IBM WebSphere DataPower Firmware Version 6.0.2.0 Security Target

Version:	**1.42**
Status:	**Final**
Last Update:	**2015-03-13**
Classification:	**Public**

Trademarks

IBM and the IBM logo are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

The following terms are trademarks of International Business Machines Corporation in the United States, other countries, or both:

- DataPower®
- IBM®
- WebSphere
- Tivoli®

ClearTrust is a registered trademark of RSA Security Inc.

Netegrity SiteMinder is a registered trademark of Computer Associates Inc.

Other company, product, and service names may be trademarks or service marks of others.

Legal Notice

This document is provided AS IS with no express or implied warranties. Use the information in this document at your own risk.

This document may be reproduced or distributed in any form without prior permission provided the copyright notice is retained on all copies. Modified versions of this document may be freely distributed provided that they are clearly identified as such, and this copyright is included intact.

Revision History

Revision	Date	Author(s)	Changes to Previous Revision
1.42	2015-03-03	Alejandro Masino	Public version.

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 Security Target Identification

Title:	IBM WebSphere DataPower Firmware Version 6.0.2.0 Security Target
Version:	1.42
Status:	Final
Date:	2015-03-13
Sponsor:	IBM Corporation
Developer:	IBM Corporation
Certification Body:	BSI
Certification ID:	BSI-DSZ-CC-0901
Keywords:	WebSphere, DataPower, Service Gateway, Integration Appliance, B2B Appliance

1.2 TOE Identification

This ST is applicable to the following TOEs:

- IBM WebSphere DataPower Service Gateway XG45 Firmware Version 6.0.2.0.
- IBM WebSphere DataPower Integration Appliance XI52 Firmware Version 6.0.2.0.
- IBM WebSphere DataPower B2B Appliance XB62 Firmware Version 6.0.2.0.

1.3 TOE Type

The TOE type is a set of applications in the network appliance firmware that provides application-level firewall, web service proxy, and message content transformation functionality.

1.4 TOE Overview

The TOE combined with its underlying operating system and hardware is a network appliance that provides application-level firewall functionality, web service proxy functionality, and message content transformation functionality.

The network appliance is used in the following scenarios:

- In the demilitarized zone (DMZ) between an enterprise and external partners, where the network appliance performs primarily security services (e.g. enforcement of security policies on incoming and outgoing traffic, message content transformation or multiprotocol bridging).
- Within the enterprise as an enterprise service bus (ESB), interconnecting disparate enterprise assets in a meaningful way (e.g message routing, multiprotocol bridging or message content transformation).

The TOE does not support clustering; in case several network appliances are used in the operational environment, each network appliance works independently from the other.

The flexibility of the configuration of the network appliance allows an enterprise to deploy a network appliance in scenarios requiring interoperability with a wide range of enterprise assets, such as:

- Authentication systems
- Databases
- Mainframe applications

- Diverse message transport systems
- Web service applications
- Web sites

The network appliances are self-contained, rack mount units with each containing a motherboard with a serial communication connector, flash memory for persistent storage, a Redundant Array of Independent Disks (RAID) for persistent storage, a power switch, a "case opened" relay sensor, a clock, and a Network Interface Card (NIC) containing multiple Ethernet connectors including separate Ethernet management connectors for managing the appliance.

The network appliance firmware contains an embedded operating system, an Secure Shell (SSH) daemon, an application called "Router", and a Watchdog application. The Router application and SSH daemon enforce all of the claimed security functionality.

The TOE consists of the Oversight subsystem (which includes the Watchdog application), the Router subsystem and the SSH daemon subsystem. All hardware and the remaining firmware are part of the Operational Environment.

The network appliance is managed by connecting a computer to the appliance through the appliance's serial connector and/or through one of the appliance's Ethernet management connectors. The Router application provides all of the administrative management functionality.

There are three variations of the TOE that are included in this Security Target (ST); each TOE provides similar security functionality and corresponds to the IBM products described below:

- The **DataPower Service Gateway XG45** is a lightweight, level entry network appliance shipped in a 1U rack system that provides the following:
  - Web service proxy.
  - Application level firewall based on information flow control policy based on protocol information, message content, and identity assertions (authentication).
  - Message content transformation based on XML Path Language (XPath) and XML Stylesheet Language Tranformations (XSLT).
- The **DataPower Integration Appliance XI52** offers all the functionality provided by the XG45 but in a more powerful 2U rack system. In addition, it provides support for more message formats and more connectivity options (not included in the evaluated configuration).
- Finally, the **DataPower B2B Appliance XB62** runs in a 2U rack system and provides business to business (B2B) functionality in addition to the features included in the XG45 and XI52 models. It supports B2B messaging protocols such as AS1, AS2, AS3 and ebMS (not included in the evaluated configuration).

1.4.1 Required and optional non-TOE hardware, software and firmware

The hardware upon which the TOE executes is part of the Operational Environment. Each of the TOEs that are part of this evaluation requires the following network appliance hardware models:

- IBM WebSphere DataPower Service Gateway XG45 Firmware: Type 7198
- IBM WebSphere DataPower Integration Appliance XI52 Firmware: Type 7199
- IBM WebSphere DataPower B2B Appliance XB62 Firmware: Type 7199

Only these models are allowed in the evaluated configuration.

There is one firmware binary version for each TOE.

The operating system upon which the TOE executes is part of the Operational Environment. The operating system for the TOE is packaged with the TOE as part of the firmware package and is required by the evaluated configuration.

To manage the TOE, at least one additional computer must exist in the Operational Environment and must be connected to the network appliance either through the serial connector or through an Ethernet management connector. To manage the TOE using the appliance's serial connector, an ASCII terminal or a computer running a terminal emulation program must be used. The serial connection must be always used to perform the initial configuration of the TOE. To manage the TOE using one or more computers connected to the appliance's Ethernet management connectors, the computers must run an SSH client that supports SSH/SCP version 2.

In addition, the operational environment may include one or more systems against which the TOE can connect to enforce certain authentication and authorization rules defined in the information flow policies. Such authentication and authorization systems include:

- LDAP server
- RADIUS server
- SAML responder

These systems must be trusted, and communication between them and the TOE must be protected.

1.4.2 Intended method of use

The TOE is intended to be used in a distributed, non-hostile environment with a well-managed user community. Logically, the network appliance running the TOE resides either between clients and backend servers of an organization or between the organization's backend servers. Physically, the network appliance running the TOE must be located in a protected environment (e.g., server room) where only trusted administrators have physical access to the hardware.

Additional systems that provide authentication and/or authorization services to the TOE must also be located in a protected environment and managed by trusted administrators. Integrity and confidentiality of the communication with the TOE must also be ensured.

Administrators manage the TOE by connecting an additional computer with a terminal emulator or a terminal to the console through the serial line, and/or by connecting one or more computers to the network management connectors. The TOE uses network security protocols (i.e., SSH version 2) to protect the network data when using the network management connectors; for the serial line, there is no such protection and the console must be established in a physically protected environment.

Administrators of the TOE and its operational environment are assumed to be trustworthy, trained and to follow the instructions provided to them with respect to the secure configuration and operation of the systems under their responsibility. Only inadvertent attempts to manipulate the secure operation of the TOE are expected from this community.

1.4.3 Major security features

The major security features of the TOE are:

- Security auditing – providing client access request outcomes and administrator accountability through event generation, storage, and review (e.g., information flow, security management, user login).

