genuscreen 8.0
Security Target

genua GmbH — Kirchheim

2023-10-10
Version 8.0.10 (7bdd69b)

genua.

Contents

1 ST Introduction

1.1 ST Reference

	ST Reference
ST Title	genuscreen 8.0 Security Target
Version	Version 8.0.10
Developer	genua GmbH
Date	2023-10-10

1.2 TOE Reference

	TOE Reference
TOE Title	genuscreen 8.0
TOE Reference	genuscreen 8.0 software
Product Name	genuscreen 8.0p15 / genucenter 8.0p7

1.3 TOE Overview

This chapter gives an overview about the Target Of Evaluation with it's two components genuscreen and genucenter.

1.3.1 genuscreen and genucenter

The TOE **genuscreen 8.0** makes VPN and firewall functionality available and easy to manage. It consists only of software and documentation. It protects networks at the border to the Internet by filtering incoming and outgoing data traffic. It also protects the data flowing between several protected networks against unauthorised inspection and modification.
One part of the TOE runs on a number (at least 2) of machines (**genuscreen** appliances) that work as network filters and IPsec router. The other part of the TOE runs on the machine to manage the network of genuscreens. This machine, the **genucenter** management system, is a central component. The genuscreens are initialised on a secure network from the genucenter or using an USB install image. The genucenter itself is installed from an USB or optical installation medium. The TOE supports IPv4 and IPv6.
After initialisation, the genuscreens can be distributed to the locations of the networks they are protecting. The **genuscreen** filter incoming and outgoing traffic for multiple networks and can thus enforce a given security policy on the data flow. The filter is implemented in the kernel of the genuscreen's operating system, OpenBSD. The genuscreen can work as bridges or routers. The genuscreens can be used in an optional high availability (HA) setup where the genuscreens synchronise their internal states.
At the same time the genuscreens can provide confidentiality and integrity for data traffic passing between the networks. This Virtual Private Network function is achieved by IPsec encryption and authentication mechanisms using up-to-date ciphers and key sizes. The IPsec transforms are implemented in the kernel. The key agreement for IPsec follows the ISAKMP Internet standard RFC2409 [21] and RFC7296 [23], and is implemented in user space by OpenBSD's `isakmpd` and `iked`.
Optionally, a SIP module can be installed on the genuscreen components in order to integrate a Session Border Controller (SBC).

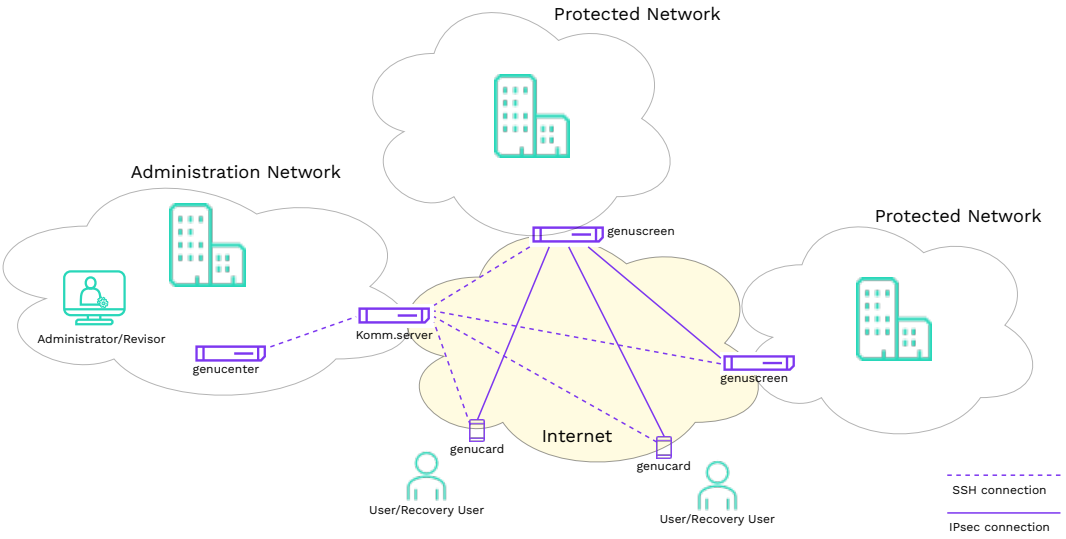


Figure 1: One genucenter managing two genuscreens and two genucards (not part of the TOE). The appliances connect to the genucenter through the communication server.

The genucenter provides administrators with a Graphical User Interface (GUI) to initialise and manage the genuscreens from a central server. The genucenter also allows collecting audit data and monitoring. It can be used to configure other appliances than genuscreen, such as genubox, genucard, genucrypt, or third party products. However, this document only targets genuscreen.
The communication server between the genuscreen appliances and the genucenter management system avoids exposing the genucenter to the Internet.
Figure 1 shows an example setup with two separate VPNs managed by one genucenter. The connection between the genucenter and genuscreen is encrypted with SSH. The VPNs are encrypted by IPsec using IKEv1 or IKEv2.

1.3.2 Alternative: Local Administration

The genuscreen also have a local GUI that can be activated when needed. This case is useful if the appliances can not be reached by the genucenter due to missing (Internet) connectivity. Also, the log files of the genuscreens can be stored locally.

1.3.3 Required non-TOE Hardware/Software/Firmware

The product is based on OpenBSD that runs on a large scale of hardware using different processors.

The following sections list the required non-TOE components of the product.

1.3.3.1 genucenter Management System The following items are required for the genucenter:

- Hardware: Intel i386 compatible CPU with at least two network interfaces, an optional CD ROM, an optional USB interface, and a hard drive as permanent storage for the configuration and log files.

  Currently, the supported hardware variants are genucenter S revision 2, 3 and 4, genucenter M revision 2, 3 and 4, and genucenter L revision 2, 3 and 4.

- Software: OpenBSD Version 6.8, kernel and user space programs, HTTPS server, DHCP server, TFTP server.

1.3.3.2 genuscreen Firewall Components The following items are required for genuscreen:

- Hardware: Intel i386 compatible CPU with at least three network interfaces, an optional USB interface, and a hard drive or CompactFlash card as permanent storage for the configuration and log files. At least one of the network interfaces must support the PXE boot protocol. Currently, the supported hardware variants are genuscreen XS revision 2, genuscreen S revision 2, 3 and 4, genuscreen M revision 2, 3 and 4, genuscreen L revision 2, 3 and 4, genuscreen XL revision 2, 3 and 4.

  The software also runs on the third party hardware cryptOHBguard and *infodas SDoT Server V3B*.

- Software: OpenBSD Version 6.8, kernel and user space programs, HTTPS server.

1.3.3.3 Legacy Hardware and Virtual genucenter The software genuscreen 8.0 runs also runs on legacy hardware revision 1 of genuscreen and genucenter with the same functionality and security measures, but running the software on the legacy hardware has not been evaluated. Also, operating the genucenter software on a virtual machine is out of scope for this certification. If the virtual genucenter is used, the end user has to ensure that all assumptions and objectives on the operational environment are met by the virtual machine.

1.4 TOE Description

The TOE is a distributed stateful packet filter firewall system with VPN capabilities and central configuration. It provides IPv4 and IPv6 support.
The TOE consists of software on a number of machines. The following sections describe the contribution of each part to the total TOE.
Not included in the TOE is the OpenBSD kernel, besides the IPsec and *pf* implementations.

1.4.1 genuscreen Appliances

These genuscreens perform the network filtering and encryption between peers. The network filtering is done either as a bridge or as a packet filter, using the *pf* from OpenBSD.
The encryption between genuscreen peers is done using IPsec. See section 1.4.4 for a description of the possible features.
As good random numbers are a requirement for proper cryptographic operation, the genuscreen checks the quality of the random numbers at start-up and initiates an action if the quality is insufficient.

The genuscreen appliances have a local administrative GUI that must explicitly be activated. This GUI should only be used if a central administration by genucenter is not feasible, e. g. if there is no network connectivity between the two systems. The switch of the administration mode (local or remote) has to be initiated by an administrator. This administrative interface can only be reached through a separate administrative network. The local administrative GUI has only one administrator and one revisor.
The appliances operate in standalone mode either by installing from the genuscreen 8.0 installation CD/USB stick or by enabling the local administrative GUI at the command line.
On startup the genuscreen appliances check the available entropy. If the entropy is not sufficient, they write a log message and disable IPsec VPN functionality, if configured accordingly.
The genuscreen can be operated in an optional high availability mode. If two genuscreens are configured as a high available pair their *pf* states and SA (security association) states are synced by two daemons. Thus a takeover can take place without interrupting connections and VPNs.
The genuscreen has two application layer proxies for FTP and SIP[1]. They are used to open dynamically negotiated ports for the respective protocols. This is done by inserting new rules into the packet filter *pf*, which is considered as the main security mechanism. Therefore this ST does not state SFRs for the proxies. The proxies themselves are not part of the TOE. However, they can be used in a certified configuration, because they have security advantages over the alternative of *a priori* allowing a large port range and do not interfere with the security properties of the TOE.

1.4.2 genucenter Management System

The genucenter is used as a central for all appliances. It allows to configure the appliances, update them and to collect the log data. The genuscreen appliances are installed at the genucenter in a secure way using a dedicated installation network. The administrative GUI allows for a tree-like hierarchical organisation of appliances in nested domains. Each domain has a list of administrators, revisors and service users that are allowed to configure or review the domain and its contained appliances and their audit data. The intermediate role service is allowed to perform maintenance activities i. e. updating applications and collecting log data. They are not allowed to do any configuration. Administration can only happen from a dedicated administrative network.
The genucenter operational administrator is a restricted administrator which cannot change the cryptographic settings. Complementary the genucenter security administrator can only change the cryptographic settings. If not explicitly mentioned, both admin roles are subsumed under the general term genucenter administrators.
The update of the genuscreen appliances is started by the appliances. They contact and authenticate at a communication server. By using particular SSH configurations, the genucenter can then transfer the configuration through SSH tunnels onto the genuscreen appliances. The communication server is a specially configured genuscreen appliance meant to protect the genucenter and is part of the TOE.
As an alternative for appliances without connection to the genucenter, the update can also be performed using a USB stick. The configuration for one or several appliances is stored in an

[1] The SIP proxy should not be confounded with the SIP relay, see section 1.4.7.

encrypted and signed form. Updates are only applied if the signature can be verified when the stick is inserted in a USB connector at the appliance.
Also the log data from the genuscreen appliances is transferred over an SSH channel to the genucenter when they are configured for central storage. The log messages can be viewed and sorted in the GUI inside the respective domain.
The genucenter is installed from the genucenter8.0 installation CD/USB stick. This medium also contains all software to install the genuscreen appliances.
The authentication of administrators and revisors at the genucenter can be configured to use an external LDAP server. This allows to integrate the genucenter management roles in an existing infrastructure. However, the LDAP infrastructure must be secured against attacks. Note that the genucenter root domain administrators cannot be configured for LDAP usage.
The genucenter can also configure other appliances than genuscreen. However, they are not part of the TOE.
The deployment server is used for a decentralised PXE installation of genuscreen appliances, usually in large setups. It is not part of the TOE.
The high availability option for genucenter is not part of the TOE.

The following sections describe non-obvious special features of the TOE.

1.4.3 Packet Filter Features

The *pf* is a powerful stateful packet filter, that can also be used for NAT and RDR rules (redirect to another recipient). It can perform packet defragmentation and normalization of TCP (and IP) options. The outgoing packets can be put in different queues allowing for Quality of Service. Packet tagging and filtering by tag help to enforce security policies. *pf* filter rules can be used to transfer packets between different routing domains.
The genucenter and genuscreen GUIs allow to mark interfaces to allow only encrypted traffic. This feature adds *pf* rules that allows only selected connections for cryptographic communications.

1.4.4 IPsec Features

The genuscreen appliances implement the protocol IKEv1 and IKEv2. IKEv1 only works with plain keys. IKEv2 can use keys or X.509 certificates [13], imported from an external CA. If the keys are generated by the genucenter or the genuscreen, ECDSA keys are used. The keys embedded in imported certificates depend on the issuing CA. Optionally, an OCSP server can be configured to check the validity of the certificates during the IPsec connection setup.
The following IPsec configurations are possible for the TOE:

Central and satellites: The satellites can only talk to the central.

Central and satellites with forwarding: The central forwards packets that are destined to the satellites network. This works by decrypting the received packet and encrypting once more for the destination satellite.

Full meshed net: All appliances talk directly to each other. This is the most general configuration. There is no central. This mode can only be configured for IKEv1.

Transport mode: If there are several networks attached to an appliance, an IPsec association has to be established for each network. With this transport mode, only one IPsec association to the target appliance is established and the packets for its attached networks are put in an IP over IP tunnel.

The default cryptographic settings are summarised in section 8 (table 7).

1.4.5 SSH Features

The TOE uses the following SSH features respective enhancements:

Log messages: Forwarding of UDP-packets of the `syslogd` through an SSH channel.

The default cryptographic settings are summarised in section 8 (table 7).

1.4.6 IPv6

The TOE can operate in IPv6 environments (see RFC2460 [14]). It supports a reasonable subset of useful IPv6 functionality, but makes no automatic translation between IPv4 and IPv6 addresses. DHCPv6 functionality is only supplied by an extension module.

1.4.7 SIP Relay as an Optional Module

The TOE includes a SIP relay to allow the usage of a Session Border Controller (SBC). The SIP relay is not included in the basic installation image but must be installed as an optional module at the genucenter. The SIP relay software is then installed on all appliances that use the relay. The SIP relay is the only module that is part of the TOE. The SIP relay is a user land process that controls the access to the SBC.
The SIP relay is more powerful than the SIP proxy because it can filter the SIP protocol and does not only open port ranges with *pf* states.

1.4.8 Network Separation using Routing Domains

The Kernel supports several different routing tables to which processes can be attached. This enables network separation through these routing domains. Selected packets can be transferred between the domains by explicitly configured *pf* rules. An example for this usage are different default routes.

1.4.9 Network Services

Both genuscreen and genucenter can be configured to use the following network services:

DNS The systems can use an external server for domain name resolution.

NTP The systems can use an external NTP server for time synchronisation[2].

SNMP The systems allow queries of status information from external SNMP agents, or send SNMP traps to configured hosts. An optional authenticated and/or encrypted connection can be configured for SNMPv3 (RFC3414 [2] and RFC6353 [20]).

[2] This implies **OE.TIMESTMP**.

syslog Syslog messages can be sent to external entities. An optional encrypted connection can be configured using a certificate. If a validation of the certificate chain is desired, respective root certificates must be installed at the appliances.

This security target does not claim any security functionality for the network services. They can, however, be used in certified configurations. If cryptographic functions are used, they are out of scope of the TOE.

1.4.10 Secure Initialisation of genuscreen (Firewall Component)

To guarantee that all genuscreens are set up correctly and know each other's and the genucenter's public keys, the following procedure is required:

1. A secure network is set up with only the genucenter and the genuscreens on it.
2. The genucenter must be installed from CD/USB stick. During installation, public/private key pairs are generated which are used later to identify and authorise the administrators.
3. The administrators initialise his/her account with a non-guessable password.
4. The administrators use the GUI to create configurations for all genuscreens. The configuration includes the creation of public/private key pairs for the genuscreens for later authentication by the Internet Key Exchange (IKE) and Secure Shell (SSH) protocols.
5. The genuscreens are installed by PXE boot from the genucenter. Among other things, the process installs on each genuscreen
   - the genucenter public key,
   - the individual genuscreen's public/private key pair,
   - all the public keys of all the genuscreens with which the individual genuscreen is configured to communicate directly.

Standalone genuscreen appliances without a managing genucenter can be installed from CD/USB stick using the provided standalone installation images.

1.4.11 Excluded Features

The following features are excluded from the TOE.

1.4.11.1 No genucard and no deployment server The genucard mobile device is not included in the scope of the TOE, athough it provides security features similar to the genuscreen appliances.
Also the deployment server is not included in the scope of the TOE.

1.4.11.2 No Smartcard The genuscreen can use a smartcard to perform cryptographic operations for IPsec usage. However, usage of the smartcard is out of scope for this TOE.
The smartcard can however be used as an entropy source both for genuscreen and genucenter for the kernel entropy pool of the DRG.3 random number generator.
The smartcards can also be used to store the X.509 certificate if IKEv2 is configured to use X.509 certificates.

1.4.11.3 Secure Boot While the products can use secure boot using coreboot on Intel hardware and similar mechanisms on other hardware architectures, it is not supported for all hardware variants. Therefore this security target does not claim any security functionality for the boot process. The secure boot mechanism, however, can be used in the certified configuration.

1.4.11.4 IKEv2 X.509 Certificates While IKEv2 supports the usage of X.509 certificates, this security target does not define any security functional requirements for the secure operation of a certification authority (CA). It is supposed that the certificates are imported from an external entity. Also the secure import of certificates is not covered by a security functional requirement. It is assumed that the Organisational Security Policy **P.CERTKEYS** defines rules for the secure import.

1.4.11.5 No VPN to Other Appliances or Mobile Clients It is possible to build VPN connections to third party (other) VPN appliances or directly to third party computers (mobile clients). These are not part of the TOE and *must not be configured*.

1.4.11.6 No L2TP VPN Although the genuscreen support the L2TP for VPN, it is excluded from the TOE and *must not be configured*.

1.4.11.7 No MOBIKE VPN The MOBIKE IKEv2 extension for roaming mobile appliances is excluded from the TOE.

1.4.11.8 No Dynamic Routing Even if the genuscreen appliances include support for dynamic routing using OSPF or BGP, the corresponding daemons are not started in the default configuration. Therefore, this Security Target does not make any claim on the secure operation when using dynamic routing. The operating organisation has to make its own security assessment when the daemons are configured.
The same considerations apply for the genuscreen specific feature dynamic routing/OSPF where OSPF messages are send through an IPsec tunnel.

1.4.11.9 No genucenter HA While the HA setup for the genuscreens is part of the evaluation. no security claims are made for the HA setup of the genucenter.
If the genucenter HA setup is used, the operating organisation has to make its own security assessment.

1.4.11.10 No Remote Maintenance The remote maintenance feature using a rendezvous genuscreen appliance is out of scope.

1.4.11.11 No getimagesfromcpt The command line tool `getimagesfromcpt` must not be used to install updates at the genucenter. Instead the facility to download or import images and patches in the genucenter GUI has to be used.

Table 1: Scope of delivery

Type	Name	Release	Medium
Software	genuscreen	8.0p15	CD-ROM / USB image
Software	genucenter	8.0p7	CD-ROM / USB image
Software	SIP module	8.0p15	TAR archive
Documentation	genuscreen	8.0	PDF download
Documentation	genucenter	8.0	PDF download

1.4.12 Physical Scope

The physical scope of the TOE consists only of software and documentation. The TOE does not include any hardware or firmware. The scope of delivery can be seen in table 1.
The basic TOE software is contained in the installation CD/USB stick. The install medium also has additional non-TOE software that is needed to get a running system. The SIP module is delivered separate from the installation media. Customers with a valid licence key can download the software from the genua webserver.
The TOE runs on CPUs with a wide range of performance characteristics, depending on the customer's need. For revision 2 and 3 of the hardware, the CPUs are Intel CPUs running in 64 bit mode. The entry level hardware models use Intel Atom or Intel Celeron CPUs, the middle level hardware use a Intel Xeon-D CPU and the high performance hardware use Intel Xeon E3 and Intel Xeon E5 CPUs. The TOE is compiled with compiler options that allow running the TOE on all CPUs. The network interfaces require on-board or PCI extension cards that are supported by the OpenBSD *em* or *ix* drivers.
Application Note: While the re-evaluation was performed only with genuscreen and genucenter hardware of revision 3, the software is expected to run with all security features also on older and newer hardware revisions, provided the hardware requirements of the preceding paragraph are met.
The optional genuscreen HA setup is only useful for appliances with similar hardware and comparable performance.
Application Note: Some CPUs allow the usage of hardware enhanced AES-NI. Please note that the evaluation was performed with disabled hardware enhancement. Users of the TOE have to judge by themselves if a hardware enhanced operation is acceptable.

