.5; FIA_UAU.7; FIA_UID.2; FMT_SMF.1; FPT_STM.1; FTA_SSL.3; FTA_TAB.1; FTA_TSE.1; FTP_ITC.1; FTP_TRP.1
O.Authorization	FAU_SAR.1; FAU_SAR.2; FAU_STG.1; FIA_SOS.1; FMT_MOF.1; FMT_SMF.1; FMT_SMR.1
O.FWValidation	FCS_COP.1; FPT_FPV.1; FPT_FLS.1; FPT_HWROT.1; FPT_RCV.3; FPT_ROTSB.1; FPT_TST.1; FTP_ITC.1; FTP_TRP.1
O.Communication	FCS_CKM.1; FCS_CKM.4; FCS_COP.1; FTA_SSL.3; FTA_TSE.1; FTP_ITC.1; FTP_TRP.1
O.Audit	FAU_GEN.1; FAU_GEN.2; FAU_SAR.1; FAU_SAR.2; FAU_STG.1; FAU_STG.3; FPT_STM.1
O.SecurityManagement	FMT_MOF.1; FMT_SMF.1; FMT_SMR.1
O.LifeCycle	FMT_SMF.1
O.GoodEntropy	FCS_RNG.1
FWU PP-module	
O.FWUValidation	FPT_FWU.1; FPT_FPV.1; FPT_TST.1
O.Ctrl_FWU	FAU_GEN.1; FAU_GEN.2; FCS_COP.1; FIA_UAU.2; FIA_UAU.5; FIA_UAU.7; FIA_UID.2; FMT_SMF.1; FMT_MOF.1; FMT_SMF.1/FWU.1; FPT_STM.1; FTA_SSL.3; FTP_ITC.1; FTP_TRP.1

7.2 Justification of the SFRs for the Base-PP

7.2.1 Justification for SFRs covering O.Authentication

The user authentication is implemented by the user identification FIA_UID.2 followed by the authentication before any action can be conducted, FIA_UAU.2. The different authentication means for local and remote users is implemented by FIA_UAU.5. The authentication process as such is visualised only by non-information leaking signs as required by FIA_UAU.7 to the human users. If the authentication process yields a fail result, then FIA_AFL.1 provides the appropriate response to the authenticating entity.

The authentication process and results are subject of logging and entries into the log file requires a reliable time stamp which is covered by the SFR FPT_STM.1.

Authenticated, but inactive users shall face an automatic termination of the corresponding communication channel before this would implement an additional threat. The user is by that required to re-login and establish a new protected communication channel. This is covered by FTA_SSL.3. In order to inform a user about an upcoming session, the requirement FTA_TAB.1 ensures that a security banner in sense of an advisory warning message is displayed in the GUI.

Of course, the TOE TSF is enabled to deny session establishments, if the preconditions of the sessions are not met. This session rejection is addressed by FTA_TSE.1.

Remote users accessing and operating on the TOE require a segregated communication path from other traffic on the service plane of the GS, with entity identification and initial user authentication. This provides FTP_ITC.1. The protection of the data from disclosure, modification and replay aside from identification of the end points is implemented by a trusted path, FTP_TRP.1.

Since the authorised user is enabled to operate security management functions including the generation of other user accounts and belonging security credentials, it is essential that these security credentials conform to a certain cryptographic quality. Trivial secrets induce vulnerabilities and attackers could be able to login. For that reason, the TOE must verify the cryptographic quality according to a defined metric. This fulfils FIA_SOS.1.

7.2.2 Justification for the SFRs covering O.Authorisation

After successful identification and authentication, the user receives a defined role and scope which are equipped with a defined set of execution rights. Each user must be authenticated before any action can be triggered which is provided by FIA_UID.2. The user identity and account management is subject of FMT_SMF.1 user management.

Authenticated users conduct management operations according to their assigned roles and operational resources of which the scope is defined by FMT_SMR.1. Also, access to the behaviour and modification of security management functions is based on the assigned role which is defined by FMT_MOF.1.

The TOE implements also logging to enable the authorised user for tracing back to a certain event and in best case to its root cause. As these data can be critical, also in sense of personal data protection regulations, access to these data are restricted to specified and authorised users, AU_SAR.1. However, for event analysis any data can be of importance so all present data must be made available to the authorised user, FAU_SAR.2. It is also important to protect the logging from deletion and modification as it could be an attack target to hide that an attack event took place. This is covered by FAU_STG.1.