- Cryptographic support – protecting communications between the TOE and remote systems (including administrative interfaces) through the use of the Transport Level Security version 1.2 (TLSv1.2) and Secure Shell version 2 (SSH-2) protocols and performing policy processing by generating and validating digital signatures, generating and validating extensive markup language (XML) signatures, and encrypting and decrypting messages.
- Identification and authentication (I&A) – supporting the I&A of administrative users with username and password as credentials, password policy enforcement and account blocking after a maximum number of attempts.
- User data protection – enforcing security policies that are used to control the flow of messages (network traffic) between systems; and enforcing security policies to control access to security management functions and objects in application domains.
- Security management – allowing administrators to administer the information flow control policy; maintain administrators and their roles; specify the password quality for authentication; and maintain digital certificates and cryptographic keys.
- Protection of the TOE security functionality - interpreting digital certificates for secure communication and providing reliable timestamps.
- Trusted channel – protecting the communication from modification and disclosure between the TOE and the application endpoints (through the use of TLS and SSH) and the TOE and its administrative interfaces (through the use of SSH).

1.5 TOE Description

1.5.1 Introduction

The TOE is a set of applications in the firmware that provides application-level firewall functionality, web service proxy functionality and service integration functionality. The TOE consists of the following subsystems:

- Oversight subsystem
- Router subsystem
- SSH daemon subsystem

The above applications are also considered the logical boundary of the TOE.

The TOE runs on top of an embedded, optimized DataPower Operating System version 7 that is included in the firmware package. The operating system, as well as the underlying hardware, are part of the Operational Environment.

Figure 1 shows the logical relationship of the TOE to the network appliance's Operational Environment. The TOE is shown in grey.

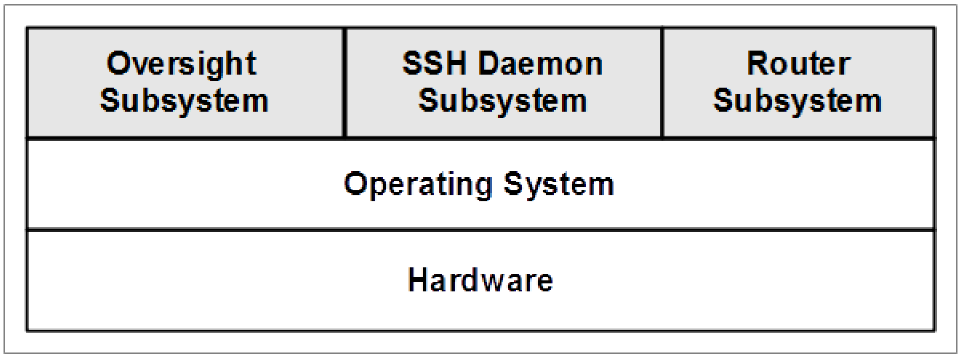

Figure 1: TOE and Operational Environment logical boundary

The Oversight subsystem initializes processes and monitors the Router application to ensure that it is always running.

The Router subsystem performs the vast majority of the security functionality. It implements the firewall and enforces the firewall policies. It implements web service proxy features by enforcing information flow control policies, and it provides a command-line interface (CLI) administrative interface.

The information flow control security policies are supported on a complex data model that can be configured by administrators to meet business needs with great flexibility. Administrators can create services using specific protocol handlers that manage communication with external IT entities, rules defining conditions (structure of the message payload, threshold for certain message properties, authentication and authorization mechanisms, validation of signatures) an incoming message needs to meet in order to proceed with its routing, and processing rules that can perform data transformations of the incoming message before being sent to the target IT entity. Additionally, these information flow control security policies can be created system wide or in the context of or one or more application domains (an application domain is an environment that allows the partition of the TOE in separate parts for a better administration of the different applications using the same appliance).

The TOE supports multiple administrative user accounts and multiple roles, that can be configured with system wide or application domain scope. The TOE enforces identification and authentication of all administrative users.

Administrators perform management tasks through a Command Line Interface (CLI). Administrators connect to the TOE either through the network appliance's Console connector (an RJ45 serial connector supporting RS-232c) or over the network appliance's Ethernet management connectors (MGT0 and MGT1) using TCP/IP. The Ethernet management connectors support the CLI over a SSH connection, which is provided through the SSH daemon subsystem. Secure Copy (SCP) is also supported via the SSH protocol.

Note: *A Web-based Graphical User Interface (WebGUI) is also available for management purposes but it is disabled by default and not allowed in the evaluated configuration.*

The Ethernet management connectors are electronically separate from other Ethernet data connectors on the network appliance to ensure that the management interfaces remain isolated from the Ethernet data connectors. The other Ethernet data connectors are used to connect the client system networks and the backend server networks to the network appliance. See Figure 2 and Figure 3 for a visual representation of the connectors. The letter labels in the figure are defined below the figure.

The administrative interfaces allow administrative users to manage the information flow policies enforced by the TOE, to manage administrative user accounts, to manage auditing, and to manage other aspects of the network appliance.

The IBM WebSphere DataPower Service Gateway XG45 Firmware is shipped in the Type 7198 hardware model, a 1U rack mountable appliance that has four 1Gb ethernet connections and two 10Gb ethernet connections. Figure 2 shows its front view.

The IBM WebSphere DataPower Integration Appliance XI52 Firmware and IBM WebSphere DataPower B2B Appliance XB62 Firmware come in multiple hardware models, but only the Type 7199 model is allowed in the evaluated configuration. This model is a 2U rack mountable appliance that has eight 1Gb ethernet connections and two 10Gb ethernet connections. Figure 3 shows its front view.

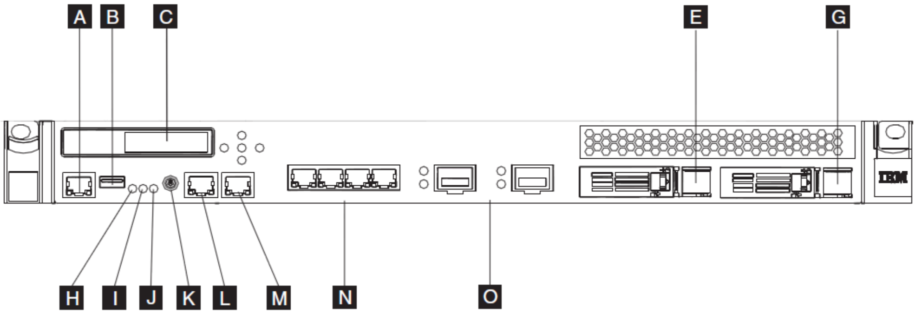

Figure 2: Type 7198 appliance front view

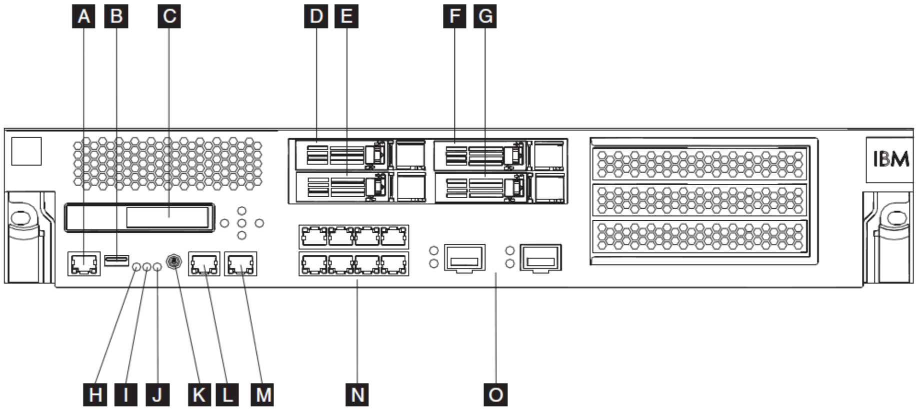

Figure 3: Type 7199 appliance front view

References:

A Console connector (RJ45 serial connector)
B USB port
C LCD module

D	Hard disk drive module 2
E	Hard disk drive module 0
F	Hard disk drive module 3
G	Hard disk drive module 1
H	Fault LED
I	Locate LED
J	Power LED
K	Power button
L	MGT0 Ethernet management connector
M	MGT1 Ethernet management connector
N	Left Ethernet modules (eight 1 GbE) (a.k.a. Ethernet data connectors)
O	Right Ethernet modules (two 10 GbE) (a.k.a. Ethernet data connectors)

1.5.2 Security features

1.5.2.1 Security auditing

The TOE records security relevant events in an audit trail. The events include user management, security function management, user identification, and all requests and decisions for information flow. Administrators can set the level of audit to define which audit events are generated by the TOE.