1.4.13 Logical Scope

The following sections define the logical scope of the TOE.

1.4.13.1 Audit The genuscreen collect audit data which can be collected, stored, displayed, sorted and searched at the genucenter. Auditable events are attempts to violate a policy. This allows the administrators, service users and revisors to view the configuration and log data. For appliances that are administered locally, the local GUI allows to inspect the current state of the respective component and the audit data.

1.4.13.2 Information Flow Protection The most important user information flow policies enforced by the TOE are:

- Each genuscreen will only forward data from and to the protected networks if the firewall information flow policy allows it.
- Data flowing between the networks protected by different genuscreens is encrypted and authenticated if the IPsec/IKE information flow policy requires it (the administrators may choose not to protect flows).
- Interfaces can be configured into distinct routing domains with different routing tables.

1.4.13.3 Security Management Administrators can modify security policies at the genucenter and transfer them to the genuscreen. Alternatively, administration can be done locally. Service users can perform maintenance operations but are not allowed to do any configuration. Revisors can view the configuration and log files.

1.4.13.4 Authentication and Identification Administrators, revisors and service users must identify to the genucenter with a user name and must authenticate successfully by password before they can perform any security function.
Administrators and revisors at the local GUI of the genuscreens must identify with a user name and must authenticate successfully by password before they can perform any security function.

1.4.13.5 Cryptographic Functionality The TOE contains cryptographic functionality. The cryptographic algorithms for IPsec and SSH are part of the TOE. This includes the random number generator which is of class DRG.3 (see AIS20 [4]). If the system is supplied with an appropriate smartcard, the smartcard is used to regularly seed the random number generator from the smartcard. By this the random number generator can be upgraded to DRG.4. However, this Security Target only claims class DRG.3.
Note, however, that this Security Target does not make any claim about the cryptography of TLS connections.

1.5 Estimated End-Of Life of the Product

The genuscreen is usually re-certified every two years. In order to give the customers sufficient time to migrate to a new certified version, the support is usually extended to one year after the next certfied version is available. However, these are only general rules. In special cases, the product is supported by releasing patches up to the end of life of the certification, if that is necessary.

2 Conformance Claims

2.1 CC Conformance Claim

This Security Target is Part 2 and 3 extended to the Common Criteria Version 3.1 Revision 5 (April 2017). [11, 12].

2.2 PP Claim, Package Claim

There are no Protection Profile claims. This Security Target claims to be conformant to the Assurance Packet EAL4 augmented with ALC_FLR.2, ASE_TSS.2 and AVA_VAN.4. These components are defined in CC Part 3. The Security Target also claims ALC_PAM.1, which is an extended assurance component defined in this Security Target.

2.3 Conformance Rationale

The Security Target has no Protection Profile claim, therefore no conformance rationale has to be given.
This Security Target uses extended functional component definitions (see sections 5.1–5.3). Therefore it is Part 2 extended. It uses extended assurance requirements (see section 5.4). Therefore it is Part 3 extended.

3 Security Problem Definition

In order to clarify the nature of the security problem that the TOE is intended to solve, this section describes the following:

- All different users.
- Any known or assumed threats to the assets against which specific protection within the TOE or its environment is required.
- Any organisational security policy statements or rules with which the TOE must comply.
- Any assumptions about the security aspects of the environment and/or of the manner in which the TOE is intended to be used.

3.1 Users

This section lists all users. From these users only the anonymous user is not considered trustworthy. The threats that follow therefore only consider anonymous users as threat agents. The other user are needed for the SFRs.[3]
The general term administrators describes the union of the genucenter root domain administrators, the genucenter administrators, the genucenter security administrator, the genucenter operational administrator, the genucenter root shell account, and the genuscreen administrator[4].
The general term service user describes the genucenter service users[5].
The general term revisors describes the union of the genucenter revisors and the genuscreen revisor[6].

3.1.1 General Users

Anonymous users Any person or software agent sending IP packets to or receiving from the components of the TOE. This includes users on the protected networks behind the genuscreens as well as all users outside those networks. Their assumed attack potential is *moderate*. It must be noted however, that the TOE genuscreens are exposed to unrestricted attackers, simply because they are exposed to the Internet. The product therefore aims to protect against more capable attackers.

3.1.2 genucenter Users

genucenter root domain administrators These are authenticated users at the genucenter that have administrative rights to configure the attributes of the the genucenter root domain administrators, genucenter administrators, the genucenter revisors, the genucenter service users, the genuscreen administrator,

[3] Note that the user operator for the genucenter and web operator for the genuscreen are used for the remote maintenance feature that is not part of the evaluation.
[4] The singular term is also used for the administrator role.
[5] The singular term is used for the service role.
[6] The singular term is also used for the revisor role.

and the genuscreen revisor, and to change the genuscreen and the genucenter configuration at the genucenter.

genucenter administrators These are authenticated users at the genucenter that have administrative rights to change the genuscreen's configuration on the genucenter inside their domain.

genucenter revisors These are authenticated users at the genucenter that are allowed to view the genuscreen and the genucenter configuration and audit data on the genucenter inside their domains.

Access is usually by the genucenter GUI, but a console access can also be configured.

genucenter root shell account This is an authenticated user that has a root shell account for administrative maintenance purposes.

The following users are a specialization of the general roles administrator/revisor for specific purposes:

genucenter security administrators These are authenticated users at the genucenter that have administrative rights to change the genuscreen cryptographic configuration on the genucenter inside their domain.

genucenter operational administrators These are authenticated users at the genucenter that have administrative rights to change the genuscreen configuration on the genucenter inside their domain, but they cannot change the cryptographic configuration.

genucenter service users These are authenticated users at the genucenter that are allowed to view the genuscreen and the genucenter configuration and audit data on the genucenter inside their domains. They are also allowed to perform all maintenance activities in the "Maintenance" menu.

3.1.3 genuscreen Users

genuscreen administrator This is an authenticated user at the genuscreen that has the administrative rights to change the genuscreen configuration on the genuscreen.

This user can also be used if the appliances are managed by a genucenter, either as a root user or as a configurable system user.

The user also has a root shell account for administrative maintenance purposes.

genuscreen revisor This is an authenticated user at the genuscreen that has the administrative rights to view the genuscreen configuration on the genuscreen.

This user can also be configured as a web revisor if the appliances are managed by a genucenter[7]

[7]The difference between the genuscreen revisor and the web revisor is that the genuscreen revisor is configured at the genuscreen GUI and the web revisor is configured at the genucenter GUI.

Besides the generic roles, the appliances also have specific users that have either an administrator or a revisor role for their intended purposes. They are configured not at the appliances themselves but at the genucenter domains and are assigned to the appliances. The users are:

- root: This is a user with root acces at the console. It maps to the **genuscreen administrator**.
- system user: This is a user with non-root access at the console. It maps to the **genuscreen revisor**.
- web operator: This user is identical to the **genuscreen administrator** but is configured at the genucenter GUI and has reduced capabilities for recovery tasks.
- web revisor: This user is identical to the **genuscreen revisor** but is configured at the genucenter GUI.
- SNMP user: This allows authenticated SNMP access at the genua appliances. It maps to the **genuscreen revisor** (or **genucenter revisor**, if assigned to the genucenter).
- L2TP user: This is a generic user account at the genuscreen for the L2TP IPsec setup (not part of the certification).

3.2 Assets

The assets that have to be protected by the TOE are:

resources in the connected neteorks The resources in the connected networks that the TOE is supposed to protect.

security sensitive data on the TOE The data on the TOE that contains security sensitive data, including configuration data, hashed passwords, and private keys.

Management data This includes configuration and log data transferred between genuscreen and genucenter through the SSH management channel. Also included is configuration data that is stored on an USB stick.

3.3 Threats

The two different components of the TOE (genucenter and genuscreen) fulfil different purposes and therefore must confront different threats.

T.NOAUTH An anonymous user might attempt to bypass the security functions of the TOE to gain unauthenticated access to resources in the protected networks. This threat must be countered by the genuscreen.

T.SNIFF An anonymous user might gain access to the sensitive data passing between the protected networks. Attack method is packet inspection of Internet traffic. This threat must be countered by the genuscreen.

T.SELPRO An anonymous user might gain access to the TOE and read, modify or destroy security sensitive data on the TOE, by sending IP packets to the TOE and exploiting a weakness of the protocol used.
This threat must be countered by the genucenter and the genuscreen.

T.MEDIAT An anonymous user might send non-permissible data that result in gaining access to resources which is not allowed by the policy. The attack method is construction of IP packets to circumvent filters.

This threat must be countered by the genuscreen.

T.MSNIFF An anonymous user might gain access to the configuration or audit data passing between the genucenter and a genuscreen. Attack method is packet inspection of Internet traffic.

This threat must be countered by the genucenter and the genuscreen.

T.MODIFY An anonymous user might modify the sensitive data passing between the protected networks. Attack method is packet interception and modification of Internet traffic.

This threat must be countered by the genuscreen.

T.MMODIFY An anonymous user might modify the configuration or audit data passing between the genucenter and a genuscreen. Attack method is packet interception and modification of Internet traffic.

This threat must be countered by the genucenter and genuscreen.

3.4 Organisational Security Policies

The Security Target defines the following Organisational Security Policies.

P.AVAIL A high availability operation must be possible where peers can take over the services of a failing system. (This policy only applies if needed.)

Application Note: This policy only applies if the genuscreen HA setup is used

P.CERTKEYS The keys embedded in the imported X.509 certificates conform the the current requirements of the TR-02102-3 [3].

Application Note: X.509 certificates can only be used for IKEv2

P.PATCH Authorised bug fixes from the developer must be applied only in a secure way.

3.5 Assumptions

The following assumptions are made in order to be able to provide security functionality.

A.PHYSEC The genucenter and the genuscreen of the TOE are physically secure. Only administrators have physical access to the TOE. This must hold for the genucenter and the genuscreens.

A.INIT The TOE was initialised according to the procedure described in the documentation [19] and [18] (summarised in section 1.4.10).

A.NOEVIL Administrators, service users and revisors are non-hostile and follow all administrator guidance; however, they are capable of error. They use passwords that are not easily guessable.

A.SINGEN Information can not flow between the internal and external network, unless it passes through the TOE.

A.TIMESTMP The environment provides reliable timestamps.

A.ADMIN Administrators, service users and revisors using the administrative GUI on the genucenter or the genuscreens work in a trusted network directly connected to the system.

A.HANET The environment provides a physical separate network for transfer of TSF data between nodes for the optional high availability setup.

Application Note: This assumption only applies if the genuscreen HA setup is used.

A.REMOTE_AUTH The server for external LDAP authentication of genucenter administrators and revisors is located in a secure network.

Application Note: This assumption only applies if an external LDAP server is used for authentication.

A.LOCAL Configuration using local files is only done by trained administrators that have a profound knowledge of OpenBSD and the installed tools. They know to estimate the security impact of the local files and only create local files that have no impact on the security functions of the TOE.

A.REST The automated clients that use the REST JSON interface store the client certificate in a secure way.

4 Security Objectives

This chapter lists all security objectives of the TOE and it's operational environment.

4.1 Security Objectives for the TOE

The TOE must ensure the objectives listed in this section.

O.AUTH The TOE must ensure that only administrators can change the packet filter, VPN and SSH configuration.

O.MEDIAT The TOE must mediate the flow of all data between all connected networks.

O.CONFID The TOE must ensure that data transferred between the networks protected by genuscreen is kept confidential unless explicitly configured otherwise.

Application Note: The TOE can be configured to work as a pure packet filter without cryptographic support in cases where **O.CONFID**, **O.INTEG** and **O.NOREPLAY** are not needed or not possible. However, when cryptographic operations are needed, the objectives must be fulfilled.

O.INTEG The TOE must ensure that data transferred between the networks protected by genuscreen cannot be modified unnoticed unless explicitly configured otherwise.

Application Note: The TOE can be configured to work as a pure packet filter without cryptographic support in cases where **O.CONFID**, **O.INTEG** and **O.NOREPLAY** are not needed or not possible. However, when cryptographic operations are needed, the objectives must be fulfilled.

O.NOREPLAY The TOE must ensure that data transferred between the networks behind the genuscreen cannot be reinjected at a later time unless explicitly configured otherwise.

Application Note: This objective only applies if the genuscreen HA setup is used.

O.AUDREC The TOE must provide an audit trail of security-related events, and a means to present a readable and searchable view to administrators, service users and revisors.

O.AVAIL The TOE must optionally provide a fail over solution where the services of a failing system are taken over by a peer machine.

Application Note: The TOE can be configured to work as a pure packet filter without cryptographic support in cases where **O.CONFID**, **O.INTEG** and **O.NOREPLAY** are not needed or not possible. However, when cryptographic operations are needed, the objectives must be fulfilled.

O.PATCH The developer provides a patch mechanismus for product updates that is integrity protected and signed with a developer key. The signature of the patch is automatically checked during installation.

If the patch is an incremental update of the software, the patch is applied in a secure and correct way. Activation of the patch and update of the identification

data shall be performed at the same time. The TOE shall always be in a defined state during the update. Each patch level is uniquely identified. The patch mechanism verifies the version and patch level information contained in the patch and only applies the patch if the patch is for the current software version and patch level.

4.2 Security Objectives for the Operational Environment

The operational environment must ensure the following security objectives.

OE.PHYSEC Those responsible for the TOE must ensure that the genucenter and the genuscreen are placed at a secured place where only administrators have access.

The communication server must be used to isolate the genucenter from the Internet.

OE.INIT Those responsible for the TOE must ensure that the initial configuration is performed according to [19] and [18]. A summary of the procedure is given in section 1.4.10.

OE.NOEVIL Those responsible for the TOE must ensure that all administrators, service users and revisors are competent, regularly trained and execute the administration in a responsible way. They must choose passwords which cannot be guessed easily.

OE.SINGEN Those responsible for the TOE must ensure that the genuscreen provide the only connection for the different networks.

OE.TIMESTMP The IT environment must supply reliable timestamps for the TOE.

OE.ADMIN The administrators, service users and revisors must use the administrative GUI on the genucenter or the genuscreen only from a trusted network directly connected to the system.

They log in with SSH only from this network and use SSH keys but no passwords to authenticate.

In some cases, however, the administration network for standalone appliances is set up ad hoc, by connecting a computer to the administration port via a cross cable. It must be ensured that the administration computer runs a defined software version and no malicious software is installed on the computer.

OE.HANET The IT-environment must supply a physical separate network for transfer of TSF data between nodes for the optional high availability setup.

Application Note: This objective for the operational environment only applies if the genuscreen HA setup is used.

OE.REMOTE_AUTH The IT-environment must ensure that the LDAP server for external authentication at the genucenter is located in a secure network.

Application Note: This objective for the operational environment only applies if external LDAP authentication is used.

OE.CERTKEYS Those responsible for the TOE must ensure that the keys of imported X.509 certificates conform to TR-02102-3 [3].

OE.LOCAL Those responsible for the TOE must ensure that configuration by local files is only done by trained administrators that are able to estimate the security impact of the local files.

OE.REST The automated clients that use the REST JSON interface store the client certificate in a secure way.

4.3 Security Objectives Rationale

This chapter contains the ST security objectives rationale. It must show that the security objectives are consistent.
Table 2 shows that all security objectives stated in this ST can be mapped to the stated threats and assumptions. All threats and assumptions are matched by at least one security objective.

Table 2: TOE Rationale

	OE.PHYSEC	OE.INIT	OE.NOEVIL	OE.SINGEN	OE.TIMESTMP	OE.ADMIN	OE.HANET	OE.REMOTE_AUTH	OE.CERTKEYS	OE.LOCAL	OE.REST	O.AUTH	O.MEDIAT	O.CONFID	O.INTEG	O.NOREPLAY	O.AUDREC	O.AVAIL	O.PATCH
A.PHYSEC	X																		
A.INIT		X																	
A.NOEVIL			X																
A.SINGEN				X															
A.TIMESTMP					X														
A.ADMIN						X													
A.HANET							X												
A.REMOTE_AUTH								X											
A.LOCAL										X									
A.REST											X								
T.NOAUTH	X	X		X								X							
T.SNIFF		X												X					
T.SELPRO												X		X	X	X	X		
T.MEDIAT				X									X		X				
T.MSNIFF		X												X					
T.MODIFY		X													X	X			
T.MMODIFY		X													X	X			
P.AVAIL																		X	
P.CERTKEYS									X										
P.PATCH																			X

4.3.1 Assumption Rationale

The following shows how the assumptions are satisfied by the environmental objectives.

4.3.1.1 A.PHYSEC The objective **OE.PHYSEC** assures that the assumption about a physically secure TOE can be made and that a communication server is used.

4.3.1.2 A.INIT The objective **OE.INIT** assures that the TOE was correctly initialised.

4.3.1.3 A.NOEVIL The objective **OE.NOEVIL** assures that the administrators, service users and revisors are trained and therefore that they are no threat to the TOE.

4.3.1.4 A.SINGEN The objective **OE.SINGEN** assures that the TOE can not be bypassed and therefore assures that the assumption is met.

4.3.1.5 A.TIMESTMP The objective **OE.TIMESTMP** provides reliable timestamps.

4.3.1.6 A.ADMIN The objective **OE.ADMIN** assures that the administration only occurs from a trusted network.

4.3.1.7 A.HANET The objective **OE.HANET** assures that the IT environment provides a secure HA network.

4.3.1.8 A.REMOTE_AUTH The objective **OE.REMOTE_AUTH** assures that the LDAP server for external authentication is located in a secure network.

4.3.1.9 A.LOCAL This threat is met by **OE.LOCAL**: The objective requires that only trained administrators configure the TOE by local files.

4.3.1.10 A.REST The objective **OE.REST** assures that the passwords for the automated access of the REST interface are secured.

4.3.2 Threat Rationale

The following shows that all threats are addressed by the objectives.

4.3.2.1 T.NOAUTH The threat that an anonymous user might bypass the security functions of the TOE is countered by **OE.PHYSEC**, **OE.INIT**, **OE.SINGEN**, and **O.AUTH**. The objectives assure that no anonymous user can interfere with the initial setup, the physical setup of the genuscreens, or use routes around the genuscreen. The **O.AUTH** objective assures that only administrators can configure the system.

4.3.2.2 T.SNIFF The threat that an anonymous user might gain access to the sensitive data passing between the protected networks is countered by objectives **OE.INIT** and **O.CONFID**. These assure that the genuscreen's public keys are initialised over an authenticated network and that all data flowing between the genuscreens is protected against eavesdropping by IPsec transforms.

4.3.2.3 T.SELPRO The threat that an anonymous user might gain access to the TOE and read, modify or destroy security sensitive data on the TOE is countered by objectives **O.AUTH**, **O.CONFID**, **O.INTEG**, **O.NOREPLAY**, and **O.AUDREC**. **O.AUTH** assures that only administrators can configure the TOE. **O.CONFID**, **O.INTEG** and **O.NOREPLAY** assure that the communication between the genucenter and the genuscreen is secured by encryption. **O.AUDREC** assures that attempts to compromise the TOE are audited.