Since the authorised user is enabled to operate security management functions including the generation of user credentials related to authentication and authorization, it is essential that these credentials conform to a certain cryptographic quality. Trivial secrets induce vulnerabilities and attackers could be able to login. For that reason, the TOE must verify the cryptographic quality according to a defined metric. This fulfils FIA_SOS.1.

7.2.3 Justification for the SFRs covering O.FWValidation

It is obvious that FW integrity is crucial for the correct operation of the TSF. Manipulated FW can lead to unpredictable and vulnerable TOE behaviour.
The TOE users, especially if remotely connected, send for the TOE operations data of any kind which can be relevant for configuration of the TOE and TSF. If an attacker would be able to read this traffic, or even jump into the session, he could be enabled to identify FW code suitable for modification, exploit the sent data, or even reuse those for replay or induce malicious FW packages or TSF data. This would constitute first step of an attack path. To prevent this the SFR FTP_ITC.1 preserves on one hand a distinct communication channel from other user traffic on the service plane of the GS and ensures that the channel can only be established between identified end points. But, even the data in transmission are protected from modification and disclosure.
Now, as the channel is established it needs to protect the communication data travelling on this channel from modification, disclosure and replay. This is implemented by FTP_TRP.1.

At every booting, FW packages are loaded from dedicated HW components. The anchor of trust is given for this procedure by the RoT based on HW storing the initial certificates respectively public keys and other credentials. These HW RoT based data are required to verify the authenticity and integrity of the FW packages at the booting phase. The SFR FPT_HWROT.1 is therefore required to cover the objective O.FWValidation.

The SFRs FPT_FPV.1 and FPT_ROTSB.1 allow to achieve a confident level of digital signature verification and to ensure the atomicity of the booting procedure.

The authenticity and integrity verification procedures are implemented with the use of specified cryptographic algorithms which justifies FCS_COP.1.

It can for whatever reason occur that a FW package validation fails during its loading when booting the TOE. In this case it is essential that on one hand the faulty FW package is not executed and on the other hand that the TOE achieves a secure state. This cannot be handled by trap and user action, as the TOE is still in the booting phase. For that reason, the SFR FPT_FLS.1 is essential and preserves the TOE in a secure state even in case of FW authenticity or integrity and other failure occurring during the FW loading at booting. The SFRs prevent the TOE operation with a faulty FW package. This covers the objective O.FWValidation.

Nevertheless, even if an FW package failure occurs, the TOE shall have the option to recover from the achieved secure state in defined ways and with authenticity and integrity verification of the loaded FW packages from another TOE internal source. These recovery paths are defined in the SFR FPT_RCV.3. As such recovery can resolve induced temporary authenticity or integrity failures from the first source and provides protected loading from a TOE internal second source, the objective O.FWValidation is met.

During the booting phase, the SFR FPT_TST.1 must be fulfilled. This ensures on one hand that the HW basis for correct integrity validation of the FW packages is working correctly, and on the other hand, that the FW packages itself are tested during runtime. Both types of testing protect the FW integrity from persistent faults in HW and ephemeral, accidental induced faults at runtime, for example voltage glitches or anything similar. This covers the objective O.FWValidation.

7.2.4 Justification for the SFRs covering O.Communication

The TOE users, especially if remotely connected, send for the TOE operations data of any kind which can be relevant for configuration of the TOE and TSF. If an attacker would be able to read this traffic, or even jump into the session, he could be enabled to identify FW code suitable for modification, exploit the sent data, or even reuse those for replay or induce malicious FW packages or TSF data. This would constitute first step of an attack path. To prevent this the SFR FTP_ITC.1 preserves on one hand a distinct communication channel from other user traffic on the service plane of the and ensures that the channel can only be established between identified end points. But, even the data in transmission are protected from modification and disclosure.
Now, as the channel is established it needs to protect the communication data travelling on this channel from modification, disclosure and replay. This is implemented by FTP_TRP.1.

The developer shall select symmetric, asymmetric, authentication and integrity cryptographic mechanisms from endorsed standards which covers then sufficiently FCS_COP.1, FCS_CKM.1 and FCS_CKM.4. This ensures that the cryptography used is publicly discussed and free of mathematical characteristics which could be exploited easily. However, there is never a guarantee for the absence of inherent vulnerabilities, but as long following the recommendation from the CBs, there was none identified during the years of publication and research on it.

Authenticated, but inactive users shall face an automatic termination of the corresponding communication channel before this would implement an additional threat. For example, the authenticated has left the working place without locking it and another person abuses the given communication path. The SFR ensures a configurable termination and in consequence, the user is by that required to establish a new protected communication channel. This is covered by FTA_SSL.3.