The audit trail is protected from unauthorized modification and deletion, and can only be reviewed by authorized administrators. The TOE also prevents any auditable information flow events in the case that the trail is full.

In addition, the operational environment provides reliable timestamps for the TOE's audit records.

1.5.2.2 Cryptographic support

The TOE implements cryptographic functionality to support secure communications over the Ethernet management connectors. The TOE supports TLSv1.2 for the web browser-based administrative interface (not part of the evaluated configuration), as well as SSH version 2 for the SSH client-based administrative CLI.

The TOE's cryptographic functionality is also used during policy processing to validate cryptographic operations, such as to establish secure communications using TLSv1.2 or SSH-2, to sign and validate digital signatures and to encrypt and decrypt messages.

1.5.2.3 Identification and authentication

The TOE supports different methods for identification and authentication of user administrators (e.g. LDAP, Radius, using an SSL certificate, etc.), but only the local authentication method, which is described below, is allowed in the evaluated configuration.

The TOE maintains administrator accounts that include identity attributes (name and password) and role attributes. The TOE identifies and authenticates administrators using the administrator name and password. The TOE tracks the number of authentication attempts and, after a configured number of failures defined by an authorized administrator, the TOE disables that account. Disablement prevents any use of that account for operations on the TOE. The account is reset (re-enabled) under control of an authorized administrator. (The TOE includes no "user" accounts. Any reference to "user" in the customer documentation should be construed as meaning "administrator".)

The TOE also supports the configuration of a password policy with the following properties: minimum length, use of digits, use of mixed case characters, use of non-alphanumeric characters, password history to avoid reuse, and the number of history passwords retained.

In addition, the TOE blocks an account after the user exceeds a configurable maximum attempt threshold, and terminates all administrator interactive sessions after an administrator-specified period of time.

1.5.2.4 User data protection

The TOE allows authorized administrators to configure policies that are used to control the flow of incoming and outgoing messages (network traffic) based on a set of attributes (see section 7.1.3 for a detailed list). If the values obtained from the message do not match any of the policies, or the message content does not conform to the corresponding protocol then the message is rejected.

Identity assertions can be part of the information control flow policy definition. The TOE can be configured to extract identity information from incoming messages and perform authentication and/or authorization, either internally (e.g. verifying the validity of a certificate or a credential against an internal XML file) or through a service provided by an authentication or authorization system (e.g., RADIUS or LDAP server).

The TOE also manages the concept of application domains, which allows the creation of separate environments in the TOE for better administration of the information flow control policies the TOE provides, and the separation of duties and information between global and application level administrators. After an administrator switches into one of the application domains that is authorized to, all configuration activities apply to only this application domain and access to directories and files are restricted based on predefined and/or configurable permissions on the domain directories.

The TOE enforces access control on files and directories defined in the system wide domain (default domain) and the application domains created by administrators. Each domain has a predefined directory structure: each directory has a specific purpose and has its own permission mask for file and directory operations (e.g., the audit: directory is for generating audit events and has read-only access). The only exception is the application domain local: directory, where administrators can configure its file permissions.

1.5.2.5 Security management

The TOE provides security management functionality for the management of several TOE security functions. The security management functionality includes

- set the time and date;
- specify the number of failed authentication attempts for account blocking;
- specify the password policy;
- manage user accounts;
- manage application domains;
- manage information flow control policies and attributes;
- set the audit level and manage audit logs; and
- manage digital certificates and cryptographic keys.

The TOE supports the following roles:

- Privileged administrator: has full access to the TOE functionality.
- Privileged domain administrator: has full access only to the assigned application domains.

1.5.2.6 Protection of the TOE security functionality

The TOE consistently interprets public key certificates and certificate revocation lists. Additionally, the TOE provides reliable timestamps for certificate validation and audit generation.

1.5.2.7 Trusted channel

The TOE can protect the communication of application end points through the establishment of a secure channel using TLSv1.2 and SSH version 2. The protocol used depends on the application protocol used to communicate the application end points (e.g. HTTPS, SFTP) and whether the information flow control policy is configured to establish communications through a secure channel.

The TOE protects the communication between itself and an administrator's SSH client (management CLI) from modification and disclosure through the use of SSH version 2.

This implies that the SSH client and the application client end points, which are part of the Operational Environment, are IT products that are trusted to function correctly and to not divulge security information.

Note: *The TOE does not provide a trusted channel between itself and the console connected through the serial line. This connection must be physically protected.*

1.5.3 TOE boundaries

1.5.3.1 Physical

The TOE can be downloaded from IBM Fix Central. The TOE guidance documentation is available online at [DPKC]☝, and comprises the following documents:

- DataPower Secure Installation Guide
- DataPower Service Gateway XG45 Administrator's Guide
- DataPower B2B Appliance XB60 and XB62 Administrator's Guide
- DataPower Integration Appliance XI50, XI50B, and XI52 Administrator's Guide
- DataPower Secure Deployment Guide

The full hardware model names for the evaluated configuration are specified in section 1.4.1.

1.5.3.2 Logical

The TOE provides the following security functionality:

- Security auditing
- Cryptographic support
- Identification and authentication
- User data protection
- Security management
- Protection of the TOE security functionality
- Trusted channel

The TOE security functionality is described with more detail in Chapter 7, TOE Summary Specification.

The logical boundary of the TOE consists of the following subsystems, as shown in Figure 1:

- Oversight subsystem
- Router subsystem

- SSH daemon subsystem

1.5.3.3 Evaluated configuration

The evaluated configuration consists of the firmware and guidance documentation specified in section 1.5.3.1 running on the hardware models specified in section 1.4.1. It includes the use of the optional IT products specified in section 1.4.1.

The specifications for configuring the TOE in the evaluated configuration are located in the guidance documentation. The consumer must read, understand, and follow the guidance documentation provided as part of the TOE for the evaluated configuration.

The following configuration information applies to the evaluated configuration:

- Audit must always be enabled.
- SSLv3.0 must be disabled. Only TLSv1.2 is allowed.
- The WebGUI for administrative management must be disabled.
- SNMP must be disabled.
- The XML Management Interface must be disabled.
- The USB port must be disabled.
- The Intelligent Platform Management Interface (IPMI) LAN channel must be disabled.

Additional configuration information can be found in the guidance documentation specified in section 1.5.3.1.

1.5.4 Security Policy Model

The security policy for the TOE is defined by the security functional requirements and divided in two distinct groups: one for enforcing information flow control, and the other to enforce access control to objects and security management functions. The following is a list of the subjects and objects, and their security attributes, that are participating in the policy.

1.5.4.1 Information Flow Control Policy

Subjects

Subjects include the following:

- Requesting applications

Their security attributes are:

- Requesting entities

Information

The TOE supports the information flow control policy through an internal data model that allows the configuration of services and rules based on one or more of the following protocols, payload formats and additional security attributes.