4.3.2.4 T.MEDIAT he threat that an anonymous user may send non-permissible data through the TOE that result in gaining access to resources in other connected networks is countered by **OE.SINGEN**, **O.MEDIAT** and **O.INTEG**. These assure that all data passes through the TOE, so that it is always checked and filtered according to the policy, and that data thus checked cannot be modified on it's way to gain access to machines in the protected networks.

4.3.2.5 T.MSNIFF The threat that an anonymous user might gain access to the configuration or audit data passing between the genucenter and the genuscreen is countered by objectives **OE.INIT** and **O.CONFID**. These assure that the genucenter and the genuscreen public keys are initialised over an authenticated network and that all data flowing between the genucenter and the genuscreens is protected against eavesdropping by SSH transforms.

4.3.2.6 T.MODIFY The threat that an anonymous user might modify the sensitive data passing between the protected networks is countered by objectives **OE.INIT**, **O.INTEG** and **O.NOREPLAY**. These assure that the genuscreen's public keys are initialised over an authenticated network and that all data flowing between the genuscreens is protected by IPsec transforms against unauthorised modification and re-injection of earlier data.

4.3.2.7 T.MMODIFY The threat that an anonymous user might modify the configuration or audit data passing between the genucenter and the genuscreen is countered by objectives **OE.INIT**, **O.INTEG** and **O.NOREPLAY**. These assure that the genucenter and the genuscreen's public keys are initialised over an authenticated network and that all data flowing between the genucenter and the genuscreens is protected by SSH transforms against modification and re-injection of earlier data.

4.3.3 Organisational Security Policy Rationale

The following shows that all organisational security policies are addressed by the objectives.

4.3.3.1 P.AVAIL The objective **O.AVAIL** assures that the policy **P.AVAIL** is met.

4.3.3.2 P.CERTKEYS The objective for the environtment **OE.CERTKEYS** assured that the Organisational Security Policies **P.CERTKEYS** is enforced.

4.3.3.3 P.PATCH The objective for the environment is met by **O.PATCH**: The signature check during patch installation guarantees that the patch is authorised by the developer and (in the case of an incremental update) has the correct patch level.

5 Extended Components Definition

5.1 Class FAU: Security audit

The family has been enhanced by one component FAU_GEN.1EX.

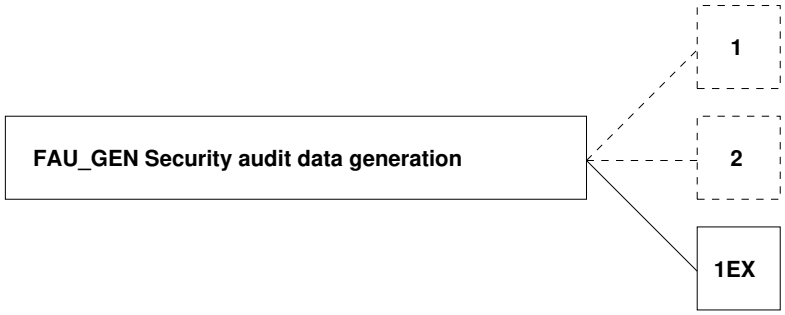
5.1.1 FAU_GEN: Security audit data generation

The component is intended to be a replacement for FAU_GEN.1 when the security function does not support audit generation for startup and shutdown of the audit functions. This component can be used as a replacement for the dependencies on FAU_GEN.1, because all other audit events can be specified as in FAU_GEN.1.

Family behaviour

This family defines requirements for recording the occurrence of security relevant events that take place under TSF control. This family identifies the level of auditing, enumerates the types of events that shall be auditable by the TSF, and identifies the minimum set of audit-related information that should be provided within various audit record types.

Component levelling



The components FAU_GEN.1 and FAU_GEN.2 are already described in [7]. Only FAU_GEN.1EX is new and described here.

Management: FAU_GEN.1EX

There are no management activities foreseen.

Audit: FAU_GEN.1EX

There are no actions identified that should be auditable if FAU_GEN Security audit data generation is included in the PP/ST.

FAU_GEN.1EX Audit data generation

Hierarchical to: No other components.

Dependencies: FPT_STM.1 Reliable time stamps.

FAU_GEN.1EX.1 The TSF shall be able to generate an audit record of the following auditable events:

a) All auditable events for the **[selection: choose one of: *minimum, basic, detailed, not specified*]** level of audit; and

b) **[assignment: other specifically defined auditable events]**.

The TSF are allowed to reduce audit data generation on the following conditions: **[assignment: conditions for reduction of audit data generation]**

FAU_GEN.1EX.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 relevant information]**.

5.2 Class FCS: Cryptographic Support

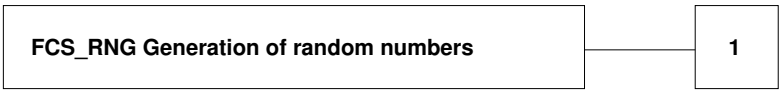
The following family has been defined in [26], a supporting document for AIS20 [4] and AIS31 [5]. For the rationale of the definition of this extended component, see [26].

5.2.1 FCS_RNG: Generation of random numbers

Family Behaviour

This family defines quality requirements for the generation of random numbers that are intended to be used for cryptographic purposes.

Component levelling



FCS_RNG.1 Generation of random numbers, requires that the random number generator implements defined security capabilities and that the random numbers meet a defined quality metric.

Management: FCS_RNG.1

There are no management activities foreseen.

Audit: FCS_RNG.1

There are no actions defined to be auditable.

FCS_RNG.1 Random number generation

Hierarchical to: No other components.

Dependencies: No dependencies.

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 random numbers that meet **[assignment: a defined quality metric]**.

5.3 Class FPT: Protection of the TSF

The class has been augmented by one family.

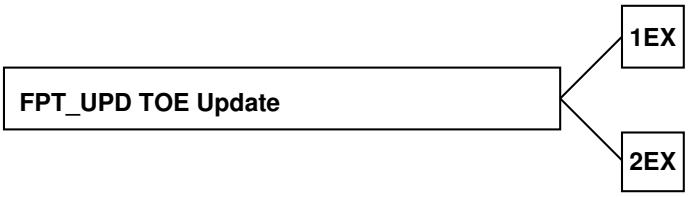
5.3.1 TOE Update (FPT_UPD)

The family specifies the secure and correct installation of patches from the developer by an administrator. The new family is added to the class FPT, because it protects the TSF from manipulation through the installation of malicious patches.

Family behaviour

The requirements of this family assure that only authorised patches from the developer can be installed in a secure and correct way by an administrator. The family has two components, which are independent from each other.

Component levelling



FPT_UPD.1EX Trusted update, requires that patches are signed using the specified cryptographic standards.
FPT_UPD.2EX Update identification data, requires that the patches have a unique patch level that is updated at the same time.

Management: FPT_UPD.1EX.1, FPT_UPD.1EX.2

The following actions could be considered for the management functions in FMT:

a) determining the time when to apply the patches.

Audit: FPT_UPD.1EX, FPT_UPD.2EX

The following actions should be auditable if FAU_UPD.1EX TOE Update is included in the PP/ST:

a) Basic: The result of the patch update.

FPT_UPD.1EX Trusted update

Hierarchical to: No other components.

Dependencies: FCS_COP.1 Cryptographic operation.

FPT_UPD.1EX.1 The TOE shall cryptographically verify additional code/patches to itself using a digital signature prior to installation using schemes specified in [assignment: *FCS_COP.1 SFR*].

FPT_UPD.1EX.2 A modification of the TOE shall only be allowed if the software update

- **is intended for the current software version,**

- **has the correct patch level and**
- **has been cryptographically verified with regard to integrity and authenticity.**

FPT_UPD.2EX Update identification data

Hierarchical to: No other components.

Dependencies: No dependencies.

FPT_UPD.2EX.1 The TSF shall verify if the activation of the patch and the update of the identification data have been both completed.

FPT_UPD.2EX.2 The TSF shall update the active identification data when the patch is applied in order to keep the system in a defined state.

FPT_UPD.2EX.3 The TSF shall use the maintenance mode to activate the final TOE.

5.4 Class ALC: Life-cycle support

The class has been augmented by one family that specifies the secure and correct generation of patches by the developer. The new family is added to the class ALC, because it handles the patch aspect of the product life-cycle that has not been considered by the CC.

5.4.1 Patch Management (ALC_PAM)

Objectives

The objective of this family is to identify procedures to be implemented in the development process, which will be applied after the initial release of a TOE.

The application of these patch management processes cannot be always determined at the time of the base evaluation, but at least, it is possible to evaluate the policies and procedures that a developer has in place to perform management processes in the future, and obtain some evidence of the correct application of the procedures during the patching of the problems found during the evaluation of other assurance classes like AVA and ATE.

These procedures shall include instructions on how to securely sign, distribute and apply patches and how the life cycle of the keys used for providing authenticity of new patches is handled.

Component levelling

This family contains only one component.

Application notes

None.

ALC_PAM.1 Patch Management Processes

Dependencies: ALC_FLR.2 Flaw reporting procedures.

Developer action elements:

ALC_PAM.1.1D The developer shall provide a Patch Management Policy.

ALC_PAM.1.2D The developer shall self-assess and confirm the application of existing policies on a regular basis saving records of its application.

ALC_PAM.1.3D The developer shall provide security patches using the defined policies and procedures at least until the estimated end-of-life of the TOE.

Content and presentation elements:

ALC_PAM.1.1C The developer's patch management policies shall describe what is the criteria used for the decision that a patch has to be released.

ALC_PAM.1.2C The Security Target shall contain the estimated end-of-life of the TOE.

ALC_PAM.1.3C The developer's patch management policies shall describe how to self-assess the security relevance of a patch (i.e. Security Impact Analysis Report, S-IAR) and which procedures have to apply due to which assessment result.

ALC_PAM.1.4C The developer's patch management policies shall describe how to update the evidence documentation used in the base evaluation.

ALC_PAM.1.5C The developer's patch management policies shall describe how unhandled (potential) flaws are documented.

ALC_PAM.1.6C The developer's patch management policies shall describe which organisational role (or group) is responsible for the patch development.

ALC_PAM.1.7C The developer's patch management policies shall describe which policies have to be applied until the end of life of the TOE during the patch management.

ALC_PAM.1.8C Each tool used for the patch management shall be documented.

ALC_PAM.1.9C The patch management policies shall describe the mandatory structure and content of the S-IAR.

ALC_PAM.1.10C Each type of documentation used to record decisions in the patch management process shall be documented.

ALC_PAM.1.11C The patch management policies shall describe the mandatory content of patch release notes.

ALC_PAM.1.12C The patch management policies shall describe the mandatory content for the guidance documents which have to be fulfilled to support the installation of the patch.

ALC_PAM.1.13C The patch management policies shall describe the mandatory procedures during patch release.

ALC_PAM.1.14C The patch management policies shall contain rules in which case the evaluation facility has to perform additional tests before the patch is released.

ALC_PAM.1.15C The patch management policies shall describe how each of the patch management Security Objectives for the Operational Environment are fulfilled until the end of life of the TOE.

Evaluator action elements:

ALC_PAM.1.1E The evaluator shall confirm that the information provided meets all requirements for content and presentation of evidence.

6 Security Requirements

This section contains the security functional requirements, the security assurance requirements, and the rationale.
Throughout this document, CC operations on security requirements are marked as follows:

- Assignments are denoted in [**bold text in square brackets**].
- Selections are denoted by [***bold slanted text in square brackets***].
- Refinements are denoted in **bold text** (added text) and/or ~~crossed out~~ (removed text).
- Iterations are denoted by affixing annotational text in parentheses to the component name, joined by an underscore.

6.1 Security Functional Requirements

This section lists the principal Security Functional Requirements claimed by the TOE. Most are derived from requirements in [7]. In the statement of the requirements, the abbreviation in parentheses defines the specific iteration of the associated Part 2 requirement.

6.1.1 Firewall SFP

This section lists the SFRs necessary for the genuscreen to enforce firewall security policies defined by the administrators.
The **FW-SFP** is concerned with the creation, modification, deletion and application of firewall security policy rules. It also provides protection against unauthorised access to the platform running the genuscreen.

6.1.1.1 FDP_IFC.1_(FW) Subset information flow control

FDP_IFC.1.1_(FW) The TSF shall enforce the [**FW-SFP**] on [

- **subjects: anonymous users;**
- **information: the data sent from one subject through the TOE to another;**
- **operation: filter the data**].

6.1.1.2 FDP_IFF.1_(FW) Simple security attributes

FDP_IFF.1.1_(FW) The TSF shall enforce the [**FW-SFP**] based on the following types of subject and information security attributes: [

- **subject security attributes: none**
- **information security attributes:**
  - **address of source subject;**
  - **address of destination subject;**
  - **transport layer protocol;**
  - **interface on which traffic arrives and departs;**
  - **IP version;**
  - **service**].

FDP_IFF.1.2_(FW) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [**subjects on a network connected to the TOE can cause information to flow through the TOE to a subject on another connected network only if all the information security attribute values are permitted by all information flow policy rules**].

FDP_IFF.1.3_(FW) The TSF shall enforce the [

- **reassembly of fragmented IPv4 and IPv6 datagrams before inspection**
- **possibility to modify parts of the TCP/IP headers to make the connections less vulnerable against hijacking attacks**].

FDP_IFF.1.4_(FW) The TSF shall explicitly authorise an information flow based on the following rules: [**none**].

FDP_IFF.1.5_(FW) The TSF shall explicitly deny an information flow based on the following rules: [

- **the TOE shall drop IP datagrams with the source routing option;**
- **the TOE shall reject fragmented IP datagrams which cannot be reassembled completely within a bounded interval;**
- **the TOE shall optionally reject requests of access or services where the information arrives on a network interface and the source address of the requesting subject does not belong to the network associated with the interface (spoofed packets) when feasible**].

6.1.1.3 FMT_MSA.1_(FW-A) Management of security attributes

FMT_MSA.1.1_(FW-A) The TSF shall enforce the [**FW-SFP**] to restrict the ability to [***modify***] the security attributes [**packet filter rules**] to [**the genucenter root domain administrators, the genucenter administrators, the genucenter operational administrators and the genuscreen administrator**].

6.1.1.4 FMT_MSA.1_(FW-R) Management of security attributes

FMT_MSA.1.1_(FW-R) The TSF shall enforce the [**FW-SFP**] to restrict the ability to [***query***] the security attributes [**packet filter rules**] to [**the genucenter root domain administrators, the genucenter administrators, the genucenter revisors, and the genucenter service users, the genuscreen administrator, the genuscreen revisor**].

6.1.1.5 FMT_MSA.3_(FW) Static attribute initialisation

FMT_MSA.3.1_(FW) The TSF shall enforce the [**FW-SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2_(FW) The TSF shall allow the [**none**] to specify alternative initial values to override the default values when an object or information is created.

6.1.1.6 FMT_SMF.1_(FW) Specification of management functions

FMT_SMF.1.1_(FW) The TSF shall be capable of performing the following security management functions: [**creation and modification of network traffic filter rules. The rules filter for the following attributes of datagrams:**

- **address of source subject;**
- **address of destination subject;**
- **transport layer protocol;**
- **interfaces on which traffic arrives and departs;**
- **IP version;**
- **service**].

6.1.2 Network Separation SFP

This section identifies the SFRs associated with the network separation using routing domains.

6.1.2.1 FDP_IFC.2_(NS) Complete information flow control

FDP_IFC.2.1_(NS) The TSF shall enforce the [**NS-SFP**] on [

- **subjects: anonymous users;**
- **information: the data sent from one subject through the TOE to another;**]

and all operations that cause that information to flow to and from subjects covered by the SFP.

FDP_IFC.2.2_(NS) The TSF shall ensure that all operations that cause any information in the TOE to flow to and from any subject in the TOE are covered by an information flow control SFP.

6.1.2.2 FDP_IFF.1_(NS) Simple security attributes

FDP_IFF.1.1_(NS) The TSF shall enforce the [**NS-SFP**] based on the following types of subject and information security attributes: [

- **subject security attributes: none**
- **information security attributes:**
  - **the incoming interface and its routing table**].

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

- **the outgoing interface is selected using the routing table of the routing domain of the incoming interface**].

FDP_IFF.1.3_(NS) The TSF shall enforce the [**none**].

FDP_IFF.1.4_(NS) The TSF shall explicitly authorise an information flow based on the following rules: [

- **a packet filter rule changes the routing domain for the respective IP packet**].

FDP_IFF.1.5_(NS) The TSF shall explicitly deny an information flow based on the following rules: [**incoming and outgoing interface are in different routing domains (unless a pf rule exists).**].

6.1.2.3 FMT_MSA.1_(NS-A) Management of security attributes

FMT_MSA.1.1_(NS-A) The TSF shall enforce the [**NS-SFP**] to restrict the ability to [***modify***] the security attributes [**routing domain and *pf* routing domain changing rules**] to [**the genucenter root domain administrators, the genucenter administrators, the genucenter operational administrators, and the genuscreen administrator**].

6.1.2.4 FMT_MSA.1_(NS-R) Management of security attributes

FMT_MSA.1.1_(NS-R) The TSF shall enforce the [**NS-SFP**] to restrict the ability to [***query***] the security attributes [**routing domain**] to [**the genucenter root domain administrators, the genucenter administrators, the genucenter revisors, and the genucenter service users, the genuscreen administrator, the genuscreen revisor**].

6.1.2.5 FMT_MSA.3_(NS) Static attribute initialisation

FMT_MSA.3.1_(NS) The TSF shall enforce the [**NS-SFP**] to provide [***permissive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2_(NS) The TSF shall allow the [**none**] to specify alternative initial values to override the default values when an object or information is created.

6.1.2.6 FMT_SMF.1_(NS) Specification of management functions

FMT_SMF.1.1_(NS) The TSF shall be capable of performing the following security management functions: [**changing the routing domain of an interface**].

6.1.3 IPSEC

This section identifies the SFRs associated with the flow control functions in relation to the VPN connections between the genuscreens. The **IKE-SFP** is the policy that models this aspect of information flow control. This section is separated from the **IKE-SFP** because these SFRs are handled by the kernel but configured from user space. When cryptographic standards are referenced, the requirements only apply to the mandatory parts.

6.1.3.1 FDP_ITT.1_(IPSEC) Basic internal transfer protection

FDP_ITT.1.1_(IPSEC) The TSF shall enforce the [**IKE-SFP**] to prevent the [***disclosure and modification***] of user data when it is transmitted between physically-separated parts of the TOE.

6.1.3.2 FDP_IFC.1_(IPSEC) Subset information flow control

FDP_IFC.1.1_(IPSEC) The TSF shall enforce the [**IKE-SFP**] on [

- **subjects: genuscreens;**
- **information: the data sent from one subject to another;**
- **operation: encrypt/decrypt the data**].

6.1.3.3 FCS_COP.1_(IPSEC-AES) Cryptographic operation

FCS_COP.1.1_(IPSEC-AES) The TSF shall perform [**data encryption and decryption**] in accordance with a specified cryptographic algorithm [**AES in GCM or CBC mode**] and cryptographic key sizes [**128 bit, 192 bit, or 256 bit**] that meet the following: [**FIPS-197 [34], NIST-SP800-38A [35], NIST-SP800-38D [36] and RFC3602 [15]**].

6.1.3.4 FCS_COP.1_(IPSEC-HMAC) Cryptographic operation

FCS_COP.1.1_(IPSEC-HMAC) The TSF shall perform [**generation and verification of message authentication code**] in accordance with a specified cryptographic algorithm [**HMAC-SHA2-256**] and cryptographic key sizes [**256 bit**] that meet the following: [**FIPS-180-4 [39], RFC2104 [27] and RFC4868 [24]**].