Of course, the TOE TSF is enabled to deny session establishments, if the preconditions of the sessions are not met. This session rejection is addressed by FTA_TSE.1.

7.2.5 Justification for the SFRs covering O.Audit

The generation of audit records of defined and configurable events is essential for administration purposes, for example tracing back to a root cause of failure or responsible user.

The information and data at least to be logged is implemented by FAU_GEN.1.

The audit process and log file entries require a reliable time stamp which is covered by the SFR FPT_STM.1 which needs to be combined with the information of user identity association which is covered by FAU_GEN.2. Only a reliable time stamp allows to trace back to the root cause of an event in the sequence of occurrence.

Log file can contain critical data, possibly even personal data such as IP addresses, and therefore, accessing and reading shall only be allowed to the authorised user role having the explicit assigned right to do so. These requirements are defined in FAU_SAR.1 and FAU_SAR.2.

Since malicious modification of the logging constitutes an attack target, as if being successful, it would enable to hide that an attack took place, the logging needs to be protected from deletion and modification. This protection is implemented with FAU_STG.1.

Audit data need to be comprehensive and complete to enable for the analysis of events. Consequently, for the case the audit trail respectively log file exceeds the size of the storage device, the TSF shall begin overwriting the oldest records. This ensures that a time synchronised sequence of most recent events is given any time the log file is read. This fulfils FAU_STG.3.

7.2.6 Justification for the SFRs covering O.SecurityManagement

The TOE specifies security management functions, roles and controls to access the behaviour of the security management functions. The definition and organization of security management function is provided by FMT_SMT.1.
When the set of security management functions is established, it requires a configuration and therewith definition of their behaviour, which is provided by FMT_MOF.1.

It is obvious that the management of the security functions and their configuration requires dedicate permission, which is given by the user role as defined in FMT_SMR.1.

7.2.7 Justification for the SFRs covering O.LifeCycle

There are two lifecycle phases where the treatment of TSF data needs to provide. The first is the initial setting into operation and the second the decommissioning or when the TOE needs to leave the protecting operational environment for other reason, for example reselling.
In the first case, the change of developer default settings into user defined settings implements the separation of legal responsibilities, and protects the TOE also from accesses without knowledge of the user. Especially, if the developer default settings would remain unchanged during operation, then those could allow the developer or an attacker knowing the default settings to remotely access the TOE without user recognition and anytime.

In the second case, the decommissioning, reselling case, or if the TOE leaves the protecting operational environment, it is a necessity that inside TOE stored credentials and secrets of any kind are protected from abuse. The reason is that the TOE is not protected from invasive attacks when leaving the protected environment.

Both, the initial change of default credentials as well as the restoration of the initial default settings, which comes along with the deletion of all user secrets and credentials on the TOE, are defined as mandatory security management functions and covered therewith by FMT_SMF.1.

7.2.8 Justification for the SFRs covering O.GoodEntropy

The presence of random numbers in appropriate quality is essential for the quality of the output of most cryptographic functions. To ensure that the random number statistics can be measured and follows a recommended quality metric, the SFR FCS_RNG.1 has been introduced.

7.3 Justification of the SFRs for the FWU PP-module

7.3.1 Justification for the SFRs covering O.FWUValidation

Validation of each single FW package FW means that its correctness is confirmed and that it is ready for execution. Correctness means on one hand that its authenticity and integrity has been verified and also that the correct FW package version has been loaded. The version control prevents that not an old, possibly vulnerable - but authenticated and integrity verified – version comes to execution.

The SFR FPT_FWU.1 defines that the verification of version control, authenticity and integrity must have been passed successfully, before a FW package can be operated.

While we have a HW ROT as trusted source of reference credentials, providing the offline authentic store for verification credentials, it needs furthermore to be defined how the authentic credentials from there can be used to achieve a confident level of digital signature verification. For that reason, FPT_FPV.1 has been introduced.

Errors which appear during FWU verification or at first execution of a newly installed FWU shall be handled by FPT_FLS.1, in order to avoid leaving the TOE in an undefined failure status.
Even a new FWU loaded from a trusted source could have flaws. As this critical for the TOE and its offered services, it must as far as possible prevented that those flaws jeopardize the TSF of the TOE. For this reason, the TSF needs to be checked before the TOE offers its services to the host. This requires FPT_TST.1.