Message Protocols:

- HTTP and HTTPS protocol messages
- FTP, FTP over SSL and SFTP protocol messages

Payload formats:

- JSON messages
- XML messages
- SOAP messages

Security attributes:

- IP source address
- IP destination address
- TCP port
- Request URL
- Protocol header (HTTP, HTTPS, FTP, FTP over SSL, SFTP) attributes
- XML Schema Definition (SOAP or XML)
- XML signature
- Identity assertion obtained from XML standards-based messages or transport layer information (see definition in FDP_IFF.1).
- Message content
- Size of message

Objects

Objects are:

- None.

1.5.4.2 Domain Access Control Policy

Subjects

Subjects include the following:

- Users

Their security attributes are:

- User's security attributes: name, password, access level, application domain membership, effective domain.

Objects

Objects are:

- Application domains
- Directories
- Files
- Objects comprising the Information Flow Control Policy
- Digital certificates and cryptographic keys

1.5.4.3 TSF and user data

TSF data can be identified as:

- The security attributes for subjects defined above.
- The security attributes for objects defined above.
- Audit records / audit trail data.

- Password policy: minimum length, use of lower case, use of upper case, use of digit, use of special character, number of historical passwords.

User data is:

- incoming and outgoing messages (network traffic) mediated by the TSF.

2 CC Conformance Claim

This Security Target is CC Part 2 extended and CC Part 3 conformant, with a claimed Evaluation Assurance Level of EAL4, augmented by ALC_FLR.3.

This Security Target does not claim conformance to any Protection Profile.

Common Criteria [CC] version 3.1 revision 4 is the basis for this conformance claim.

3 Security Problem Definition

3.1 Threat Environment

This section describes the threat model for the TOE and identifies the individual threats that are assumed to exist in the TOE environment.

The **assets** to be protected by the TOE are the TSF data and user data, as described in section 1.5.4.3.

The **threat agents** having an interest in obtaining or tampering with these assets can be categorized as either:

- Unauthorized individuals ("attackers") which are unknown to the TOE and its runtime environment.
- Administrators of the TOE who try to access data and perform functions for which they are not authorized.
- External IT entities authorized or not, attempting to perform actions that are not allowed by the information flow policy (e.g., access data protected by the TOE, pass data through the TOE, or make the TOE to process data).

The TOE is able to withstand attackers with an "Enhanced-Basic" attack potential.

Threat agents originate from a well managed user community within an organization's internal network. Hence, only inadvertent or casual attempts to breach system security are expected from this community.

3.1.1 Threats countered by the TOE

T.MEDIAT

An unauthorized individual or an IT external entity may send messages through the TOE, which violates the permissible information flow rules enforced by the TOE.

T.IA

Unauthorized individuals may impersonate an authorized user of the TOE to gain access to the TSF data and its security functions.

T.ACCESS

An administrator may gain access to administrative resources or perform administrative operations for which no access rights have been granted.

T.COMPROT

An unauthorized individual may be able to view, modify, and/or delete data that is sent between a remotely located authorized administrator and the TOE.

T.MSGPROT

Messages may be compromised (disclosed to or modified by unauthorized individuals) during processing of information flow policy.

3.2 Assumptions

3.2.1 Intended usage of the TOE

A.NOEVIL

The administrators of the TOE who are involved in protecting TSF data or providing functionality that the TOE depends on are assumed not to be careless, willfully negligent, or hostile. They will follow and abide by the instructions provided in the administrator guidance that is part of the TOE. They are well trained to securely and responsibly administer all aspects of the TOE operations in accordance to this Security Target.

A.AAASEC

It is assumed that the systems providing authentication and authorization services to the TOE are protected against unauthorized physical access and modification in the operational environment. Communication between the TOE and those systems is also protected from eavesdropping and modification.

A.NS

It is assumed that the network services used by the TOE are reliable and protected against unauthorized physical access and modification in the operational environment.

A.PHYSEC

It is assumed that the TOE is protected against unauthorized physical access and modification.

A.PUBLIC

It is assumed that the operational environment providing the runtime environment for the TOE are used solely for this purpose and not to run other application software except as required for the support of the TOE and for the management and maintenance of the underlying hardware and software.

A.BRIDGE

It is assumed that the TOE is the only interface (i.e. bridge) between the systems where the information flow policy needs to be enforced by the TOE.

A.NTP

Any Network Time Protocol server the TOE uses to synchronize the real time clock is a reliable time source.

A.CLOCK

The real time clock of the underlying operating system provides reliable time stamps.

A.PKI

It is assumed that digital certificates, certificate revocation lists (CRLs) used for certificate validation and private and public keys used for SSH authentication are generated externally, meeting the corresponding standards and providing sufficient security strength through the use of appropriate key lengths and message digest algorithms. It is also assumed that Administrators verify the integrity and authenticity of digital certificates and key material before importing them into the TOE.

3.3 Organizational Security Policies

P.ACCOUNTABILITY

External IT entities and administrators of the TOE shall be held accountable for their security-relevant actions within the TOE.

4 Security Objectives

4.1 Objectives for the TOE

O.ACCOUNT

The TOE must provide accountability for information flow through the TOE and user accountability for the use of security management functions by administrators.

O.AUDREC

The TOE must provide a means to record a readable audit trail of information flows through the TOE and for authorized administrator use of security functions related to audit, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes. Also, the TOE must prevent unauthorized users from accessing the audit trail.

O.COMPROT

The TOE must protect information transmitted between a remotely located authorized administrator and the TOE against disclosure and modification.

O.MSGPROT

The TOE must provide cryptographic means including generation and validation of digital signatures, generation and validation of XML signatures, XML payload encryption and decryption, and encryption and decryption of messages during processing of information flow control.

O.IDAUTH

The TOE must uniquely identify and authenticate the claimed identity of all TOE administrators, before granting access to the TOE and the TOE management functions in the effective application domain.

O.ACCESS

The TOE must control access to administrative resources as well as administrative operations based on the role an administrator is assigned to. The TOE must allow authorized administrators to specify the access rights of administrators to resources.

O.MEDIAT

The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE, and must ensure that residual information in the TOE from a previous information flow is not transmitted in any way.

4.2 Objectives for the Operational Environment

OE.NOEVIL

The administrators of the TOE and the systems in the TOE's operational environment involved in protecting TSF data or providing functionality that the TOE depends on, are assumed not to be careless, willfully negligent, or hostile. They will follow and abide by the instructions provided in the administrator guidance that is part of the TOE. They are well trained to securely and responsibly administer all aspects of the TOE operations in accordance this Security Target.

OE.PHYSEC

The TOE is protected against unauthorized physical access and modification.

OE.AAASEC

Systems providing authentication and authorization services to the TOE are protected against unauthorized physical access and modification in the operational environment. Communication between the TOE and those systems is also protected from eavesdropping and modification.

OE.NS

Network services running in the operational environment that are used by the TOE are reliable and protected against unauthorized physical access and modification.

OE.PUBLIC

The operational environment providing the runtime environment for the TOE are used solely for this purpose and not to run other application software except as required for the support of the TOE and for the management and maintenance of the underlying hardware and software.

OE.BRIDGE

The operational environment assures that the TOE is the only interface (i.e. bridge) between the systems where the information flow policy has to be enforced by the TOE.

OE.NTP

Any Network Time Protocol server the TOE uses to synchronize the realtime clock shall be a reliable time source.

OE.CLOCK

The real time clock of the underlying operating system shall provide reliable time stamps.

OE.PKI

Digital certificates, CRLs used for certificate validation and private and public keys used for SSH authentication are generated externally and imported into the TOE. This material must meet the coresponding standards and provide sufficient strength, through the use of appropriate key lengths and message digest algorithms.