Application Note: This SFR only applies if AES in CBC mode is used. In GCM mode, no additional MAC is needed.

6.1.3.5 FCS_CKM.4_(IPSEC) Cryptographic key destruction

FCS_CKM.4.1_(IPSEC) The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**overwriting with zeros**] that meets the following: [**none**].

6.1.4 IKEv1 and IKEv2

This section identifies the SFRs associated with cryptographic functions in relation to the key management of the VPN connections between the genuscreens. The **IKE-SFP** is the policy that models this aspect of information flow control. When cryptographic standards are referenced, the requirements only apply to the mandatory parts. The **IKE-SFP** contains both the IKEv1 and IKEv2 protocols.

6.1.4.1 FDP_ITT.1_(IKE) Basic internal transfer protection

FDP_ITT.1.1_(IKE) The TSF shall enforce the [**IKE-SFP**] to prevent the [***disclosure and modification***] of user data when it is transmitted between physically-separated parts of the TOE.

Application Note: The data transmitted is in fact the key agreement for subsequent IPsec transforms.

6.1.4.2 FDP_IFC.1_(IKE) Subset information flow control

FDP_IFC.1.1_(IKE) The TSF shall enforce the [**IKE-SFP**] on [

- **subjects: genuscreens;**
- **information: the data sent from one subject through the environment to another;**
- **operation: negotiate keys for IPsec usage**].

6.1.4.3 FDP_IFF.1_(IKE) Simple security attributes

FDP_IFF.1.1_(IKE) The TSF shall enforce the [**IKE-SFP**] based on at least the following types of subject and information security attributes: [

- **subject security attributes: public keys associated with the subject.**
- **information security attributes: none**].

FDP_IFF.1.2_(IKE) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [**subjects can cause information to flow through their respective components of the TOE if based on the subject's public keys a secure IPsec connection can be negotiated between the subjects via the IKE protocol**].

FDP_IFF.1.3_(IKE) The TSF shall enforce the [**none**].

FDP_IFF.1.4_(IKE) The TSF shall explicitly authorise an information flow based on the following rules: [**none**].

FDP_IFF.1.5_(IKE) The TSF shall explicitly deny an information flow based on the following rules: [**the validation check fail for IKEv2 certificates:**

- **the checks for the following certificate (see RFC5280 [13]) fields fail: certificate chain, name/alt name attribute, validity, extended attributes**].
- **the online certificate status protocol (OCSP, RFC6960 [40]) checks fail for the certificate (if configured).**

6.1.4.4 FCS_CKM.1_(IKE-AES) Cryptographic key generation

FCS_CKM.1.1_(IKE-AES) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**AES symmetric key generation**] and specified cryptographic key sizes [**128 bit, 192 bit (default), or 256 bit**] that meet the following: [**RFC3602 [15]**].

Application Note: The key generation function use the random number generator FCS_RNG.1 in chapter 6.1.11.

6.1.4.5 FCS_COP.1_(IKE-AES) Cryptographic operation

FCS_COP.1.1_(IKE-AES) The TSF shall perform [**data encryption and decryption**] in accordance with a specified cryptographic algorithm [**AES in CBC or GCM mode**] and cryptographic key sizes [**128 bit, 192 bit, or 256 bit**] that meet the following: [**FIPS-197 [34], NIST-SP800-38A [35], NIST-SP800-38D [36] and RFC3602 [15]**].

Application Note: IKEv1 allows only CBC mode in phase 1.

6.1.4.6 FCS_CKM.1_(IKE-ECDH) Cryptographic key generation

FCS_CKM.1.1_(IKE-ECDH) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**256-bit random ECP group**] and specified cryptographic key sizes [**256 bit**] that meet the following: [**RFC5114 [29] and RFC5903 [17]**].

Application Note: The cryptographic elliptic curve algorithm contains both the cryptographic key generation and the key exchange.

Application Note: The key generation function use the random number generator FCS_RNG.1 in chapter 6.1.11.

6.1.4.7 FCS_CKM.1_(IKE-HMAC) Cryptographic key generation

FCS_CKM.1.1_(IKE-HMAC) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**HMAC-SHA2-256**] and specified cryptographic key sizes [**256 bit**] that meet the following: [**FIPS-180-4 [39], RFC2104 [27] and RFC4868 [24]**].

Application Note: The key generation function use the random number generator FCS_RNG.1 in chapter 6.1.11.

6.1.4.8 FCS_COP.1_(IKE-HMAC) Cryptographic operation

FCS_COP.1.1_(IKE-HMAC) The TSF shall perform [**generation and verification of message authentication code**] in accordance with a specified cryptographic algorithm [**HMAC-SHA2-256**] and cryptographic key sizes [**256 bit**] that meet the following: [**FIPS-180-4 [39], RFC2104 [27] and RFC4868 [24]**].

Application Note: This SFR only applies if AES in CBC mode is used. In GCM mode, no additional MAC is needed.

6.1.4.9 FCS_CKM.1_(IKE-ECDSA) Cryptographic key generation

FCS_CKM.1.1_(IKE-ECDSA) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**ECDSA key generation**] and specified cryptographic key sizes [**256 bit**] that meet the following: [**ECDSA-256, RFC4754 [16]**].

Application Note: ECDSA keys are only generated at the genucenter GUI. For the genuscreen local GUI externally generated keys must be imported.
Application Note: The key generation function use the random number generator FCS_RNG.1 in chapter 6.1.11.

6.1.4.10 FCS_COP.1_(IKE-ECDSA) Cryptographic operation

FCS_COP.1.1_(IKE-ECDSA) The TSF shall perform [**digital signature creation and verification**] in accordance with a specified cryptographic algorithm [**ECDSA signature**] and cryptographic key sizes [**256 bit**] that meet the following: [**256-bit random ECP group, RFC5903 [17]**].

6.1.4.11 FCS_CKM.4_(IKE) Cryptographic key destruction

FCS_CKM.4.1_(IKE) The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**overwriting with zeros**] that meets the following: [**none**].

Application Note: The key destruction function is identical for FCS_CKM.1_(IKE-ECDH), FCS_CKM.1_(IKE-AES), FCS_CKM.1_(IKE-HMAC) and FCS_CKM.1_(IKE-ECDSA), so there is only one iteration of FCS_CKM.4 for all four SFRs.

6.1.4.12 FMT_MSA.1_(IKE-A) Management of security attributes

FMT_MSA.1.1_(IKE-A) The TSF shall enforce the [**IKE-SFP**] to restrict the ability to [***modify***] the security attributes [**IKE configuration**] to [**the genucenter root domain administrators, the genucenter administrators, the genucenter security administrators, and the genuscreen administrator**].

6.1.4.13 FMT_MSA.1_(IKE-R) Management of security attributes

FMT_MSA.1.1_(IKE-R) The TSF shall enforce the [**IKE-SFP**] to restrict the ability to [***query***] the security attributes [**IKE configuration**] to [**the genucenter root domain administrators, the genucenter administrators, the genucenter revisors, the genucenter service users, the genuscreen administrator, and the genuscreen revisor**].

6.1.4.14 FMT_MSA.2_(IKE) Secure security attributes

FMT_MSA.2.1_(IKE) The TSF shall ensure that only secure values are accepted for [**the IKE configuration**].

6.1.4.15 FMT_MSA.3_(IKE) Static attribute initialisation

FMT_MSA.3.1_(IKE) The TSF shall enforce the [**IKE-SFP**] to provide [**restrictive**] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2_(IKE) The TSF shall allow the [**the genucenter root domain administrators, the genucenter administrators, the genucenter security administrators, and the genuscreen administrator**] to specify alternative initial values to override the default values when an object or information is created.

6.1.4.16 FMT_SMF.1_(IKE) Specification of management functions

FMT_SMF.1.1_(IKE) The TSF shall be capable of performing the following security management functions: [**modification and deletion of public and secret keys associated with genuscreens by the IKE daemon**].

6.1.5 SSH-SFP

This section identifies the SFRs associated with the flow control functions in relation to the communication between genucenter and the genuscreens. The SSH-SFP is the policy that models this aspect of information flow control. When cryptographic standards are referenced, the requirements only apply to the mandatory parts.

6.1.5.1 FPT_ITT.1_(SSH) Basic internal TSF data transfer protection

FPT_ITT.1.1_(SSH) The TSF shall protect TSF data from [***disclosure and modification***] when it is transmitted between separate parts of the TOE.

6.1.5.2 FDP_ITT.1_(SSH) Basic internal transfer protection

FDP_ITT.1.1_(SSH) The TSF shall enforce the [**SSH-SFP**] to prevent the [***disclosure and modification***] of user data when it is transmitted between physically-separated parts of the TOE.

6.1.5.3 FDP_IFC.1_(SSH) Subset information flow control

FDP_IFC.1.1_(SSH) The TSF shall enforce the [**SSH-SFP**] on [

- **subjects: genucenter and genuscreens;**
- **information: the data sent from one subject through the environment to another;**
- **operation: encrypt/decrypt the data**].

6.1.5.4 FDP_IFF.1_(SSH) Simple security attributes

FDP_IFF.1.1_(SSH) The TSF shall enforce the [**SSH-SFP**] based on **at least** the following types of subject and information security attributes: [

- **subject security attributes:**
  - **SSH host keys and user keys installed on the platforms hosting the TOE components.**
- **information security attributes: none**].

FDP_IFF.1.2_(SSH) The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [**subjects can cause information to flow through their respective components of the TOE if based on the subject's host keys and user keys a secure connection can be negotiated between the subjects via the SSH protocol**].

FDP_IFF.1.3_(SSH) The TSF shall enforce the [**none**].

FDP_IFF.1.4_(SSH) The TSF shall explicitly authorise an information flow based on the following rules: [**none**].

FDP_IFF.1.5_(SSH) The TSF shall explicitly deny an information flow based on the following rules: [**none**].

6.1.5.5 FCS_CKM.1_(SSH-AES) Cryptographic key generation

FCS_CKM.1.1_(SSH-AES) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**AES symmetric key generation**] and specified cryptographic key sizes [**128 bit**] that meet the following: [**RFC4253 [43] with the ETM extension**].

Application Note: The key generation function use the random number generator FCS_RNG.1 in chapter 6.1.11.

6.1.5.6 FCS_COP.1_(SSH-AES) Cryptographic operation

FCS_COP.1.1_(SSH-AES) The TSF shall perform [**data encryption and decryption**] in accordance with a specified cryptographic algorithm [**AES in CTR mode**] and cryptographic key sizes [**128 bit**] that meet the following: [**FIPS-197 [34], NIST-SP800-38A [35] and NIST-SP800-38D [36]**].

6.1.5.7 FCS_CKM.1_(SSH-ECDH) Cryptographic key generation

FCS_CKM.1.1_(SSH-ECDH) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**elliptic curve ecdh-sha2-brainpoolp256r1**] and specified cryptographic key sizes [**256 bit**] that meet the following: [**RFC5639 [30] and [31]**].

Application Note: The cryptographic elliptic curve algorithm contains both the cryptographic key generation and the key exchange.

Application Note: The key generation function use the random number generator FCS_RNG.1 in chapter 6.1.11.

6.1.5.8 FCS_CKM.1_(SSH-UMAC) Cryptographic key generation

FCS_CKM.1.1_(SSH-UMAC) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**UMAC-128**] and specified cryptographic key sizes [**256 bit**] that meet the following: [**RFC4418 [28]**].

Application Note: The key generation function use the random number generator FCS_RNG.1 in chapter 6.1.11.

6.1.5.9 FCS_COP.1_(SSH-UMAC) Cryptographic operation

FCS_COP.1.1_(SSH-UMAC) The TSF shall perform [**generation and verification of message authentication code**] in accordance with a specified cryptographic algorithm [**UMAC-128-ETM**] and cryptographic key sizes [**256 bit**] that meet the following: [**RFC4418 [28] using AES, UMAC [32]**].

6.1.5.10 FCS_CKM.1_(SSH-ECDSA) Cryptographic key generation

FCS_CKM.1.1_(SSH-ECDSA) The TSF shall generate cryptographic keys in accordance with a specified cryptographic key generation algorithm [**ECDSA key generation**] and specified cryptographic key sizes [**256 bit**] that meet the following: [**ecdsa-sha2-nistp256, RFC6239 [22]**]].

Application Note: The key generation function use the random number generator FCS_RNG.1 in chapter 6.1.11.

6.1.5.11 FCS_COP.1_(SSH-ECDSA) Cryptographic operation

FCS_COP.1.1_(SSH-ECDSA) The TSF shall perform [**authentication**] in accordance with a specified cryptographic algorithm [**ECDSA signature generation and verification**] and cryptographic key sizes [**256 bit**] that meet the following: [**ecdsa-sha2-nistp256, RFC6239 [22]**]].

6.1.5.12 FCS_CKM.4_(SSH) Cryptographic key destruction

FCS_CKM.4.1_(SSH) The TSF shall destroy cryptographic keys in accordance with a specified cryptographic key destruction method [**overwriting with zeros**] that meets the following: [**none**].

Application Note: The key destruction function is identical for FCS_CKM.1_(SSH-ECDH), FCS_CKM.1_(SSH-AES), FCS_CKM.1_(SSH-UMAC) and FCS_CKM.1_(SSH-ECDSA), so there is only one iteration of FCS_CKM.4 for all four SFRs.

6.1.5.13 FMT_MSA.1_(SSH-A) Management of security attributes

FMT_MSA.1.1_(SSH-A) The TSF shall enforce the [**SSH-SFP**] to restrict the ability to [***modify***] the security attributes [**SSH configuration**] to [**the genucenter root domain administrators, the genucenter administrators, the genucenter security administrators, and the genuscreen administrator**].

6.1.5.14 FMT_MSA.1_(SSH-R) Management of security attributes

FMT_MSA.1.1_(SSH-R) The TSF shall enforce the [**SSH-SFP**] to restrict the ability to [***query***] the security attributes [**SSH configuration**] to [**the genucenter root domain administrators, the genucenter administrators, the genucenter revisors, the genucenter service users, the genuscreen administrator, and the genuscreen revisor**].

6.1.5.15 FMT_MSA.2_(SSH) Secure security attributes

FMT_MSA.2.1_(SSH) The TSF shall ensure that only secure values are accepted for [**the SSH configuration**].

6.1.5.16 FMT_MSA.3_(SSH) Static attribute initialisation

FMT_MSA.3.1_(SSH) The TSF shall enforce the [**SSH-SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2_(SSH) The TSF shall allow the [**the genucenter root domain administrators. the genucenter administrators, and the genucenter security administrators**] to specify alternative initial values to override the default values when an object or information is created.

6.1.5.17 FMT_SMF.1_(SSH) Specification of management functions

FMT_SMF.1.1_(SSH) The TSF shall be capable of performing the following security management functions: [**modification and deletion of public and secret keys associated with the genuscreen by the SSH daemon**].

Application Note: The key destruction is done on deletion of the associated genuscreen.

6.1.6 SIP Relay

This section identifies the SFRs associated with the access control by the SIP relay.

6.1.6.1 FDP_IFC.1_(SIP) Complete information flow control

FDP_IFC.1.1_(SIP) The TSF shall enforce the [**SIP-SFP**] on [

- **subjects: users that send and receive information through the TOE to one another;**
- **information: traffic sent through the TOE from one subject to another;**
- **operation: perform access control**]

6.1.6.2 FDP_IFF.1_(SIP) Simple security attributes

FDP_IFF.1.1_(SIP) The TSF shall enforce the [**SIP-SFP**] based on the following types of subject and information security attributes: [

- **IP and TCP header;**
- **SIP protocol and application data**].

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

- **The SIP relay is installed and configured**].

FDP_IFF.1.3_(SIP) The TSF shall enforce the [**none**].

FDP_IFF.1.4_(SIP) The TSF shall explicitly authorise an information flow based on the following rules: [

- **The tests for the configured internal and external domains and RTP port ranges pass.**

- **The ACL and request method checks pass**].

FDP_IFF.1.5_(SIP) The TSF shall explicitly deny an information flow based on the following rules: [

- **The tests for the configured internal and external domains and RTP port ranges fail.**
- **The ACL and request method checks fail**].

6.1.6.3 FMT_MSA.1_(SIP-A) Management of security attributes

FMT_MSA.1.1_(SIP-A) The TSF shall enforce the [**SIP-SFP**] to restrict the ability to [***modify***] the security attributes [**SIP relay configuration**] to [**the genucenter root domain administrators, the genucenter administrators, the genucenter operational administrators, and the genuscreen administrator**].

6.1.6.4 FMT_MSA.1_(SIP-R) Management of security attributes

FMT_MSA.1.1_(SIP-R) The TSF shall enforce the [**SIP-SFP**] to restrict the ability to [***query***] the security attributes [**SIP relay configuration**] to [**the genucenter root domain administrators, the genucenter administrators, the genucenter revisors, and the genucenter service users, the genuscreen administrator, and the genuscreen revisor**].

6.1.6.5 FMT_MSA.3_(SIP) Static attribute initialisation

FMT_MSA.3.1_(SIP) The TSF shall enforce the [**SIP-SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2_(SIP) The TSF shall allow the [**none**] to specify alternative initial values to override the default values when an object or information is created.

6.1.6.6 FMT_SMF.1_(SIP) Specification of management functions

FMT_SMF.1.1_(SIP) The TSF shall be capable of performing the following security management functions: [**installation and configuration of the SIP relay**].

6.1.7 Administration

These SFRs are related to the administration of the TOE.

6.1.7.1 FDP_IFC.1_(ADM) Subset information flow control

FDP_IFC.1.1_(ADM) The TSF shall enforce the [**ADM-SFP**] on [

- **subjects: administrators from the administration network that interact with the administrative web server of the TOE;**
- **information: HTML form or REST JSON data for administration;**
- **operation: perform access control**].

6.1.7.2 FDP_IFF.1_(ADM) Simple security attributes

FDP_IFF.1.1_(ADM) The TSF shall enforce the [**ADM-SFP**] based on the following types of subject and information security attributes: [

- **the current domain (URL)**
- **the current administrator/service user/revisor (identified by cookie, basic-auth or API token)**].

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

- **the cookie or basic-auth is still valid**
- **the administrator/service user/revisor is allowed to configure/review the domain**].

FDP_IFF.1.3_(ADM) The TSF shall enforce the [**none**].

FDP_IFF.1.4_(ADM) The TSF shall explicitly authorise an information flow based on the following rules: [**none**].

FDP_IFF.1.5_(ADM) The TSF shall explicitly deny an information flow based on the following rules: [**none**].

6.1.7.3 FMT_MSA.1_(ADM-A) Management of security attributes

FMT_MSA.1.1_(ADM-A) The TSF shall enforce the [**ADM-SFP**] to restrict the ability to [***modify***] the security attributes [**TOE configuration**] to [**the genucenter root domain administrators, the genucenter administrators, the genucenter operational administrators, and the genuscreen administrator**].

Application Note: The term TOE configuration includes all configuration attributes besides those described in FMT_MSA.1.1_(ADM-ROOT).

6.1.7.4 FMT_MSA.1_(ADM-R) Management of security attributes

FMT_MSA.1.1_(ADM-R) The TSF shall enforce the [**ADM-SFP**] to restrict the ability to [***query***] the security attributes [**TOE configuration**] to [**the genucenter root domain administrators, the genucenter administrators, the genucenter revisors, the genucenter service users, the genuscreen administrator, and the genuscreen revisor**].

Application Note: The term TOE configuration includes all configuration attributes besides those described in FMT_MSA.1.1_(ADM-ROOT).