7.3.2 Justification for the SFRs covering O.Ctrl_FWU

First of all, any FW update modifies the original TOE configuration and as such the conduct and even data must be subject of logging. This is also essential for the case that something went wrong during the update and an authorised user needs to trace back to the root cause. This requires the SFRs FAU_GEN.1 being fulfilled. In this context, it is specifically of interest the get the information about the user identity causing the logging event from the logging. This requires FAU_GEN.2 being fulfilled.

Only identified users shall be allowed to initiate any TSF mediated action. That means that only known users can go the next step and go for authentication and authorization. Unknown users are rejected even before the step of authentication can be achieved. This separates the service plane users from the users able to access the TOE. This is implemented with FIA_UID.2

It is obvious that updating TOE’s FW is a management function and should only be allowed to the authenticated and authorised user. The authentication requires fulfilment of FIA_UAU.2 as there shall be no TSF activity prior the authentication was successful. Since users can be local or remote and the authentication mechanism operated can vary between PW only (recommended for local users only) and multi-factor authentication, for example deploying a one-time-PW sent by SMS, multiple authentication mechanism must be possible, which implements FIA_UAU.5. The authentication mechanisms require the user to enter a PW. During the user input no leaking feedback of the currently input digit shall be given to the user. This is ensured with FIA_UAU.7.

It is essential that an FWU is only possible between two identified and trusted entities, as else an attacker could induce malicious code into the TOE. The source of the FWU must be trustworthy which makes FTP_TRP.1 essential.

If then a trusted path channel is established and all is ready to download FW update packages, it is essential to operate this with the right settings. For this the FW update needs a managed configuration before download, verification and execution can be done. This justifies the iteration of FMT_SMF.1/ FWU.1 as the management function FW update configuration is not present in the Base-PP.

If the trusted path as required with FTP_TRP.1 has been established, and all is ready to download the FW update packages, it is essential to operate this with the right settings. For this the FW update needs a managed configuration before download, verification and execution can be done. This justifies the iteration of FMT_SMF.1/ FWU.1 as the management function FW update configuration is not present in the Base-PP. The management of FMT_SMF.1/ FWU.1, which means configuration of the FWU, must also be limited by the TOE to the desired user role. This follows FMT_MOF.1 and avoids malicious or erroneous tampering of the FWU configuration. But, also the other management function defined with FMT_SMF.1 needs to be correctly fulfilled for the conduct of FWU as the single extension FMT_SMF.1/ FWU.1 does only cover the one specific component of FWU configuration.

FW update packages are relevant for configuration of the TOE and TSF. If an attacker would be able to read this traffic, or even jump into the session, he could be enabled to identify FW code suitable for modification, exploit the sent data, or even reuse those for replay or induce malicious FW packages or TSF data. This would constitute first step of an attack path. To prevent this the SFR FTP_ITC.1 preserves on one hand a distinct communication channel from other user traffic on the service plane of the GS and ensures that the channel can only be established between identified end points. But, even the data in transmission are protected from modification and disclosure. This involves also the SFR FCS_COP.1 to cryptographically protect the communication.

Any via the trusted path successfully received FW package is required to be verified authenticity and integrity verified aside from being version controlled. This verification makes use of cryptographic functions as specified with FCS_COP.1.

An FWU is an important and fundamental change of the TOE compared to its original version. And, for that reason it is important to put this change to the audit records with the reliable time stamp. This is specifically important to trace back to the root cause in case of error. The SFR FPT_STM.1 is required for this reason.

When the FW updated was finalized, it is important that the TOE is able to terminate the session if there is no further communication and the channel is not further used. The termination in appropriate time protects from abusing an inactive session by another entity outside. This protection is implemented with FTA_SSL.3.

7.4 Security Functional Requirements Dependency Rationale

The table below lists the SFRs used in this PP, their dependencies and whether these dependencies are covered by other SFRs in this PP. The subsequent text discusses the remaining cases.

Since the FWU PP-module reuses an SFR selection of the Base-PP the matching dependency discussion of the Base-PP applies also to the optional FWU PP-module.

The additional SFRs for the FWP PP-module are discussed separately in chapter 6.3.

The applicability of an SFR to the Base-PP and to the FWU PP-module, or if an SFR is for the FWU PP-module is marked in following table. In other words, the PP configuration is built of the SFRs assigned to the Base-PP, and, if by the ST writer claimed, with the SFRs added by the FWU PP-module.

Table 7 The SFR dependencies and fulfillment.