4.3 Security Objectives Rationale

4.3.1 Coverage

The following table provides a mapping of TOE objectives to threats and policies, showing that each objective counters or enforces at least one threat or policy, respectively.

Objective	Threats / OSPs
O.ACCOUNT	P.ACCOUNTABILITY
O.AUDREC	P.ACCOUNTABILITY
O.COMPROT	T.COMPROT
O.MSGPROT	T.MSGPROT
O.IDAUTH	T.IA
O.ACCESS	T.ACCESS
O.MEDIAT	T.MEDIAT

Table 1: Mapping of security objectives to threats and policies

The following table provides a mapping of the objectives for the Operational Environment to assumptions, threats and policies, showing that each objective holds, counters or enforces at least one assumption, threat or policy, respectively.

Objective	Assumptions / Threats / OSPs
OE.NOEVIL	A.NOEVIL
OE.PHYSEC	A.PHYSEC
OE.AAASEC	A.AAASEC
OE.NS	A.NS
OE.PUBLIC	A.PUBLIC
OE.BRIDGE	A.BRIDGE
OE.NTP	A.NTP
OE.CLOCK	A.CLOCK
OE.PKI	A.PKI

Table 2: Mapping of security objectives for the Operational Environment to assumptions, threats and policies

4.3.2 Sufficiency

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

Threat	Rationale for security objectives
T.MEDIAT	O.MEDIAT assures that the TOE must control the flow of information and enforce the configured information flow policy rules for the TOE.
T.IA	O.IDAUTH assures that the only authorized users are allowed to access the TOE functions and that they must be successfully identified and authenticated before any TOE security functions can be accessed.
T.ACCESS	The threat of an administrator accessing information resources without authorization is removed by O.ACCESS.
T.COMPROT	O.COMPROT assures that the TOE must protect information transmitted between a remotely located authorized administrator and the TOE against disclosure and modification.
T.MSGPROT	O.MSGPROT assures that the TOE must provide cryptographic means including digital signature generation and validation, XML signature generation and validation, XML payload encryption and decryption, and message encryption and decryption during processing of information flow control.

Table 3: Sufficiency of objectives countering threats

The following rationale provides justification that the security objectives for the environment are suitable to cover each individual assumption, that each security objective for the environment that traces back to an assumption about the environment of use of the TOE, when achieved, actually contributes to the environment achieving consistency with the assumption, and that if all security objectives for the environment that trace back to an assumption are achieved, the intended usage is supported.

Assumption	Rationale for security objectives
A.NOEVIL	OE.NOEVIL assures that those responsible for the operation of the TOE are not careless, willfully negligent, or hostile, and that they are well trained and will follow the provided administrator guidance to configure and operate the TOE.
A.AAASEC	OE.AAASEC assures that systems in the operational environment are protected from unauthorized physical access and modification, and the integrity and confidentiality of the communication between the TOE and those systems.
A.NS	OE.NS assures that network services used by the TOE and running in the operational environment are reliable and protected against unauthorized physical access and modification.

Assumption	Rationale for security objectives
A.PHYSEC	OE.PHYSEC assures that the TOE is protected against unauthorized physical access and modification.
A.PUBLIC	OE.PUBLIC assures that the systems providing the runtime environment for the TOE are used solely for this purpose and not to run other application software except as required for the support of the TOE and for the management and maintenance of the underlying hardware and software.
A.BRIDGE	OE.BRIDGE assures that there is no other interface between the systems where the information flow policy needs to be enforced, in other words, there is no alternative path through which the information flow policy enforced by the TOE can be bypassed.
A.NTP	OE.NTP assures that the TOE uses a reliable time source to synchronize the real time clock.
A.CLOCK	OE.CLOCK assures that the TOE uses a reliable time source to synchronize the real time clock.
A.PKI	OE.PKI assures that the TOE uses valid digital certificates, CRLs and public and private keys, providing sufficient security strength.

Table 4: Sufficiency of objectives holding assumptions

The following rationale provides justification that the security objectives are suitable to cover each individual organizational security policy (OSP), that each security objective that traces back to an OSP, when achieved, actually contributes to the implementation of the OSP, and that if all security objectives that trace back to an OSP are achieved, the OSP is implemented.

OSP	Rationale for security objectives
P.ACCOUNTABILITY	O.ACCOUNT assures that the TOE offers an audit mechanism that provides user accountability for information flows through the TOE and for authorized administrator use of security functions related to audit. O.AUDREC assures that the TOE provides a means to record a readable audit trail of information flows through the TOE and for authorized administrator use of security functions related to audit, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes. Also, O.AUDREC assures that the TOE prevents unauthorized users from accessing the audit trail.

Table 5: Sufficiency of objectives enforcing Organizational Security Policies

5 Extended Components Definition

5.1 Class FCS: Cryptographic support

This section describes the functional requirements for the generation of random numbers to be used as secrets for cryptographic purposes or authentication according to the additional requirements of the German Scheme (BSI) specified in [AIS20] and [AIS31].

5.1.1 Generation of random numbers (RNG)

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 audit events foreseen.

5.1.1.1 FCS_RNG.1 - Random number generation

Hierarchical to:	No other components.
Dependencies:	No dependencies.

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

a) DRG.2.1: If initialized with a random seed [selection: **using PTRNG of class PTG.2 as random source, using PTRNG of class PTG.3 as random source, using NPTRNG of class NTG.1 as random source, [assignment: other requirements for seeding]**], the internal state of the RNG shall [selection: **have [assignment: amount of entropy], have [assignment: work factor], require [assignment: guess work]**].

b) DRG.2.2: The RNG provides forward secrecy.

c) DRG.2.3: The RNG provides backward secrecy.

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

a) DRG.2.4: The RNG initialized with a random seed [assignment: **requirements for seeding**] generates output for which [assignment: **number of strings**] strings of bit length 128 are mutually different with probability [assignment: **probability**]

b) DRG.2.5: Statistical test suites cannot practically distinguish the random numbers from output sequences of an ideal RNG. The random numbers must pass test procedure A [assignment: **additional test suites**].

Rationale

The quality of the random number generator is defined using this SFR. The quality metric required in FCS_RNG.1.2 is detailed in the German Scheme [AIS20] and [AIS31].

6 Security Requirements

6.1 TOE Security Functional Requirements

The following table shows the security functional requirements (SFRs) for the TOE, and the operations performed on the components according to CC part 2: iteration (Iter.), refinement (Ref.), assignment (Ass.) and selection (Sel.).

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
FAU - Security audit	FAU_GEN.1 Audit data generation		CC Part 2	No	No	Yes	Yes
	FAU_SAR.1 Audit review		CC Part 2	No	No	Yes	No
	FAU_SAR.3 Selectable audit review		CC Part 2	No	No	Yes	No
	FAU_SEL.1 Selective audit		CC Part 2	No	No	No	Yes
	FAU_STG.1 Protected audit trail storage		CC Part 2	No	No	No	Yes
	FAU_STG.4 Prevention of audit data loss		CC Part 2	No	Yes	Yes	Yes
FCS - Cryptographic support	FCS_CKM.1 Cryptographic key generation		CC Part 2	No	No	Yes	No
	FCS_CKM.2 Cryptographic key distribution		CC Part 2	No	No	Yes	No
	FCS_COP.1(ENC) Cryptographic operation	FCS_COP.1	CC Part 2	Yes	No	Yes	No
	FCS_COP.1(MAC) Cryptographic operation	FCS_COP.1	CC Part 2	Yes	No	Yes	No
	FCS_COP.1(MD) Cryptographic operation	FCS_COP.1	CC Part 2	Yes	No	Yes	No
	FCS_COP.1(SGN) Cryptographic operation	FCS_COP.1	CC Part 2	Yes	No	Yes	No
	FCS_RNG.1 Random number generation		ECD	No	No	Yes	Yes
FDP - User data protection	FDP_ACC.1 Subset access control		CC Part 2	No	No	Yes	No
	FDP_ACF.1 Security attribute based access control		CC Part 2	No	No	Yes	No
	FDP_IFC.1 Subset information flow control		CC Part 2	No	No	Yes	No
	FDP_IFF.1 Simple security attributes		CC Part 2	No	Yes	Yes	No