6.1.7.5 FMT_MSA.1_(ADM-O) Management of security attributes

FMT_MSA.1.1_(ADM-O) The TSF shall enforce the [**ADM-SFP**] to restrict the ability to [***update***] the security attributes [**TOE data**] to [**the genucenter root domain administrators, the genucenter administrators, the genucenter operational administrators, the genucenter service user, and the genuscreen administrator**].

Application Note: The term **Update** includes the security management functions: transfer of configuration data onto the genuscreens; collecting log data from the firewall components.

Application Note: The term **TOE data** includes both the configuration and the log data of the respective appliance.

6.1.7.6 FMT_MSA.1_(ADM-ROOT) Management of security attributes

FMT_MSA.1.1_(ADM-ROOT) The TSF shall enforce the [**ADM-SFP**] to restrict the ability to [***modify***] the security attributes [**administrative role, password, administrative domain**] to [**the genucenter root domain administrators**].

6.1.7.7 FMT_MSA.3_(ADM) Static attribute initialisation

FMT_MSA.3.1_(ADM) The TSF shall enforce the [**ADM-SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2_(ADM) The TSF shall allow the [**genucenter root domain administrators**] to specify alternative initial values to override the default values when an object or information is created.

6.1.7.8 FMT_SMF.1_(ADM) Security management functions

FMT_SMF.1.1_(ADM) The TSF shall be capable of performing the following security management functions: [

- **assigning names and passwords for the administrators;**
- **assigning names and passwords for the service users;**
- **assigning names and passwords for the revisors;**
- **assigning genucenter administrators to domains;**
- **assigning genucenter service users to domains;**
- **assigning genucenter revisors to domains;**
- **initial configuration of the genuscreens;**
- **transfer of configuration data onto the genuscreens;**
- **collecting log data from the genuscreens;**
- **switch administration mode for the genuscreen**].

6.1.8 Identification and Authentication

These SFRs are related to identification and authentication of administrators, service users and revisors.

6.1.8.1 FIA_ATD.1_(IA) User attribute definition

FIA_ATD.1.1_(IA) The TSF shall maintain the following list of security attributes belonging to individual users: [

- **administrator role: name, password, administrative domains**
- **service role: name, password, administrative domains**
- **revisor role: name, password, administrative domains**].

6.1.8.2 FIA_SOS.1_(IA) Verification of secrets

FIA_SOS.1.1_(IA) The TSF shall provide a mechanism to verify that secrets meet [**the passwords for the genucenter root domain administrators, the genucenter root shell account, the genucenter service users, the genucenter revisors, the genuscreen administrator and the genuscreen revisor must be at least 8 characters in length when changed in the administrative GUI**].

Application Note: There is no such requirement for changing passwords at the console.

Application Note: This SFR does not apply if an external LDAP server is used for administrator and revisor authentication.

6.1.8.3 FIA_UAU.2_(IA) User authentication before any action

FIA_UAU.2.1_(IA) The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.1.8.4 FIA_UAU.6_(IA) Re-authenticating

FIA_UAU.6.1_(IA) The TSF shall re-authenticate the ~~user~~**the genucenter root domain administrators, genucenter administrators, the genucenter revisors and the genucenter service users** under the conditions [**after 10 minutes idle time at the administrative GUI**].

6.1.8.5 FIA_UID.2_(IA) User identification before any action

FIA_UID.2.1_(IA) The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.1.9 Audit

This section provides SFRs relating to the audit capabilities of the TOE.

6.1.9.1 FAU_GEN.1EX_(AU) Audit data generation

FAU_GEN.1EX.1_(AU) The TSF shall generate an audit record of the following auditable events:

a) All auditable events for the [**not specified**] level of audit; and
b) [

1. **Starting of genuscreens**
2. **IP datagrams matching log filters in firewall rules**].

The TSF are allowed to reduce audit data generation on the following conditions: [**the log rate exceeds the threshold: 30000 log messages per second.**]

FAU_GEN.1EX.2_(AU) 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, 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, [**no other audit relevant information**].

6.1.9.2 FAU_SAR.1_(AU) Audit review

FAU_SAR.1.1_(AU) The TSF shall provide [**the genucenter root domain administrators, the genucenter administrators, the genucenter revisors, the genucenter service users, the genuscreen administrator, and the genuscreen revisor**] with the capability to read [**the audit data from the administrator's/service user's domain/revisor's domain**] from the audit records.

FAU_SAR.1.2_(AU) The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.1.9.3 FAU_SAR.3_(AU) Selectable audit review

FAU_SAR.3.1_(AU) The TSF shall provide the ability to apply [***searches***] of audit data based on: [

- **range of time and date;**
- **the genuscreen that produced the audit data;**
- **for log data of firewall rules: IP addresses and ports, where applicable**].

6.1.10 General Management Facilities

This section provides SFRs relating to the general management of the TOE.

6.1.10.1 FMT_MOF.1_(GEN) Management of security functions behaviour

FMT_MOF.1.1_(GEN) The TSF shall restrict the ability to [***modify the behaviour of***] the functions [**logging, reaction to failed random number generator test**] to [**the genucenter root domain administrators, the genucenter administrators, the genucenter operational administrators, and the genuscreen administrator**].

6.1.10.2 FMT_SMF.1_(GEN) Specification of management functions

FMT_SMF.1.1_(GEN) The TSF shall be capable of performing the following security management functions: [**configuration of the audit system; configuration of the reaction to failed random number generator test**].

6.1.10.3 FMT_SMR.1_(GEN) Security roles

FMT_SMR.1.1_(GEN) The TSF shall maintain the roles [

- **administrator: genucenter root domain administrators, genucenter administrators, genucenter security administrators, genucenter operational administrators, genucenter root shell account, genuscreen administrator;**
- **service: genucenter service users;**
- **revisor: genucenter revisors, genuscreen revisor**].

FMT_SMR.1.2_(GEN) The TSF shall be able to associate users with roles.

6.1.10.4 FPT_TEE.1_(GEN) Testing of external entities

FPT_TEE.1.1_(GEN) The TSF shall run a suite of tests [***during initial start-up***] to check the fulfilment of [**a minimum quality of random numbers generated]**.

FPT_TEE.1.2_(GEN) If the test fails, the TSF shall [**execute an administrator defined action (log the event and disable VPN functionality)**].

Application Note: Remote access by SSH is not disabled in order to guarantee reachability.

6.1.10.5 FPT_TRC.1_(GEN) Internal TOE TSF data replication consistency

FPT_TRC.1.1 The TSF shall ensure that TSF data is consistent when replicated between parts of the TOE.

FPT_TRC.1.2 When parts of the TOE containing replicated TSF data are disconnected, the TSF shall ensure the consistency of the replicated TSF data upon ~~reconnection before processing any requests for~~**takeover for** [***pf* states and IPsec security associations**].

Application Note: This SFR only applies if the genuscreen HA setup is used. The refinement reflects the characteristic of the TOE to continuously synchronise the replicated TSF data so that consistency is maintained at takeover time.

6.1.11 Random Number Generation

This section describes the SFRs for the generated random numbers. The assignments in this section were taken from [26]. Therefore the text contains nested assignments and selections without extra markup.

6.1.11.1 FCS_RNG.1 Random number generation (Class DRG.3)

FCS_RNG.1.1 The TSF shall provide a [***deterministic***] random number generator that implements: **[**

(DRG.3.1) **If initialized with a random seed [from a custom entropy pool], the internal state of the RNG shall [have at least 64 bit of entropy].**

(DRG.3.2) **The RNG provides forward secrecy.**

(DRG.3.3) **The RNG provides backward secrecy even if the current internal state is known.**

]

FCS_RNG.1.2 The TSF shall provide random numbers that meet: **[**

(DRG.3.4) **The RNG, initialized with a random seed [with an entropy of 128 bit], generates output for which [$k > 2^{26}$] strings of bit length 128 are mutually different with probability [$\epsilon < 2^{-12}$].**

(DRG.3.5) **Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A [and the DieHarder[8] random number test suite].**

]

6.1.12 Patch Installation

This section provides SFRs relating to the patch installation process.

6.1.12.1 FCS_COP.1_(PI) Cryptographic operation

FCS_COP.1.1_(PI) The TSF shall perform [**signature verification for the integrity check of update packages**] in accordance with a specified cryptographic algorithm [**RSA signature verification**] and cryptographic key sizes [**4096 bit**] that meet the following: [**RFC8017 [33], RSA signatures according to PKCS#1, v2.2 using RSASSA-PKCS1-v1_5 and SHA-512 (default), SHA-384 or SHA-256**].

6.1.12.2 FPT_UPD.1EX_(PI) Trusted Update

FPT_UPD.1EX.1_(PI) The TOE shall cryptographically verify additional code/patches to itself using a digital signature prior to installation using schemes specified in [**FCS_COP.1_(PI)**].

FPT_UPD.1EX.2_(PI) A modification of the TOE shall only be allowed if the software update

- is intended for the current software version,
- has the correct patch level and
- has been cryptographically verified with regard to integrity and authenticity.

Application Note: This component only applies to genucenter patches.

6.1.12.3 FPT_UPD.2EX_(PI) Update identification data

FPT_UPD.2EX.1_(PI) The TSF shall verify if the activation of the patch and the update of the identification data have been both completed.

FPT_UPD.2EX.2_(PI) The TSF shall update the active identification data when the patch is applied in order to keep the system in a defined state.

FPT_UPD.2EX.3_(PI) The TSF shall use the maintenance mode to activate the final TOE.

Application Note: This SFR only applies to genucenter patches.

[8] http://www.phy.duke.edu/~rgb/General/dieharder.php

6.2 Security Assurance Requirements

In order to handle patch management, the Security Target defines one new assurance component for the class ALC: Life-cycle support, defined in chapter 5.4.1.
Table 3 shows the Security Assurance Requirements for the level EAL4. The augmented components ALC_FLR.2, ASE_TSS.2 and AVA_VAN.4 are set in a bold font. For the level EAL4, the SARs ADV_INT and ADV_SPM are not needed.
The table also contains the new assurance component ALC_PAM.1.

Table 3: Security Assurance Rationale

Class	Family	Level	Name
Development	ADV_ARC	ADV_ARC.1	Security architecture description
	ADV_FSP	ADV_FSP.4	Complete functional specification
	ADV_IMP	ADV_IMP.1	Implementation representation of the TSF
	ADV_INT		TSF internals
	ADV_SPM		Security policy modelling
	ADV_TDS	ADV_TDS.3	Basic modular design
Guidance	AGD_OPE	AGD_OPE.1	Operational user guidance
	AGD_PRE	AGD_PRE.1	Preparative procedures
Life-cycle	ALC_CMC	ALC_CMC.4	Production support, acceptance procedures and automation
	ALC_CMS	ALC_CMS.4	Problem tracking CM coverage
	ALC_DEL	ALC_DEL.1	Delivery procedures
	ALC_DVS	ALC_DVS.1	Identification of security measures
	ALC_FLR	**ALC_FLR.2**	Flaw reporting procedures
	ALC_LCD	ALC_LCD.1	Developer defined life-cycle model
	ALC_TAT	ALC_TAT.1	Developer defined life-cycle model
	ALC_PAM	**ALC_PAM.1**	Patch management processes
Security Target	ASE_CCL	ASE_CCL.1	Conformance claims
	ASE_ECD	ASE_ECD.1	Extended components definition
	ASE_INT	ASE_INT.1	ST introduction
	ASE_OBJ	ASE_OBJ.2	Security objectives
	ASE_REQ	ASE_REQ.2	Derived security requirements
	ASE_SPD	ASE_SPD.1	Security problem definition
	ASE_TSS	**ASE_TSS.2**	TOE summary specification with architectural design summary
Tests	ATE_COV	ATE_COV.2	Analysis of coverage
	ATE_DPT	ATE_DPT.1	Testing: basic design
	ATE_FUN	ATE_FUN.1	Functional testing
	ATE_IND	ATE_IND.2	Independent testing - sample
Vulnerability	AVA_VAN	**AVA_VAN.4**	Methodical vulnerability analysis

6.3 Security Functional Requirements Rationale

The table 4 lists the SFRs and their dependencies. The dependency on FIA_UID.1 is met by FIA_UID.2, which is hierarchical. The dependency on FDP_IFC.1_(NS) is met by FDP_IFC.2_(NS), which is hierarchical. The SFR FPT_STM.1 must be met by the environment.

Table 4: SFR dependencies

ID	SFR	Dependency	Solution
		FW-SFP	
A01	FDP_IFC.1_(FW)	FDP_IFF.1	A02
A02	FDP_IFF.1_(FW)	FDP_IFC.1	A01
		FMT_MSA.3	A04
A03-A	FMT_MSA.1_(FW-A)	FDP_IFC.1	A01
		FMT_SMR.1	K03
		FMT_SMF.1	A05
A03-R	FMT_MSA.1_(FW-R)	FDP_IFC.1	A01
		FMT_SMR.1	K03
		FMT_SMF.1	A05
A04	FMT_MSA.3_(FW)	FMT_MSA.1	A03-A, A03-R
		FMT_SMR.1	K03
A05	FMT_SMF.1_(FW)	-	-
		NS-SFP	
B01	FDP_IFC.2_(NS)	FDP_IFF.1	B02
B02	FDP_IFF.1_(NS)	FDP_IFC.1	B01 (hierarchical)
		FMT_MSA.3	B04
B03-A	FMT_MSA.1_(NS-A)	FDP_IFC.1	B01 (hierarchical)
		FMT_SMR.1	K03
		FMT_SMF.1	B05
B03-R	FMT_MSA.1_(NS-R)	FDP_IFC.1	B01 (hierarchical)
		FMT_SMR.1	K03
		FMT_SMF.1	B05
B04	FMT_MSA.3_(NS)	FMT_MSA.1	B03-A, B03-R
		FMT_SMR.1	K03
B05	FMT_SMF.1_(NS)	-	-
		IPSEC	
D01	FDP_ITT.1_(IPSEC)	FDP_IFC.1	D02
D02	FDP_IFC.1_(IPSEC)	FDP_IFF.1	E03
D03	FCS_COP.1_(IPSEC-AES)	FCS_CKM.1	E06
		FCS_CKM.4	D05
D04	FCS_COP.1_(IPSEC-HMAC)	FCS_CKM.1	E06
		FCS_CKM.4	D05
D05	FCS_CKM.4_(IPSEC)	FCS_CKM.1	E06
		IKE-SFP	
E01	FDP_ITT.1_(IKE)	FDP_IFC.1	E02
E02	FDP_IFC.1_(IKE)	FDP_IFF.1	E03
E03	FDP_IFF.1_(IKE)	FDP_IFC.1	E02
		FMT_MSA.3	E15
E04	FCS_CKM.1_(IKE-AES)	FCS_COP.1	E05
		FCS_CKM.4	E12
E05	FCS_COP.1_(IKE-AES)	FCS_CKM.1	E04
		FCS_CKM.4	E12
E06[9]	FCS_CKM.1_(IKE-ECDH)	FCS_COP.1	D03, D04
		FCS_CKM.4	E12, D05
E08	FCS_CKM.1_(IKE-HMAC)	FCS_COP.1	E09
		FCS_CKM.4	E12
E09	FCS_COP.1_(IKE_HMAC)	FCS_CKM.1	E08
		FCS_CKM.4	E12
E10	FCS_CKM.1_(IKE-ECDSA)	FCS_COP.1	E11

ID	SFR	Dependency	Solution
		FCS_CKM.4	E12
E11	FCS_COP.1_(IKE-ECDSA)	FCS_CKM.1	E10
		FCS_CKM.4	E12
E12	FCS_CKM.4_(IKE)	FCS_CKM.1	E04, E06, E08, E10
E13-A	FMT_MSA.1_(IKE-A)	FDP_IFC.1	E02
		FMT_SMR.1	K03
		FMT_SMF.1	E16
E13-R	FMT_MSA.1_(IKE-R)	FDP_IFC.1	E02
		FMT_SMR.1	K03
		FMT_SMF.1	E16
E14	FMT_MSA.2_(IKE)	FDP_IFC.1	E02
		FMT_MSA.1	E13-A, E13-R
		FMT_SMR.1	K03
E15	FMT_MSA.3_(IKE)	FMT_MSA.1	E13-A, E13-R
		FMT_SMR.1	K03
E16	FMT_SMF.1_(IKE)	-	-
SSH-SFP			
F01	FPT_ITT.1_(SSH)	-	-
F02	FDP_ITT.1_(SSH)	FDP_IFC.1	F03
F03	FDP_IFC.1_(SSH)	FDP_IFF.1	F04
F04	FDP_IFF.1_(SSH)	FDP_IFC.1	F03
		FMT_MSA.3	F16
F05	FCS_CKM.1_(SSH-AES)	FCS_COP.1	F06
		FCS_CKM.4	F13
F06	FCS_COP.1_(SSH-AES)	FCS_CKM.1	F05
		FCS_CKM.4	F13
F07[9]	FCS_CKM.1_(SSH-ECDH)	FCS_COP.1	F07
		FCS_CKM.4	F13
F09	FCS_CKM.1_(SSH-UMAC)	FCS_COP.1	F10
		FCS_CKM.4	F13
F10	FCS_COP.1_(SSH-UMAC)	FCS_CKM.1	F09
		FCS_CKM.4	F13
F11	FCS_CKM.1_(SSH-ECDSA)	FCS_COP.1	F12
		FCS_CKM.4	F13
F12	FCS_COP.1_(SSH-ECDSA)	FCS_CKM.1	F11
		FCS_CKM.4	F13
F13	FCS_CKM.4_(SSH)	FCS_CKM.1	F05, F07, F09, F11
F14-A	FMT_MSA.1_(SSH-A)	FDP_IFC.1	F03
		FMT_SMR.1	K03
		FMT_SMF.1	F17
F14-R	FMT_MSA.1_(SSH-R)	FDP_IFC.1	F03
		FMT_SMR.1	K03
		FMT_SMF.1	F17
F15	FMT_MSA.2_(SSH)	FDP_IFC.1	F03
		FMT_MSA.1	F14-A, F14-R
		FMT_SMR.1	K03
F16	FMT_MSA.3_(SSH)	FMT_MSA.1	F14-A, F14-R
		FMT_SMR.1	K03
F17	FMT_SMF.1_(SSH)	-	-
SIP-SFP			
G01	FDP_IFC.1_(SIP)	FDP_IFF.1	G02

ID	SFR	Dependency	Solution
G02	FDP_IFF.1_(SIP)	FDP_IFC.1	G01
		FMT_MSA.3	G04
G03-A	FMT_MSA.1_(SIP-A)	FDP_IFC.1	G01 (hierarchical)
		FMT_SMR.1	K03
		FMT_SMF.1	G05
G03-R	FMT_MSA.1_(SIP-R)	FDP_IFC.1	G01 (hierarchical)
		FMT_SMR.1	K03
		FMT_SMF.1	G05
G04	FMT_MSA.3_(SIP)	FMT_MSA.1	G03-A, G03-R
		FMT_SMR.1	K03
G05	FMT_SMF.1_(SIP)	-	-
Administration			
H01	FDP_IFC.1_(ADM)	FDP_IFF.1	H02
H02	FDP_IFF.1_(ADM)	FDP_IFC.1	H01
		FMT_MSA.3	H05
H03-A	FMT_MSA.1_(ADM-A)	FDP_IFC.1	H01
		FMT_SMR.1	K03
		FMT_SMF.1	H06
H03-R	FMT_MSA.1_(ADM-R)	FDP_IFC.1	H01
		FMT_SMR.1	K03
		FMT_SMF.1	H06
H03-O	FMT_MSA.1_(ADM-O)	FDP_IFC.1	H01
		FMT_SMR.1	K03
		FMT_SMF.1	H06
H04	FMT_MSA.1_(ADM-ROOT)	FDP_IFC.1	H01
		FMT_SMR.1	K03
		FMT_SMF.1	H06
H05	FMT_MSA.3_(ADM)	FMT_MSA.1	H03-A. H03-R, H03-O, H04
		FMT_SMR.1	K03
H06	FMT_SMF.1_(ADM)	-	-
Identification and Authentication			
I01	FIA_ATD.1_(IA)	-	-
I02	FIA_SOS.1_(IA)	-	-
I03	FIA_UAU.2_(IA)	FIA_UID.1	I05 (hierarchical)
I04	FIA_UAU.6_(IA)	-	-
I05	FIA_UID.2_(IA)	-	-
Audit			
J01	FAU_GEN.1EX_(AU)	FPT_STM.1	environment (OE.TIMESTMP)
J02	FAU_SAR.1_(AU)	FAU_GEN.1	J01
J03	FAU_SAR.3_(AU)	FAU_SAR.1	J02
General Management Facilities			
K01	FMT_MOF.1_(GEN)	FMT_SMR.1	K03
		FMT_SMF.1	K02
K02	FMT_SMF.1_(GEN)	-	-
K03	FMT_SMR.1_(GEN)	FIA_UID.1	I05 (hierarchical)
K04	FPT_TEE.1_(GEN)	-	-
K05	FPT_TRC.1_(GEN)	FPT_ITT.1	Environment (OE.HANET)
Random Number Generation			
L01	FCS_RNG.1	-	-
TOE Update			
M01	FPT_UPD.1EX_(PI)	FCS_COP.1	M03

ID	SFR	Dependency	Solution
M02	FPT_UPD.2EX_(PI)	-	-
M03	FCS_COP.1_(PI)	FDP_ITC.1	ALC_DEL
		FCS_CKM.4	N/A

[9]**Application Note**: The IDs E07 and F08 are missing from the table. See rationale for the reason.