SFR	Dependencies as given with [CPP2]	Fulfilment by one or more SFRs
Base-PP		
FAU_GEN.1	FPT_STM.1	Fulfilled by FPT_STM.1
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	Fulfilled by FAU_GEN.1 Fulfilled by FIA_UID.2
FAU_SAR.1	FAU_GEN.1	Fulfilled by FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	Fulfilled by FAU_SAR.1
FAU_STG.1	FAU_GEN.1	Fulfilled by FAU_GEN.1
FAU_STG.3	FAU_STG.1	Fulfilled by FAU_STG.1
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1] FCS_CKM.4	Fulfilled with FCS_COP.1 and FCS_CKM.4.
FCS_CKM.4	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	Fulfilled with FDP_ITC.1 or FCS_CKM.1.

FCS_COP.1	[FDP_ITC.1, or FDP_ITC.2, or FCS_CKM.1] FCS_CKM.4	Fulfilled with FDP_ITC.1, FCS_CKM.1 or FCS_CKM.4.
FCS_RNG.1	None	No dependency
FIA_AFL.1	FIA_UAU.1	Fulfilled by FIA_UAU.2
FIA_SOS.1	None	No dependency.
FIA_UAU.2	FIA_UID.1	Fulfilled by FIA_UAU.2
FIA_UAU.5	None	No dependency
FIA_UAU.7	FIA_UAU.1	Fulfilled by FIA_UAU.2
FMT_MOF.1	FMT_SMR.1 FMT_SMF.1	Fulfilled by FMT_SMR.1 and FMT_SMF.1
FMT_SMF.1	None	No dependency
FMT_SMR.1	FIA_UID.1	Fulfilled by FIA_UAU.2
FPT_FLS.1	None	No dependency
FPT_HWROT.1	None	No dependency
FPT_RCV.3	AGD_OPE.1	Fulfilled by AGD_OPE.1
FPT_ROTSB.1	FPT_FPV.1 FPT_FLS.1.1	Fulfilled by FPT_FPV.1, and FPT_FLS.1
FPT_FPV.1	FPT_HWROT.1, FCS_COP.1	Fulfilled by FPT_HWROT.1, and FCS_COP.1
FPT_STM.1	None	No dependency
FPT_TST.1	None	No dependency
FTA_SSL.3	None	No dependency

FTA_TAB.1	None	No dependency
FTA_TSE.1	None	No dependency
FTP_ITC.1	None	No dependency
FTP_TRP.1	None	No dependency
FWU PP-module		
FMT_SMF.1/ FWU.1	None	No dependency
FPT_FWU.1	FPT_FPV.1 FPT_RCV.3 FMT_SMF.1	Fulfilled by FPT_FPV.1, FPT_RCV.3, FMT_SMF.1/ FWU.1,

8 Security Assurance Requirements

8.1 Security Assurance Requirements Rationale

For CC, the set of security assurance components as defined with [CCP3] shall meet the claims given in chapter 2 and even though define just a bottom line of shall have SARs. This bottom line has been defined based on a risk assessment and threat analysis to the assets in a typical user environment. The definition therefore considers also the setup provided by the operational environment with related assumptions.

Due to this protective setup, the TOE is all in all required to defence against basic and non-invasive attacks only. The main reason is that the TOE is operated in secure environments only which excludes direct physical threats and attacks. On the other hand, this adds crucial requirements and security policies to the operation environment where the TOE is operated.

All [CCP3] defined security assurance requirements shall be fulfilled, whereas the ST writer is free to supplement with additional SARs.

The SARs of the CC targeted assurance level as claimed in chapter 2 apply completely.

8.2 ALC_FLR.1 Basic flaw remediation

The augmentation with ALC_FLR.1 provides a minimal set of requirements ensuring that the developer properly treats flaws reported to him from user side. In consequence, the developer is required to support the user with corrective actions, guidance and not leaving the user alone with the discovered flaw.

ALC_FLR.1 Basic flaw remediation	
Dependencies:	No dependencies
Developer action elements	
ALC_FLR.1.1D	The developer shall document and provide flaw remediation procedures addressed to TOE developers.
Content and presentation elements	
ALC_FLR.1.1C	The flaw remediation procedures documentation shall describe the procedures used to track all reported security flaws in each release of the TOE.
ALC_FLR.1.2C	The flaw remediation procedures shall require that a description of the nature and effect of each security flaw be provided, as well as the status of finding a correction to that flaw.

ALC_FLR.1.3C	The flaw remediation procedures shall require that corrective actions be identified for each of the security flaws.
ALC_FLR.1.4C	The flaw remediation procedures documentation shall describe the methods used to provide flaw information, corrections and guidance on corrective actions to TOE users.