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
FIA - Identification and authentication	FIA_AFL.1 Authentication failure handling		CC Part 2	No	No	Yes	Yes
	FIA_ATD.1 User attribute definition		CC Part 2	No	Yes	Yes	No
	FIA_SOS.1 Verification of secrets		CC Part 2	No	Yes	Yes	No
	FIA_UAU.2 User authentication before any action		CC Part 2	No	No	No	No
	FIA_UID.2 User identification before any action		CC Part 2	No	No	No	No
	FIA_USB.1 User-subject binding		CC Part 2	No	No	Yes	No
FMT - Security management	FMT_MOF.1(AUD) Management of security functions behaviour (Audit level)	FMT_MOF.1	CC Part 2	Yes	No	Yes	Yes
	FMT_MSA.1(DACP) Management of security attributes for the Domain Access Control Policy	FMT_MSA.1	CC Part 2	Yes	No	Yes	Yes
	FMT_MSA.1(IFCP) Management of security attributes for the Information Flow Control Policy	FMT_MSA.1	CC Part 2	Yes	No	Yes	Yes
	FMT_MSA.3(DACP) Static attribute initialisation for the Domain Access Control Policy	FMT_MSA.3	CC Part 2	Yes	No	Yes	Yes
	FMT_MSA.3(IFCP) Static attribute initialisation for the Information Flow Control Policy	FMT_MSA.3	CC Part 2	Yes	No	Yes	Yes
	FMT_MTD.1(AUD) Management of TSF data (audit trail data)	FMT_MTD.1	CC Part 2	Yes	Yes	Yes	Yes
	FMT_MTD.1(TIME) Management of TSF data (time and date)	FMT_MTD.1	CC Part 2	Yes	No	Yes	Yes
	FMT_MTD.1(DACP) Management of TSF data (Domain Access Control Policy)	FMT_MTD.1	CC Part 2	Yes	Yes	Yes	Yes
	FMT_MTD.1(IFCP) Management of TSF data (Information Flow Control Policy)	FMT_MTD.1	CC Part 2	Yes	Yes	Yes	Yes
	FMT_MTD.1(CRYPTO) Management of TSF data (Cryptographic Material)	FMT_MTD.1	CC Part 2	Yes	Yes	Yes	Yes

Security functional group	Security functional requirement	Base security functional component	Source	Operations			
				Iter.	Ref.	Ass.	Sel.
	FMT_MTD.2 Management of limits on TSF data		CC Part 2	No	No	Yes	No
	FMT_SMF.1 Specification of Management Functions		CC Part 2	No	No	Yes	No
	FMT_SMR.1 Security roles		CC Part 2	No	No	Yes	No
FPT - Protection of the TSF	FPT_TDC.1 Inter-TSF basic TSF data consistency		CC Part 2	No	No	Yes	No
	FPT_STM.1 Reliable time stamps		CC Part 2	No	Yes	No	No
FTA - TOE access	FTA_TSE.1 TOE session establishment		CC Part 2	No	No	Yes	No
FTP - Trusted path/channels	FTP_ITC.1 Inter-TSF trusted channel		CC Part 2	No	Yes	Yes	Yes
	FTP_TRP.1 Trusted path		CC Part 2	No	Yes	Yes	Yes

Table 6: Security functional requirements (SFRs) for the TOE

6.1.1 Security audit (FAU)

6.1.1.1 Audit data generation (FAU_GEN.1)

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

a) Start-up and shutdown of the audit functions;

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

c) [**the events listed in Table 7**].

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

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**information specified in rightmost column of Table 7**].

Functional component	Auditable event	Audit level		Additional audit record contents
		std.	full	
FAU_STG.1	Archiving of audit trail (audit-log file) to audit backup trail (audit-log.1 file)	✓	✓	None.
	Deletion of audit backup trail (audit-log.1)	✓	✓	The identity of the administrator performing the operation.

Functional component	Auditable event	Audit level		Additional audit record contents
		std.	full	
FDP_ACF.1	Operations on files and directories	✓	✓	The identity of the administrator performing the operation, the effective application domain and the operation performed.
FDP_IFF.1	Events on information flow		✓	The presumed IP addresses of the source and destination subject.
	Decision on information flow		✓	The presumed IP addresses of the source and destination subject.
FIA_AFL.1	The reaching of the threshold for unsuccessful authentication attempts.	✓	✓	The identity of the offending user.
	Restoration by an authorized administrator of the user's capability to authenticate.	✓	✓	The identity of the administrator who resets the account.
FIA_SOS.1	Failures in changing or setting password due to password policy.	✓	✓	The identity of the administrator performing the operation.
FIA_UAU.2	Any use of the authentication mechanism.	✓	✓	The identity of the administrator performing the operation.
FIA_UID.2	All use of the user identification mechanism.	✓	✓	The identity of the administrator performing the operation.
FMT_MTD.1(TIME)	Changes to date and time.	✓	✓	The identity of the administrator performing the operation and the date and/or time set.
FMT_MTD.1(DACP)	All operations on users and application domains.	✓	✓	The identity of the administrator performing the operation.
FMT_MTD.1(IFCP)	All operations on Information Flow Control Policy objects.	✓	✓	The identity of the administrator performing the operation.
FMT_MTD.1(CRYPTO)	All operations on digital certificates, cryptographic keys and CRLs.	✓	✓	The identity of the administrator performing the operation.
FMT_SMR.1	Assignment of access-level and application domains (which determine the role) to an administrator.	✓	✓	The identity of the administrator performing the operation, the access level and application domain being associated.
FPT_STM.1	Changes to the date and time	✓	✓	The identity of the administrator performing the operation.

Functional component	Auditable event	Audit level		Additional audit record contents
		std.	full	
	Changes to the NTP service configuration	✓	✓	The identity of the administrator performing the operation.

Table 7: Auditable events

6.1.1.2 Audit review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide [**administrators with the privileged administrator or the privileged domain administrator roles**] with the capability to read [**all audit trail data**] from the audit records.

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

6.1.1.3 Selectable audit review (FAU_SAR.3)

FAU_SAR.3.1 The TSF shall provide the ability to apply [**searches and sorting**] of audit data based on [

- **user identity**
- **presumed subject address**
- **ranges of dates**
- **ranges of times**
- **ranges of addresses**

].

6.1.1.4 Selective audit (FAU_SEL.1)

FAU_SEL.1.1 The TSF shall be able to select the set of events to be audited from the set of all auditable events based on the following attributes: [

a) [**audit level**]

]

Application Note: *Possible values for the audit level are "standard" and "full". See FAU_GEN.1 for the audit events generated in each audit level.*

6.1.1.5 Protected audit trail storage (FAU_STG.1)

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorised deletion.

FAU_STG.1.2 The TSF shall be able to [**prevent**] unauthorised modifications to the stored audit records in the audit trail.

6.1.1.6 Prevention of audit data loss (FAU_STG.4)

FAU_STG.4.1 The TSF shall [**prevent audited events, except those taken by ~~the authorised user with special rights~~*an administrator with the privileged administrator or the privileged domain administrator roles***] and [**cease the process of incoming and outgoing messages covered by the Information Flow Control Policy**] if the audit trail is full.