The rationale for the solution of the dependencies is as follows:

- The FCS_COP.1_(IPSEC-AES) and FCS_COP.1_(IPSEC-HMAC) depend on a FCS_CKM.1 SFR for key creation. The keying material for the in-kernel IPsec transforms is generated dynamically by the IKE daemons. Thus the FCS_CKM.1_(IKE) SFR satisfies the dependency. The algorithms and key sizes are dictated by the configuration of the IKE daemons, so that requirement FMT_MSA.2_(IKE) also enforces a requirement on FCS_COP.1_(IPSEC-AES) and FCS_COP.1_(IPSEC-HMAC), which makes a special FMT_MSA.2 for the IPsec cryptographic operations unnecessary.
- The FAU_GEN.1EX depends on FPT_STM.1 that requires reliable timestamps. The objective **OE.TIMESTMP** exactly provides these reliable timestamps, therefore the dependency is satisfied by the environment.
- The FPT_TRC.1_(GEN) depends on FPT_ITT.1_(SSH) which requires the protection of the TSF transfer against disclosure (or modification). This requirement is satisfied by the objective **OE.HANET** that requires a physical network for the transfer that prohibits disclosure.
- The cryptographic elliptic curve algorithm contains both the cryptographic key generation and the cryptographic operation. Therefore the dependence of FCS_CKM.1_(SSH-ECDH) on SFR FCS_COP.1 is fulfilled by itself (and the ID E07 is missing in the table).
- The cryptographic elliptic curve algorithm contains both the cryptographic key generation and the cryptographic operation. Therefore the dependence of FCS_CKM.1_(SSH-ECDH) on SFR FCS_COP.1 is fulfilled by itself (and the ID F08 is missing in the table).
- FCS_COP.1_(PI) depends on FDP_ITC.1. The (public) key to verify the signature of the patch is distributed on the installation medium that is secured by the delivery process in ALC_DEL. Therefore no explicit import function is necessary.
  The SFR also depends on FCS_CKM.4. Only the public key is needed, therefore the SFR is not needed.

Table 5 shows how the SFRs can be traced back to the objectives.

Table 5: Objectives

		O.AUTH	O.MEDIAT	O.CONFID	O.INTEG	O.NOREPLAY	O.AUDREC	O.AVAIL	O.PATCH
A01	FDP_IFC.1_(FW)		X						
A02	FDP_IFF.1_(FW)		X						
A03-A	FMT_MSA.1_(FW-A)		X						
A03-R	FMT_MSA.1_(FW-R)		X						
A04	FMT_MSA.3_(FW)		X						
A05	FMT_SMF.1_(FW)		X						
B01	FDP_IFC.2_(NS)		X						
B02	FDP_IFF.1_(NS)		X						
B03-A	FMT_MSA.1_(NS-A)		X						
B03-R	FMT_MSA.1_(NS-R)		X						
B04	FMT_MSA.3_(NS)		X						
B05	FMT_SMF.1_(NS)		X						
D01	FDP_ITT.1_(IPSEC)			X	X	X			
D02	FDP_IFC.1_(IPSEC)			X	X	X			
D03	FCS_COP.1_(IPSEC-AES)			X	X	X			
D04	FCS_COP.1_(IPSEC-HMAC)			X	X	X			
D05	FCS_CKM.4_(IPSEC)			X	X	X			
E01	FDP_ITT.1_(IKE)			X	X	X			
E02	FDP_IFC.1_(IKE)			X	X	X			
E03	FDP_IFF.1_(IKE)			X	X	X			
E04	FCS_CKM.1_(IKE-AES)			X	X	X			
E05	FCS_COP.1_(IKE-AES)			X	X	X			
E06[10]	FCS_CKM.1_(IKE-ECDH)			X	X	X			
E08	FCS_CKM.1_(IKE-HMAC)			X	X	X			
E09	FCS_COP.1_(IKE_HMAC)			X	X	X			
E10	FCS_CKM.1_(IKE-ECDSA)			X	X	X			
E11	FCS_COP.1_(IKE-ECDSA)			X	X	X			
E12	FCS_CKM.4_(IKE)			X	X	X			
E13-A	FMT_MSA.1_(IKE-A)			X	X	X			
E13-R	FMT_MSA.1_(IKE-R)			X	X	X			
E14	FMT_MSA.2_(IKE)			X	X	X			
E15	FMT_MSA.3_(IKE)			X	X	X			
E16	FMT_SMF.1_(IKE)			X	X	X			
F01	FPT_ITT.1_(SSH)			X	X	X			
F02	FDP_ITT.1_(SSH)			X	X	X			
F03	FDP_IFC.1_(SSH)			X	X	X			
F04	FDP_IFF.1_(SSH)			X	X	X			
F05	FCS_CKM.1_(SSH-AES)			X	X	X			

		O.AUTH	O.MEDIAT	O.CONFID	O.INTEG	O.NOREPLAY	O.AUDREC	O.AVAIL	O.PATCH
F06	FCS_COP.1_(SSH-AES)			X	X	X			
F07[10]	FCS_CKM.1_(SSH-ECDH)			X	X	X			
F09	FCS_CKM.1_(SSH-UMAC)			X	X	X			
F10	FCS_COP.1_(SSH-UMAC)			X	X	X			
F11	FCS_CKM.1_(SSH-ECDSA)			X	X	X			
F12	FCS_COP.1_(SSH-ECDSA)			X	X	X			
F13	FCS_CKM.4_(SSH)			X	X	X			
F14-A	FMT_MSA.1_(SSH-A)			X	X	X			
F14-R	FMT_MSA.1_(SSH-R)			X	X	X			
F15	FMT_MSA.2_(SSH)			X	X	X			
F16	FMT_MSA.3_(SSH)			X	X	X			
F17	FMT_SMF.1_(SSH)			X	X	X			
G01	FDP_IFC.1_(SIP)		X						
G02	FDP_IFF.1_(SIP)		X						
G03-A	FMT_MSA.1_(SIP-A)		X						
G03-R	FMT_MSA.1_(SIP-R)		X						
G04	FMT_MSA.3_(SIP)		X						
G05	FMT_SMF.1_(SIP)		X						
H01	FDP_IFC.1_(ADM)		X						
H02	FDP_IFF.1_(ADM)		X						
H03-A	FMT_MSA.1_(ADM-A)		X						
H03-R	FMT_MSA.1_(ADM-R)		X						
H03-O	FMT_MSA.1_(ADM-O)		X						
H04	FMT_MSA.1_(ADM-ROOT)		X						
H05	FMT_MSA.3_(ADM)		X						
H06	FMT_SMF.1_(ADM)		X						
I01	FIA_ATD.1_(IA)	X							
I02	FIA_SOS.1_(IA)	X							
I03	FIA_UAU.2_(IA)	X							
I04	FIA_UAU.6_(IA)	X							
I05	FIA_UID.2_(IA)	X							
J01	FAU_GEN.1EX_(AU)						X		
J02	FAU_SAR.1_(AU)						X		
J03	FAU_SAR.3_(AU)						X		
K01	FMT_MOF.1_(GEN)						X		
K02	FMT_SMF.1_(GEN)						X		
K03	FMT_SMR.1_(GEN)		X				X		
K04	FPT_TEE.1_(GEN)			X	X	X			
K05	FPT_TRC.1_(GEN)							X	
L01	FCS_RNG.1			X	X	X			
M01	FPT_UPD.1EX_(PI)								X
M02	FPT_UPD.2EX_(PI)								X
M03	FCS_COP.1_(PI)								X

[10] **Application Note**: The IDs E07 and F08 are missing from the table.

6.3.1 O.AUTH

This objective is met by the SFRs FIA_ATD.1_(IA), FIA_SOS.1_(IA), FIA_UAU.2_(IA), FIA_UAU.6_(IA), and FIA_UID.2_(IA). They handle authentication failures, user attribute definition, the verification of secrets, user authentication, re-authentication and user identification.

6.3.2 O.MEDIAT

This objective is met by several groups of SFRs.
FDP_IFC.1_(FW), FDP_IFF.1_(FW), FMT_MSA.1_(FW-A), FMT_MSA.1_(FW-R), FMT_MSA.3_(FW), and FMT_SMF.1_(FW) handle the firewall security policy. They define the access methods, the security attributes and their management.
FDP_IFC.2_(NS), FDP_IFF.1_(NS), FMT_MSA.1_(NS-A), FMT_MSA.1_(NS-R), FMT_MSA.3_(NS), and FMT_SMF.1_(NS) handle the network separation policy. They define the access methods, the security attributes and their management.
FDP_IFC.1_(SIP), FDP_IFF.1_(SIP), FMT_MSA.1_(SIP-A), FMT_MSA.1_(SIP-R), FMT_MSA.3_(SIP), and FMT_SMF.1_(SIP) handle the SIP-policy. They define the access methods, the security attributes and their management.
FDP_IFC.1_(ADM), FDP_IFF.1_(ADM), FMT_MSA.1_(ADM-A), FMT_MSA.1_(ADM-R), FMT_MSA.1_(ADM-O), FMT_MSA.1_(ADM-ROOT), FMT_MSA.3_(ADM), and FMT_SMF.1_(ADM) handle the administrative interface. They define the access method, the security attributes, and their management.
FMT_SMR.1_(GEN) defines the roles that can change the configuration.

6.3.3 O.CONFID

This objective is met by several groups of SFRs.
FDP_ITT.1_(IPSEC), FDP_IFC.1_(IPSEC), FCS_COP.1_(IPSEC-AES), FCS_COP.1_(IPSEC-HMAC), and FCS_CKM.4_(IPSEC) handle the IPsec functionality. They define the access methods, the security attributes, their management and cryptographic behaviour.
FDP_ITT.1_(IKE), FDP_IFC.1_(IKE), FDP_IFF.1_(IKE), FCS_CKM.1_(IKE-AES), FCS_COP.1_(IKE-AES), FCS_CKM.1_(IKE-ECDH), FCS_COP.1_(IKE-ECDH), FCS_CKM.1_(IKE-HMAC), FCS_COP.1_(IKE_HMAC), FCS_CKM.1_(IKE-ECDSA), FCS_COP.1_(IKE-ECDSA), FCS_CKM.4_(IKE), FMT_MSA.1_(IKE-A), FMT_MSA.1_(IKE-R), FMT_MSA.2_(IKE), FMT_MSA.3_(IKE), and FMT_SMF.1_(IKE) handle the IKE functionality. They define the access methods, the security attributes, their management and cryptographic behaviour.
FPT_ITT.1_(SSH), FDP_ITT.1_(SSH), FDP_IFC.1_(SSH), FDP_IFF.1_(SSH), FCS_CKM.1_(SSH-AES), FCS_COP.1_(SSH-AES), FCS_CKM.1_(SSH-ECDH), FCS_CKM.1_(SSH-UMAC), FCS_COP.1_(SSH-UMAC), FCS_CKM.1_(SSH-ECDSA), FCS_COP.1_(SSH-ECDSA), FCS_CKM.4_(SSH), FMT_MSA.1_(SSH-A), FMT_MSA.1_(SSH-R), FMT_MSA.2_(SSH), FMT_MSA.3_(SSH), and FMT_SMF.1_(SSH) handle the administrative SSH connections between the genuscreen and the genuscreen. They define the access methods, the security attributes, their management and cryptographic behaviour.
FPT_TEE.1_(GEN) checks if the random numbers have a sufficient quality for cryptographic operations.
FCS_RNG.1 provides random input for cryptographic operations.

6.3.4 O.INTEG

This objective is met by several groups of SFRs.
FDP_ITT.1_(IPSEC), FDP_IFC.1_(IPSEC), FCS_COP.1_(IPSEC-AES), FCS_COP.1_(IPSEC-HMAC), and FCS_CKM.4_(IPSEC) handle the IPsec functionality. They define the access methods, the security attributes, their management and cryptographic behaviour.
FDP_ITT.1_(IKE), FDP_IFC.1_(IKE), FDP_IFF.1_(IKE), FCS_CKM.1_(IKE-AES), FCS_COP.1_(IKE-AES), FCS_CKM.1_(IKE-ECDH), FCS_COP.1_(IKE-ECDH), FCS_CKM.1_(IKE-HMAC), FCS_COP.1_(IKE_HMAC), FCS_CKM.1_(IKE-ECDSA), FCS_COP.1_(IKE-ECDSA), FCS_CKM.4_(IKE), FMT_MSA.1_(IKE-A), FMT_MSA.1_(IKE-R), FMT_MSA.2_(IKE), FMT_MSA.3_(IKE), and FMT_SMF.1_(IKE) handle the IKE functionality. They define the access methods, the security attributes, their management and cryptographic behaviour.
FPT_ITT.1_(SSH), FDP_ITT.1_(SSH), FDP_IFC.1_(SSH), FDP_IFF.1_(SSH), FCS_CKM.1_(SSH-AES), FCS_COP.1_(SSH-AES), FCS_CKM.1_(SSH-ECDH), FCS_CKM.1_(SSH-UMAC), FCS_COP.1_(SSH-UMAC), FCS_CKM.1_(SSH-ECDSA), FCS_COP.1_(SSH-ECDSA), FCS_CKM.4_(SSH), FMT_MSA.1_(SSH-A), FMT_MSA.1_(SSH-R), FMT_MSA.2_(SSH), FMT_MSA.3_(SSH), and FMT_SMF.1_(SSH) handle the administrative SSH connections between genucenter and genuscreen. They define the access methods, the security attributes, their management and cryptographic behaviour.
FPT_TEE.1_(GEN) checks if the random numbers have a sufficient quality for cryptographic operations.
FCS_RNG.1 provides random input for cryptographic operations.

6.3.5 O.NOREPLAY

This objective is met by several groups of SFRs.
FDP_ITT.1_(IPSEC), FDP_IFC.1_(IPSEC), FCS_COP.1_(IPSEC-AES), FCS_COP.1_(IPSEC-HMAC), and FCS_CKM.4_(IPSEC) handle the IPsec functionality.
They define the access methods, the security attributes, their management and cryptographic behaviour.
FDP_ITT.1_(IKE), FDP_IFC.1_(IKE), FDP_IFF.1_(IKE), FCS_CKM.1_(IKE-AES), FCS_COP.1_(IKE-AES), FCS_CKM.1_(IKE-ECDH), FCS_COP.1_(IKE-ECDH), FCS_CKM.1_(IKE-HMAC), FCS_COP.1_(IKE_HMAC), FCS_CKM.1_(IKE-ECDSA), FCS_COP.1_(IKE-ECDSA), FCS_CKM.4_(IKE), FMT_MSA.1_(IKE-A), FMT_MSA.1_(IKE-R), FMT_MSA.2_(IKE), FMT_MSA.3_(IKE), and FMT_SMF.1_(IKE) handle the IKE functionality. They define the access methods, the security attributes, their management and cryptographic behaviour.
FPT_ITT.1_(SSH), FDP_ITT.1_(SSH), FDP_IFC.1_(SSH), FDP_IFF.1_(SSH), FCS_CKM.1_(SSH-AES), FCS_COP.1_(SSH-AES), FCS_CKM.1_(SSH-ECDH), FCS_CKM.1_(SSH-UMAC), FCS_COP.1_(SSH-UMAC), FCS_CKM.1_(SSH-ECDSA), FCS_COP.1_(SSH-ECDSA), FCS_CKM.4_(SSH), FMT_MSA.1_(SSH-A), FMT_MSA.1_(SSH-R), FMT_MSA.2_(SSH), FMT_MSA.3_(SSH), and FMT_SMF.1_(SSH) handle the administrative SSH connections between genucenter and the genuscreens. They define the access methods, the security attributes, their management and cryptographic behaviour.
FPT_TEE.1_(GEN) checks if the random numbers have a sufficient quality for cryptographic operations.
FCS_RNG.1 provides random input for cryptographic operations.

6.3.6 O.AUDREC

FAU_GEN.1EX_(AU), FAU_SAR.1_(AU), and FAU_SAR.3_(AU) handle the audit data generation and its review.
FMT_MOF.1_(GEN) and FMT_SMF.1_(GEN) define the security functions that can be configured by the administrators.
FMT_SMR.1_(GEN) defines the roles that can change the configuration.

6.3.7 O.AVAIL

FPT_TRC.1_(GEN) requires the synchronisation of *pf* states and IPsec security associations between HA peers. The synchronisation fulfils the availability requirements.

6.3.8 O.PATCH

The component FPT_UPD.1EX_(PI) defines the checks for authentic patches.
The component FPT_UPD.2EX_(PI) defines unique patch levels and its display.
The component FCS_COP.1_(PI) defines the cryptographic operations for patch signature verification.

6.4 Security Assurance Requirements Rationale

The overall security claim of this Security Target is aimed at EAL4.
The attack potential of the anonymous users is moderate. It must be noted, however, that the genuscreens are exposed to unrestricted attackers, simply because they are exposed to the Internet. Therefore the vulnerability analysis has been augmented to AVA_VAN.4 in order to match the resistance to attackers with a moderate attack potential.
For the same reason the TOE summary specification has been augmented to ASE_TSS.2. This augmentation explains the security architecture of the product.
The life cycle support has been augmented by ACL_FLR.2 to demonstrate genua's flaw handling procedures.
The component ALC_PAM.1 has been included in order to have a well defined, secure and correct patch generation process.
The new components are necessary, because application of patches has not been addressed by Common Criteria.
Table 6 lists the SAR dependencies. The table shows that all dependencies are met.