8.3 Dependencies of Assurance Components

The ST writer shall consider the dependencies of the SARs - as defined in [CCP3] and claimed in chapter 2 with the targeted evaluation assurance level - to full extent.

The augmentation with ALC_FLR family-elements do not implement additional dependencies.

9 Glossary and Abbreviations

9.1 Abbreviations

BMC	Baseboard Management Controller, the TOE, also called management plane in many server architectures
CB	Certification Body
CC	Common Criteria
DDoS	Distributed Denial of Service
DoS	Denial of Service
EAL	Evaluation Assurance Level
FW	Firmware
FWU	TOE’s FW Update mechanism
GS	General Server, hosting the TOE
GDPR	General Data Protection Regulation
GUI	Graphical User Interface (usually a browser-based visualization)
HSM	HW Security Module
HW	Hardware
IC	Integrated Circuit
IEC	International Electrotechnical Commission
ITSEF	Information Technology Security Evaluation Facility
Kerberos	Authentication protocol server (name stems from Greek mythology)
LDAP	Lightweight Directory Access Protocol
LPC	Low Pin Count interface

MSSR	Minimum Site Security Requirements
NTP	Network Time Protocol
NVM	Non-Volatile Memory
OS	Operating System
OTP	One-Time-Programmable memory
PCB	Printed Circuit Board
PCIE	Peripheral Component Interconnect Express
PP	Protection Profile
RNG	Random Number Generation
RMT	Remote Management Terminal
SoC	System on Chip
SAR	Security Assurance Requirement
SE	Secure Element
SFR	Security Functional Requirement
SOGIS	Senior Officials Group Information Systems Security
ST	Security Target
SW	Software
TOE	Target Of Evaluation
TSF	TOE Security Functionality

9.2 Glossary

HSM	HW Security Module and in this context an encapsulated, access protected dedicated key generation and management device, operated in production premises.
LDAP	LDAP is a commonly known application protocol used for accessing and maintaining directory information services over an Internet Protocol (IP) network. It is often used in the course of authentication protocols.
MSSR	Minimum Site Security Requirements document provided for download by SOGIS at https://www.sogis.eu/
NTP	The network time protocol is used for a time synchronization of connected network components. This is for example of relevance for the SYS Log
RoT	The Root of Trust, or the so-called trust anchor of the BMC essential for secure booting and updating. The RoT is basically constituted out of the immutable memory, storing the initial credentials and parameters, together with the other protection means of the TOE by HW and SW, deployed for secure booting and updating.
SoC	A SE or security controller implemented on IC level into a bigger IC-level-controller respectively bigger application processor. Both constitute from outside one physical IC.
SYS Log	In order to retrieve the root cause of defined events, for example such as exceeding the threshold of false authentication attempts, it is essential to maintain a log file. The log file is stored and accessed outside the TOE and usually underlies a regular backup stored outside the host.

10 Literature

BSI-1	BSI, Cryptographic Mechanisms: Recommendations and Key Lengths, BSI TR-02102-1, 2020-01 as of 2020-03-24
BSI-3	BSI- AIS 31, A proposal for: Functionality classes for random number generators1, Version 2.0, 18 September 2011
CCP1	Common Criteria for Information Technology, Security Evaluation, Part 1: Introduction and general model April 2017, Version 3.1 Revision 5
CCP2	Common Criteria for Information Technology, Security Evaluation, Part 2: Security functional components April 2017, Version 3.1 Revision 5
CCP3	Common Criteria for Information Technology, Security Evaluation, Part 3: Security assurance components April 2017, Version 3.1 Revision 5
CEM	Common Methodology for Information Technology Security Evaluation, Evaluation Methodology April 2017, Version 3.1 Revision 5
GDPR	General Data Protection Regulation (EU) 2016/679
IEC-1	Security for industrial automation and control systems – Part 4-2: Technical security requirements for IACS components, edition 1.0 as of 2019-02, IEC 62443-4-2
MSSR	Joint Interpretation Library (JIL) Minimum Site Security Requirements, version 3.0 as of February 2020 or newer version
NIST-1	NIST Special Publication 800-193 as of May 2018
PP0084	Security IC Platform Protection Profile with Augmentation Packages Version 1.0; BSI-CC-PP-0084-2014; v1.0, 2014-01-13
SOGIS	SOG-IS Crypto Working Group, SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, version 1.2, January 2020