6.1.2 Cryptographic support (FCS)

6.1.2.1 Cryptographic key generation (FCS_CKM.1)

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

- **SSH-2: generation of encryption keys and MAC keys**
- **TLSv1.2: generation of encryption keys and MAC keys**
- **XML encryption: generation of ephemeral keys**

] and specified cryptographic key sizes [

- **SSH-2:**
  - **AES keys: 128, 192, and 256 bits**
  - **Triple-DES keys: 168 bits**
  - **HMAC keys: 160 bits**
- **TLSv1.2:**
  - **AES keys: 128 and 256 bits**
  - **Triple-DES keys: 168 bits**
  - **HMAC keys: 160 and 256 bits**
- **XML encryption:**
  - **AES keys: 128, 192 and 256 bits**
  - **Triple-DES keys: 168 bits**

] that meet the following: [

- **SSH-2: conformant to [RFC4253]**
- **TLSv1.2: conformant to [RFC5246]**
- **XML encryption: conformant to [W3CXMLENC]**

].

Application Note: *This SFR covers the generation of the client and server encryption keys and client and server MAC keys for the TLS protocol (derived from the master secret) and the SSH protocol (derived from the shared secret), as well as the ephemeral symmetric keys used to encrypt XML payloads.*

6.1.2.2 Cryptographic key distribution (FCS_CKM.2)

FCS_CKM.2.1 The TSF shall distribute cryptographic keys in accordance with a specified cryptographic key distribution method [

- **SSH-2:**

    - **Diffie-Hellman key agreement method (diffie-hellman-group-exchange-sha1, diffie-hellman-group14-sha1, diffie-hellman-group1-sha1)**
- **TLSv1.2:**
    - **Key exchange using RSAES-PKCS1-v1_5**
- **XML encryption:**
    - **key transport using RSAES-PKCS1-v1_5 and RSAES-OAEP**
    - **symmetric key wrap using Triple-DES and AES**

] that meets the following: [

- **SSH-2: conformant to [RFC4253]**☝
- **TLSv1.2: conformant to [RFC5246]**☝
- **XML encryption: conformant to [W3CXMLENC]**☝

].

Application Note: *This SFR covers the key establishment in the TLS and SSH protocols, and key transport for XML encryption.*

6.1.2.3 Cryptographic operation (FCS_COP.1(ENC))

FCS_COP.1.1 The TSF shall perform [**encryption and decryption**] in accordance with a specified cryptographic algorithm [

- **SSH-2: Triple-DES (CBC mode)**
- **TLSv1.2:**
    - **RSA Encryption Scheme with PKCS#1 v1.5 (RSAES-PKCS1-v1_5)**
    - **Triple-DES (CBC mode)**
- **XML encryption:**
    - **RSA Encryption Scheme with OAEP (RSAES-OAEP)**
    - **RSA Encryption Scheme with PKCS#1 v1.5 (RSAES-PKCS1-v1_5)**
    - **AES (CBC mode)**
    - **Triple-DES (CBC mode)**

] and cryptographic key sizes [

- **SSH-2: Triple-DES: 168 bits**
- **TLSv1.2:**
    - **RSAES-PKCS1-v1_5: 1024, 2048, and 4096 bits**
    - **Triple-DES: 168 bits**
- **XML encryption:**
    - **RSAES-OAEP and RSAES-PKCS1-v1_5: 1024, 2048, and 4096 bits**
    - **AES: 128, 192 and 256 bits**
    - **Triple-DES: 168 bits**

] that meet the following: [

- **SSH-2: conformant to [RFC4253]**☝ **and [RFC4344]**☝
- **TLSv1.2: conformant to [RFC5246]**☝

- **XML encryption: conformant to [W3CXMLENC]☝**
- **RSAES-OAEP and RSAES-PKCS1-v1_5: conformant to [RFC3447]☝**
- **AES: algorithm processing conformant to [FIPS197]☝, conformant to [SP800-38A]☝ (CBC and CTR modes)**
- **Triple-DES: conformant to [SP800-67]☝, conformant to [SP800-38A]☝ (CBC mode)**

].

Application Note: *This SFR covers asymmetric encryption/decryption for key exchange in TLS and key transport in XML encryption. It also covers symmetric encryption/decryption as part of the XML encryption protocol, but in this case limited to the algorithm processing part since it relies on the Intel AES-NI instructions. The Intel AES-NI instructions are conformant to the industrial standard [AESNI]☝, but not part of the TOE and therefore not evaluated.*

6.1.2.4 Cryptographic operation (FCS_COP.1(MAC))

FCS_COP.1.1 The TSF shall perform [**message authentication code generation**] in accordance with a specified cryptographic algorithm [

- **SSH-2:**
  - **HMAC-SHA-1**
- **TLSv1.2:**
  - **HMAC-SHA-1**
  - **HMAC-SHA-256**
- **XML signature:**
  - **HMAC-SHA-1**

] and cryptographic key sizes [

- **SSH-2:**
  - **160 bits (HMAC-SHA-1)**
- **TLSv1.2:**
  - **160 bits (HMAC-SHA-1)**
  - **256 bits (HMAC-SHA-256)**
- **XML signature:**
  - **160 bits, minimum 80 bits (HMAC-SHA-1)**

] that meet the following: [

- **SSH-2: conformant to [RFC4253]☝**
- **TLSv1.2: conformant to [RFC5246]☝**
- **XML signature: conformant to [W3CXMLSIG]☝**
- **HMAC: conformant to [RFC2104]☝**
- **SHA-1, SHA-256: conformant to [FIPS180-4]☝**

].

Application Note: *This SFR covers message integrity for the TLS, SSH and XML signature protocols.*

6.1.2.5 Cryptographic operation (FCS_COP.1(MD))

FCS_COP.1.1 The TSF shall perform [**message digest generation**] in accordance with a specified cryptographic algorithm [

- **SSH-2:**
  - **SHA-1**
- **TLSv1.2:**
  - **SHA-1**
  - **SHA-256**
- **XML signature:**
  - **SHA-1**
  - **SHA-256**
  - **SHA-384**
  - **SHA-512**
- **XML encryption:**
  - **SHA-1**
  - **SHA-256**
  - **SHA-384**
  - **SHA-512**

] and cryptographic key sizes [**none**] that meet the following: [

- **SSH-2: conformant to [RFC4253]**☝
- **TLSv1.2: conformant to [RFC5246]**☝
- **XML signature: conformant to [W3CXMLSIG]**☝
- **XML encryption: conformant to [W3CXMLENC]**☝
- **SHA-1, SHA-256, SHA-384, SHA-512: conformant to [FIPS180-4]**☝

].

Application Note: *This SFR covers digital signature generation for the TLS, SSH, XML signature and XML encryption protocols.*

6.1.2.6 Cryptographic operation (FCS_COP.1(SGN))

FCS_COP.1.1 The TSF shall perform [**digital signature generation and verification**] in accordance with a specified cryptographic algorithm [

- **SSH-2:**
  - **DSA with SHA-1**
  - **RSA Signature Scheme with Appendix PKCS#1 v1.5 (RSASSA-PKCS1-v1_5) with SHA-1**
- **TLSv1.2:**
  - **RSASSA-PKCS1-v1_5 with SHA-1 and SHA-256**
- **XML signature:**
  - **DSA with SHA-1**
  - **RSASSA-PKCS1-v1_5 with SHA-1, SHA-256, SHA-384 and SHA-512**

] and cryptographic key sizes [

- **SSH-2:**
  - **DSA: L = 1024 bits, N = 160 bits**
  - **RSASSA-PKCS1-v1_5: 1024, 2048, and 4096 bits**
- **TLSv1.2:**
  - **RSASSA-PKCS1-v1_5: 1024, 2048, and 4096 bits**
- **XML signature:**
  - **DSA: L = 1024 bits, N = 160 bits**
  - **RSASSA-PKCS1-v1_5: 1024, 2048, and 4096 bits**

] that meet the following: [

- **SSH-2: conformant to [RFC4253]**☝
- **TLSv1.2: conformant to [RFC5246]**☝
- **XML signature: conformant to [W3CXMLSIG]**☝
- **DSA: conformant to [RFC4253]**☝
- **RSASSA-PKCS1-v1_5: conformant to [RFC3447]**☝
- **SHA-1, SHA-256, SHA-384, SHA-512: conformant to [FIPS180-4]**☝

].