Table 6: SAR dependencies

ID	Requirement	Dependency	Solution
R01	ADV_ARC.1	ADV_FSP.1	R02
		ADV_TDS.1	R04
R02	ADV_FSP.4	ADV_TDS.1	R04
R03	ADV_IMP.1	ADV_TDS.3	R04
		ADV_TAT.1	R14
R04	ADV_TDS.3	ADV_FSP.4	R02
R05	AGD_OPE.1	ADV_FSP.1	R02

ID	Requirement	Dependency	Solution
R06	AGD_PRE.1	-	-
R07	ALC_CMC.4	ALC_CMS.1	R08
		ALC_DVS.1	R10
		ALC_LCD.1	R13
R08	ALC_CMS.4	-	-
R09	ALC_DEL.1	-	-
R10	ALC_DVS.1	-	-
R11	ALC_PAM.1	ALC_FLR.2	R12
R12	**ALC_FLR.2**	-	-
R13	ALC_LCD.1	-	-
R14	ALC_TAT.1	ADV_IMP.1	R03
R15	ASE_CCL.1	ASE_INT.1	R17
		ASE_ECD.1	R16
		ASE_REQ.1	R19
R16	ASE_ECD.1	-	-
R17	ASE_INT.1	-	-
R18	ASE_OBJ.2	ASE_SPD.1	R20
R19	ASE_REQ.2	ASE_OBJ.2	R18
		ASE_ECD.1	R16
R20	ASE_SPD.1	-	-
R21	**ASE_TSS.2**	ASE_INT.1	R17
		ASE_REQ.1	R19
		ADV_ARC.1	R01
R22	ATE_COV.2	ADV_FSP.2	R02
		ATE_FUN.1	R24
R23	ATE_DPT.1	ADV_ARC.1	R01
		ADV_TDS.2	R04
		ATE_FUN.1	R24
R24	ATE_FUN.1	ATE_COV.1	R22
R25	ATE_IND.2	ADV_FSP.2	R02
		AGD_OPE.1	R05
		AGD_PRE.1	R06
		ATE_COV.1	R22
		ATE_FUN.1	R24
R26	**AVA_VAN.4**	ADV_ARC.1	R01
		ADV_FSP.4	R02
		ADV_TDS.3	R04
		ADV_IMP.1	R03
		AGD_OPE.1	R05
		AGD_PRE.1	R06
		ATE_DPT.1	R23

7 TOE Summary Specification

7.1 TOE Summary Specification

7.1.1 SF_PF: Packet Filter

7.1.1.1 SF_PF.1: The genuscreen implement the flow control as routers or as bridges, on the network layer (IP) and transport layer (TCP/UDP/ICMP). The filter takes the information from the IP and TCP/UDP/ICMP header (where applicable) in order to apply the filter rules. The filter rules allow to filter by the criteria:

- address of source
- address of destination
- transport layer protocol
- interface on which traffic arrives and departs
- IP version (IPv4 or IPv6)
- differentiated services field

7.1.1.2 SF_PF.2: The genuscreen reassembles fragmented IP datagrams before further processing is performed on the data. IP datagrams which cannot be reassembled in a predefined span of time are dropped.

7.1.1.3 SF_PF.3: Packets with presumed spoofed source- or destination-IP addresses are dropped if the option is activated and spoofing recognition is possible. Packets with source routing options are dropped. No spoofing check is possible when the genuscreens operate as bridges.

7.1.1.4 SF_PF.4: The genuscreen can modify headers to make the information flows less susceptible to hijacking attacks.

This Security Function addresses the FDP_IFC.1_(FW) and FDP_IFF.1_(FW).

7.1.2 SF_NS Network Separation

7.1.2.1 SF_NS.1: The genuscreen implement the network separation with routing domains. All interfaces that are tagged with the same routing table index are part of the same routing domain. Routes for that routing domain determine how IP packets are forwarded.

7.1.2.2 SF_NS.2: A change in the routing domain for specific IP packets can be achieved by adding explicit *pf* rules.

7.1.2.3 SF_NS.3: Daemons that are configured for network interfaces in routing domains are put into the respective routing domain at boot time and during reconfiguration.

This Security Function addresses the SFRs FDP_IFC.2_(NS) and FDP_IFF.1_(NS).

7.1.3 SF_IPSEC: IPsec Filtering

7.1.3.1 SF_IPSEC.1: Connections between networks protected by different genuscreens can be protected by IPsec transforms against eavesdropping, modification and replay attacks. The transforms use the following probabilistic or permutational functions according to FIPS-197 NIST-SP800-38A and NIST-SP800-38D: AES block cipher in CBC or GCM mode with a key size of 128 bit, 192 bit, or 256 bit for confidentiality. For CBC mode the HMAC-SHA2-256 with a key size of 256 bit is used for integrity. ECDH with a key size of 256 bit is used for cryptographic key agreement, and ECDSA signatures with a key size of 256 bit for authentication. Expired keys are overwritten with zeros.
Application Note: IKEv1 allows only CBC mode in phase 1.

7.1.3.2 SF_IPSEC.2: If external certificates are used for IKEv2 authentication, the following optional steps are performed to check the validity of the certificates:

X.509 certificate: the certificate is checked for valid values for the following fields: certificate chain, name/alt name attribute, validity, extended attributes
OCSP: the online check of the certificate passes.

This Security Function addresses the SFRs FDP_ITT.1_(IPSEC), FDP_IFC.1_(IPSEC), FCS_COP.1_(IPSEC-AES), FCS_COP.1_(IPSEC-HMAC), FCS_CKM.4_(IPSEC), FDP_ITT.1_(IKE), FDP_IFC.1_(IKE), FDP_IFF.1_(IKE), FCS_CKM.1_(IKE-AES), FCS_COP.1_(IKE-AES), FCS_CKM.1_(IKE-ECDH), FCS_COP.1_(IKE-ECDH), FCS_CKM.1_(IKE-HMAC), FCS_COP.1_(IKE-HMAC), FCS_CKM.1_(IKE-ECDSA), FCS_COP.1_(IKE-ECDSA), FCS_CKM.4_(IKE), and FCS_RNG.1.

7.1.4 SF_SIP: SIP Relay

7.1.4.1 SF_SIP.1: The SIP relay module can be installed by a genucenter administrator. The software is transferred to all appliances that have the SIP relay configured. This requires a separate relay installation job.

7.1.4.2 SF_SIP.2: The SIP relay performs access control on the following parameters:

- internal and external SIP domain
- RTP port range
- IP ACL
- request method ACL

This Security Function addresses the FDP_IFC.1_(SIP) and FDP_IFF.1_(SIP).

7.1.5 SF_IA: Identification and Authentication

7.1.5.1 SF_IA.1: The TOE guarantees that the administrators, service users and revisors have to identify and authenticate to the genucenter GUI and the standalone GUI with a user name and password.

7.1.5.2 SF_IA.2: The genucenter and genuscreen administrative GUIs check the password quality of the genucenter administrators, the genucenter root administrators, the genucenter service users, the genucenter revisors, the genuscreen administrator and the genuscreen revisor: it must be at least 8 characters in length.

7.1.5.3 SF_IA.3: After 10 minutes of inactivity at the genucenter GUI, the administrators, service users and revisors must re-authenticate themselves.

This Security Function addresses the SFRs FDP_IFC.1_(ADM), FDP_IFF.1_(ADM), FIA_ATD.1_(IA), FIA_SOS.1_(IA), FIA_UAU.2_(IA), FIA_UAU.6_(IA), and FIA_UID.2_(IA).

7.1.6 SF_AU: Audit

7.1.6.1 SF_AU.1: The TOE shall generate audit records for

1. Starting of genuscreens
2. Datagrams received or sent through a genuscreen's network interfaces if they match configured patterns.

7.1.6.2 SF_AU.2: Each audit record shall include the following information:

1. Date and time
2. The affected genuscreen
3. The type of the event
4. The subject identity (source IP)

For log data of firewall rules, the following additional information shall be included:

1. The affected interface
2. Direction
3. Action (`pass` or `block`)
4. Optional further information, e.g. IP addresses and ports. This depend on the protocols.

7.1.6.3 SF_AU.3: The TOE shall provide the genucenter administrators, genucenter root administrators, the genucenter service users and the genucenter revisors with a display of audit data on the genucenter within their administrative domain. The audit data shall be searchable by

1. Date and time,
2. genuscreen that created the audit record,
3. For log data of firewall rules: IP addresses and ports, where applicable.

7.1.6.4 SF_AU.4: The TOE shall provide the genuscreen administrator, the genuscreen revisor and the genuscreen service user with a display of audit data on the genuscreens. The audit data shall be searchable by

1. Date and time
2. genuscreen that created the audit record,
3. For log data of firewall rules: IP addresses and ports, where applicable.

7.1.6.5 SF_AU.5: The TSF is allowed to drop log messages to maintain a defined behaviour if the log rate is larger than the following threshold: 30000 log messages per second. The number of dropped messages is logged by the genucenter.

This Security Function addresses the SFRs FAU_GEN.1EX_(AU), FAU_SAR.1_(AU), FAU_SAR.3_(AU).

7.1.7 SF_SSH: SSH Channel

7.1.7.1 SF_SSH.1: Connections between the genuscreens and the genucenter are protected by SSH transforms against eavesdropping, modification and replay attacks. The transforms use the following probabilistic or permutational functions.

Data encryption and decryption This operation uses an AES block cipher in CTR mode with a cryptographic key size of 128 bit, according to FIPS-197 [34], NIST-SP800-38A [35] and NIST-SP800-38D [36].

Cryptographic key agreement This operation uses the elliptic curve algorithm ecdh-sha2-brainpoolp256r1 with a key size of 256 bit, according to RFC5639 [30] and [31].

Generation and verification of message authentication code This operation uses the UMAC-128-ETM algorithm with a key size of 256 bit, according to RFC4418 [28].

Authentication This operation uses ECDSA signatures with a key size of 256 bit, according to [42].

7.1.7.2 SF_SSH.2: Expired keys are overwritten with zeros.

This Security Function addresses the SFRs FPT_ITT.1_(SSH), FDP_ITT.1_(SSH), FDP_IFC.1_(SSH), FDP_IFF.1_(SSH), FCS_CKM.1_(SSH-AES), FCS_COP.1_(SSH-AES), FCS_CKM.1_(SSH-ECDH), FCS_CKM.1_(SSH-UMAC), FCS_COP.1_(SSH-UMAC), FCS_CKM.1_(SSH-ECDSA), FCS_COP.1_(SSH-ECDSA), FCS_CKM.4_(SSH), and FCS_RNG.1.

7.1.8 SF_ADM: Administration

7.1.8.1 SF_ADM.1: The TOE allows the genucenter root domain administrators, the genucenter administrators, and the genucenter security administrators to change the IKE/IPsec configuration and the SSH configuration at the genucenter within their respective domain.
The TOE allows the genucenter root domain administrators, the genucenter administrators, and the genucenter operational administrators to change the packet filter configuration, the network separation (routing domain) configuration, and the SIP configuration at the genucenter within their respective domain.
The TOE allows the genuscreen administrator to change the IKE configuration, the packet filter configuration, and the network interface classification at the genuscreen.
The TOE allows the genucenter administrators and the genucenter root administrators to change the SSH configuration at the genucenter within their respective domain.
The TOE allows the genucenter service users and revisors to view the IKE configuration, the packet filter configuration, the network separation (routing domain) configuration, and the SIP configuration at the genucenter within their respective domain.

The TOE allows the genuscreen revisor to view the IKE configuration, the packet filter configuration the network separation (routing domain) configuration, and the SIP configuration at the genuscreen.
The TOE allows the genucenter service users and revisors to view the SSH configuration at the genucenter within their respective domain.

7.1.8.2 SF_ADM.2: The IKE configuration, the SSH configuration, and the packet filter configuration have restrictive defaults.
The network separation (routing domain) configuration has permissive defaults.

7.1.8.3 SF_ADM.3: The TOE allows the genucenter root domain administrators, the genucenter administrators, and the genucenter service users to transfer the configuration data to the genuscreens and to update software on the genuscreens within their administrative domain.

7.1.8.4 SF_ADM.4: The TOE allows the genucenter root domain administrators, the genucenter administrators, the genucenter service users, and the genucenter revisors to view the configuration and log data on the genucenter within their administrative domain.
The TOE allows the genuscreen administrator and the genuscreen revisor to view the configuration and log data on the genuscreen.

7.1.8.5 SF_ADM.5: The TOE allows the genucenter root domain administrators to alter the passwords for the genucenter administrators, the genucenter administrators, the genucenter service users, the genucenter revisors, the genuscreen administrator, and the genuscreen revisor at the genucenter.

7.1.8.6 SF_ADM.6: The TOE allows the genuscreen administrator to alter the passwords for the genuscreen administrator and the genuscreen revisor at the genuscreen.

This Security Function addresses the SFRs FMT_MSA.1_(FW-A), FMT_MSA.1_(FW-R), FMT_MSA.3_(FW), and FMT_SMF.1_(FW).
This Security Function addresses the SFRs FMT_MSA.1_(NS-A), FMT_MSA.1_(NS-R), FMT_MSA.3_(NS), and FMT_SMF.1_(NS).
This Security Function addresses the FMT_MSA.1_(IKE-A), FMT_MSA.1_(IKE-R), FMT_MSA.2_(IKE), FMT_MSA.3_(IKE), and FMT_SMF.1_(IKE).
This Security Function addresses the SFRs FMT_MSA.1_(SSH-A), FMT_MSA.1_(SSH-R), FMT_MSA.2_(SSH), FMT_MSA.3_(SSH), and FMT_SMF.1_(SSH).
This Security Function addresses the SFRs FMT_MSA.1_(SIP-A), FMT_MSA.1_(SIP-R), FMT_MSA.3_(SIP), and FMT_SMF.1_(SIP).
This Security Function addresses the SFRs FMT_MSA.1_(ADM-A), FMT_MSA.1_(ADM-R), FMT_MSA.1_(ADM-O), FMT_MSA.1_(ADM-ROOT), FMT_MSA.3_(ADM), and FMT_SMF.1_(ADM).

7.1.9 SF_GEN: General Management Facilities

7.1.9.1 SF_GEN.1: The TOE allows the genucenter administrators, the genucenter root administrators, and the genuscreen administrator to change the logging configuration and the reaction to the failed random number generator test.

7.1.9.2 SF_GEN.2: The TOE knows the following roles:

administrator Depending on the administrated system and/or administrative domain, this role is filled by the genucenter administrators, the genucenter root domain administrators, the genucenter root shell account, or the genuscreen administrator.
service This role is filled by the genucenter service users.
revisor Depending on the administrated system and/or the administrative domain, this role is filled by the genucenter revisors or the genuscreen revisor.

7.1.9.3 SF_GEN.3: The TOE runs a random number generator test at start-up. If the quality of the random numbers generated is not sufficient, it takes an action. The action contains two parts:

- create a log entry,
- and disable VPN operation.

7.1.9.4 SF_GEN.4: The program `sasyncd` synchronises the IPsec security associations between HA peers. The *pf* uses the `pfsync` interface to synchronise the *pf* states between HA peers. The granularity of this synchronisation are single *pf* states and single SAs. The data is transferred as clear text.
Application Note: **SF_GEN.4** only applies if the genuscreen HA setup is used.

This Security Function addresses the SFRs FMT_MOF.1_(GEN), FMT_SMF.1_(GEN), FMT_SMR.1_(GEN), FPT_TEE.1_(GEN), and FPT_TRC.1_(GEN).

7.1.10 SF_PI: Patch installation

7.1.10.1 SF_PI.1: The TOE shall verify the integrity of patches using RSA signatures with a key size of 4096 bit according to PKCS#1, v2.1 using RSASSA-PKCS1-v1_5 and SHA-512 (default), SHA-384 or SHA-256. The patches are signed during the patch generation process and the signature is checked during patch installation.

7.1.10.2 SF_PI.2: During installation of the patch the current patch level is stored on the system in a defined way.
Application Note: This part only applies to genucenter patches. The update process for genuscreen uses complete images.

This Security Function addresses the SFR: FPT_UPD.1EX_(PI), FPT_UPD.2EX_(PI), and FCS_COP.1_(PI).

7.2 Self-protection against interference and logical tampering

The product takes the following self-protection measures, supplied by the TOE:

- The configuration of the genuscreen from the genucenter uses SSH as a cryptographic measure. The SSH configuration inhibits eavesdropping, man-in-the-middle, and reply attacks.
- The collection of the log data from the genuscreen uses an SSH channel as a cryptographic measure. The SSH configuration inhibits eavesdropping, man-in-the-middle, and reply attacks.
- The ISAKMP daemon uses cryptographic measures for key exchange and data transmission. The IKE configuration inhibits eavesdropping, man-in-the-middle, and reply attacks.

The following self-protection measures are supplied by the environment:

- The OpenBSD kernel uses a randomized stack top, a stack canary to detect stack overflow, and exclusive write or executable memory segments (`W^X`) to mitigate exploits.
- The OpenBSD applications use a randomized stack top, a stack canary to detect stack overflow, and exclusive write or executable memory segments (`W^X`) to mitigate exploits. Further, they use random library memory locations, random `mmap` and `malloc` function results, a read-only data segment `.rodata` for constant data to mitigate exploits.
- The OpenBSD daemons use either privilege revocation or privilege separation if they temporary need enhanced privileges.
- Both the OpenBSD kernel and the core OpenBSD applications use the functions `strlcat` and `strlcpy` to replace `strncat` and `strncpy` that guarantee to null-terminate the result.
- The OpenBSD application use the `pledge` system call to minimize their usage of system calls.
- The servers and appliances implement the secure boot process with UEFI and coreboot (or other secure boot implementations) if supported by the underlying hardware.
- The OpenBSD based products use LibreSSL instead of OpenSSL.

The measures together build up a multilayered security barrier that results in a sufficient level of self-protection:

- The low level `strlcat` and `strlcpy` functions prohibit overwriting the allocated memory.
- The stack and memory protection mechanisms make it difficult to insert shell code.
- The privilege reduction functions inhibit a successful attacker to gain further privileges.

Further, encryption of the TOE data when it is transported over an insecure path prevent an attacker to obtain information for continued attacks.
The TOE supplies a configuration GUI that check the parameters entered in the HTML forms or passed through the REST API: This helps to mitigate misconfigurations by administrators. It also gives a clear user interface for the administrators, service users and revisors.

7.3 Self-protection against bypass

As the TOE is a firewall system, there can be no bypassing if it is installed properly. The assumption **A.SINGEN** reflects this.

8 Use of Cryptographic Functions

The use of cryptographic functions is summarised in table 7. Please note that the table does not contain functions to create and manage X.509 certificates for IKEv2 but only their usage.

Table 7: Cryptographic functions

No	Purpose	Cryptographic Mechanism	Standard of Implementation	Key Size in Bits	Security Level above 100 Bits
IPsec IKEv1/IKEv2					
1	Authentication	ECDSA-256	FIPS-186-4 [38], RFC4754 [16]	Key length = 256	yes
2	Key Agreement	256-bit random ECP group	RFC5114 [29], RFC5903 [17]	P length = 256	yes
3	Confidentiality	AES-128-CBC (phase 1), AES-128-GCM (phase 2)	FIPS-197 [34], NIST-SP800-38A [35], NIST-SP800-38D [36], RFC3602 [15]	|k| = 128, 192 or 256	yes
4	Integrity	HMAC-SHA2-SHA256 (for CBC mode)	FIPS-180-4 [39], RFC2104 [27], RFC4868 [24]	|k| = 256	yes
5	Trusted Channel	IKEv1, IKEv2 and IPsec	RFC2409 [21], RFC4301 [25], RFC4307 [41], RFC7296 [23]		n/a
SSH-2					
6	Authentication	ecdsa-sha2-nistp256	FIPS-186-4 [38], RFC6239 [22]	Key length = 256	yes
7	Key Agreement	ecdh-sha2-brainpoolp256r1	RFC5639 [30]	P length = 256	yes
8	Confidentiality	AES-192-CTR	FIPS-197 [34], NIST-SP800-38A [35], NIST-SP800-38D [36], RFC4344 [1]	|k| = 128, 192 or 256	yes
9	Integrity	umac-128-etm@openssh.com	RFC4418 [28]	|k| = 256	yes
10	Trusted Channel	SSH v2.0	RFC4253 [43] with the ETM extension		n/a

Patch Installation

11	Signature verification	RSASSA-PKCS1-v1_5 with SHA-521, SHA-384 or SHA-256	RFC8017 [33]	Key length = 256, 384 or 512	yes

A Evaluation Methology for ALC_PAM

A.1 Objectives

The objective of this sub-activity is to determine if the patch release process is sufficiently documented.

A.2 Input

The evaluation evidence for this sub-activity is:

a) the ST;

b) the operational user guidance;

c) documentation of the patch release process of the developer;

d) developer evidence documentation;

A.3 Action ALC_PAM.1.1E

ALC_PAM.1.1C ***The developer's patch management policies shall describe what is the criteria used for the decision that a patch has to be released.***

ALC_PAM.1-1 The evaluator shall check for the definition of criteria and check for the implementation as a policy. Example of a list of criteria:

- Complexity of backports
- Operational stability, development teams is able to estimate effect for operational stability
- security impact
- customer impact (i.e. practical problems, theoretical problems)
- timely impact, i.e. customer expect patches each quarter of a year, i.e. also minor security problems have to be fixed

ALC_PAM.1-2 The evaluator shall check the status of the implementation of the policies for patch releases and verify if the policies for patch releases have the same level of detail as other developer evidences provided for ALC.

ALC_PAM.1-3 The evaluator shall verify if the following mandatory policy content was implemented as policy:

- responsible roles for the final decision to release a patch
- unique label for each patch to identify all release items

ALC_PAM.1.2C ***The Security Target shall contain the estimated end-of-life of the TOE.***

ALC_PAM.1-4 The evaluator shall check for estimated TOE end-of-life information in the ST and for estimated TOE end-of-life information in user information material, i.e. the guidance, release notes, product (support) website.

ALC_PAM.1.3C ***The developer's patch management policies shall describe how to self-assess the security relevance of a patch (i.e. Security Impact Analysis Report, S-IAR) and which procedures have to apply due to which assessment result.***

ALC_PAM.1-5 The evaluator shall check if at least two assessment result categories were defined for patch management. For example:

- Category 1: no patch required
- Category 2: patch is required

ALC_PAM.1.4C ***The developer's patch management policies shall describe how to update the evidence documentation used in the base evaluation.***

ALC_PAM.1-6 The evaluator shall check if the patch management policies describe how to update the evidence documentation in a consistent way with the evaluation assurance level.

ALC_PAM.1.5C ***The developer's patch management policies shall describe how unhandled (potential) flaws are documented.***

ALC_PAM.1-7 The evaluator shall check the status of the implementation of the unhandled flaw documentation policy.

ALC_PAM.1.6C ***The developer's patch management policies shall describe which organisational role (or group) is responsible for the patch development.***

ALC_PAM.1-8 The evaluator shall check the organisational definitions and responsibilities of all roles involved in the patch development process. Examples for definitions of patch development responsibilities:

- patch development tasks as part of RACI matrix
- patch development tasks as function of a product development team

ALC_PAM.1.7C ***The developer's patch management policies shall describe which policies have to be applied until the end of life of the TOE during the patch management.***

ALC_PAM.1-9 The evaluator shall check for the implementation of internal policies that have to be applied during TOE maintenance. Examples for policies regarding 3rd party libraries:

- update only libraries that are still supported as well
- backport latest changes to used library version
- upgrade to latest library version

ALC_PAM.1.8C ***Each tool used for the patch management shall be documented.***

ALC_PAM.1-10 The evaluator shall check the list of tools the developer uses for patch management.

ALC_PAM.1.9C ***The patch management policies shall describe the mandatory structure and content of the S-IAR.***

ALC_PAM.1-11 The evaluator shall check the format of the S-IAR used by the developer. Mandatory elements of the S-IAR are:

- Description how to use bug tracker information for the S-IAR
- Security relevance criteria: e.g. remote execution, only product type specific
- Category criteria: e.g. CWE (common weakness enumeration)

ALC_PAM.1.10C ***Each type of documentation used to record decisions in the patch management process shall be documented.***

ALC_PAM.1-12 The evaluator shall check if the patch management policies describe how to record decisions.

ALC_PAM.1.11C ***The patch management policies shall describe the mandatory content of patch release notes.***

ALC_PAM.1-13 The evaluator shall check if the patch management policies contain the elements that shall be mandatory in a developer's patch release notes.

ALC_PAM.1.12C ***The patch management policies shall describe the mandatory content for the guidance documents which have to be fulfilled to support the installation of the patch.***

ALC_PAM.1-14 The evaluator shall check the developer's patch management policies for release note or update guidance requirements (e.g. checklist for steps to describe during patch installation).

ALC_PAM.1.13C ***The patch management policies shall describe the mandatory procedures during patch release.***

ALC_PAM.1-15 The evaluator shall check the developer's patch management policies for mandatory patch release procedures. Examples:

- procedure steps for (patch) release: Build → QA test → HW integration test → Release
- process definition should contain the failure of test/validation steps and how to handle these cases

ALC_PAM.1.14C ***The patch management policies shall contain rules in which case the evaluation facility has to perform additional tests before the patch is released.***

ALC_PAM.1-16 The evaluator shall check the developer's patch management policies for rules that require testing of the evaluation facility.

- e.g. ruleset for different acting roles in the (patch) release procedure
- relevant roles: development, QA department, product owner, etc.

- hardware release decisions that require software updates in the drivers for the new hardware.

ALC_PAM.1.15C ***The patch management policies shall describe how each of the patch management Security Objectives for the Operational Environment are fulfilled until the end of life of the TOE.***

ALC_PAM.1-17 The evaluator shall check the developer's patch management policies for a description of how the Patch Management Security Objectives are fulfilled.

ALC_PAM.1-18 The evaluator shall verify if the patch management processes address the following requirements:

- How the cryptographic keys involved in signing and/or distributing patches are generated and managed during its entire life-cycle so they have enough strength to protect the authenticity of the updates.
  - How the cryptographic keys are created
  - How the cryptographic keys are securely stored
  - The process for revocation and loading of a new cryptographic key if it is compromised
  - How the cryptographic keys are destroyed or archived at the end-of-life of the product
- The process for approving, signing and releasing new updates in a secure and audited environment.
  - Who approves the releasing of updates
  - Who can access the cryptographic keys used for signing updates
  - How the update is moved from the development environment to the signing environment so that it is not tampered
  - How this process generates logs
  - How this logs are audited
- How the user is notified of the availability of a new patch due to a security issue:
  - Through email
  - Through automatic checks to a website handled by the product
- How the patches are made available and securely distributed to the end user
  - Uploaded to a website by the developer and automatically downloaded by the TOE by using an appropriate and declared security protocol
- Sent to the end-user using delivery services and providing installation instructions where administrator rights must be implemented using password/authentication codes and/or cryptographic authentication techniques

A.4 Implied evaluator action ALC_PAM.1.2D

ALC_PAM.1.2D ***The developer shall self-assess and confirm the application of existing policies on a regular basis saving records of its application.***

ALC_PAM.1-19 The evaluator shall verify evidences of developer's self-assessment procedures.

ALC_PAM.1-20 The evaluator shall check if results or evidences for the self-assessment can be presented. For example:

- publication of developer self-declaration with reference to product certification ID
- internal (or external) audit report, in general annual audit

ALC_PAM.1-21 The evaluator shall check if existing unhandled flaw documentation exists and if these fulfil the policy requirements.

ALC_PAM.1-22 The evaluator shall check if decisions in the patch management process were documented.

ALC_PAM.1-23 The evaluator shall check the patch release notes for the content elements required by the patch management policies.

ALC_PAM.1-24 The evaluator shall select and examine a sample of evidence covering each type of relevant event (e.g. signing logs, approval of updates, S-IAR, fulfilled checklists, bug tracker evidence...) to confirm that all operations of the patch management policies and procedures are carried out in line with the documentation. The evaluator may choose to sample the evidence.

- For guidance on sampling see ISO/IEC 18045, A.2, Sampling.
- Further confidence in the correct operation of the patch management policies and procedures may be established by means of interviews with selected development staff. Note that such interviews should complement rather than replace the examination of documentary evidence, and may not be necessary if the documentary evidence alone satisfies the requirement.
- The evaluator may visit the development site in support of this activity.
- For guidance on site visits see ISO/IEC 18045, A.4, Site Visits.

A.5 Implied evaluator action ALC_PAM.1.3D

ALC_PAM.1.3D ***The developer shall provide security patches using the defined policies and procedures at least until the estimated end-of-life of the TOE.***

ALC_PAM.1-25 The evaluator shall examine aspects of the patch management procedure to determine that the patch management procedures are being used.

- In addition to examination of the procedures themselves, the evaluator seeks some assurance that they are applied in practise. Some possible approaches are:
  - a visit to the development site(s) where practical application of the procedures may be observed;

  - observing that the process is applied in practise when the evaluator obtains new updates solving the vulnerabilities found during the Vulnerability Analysis.
- If a Site Visit is already included in the evaluation plan, the evaluator shall apply option (a) to check that the processes are applied in practice.
- For guidance on site visits see A.4, Site Visits.

B Abbreviations

AES Advanced Encryption Standard
API Application Programming Interface
Basic-auth Basic Access Authentication, RFC 7617
CA Certification Authority
CBC Cipher Block Chaining (a block cipher mode of operation)
CTR Counter (a block cipher mode of operation)
CWE Common Weakness Enumeration
DH Diffie-Hellman
ECDH Elliptic Curve Diffie-Hellman
ECP Group Elliptic Curve Groups modulo a Prime
ECDSA Elliptic Curve Digital Signature Algorithm
ESP Encapsulated Security Payload
ETM Encrypt Then MAC
FTP File Transfer Protocol.
GUI Graphical User Interface
HA High Availability
HMAC Hashed Message Authentication Code
HTTP Hypertext Transfer Protocol
IKE Internet Key Exchange
IP Internet Protocol
IPsec Internet Protocol Security protocol suite
ISAKMP Internet Security Association Key Management Protocol
JSON JavaScript Object Notation
L2TP Layer 2 Tunneling Protocol
LDAP Lightweight Directory Access Protocol
NAT Network address translation
OCSP Online Certificate Status Protocol
OSPF Open Shortest Path First
PFS Perfect Forward Secrecy
PXE Preboot eXecution Environment
SCEP Simple Certificate Enrollment Protocol
RACI Responsible, Accountable, Consulted, Informed
RDR Redirect rule
REST Representational state transfer
RFC Request for comment
RSA Rivest Shamir Adleman
RTP Real-Time Transport Protocol
SA Security Association
SBC Session Border Controller
SHA Secure Hash Algorithm
SIP Session Initiation Protocol
SSH Secure Shell
TCP Transmission Control protocol

TOE Target of Evaluation
UDP User Datagram Protocol
UMAC Universal Hashing Message Authentication Code

C References

[1] M. Bellare, T. Kohno, and C. Namprempre. The Secure Shell (SSH) Transport Layer Encryption Modes. RFC 4344, Internet Engineering Task Force, January 2006. http://www.ietf.org/rfc/rfc4344.txt.

[2] U. Blumenthal and B. Wijnen. User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3). RFC 3414, Internet Engineering Task Force, December 2002. Updated by RFC 5590. http://www.ietf.org/rfc/rfc3414.txt.

[3] Bundesamt für Sicherheit in der Informationstechnik. Technische Richtlinie TR-02102-3 – Kryptographische Verfahren: Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2). Version 2021-01.

[4] Bundesamt für Sicherheit in der Informationstechnik. Anwendungshinweise und Interpretationen zum Schema (AIS) AIS 20. Technical report, Bundesamt für Sicherheit in der Informationstechnik, Bonn, Germany, 15. Mai 2013. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_20_pdf.html.

[5] Bundesamt für Sicherheit in der Informationstechnik. Anwendungshinweise und Interpretationen zum Schema (AIS) AIS 31. Technical report, Bundesamt für Sicherheit in der Informationstechnik, Bonn, Germany, 15 .Mai 2013. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_pdf.html.

[6] Common Criteria. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, Version 3.1 Revision 5. Technical report, Common Criteria, April 2017. CCMB-2017-04-001.

[7] Common Criteria. Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components, Version 3.1 Revision 5. Technical report, Common Criteria, April 2017. CCMB-2017-04-002.

[8] Common Criteria. Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components, Version 3.1 Revision 5. Technical report, Common Criteria, April 2017. CCMB-2017-04-003.

[9] Common Criteria. Common Methodology for Information Technology Security Evaluation, Evaluation methodology, Version 3.1 Revision 5. Technical report, Common Criteria, April 2017. CCMB-2017-04-004.

[10] Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. Version 3.1, Revision 5, September 2017.

[11] Common Criteria for Information Technology Security Evaluation. Part 2: Security functional components. Version 3.1, Revision 5, September 2017.

[12] Common Criteria for Information Technology Security Evaluation. Part 3: Security assurance components. Version 3.1, Revision 5, September 2017.

[13] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. RFC 5280, Internet Engineering Task Force, May 2008. Updated by RFC 6818. http://www.ietf.org/rfc/rfc5280.txt.

[14] S. Deering and R. Hinden. Internet Protocol, Version 6 (IPv6) Specification. RFC 2460, Internet Engineering Task Force, December 1998. Updated by RFCs 5095, 5722, 5871, 6437, 6564, 6935, 6946, 7045, 7112. http://www.ietf.org/rfc/rfc2460.txt.

[15] S. Frankel, R. Glenn, and S. Kelly. The AES-CBC Cipher Algorithm and Its Use with IPsec. RFC 3602, Internet Engineering Task Force, September 2003. http://www.ietf.org/rfc/rfc3602.txt.

[16] D. Fu and J. Solinas. IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA). RFC 4754, Internet Engineering Task Force, January 2007. http://www.ietf.org/rfc/rfc4754.txt.

[17] D. Fu and J. Solinas. Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2. RFC 5903, Internet Engineering Task Force, June 2010. http://www.ietf.org/rfc/rfc5903.txt.

[18] genua GmbH. genucenter Installations- und Konfigurationshandbuch, Version 8.0, 2023.

[19] genua GmbH. genuscreen Installations- und Konfigurationshandbuch, Version 8.0, 2023.

[20] W. Hardaker. Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP). RFC 6353, Internet Engineering Task Force, July 2011. http://www.ietf.org/rfc/rfc6353.txt.

[21] D. Harkins and D. Carrel. The Internet Key Exchange (IKE). RFC 2409, Internet Engineering Task Force, November 1998. Obsoleted by RFC 4306, updated by RFC 4109. http://www.ietf.org/rfc/rfc2409.txt.

[22] K. Igoe. Suite B Cryptographic Suites for Secure Shell (SSH). RFC 6239, Internet Engineering Task Force, May 2011. http://www.ietf.org/rfc/rfc6239.txt.

[23] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, and T. Kivinen. Internet Key Exchange Protocol Version 2 (IKEv2). RFC 7296, Internet Engineering Task Force, October 2014. Updated by RFC 7427. http://www.ietf.org/rfc/rfc7296.txt.

[24] S. Kelly and S. Frankel. Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec. RFC 4868, Internet Engineering Task Force, May 2007. http://www.ietf.org/rfc/rfc4868.txt.

[25] S. Kent and K. Seo. Security Architecture for the Internet Protocol. RFC 4301, Internet Engineering Task Force, December 2005. Updated by RFC 6040. http://www.ietf.org/rfc/rfc4301.txt.

[26] Wolfgang Killmann and Werner Schindler. A proposal for: Functionality classes for random number generators. Technical report, Bundesamt für Sicherheit in der Informationstechnik, Bonn, Germany, 18. September 2011. Version 2.0. https://www.bsi.bund.de/SharedDocs/

Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_Functionality_classes_for_random_number_generators_e.pdf?__blob=publicationFile.

[27] H. Krawczyk, M. Bellare, and R. Canetti. HMAC: Keyed-Hashing for Message Authentication. RFC 2104, Internet Engineering Task Force, February 1997. Updated by RFC 6151. http://www.ietf.org/rfc/rfc2104.txt.

[28] T. Krovetz. UMAC: Message Authentication Code using Universal Hashing. RFC 4418, Internet Engineering Task Force, March 2006. http://www.ietf.org/rfc/rfc4418.txt.

[29] M. Lepinski and S. Kent. Additional Diffie-Hellman Groups for Use with IETF Standards. RFC 5114, Internet Engineering Task Force, January 2008. http://www.ietf.org/rfc/rfc5114.txt.

[30] M. Lochter and J. Merkle. Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation. RFC 5639, Internet Engineering Task Force, March 2010. http://www.ietf.org/rfc/rfc5639.txt.

[31] Manfred Lochter. ECC Brainpool - ECC Brainpool Standard Curves and Curve Generation, Oktober 2005. http://www.ecc-brainpool.org/download/Domain-parameters.pdf.

[32] D. Miller and P. Valchev. The use of UMAC in the SSH Transport Layer Protocol. Internet draft, Network Working Group, September 3 2007. https://tools.ietf.org/html/draft-miller-secsh-umac-01.

[33] Kathleen M. Moriarty, Burt Kaliski, Jakob Jonsson, and Andreas Rusch. PKCS #1: RSA Cryptography Specifications Version 2.2. *RFC*, 8017:1–78, 2016. https://doi.org/10.17487/RFC8017, doi:10.17487/RFC8017.

[34] NIST. Announcing the ADVANCED ENCRYPTION STANDARD (AES). Federal Information Processing Standards 197, U.S. Department of Commerce / National Institute of Standards and Technology, 26. November 2001. http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.

[35] NIST. Recommendation for Block Cipher Modes of Operation – Modes and Techniques. Special Publication 800-38A, U.S. Department of Commerce / National Institute of Standards and Technology, 2001. http://dx.doi.org/10.6028/NIST.SP.800-38A.

[36] NIST. Recommendation for Block Cipher Modes of Operation – Galois/Counter Mode (GCM) and GMAC. Special Publication 800-38D, U.S. Department of Commerce / National Institute of Standards and Technology, November 2007. http://dx.doi.org/10.6028/NIST.SP.800-38D.

[37] NIST. Digital Signature Standard (DSS). Federal Information Processing Standards 186-3, U.S. Department of Commerce / National Institute of Standards and Technology, Juny 2009.

[38] NIST. Digital Signature Standard (DSS). Federal Information Processing Standards 186-4, U.S. Department of Commerce / National Institute of Standards and Technology, July 2013. doi:10.6028/NIST.FIPS.186-4.

[39] NIST. Secure Hash Standard (SHS). Federal Information Processing Standards 180-4, U.S. Department of Commerce / National Institute of Standards and Technology, August 2015. doi:10.6028/NIST.FIPS.180-4.

[40] S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin, and C. Adams. X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. RFC 6960, Internet Engineering Task Force, June 2013. http://www.ietf.org/rfc/rfc6960.txt.

[41] J. Schiller. Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2). RFC 4307, Internet Engineering Task Force, December 2005. http://www.ietf.org/rfc/rfc4307.txt.

[42] D. Stebila and J. Green. Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer. RFC 5656, Internet Engineering Task Force, December 2009. http://www.ietf.org/rfc/rfc5656.txt.

[43] T. Ylonen and C. Lonvick. The Secure Shell (SSH) Transport Layer Protocol. RFC 4253, Internet Engineering Task Force, January 2006. Updated by RFC 6668. http://www.ietf.org/rfc/rfc4253.txt.