Application Note: *This SFR covers digital signature generation and verification for the TLS, SSH and XML signature protocols.*

Application Note: *XML files are canonicalized according to* [W3CXMLC14N]☝ *and* [W3CXMLEXCC14N]☝ *before signatures are generated.*

6.1.2.7 Random number generation (FCS_RNG.1)

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

a) DRG.2.1: If initialized with a random seed [**using NPTRNG of class NTG.1 as random source**], the internal state of the RNG shall [**have [at least 48 bits of entropy]**].

b) DRG.2.2: The RNG provides forward secrecy.

c) DRG.2.3: The RNG provides backward secrecy.

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

a) DRG.2.4: The RNG initialized with a random seed [**of 256 bits with at least 48 bits of entropy**] generates output for which [**2^{20}**] strings of bit length 128 are mutually different with probability [**greater than or equal $1 - 2^{-10}$**].

b) DRG.2.5: 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 no other test procedure**].

Application Note: *The Deterministic Random Number Generator is implemented in software and uses as the entropy input source the Linux RNG (/dev/random) provided by the DataPower Operating System version 7, which is included in the firmware package and is part of the Operational Environment.*

6.1.3 User data protection (FDP)

6.1.3.1 Subset access control (FDP_ACC.1)

FDP_ACC.1.1 The TSF shall enforce the [**Domain Access Control Policy**] on [

a) **Subjects: administrators**

b) **Objects:**

- **objects that comprise the Information Flow Control Policy**
- **cryptographic material: digital certificates and cryptographic keys**
- **directories**
- **files**

c) **Operations:**

- **on information control flow policy objects: all security management functions allowed for each object**
- **on cryptographic material: all security management functions allowed for each object**
- **on directories: create, remove**
- **on files: create, read, write, delete, execute, show contents**

].

6.1.3.2 Security attribute based access control (FDP_ACF.1)

FDP_ACF.1.1 The TSF shall enforce the [**Domain Access Control Policy**] to objects based on the following: [

a) **Subject security attributes:**

- **the administrator role**
- **the application domain membership**

b) **Object attributes:**

- **all objects: application domain**
- **directory: file permissions (CopyFrom, CopyTo, Delete, Subdir, Display, Exec)**

].

FDP_ACF.1.2 The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [

a) **For operations on Information Flow Control Policy objects or cryptographic material objects available in an application domain: if the administrator has the administrator privileged role or is a member of the application domain, and if the effective domain of the session is the same as the application domain of the object, then access is allowed.**

b) **For operations on Information Flow Control Policy objects or cryptographic material objects in the "default" domain: if the administrator has the administrator privileged role and the effective domain is the "default" domain, then access is allowed.**

c) **For the show operation on Information Flow Control Policy objects available in an application domain: if the user is a member of the application domain, and if the effective domain of the session is the same as the application domain of the object, then access is allowed.**

d) **For operations on files and directories in the "default" domain: if the administrator has the administrator privileged role, the effective domain is the "default" domain, and the required permission for the operation according to Table 8 is fulfilled by the file permissions assigned to the directory where the object belongs according to Table 10, then access is allowed.**

e) **For operations on files or directories located in the "local:" directory of the effective domain: if the required permission for the operation according to Table 8 is fulfilled by the file permissions assigned to the "local:" directory of the effective domain, then access is allowed.**

f) **For operations on files and directories located in a directory of the effective domain other than "local:": if the effective domain is not the "default" domain, and the required permission for the operation according to Table 8 is fulfilled by the file permissions assigned to the directory according to Table 9, then access is allowed.**

].

Operation	CopyFrom	CopyTo	Delete	Subdir	Display	Exec
Create file		✓				
Read file	✓					
Write file		✓				
Delete file			✓			
Execute file						✓
Show file contents					✓	
Create directory				✓		
Remove directory				✓		

Table 8: Permissions for file and directory operations

Directory	Domain	CopyFrom	CopyTo	Delete	Subdir	Display	Exec
audit:	default*	✓				✓	
pubcert:	default	✓				✓	
sharedcert:	default						✓
store:	default*	✓				✓	
cert:	effective		✓	✓			

Directory	Domain	CopyFrom	CopyTo	Delete	Subdir	Display	Exec
chkpoints:	effective	✓	✓	✓			
config:	effective	✓	✓	✓		✓	✓
export:	effective	✓		✓			
local:	effective	See Application Note 2					
logstore:	effective	✓				✓	
logtemp:	effective	✓		✓		✓	
temporary:	effective	✓	✓	✓		✓	✓

Table 9: Permissions of directories in application domains

Application Note 1: *directories marked as "default*" are located in the default domain and visible from an application domain only if the default domain is configured to be visible from that application domain. Directories marked as "default" are located in the default domain and always visible from any application domain.*

Application Note 2: *access permissions in the local: directory are set using the Command Line Interface (file-permissions command in Application Domain mode).*

Directory	CopyFrom	CopyTo	Delete	Subdir	Display	Exec
store:	✓	✓	✓		✓	
temporary:	✓	✓	✓		✓	✓
image:	✓	✓	✓		✓	
config:	✓	✓	✓		✓	✓
cert:		✓	✓			
dpcert:		✓	✓			
sharedcert:		✓	✓			
pubcert:	✓	✓	✓		✓	
tasktemplates:	✓	✓	✓		✓	
logtemp:	✓		✓		✓	
logstore:	✓		✓		✓	
audit:	✓				✓	
chkpoints:	✓	✓	✓			

Directory	CopyFrom	CopyTo	Delete	Subdir	Display	Exec
export:	✓		✓			
local:	✓	✓	✓	✓	✓	✓
backtraces:	✓				✓	

Table 10: Permissions of directories in the default domain

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [

a) **If the object belongs to the "store:" directory of the "default" domain and the effective domain is not the "default" domain: if the subject has the privileged administrator role or the privileged administrator domain role, the "default" domain exists in the list of visible domains of the effective domain, and the operation is read or show contents, then access is allowed.**

b) **If the object belongs to the "local:" directory of an application domain that is not the "default" domain: if the subject has the privileged administrator role or the privileged administrator domain role, the domain exists in the list of visible domains of the effective domain, and the operation is read or show contents, then access is allowed.**

].

Application Note: *The "local:" directory of application domains can have visibility from other application domains: an alias with the name of the application domain (e.g. domainA:///file.txt) is used to reference that directory. Likewise, the "store:" directory of the "default" domain can have visibility from other application domains: the same directory name is used for reference (e.g. store:///file.txt). All objects under the visible directories have read-only access from the effective application domain.*

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**none**].

6.1.3.3 Subset information flow control (FDP_IFC.1)

FDP_IFC.1.1 The TSF shall enforce the [**Information Flow Control Policy**] on [

a) **Subjects: requesting application**

b) **Information:**

- **messages transported by the protocols shown in Table 11 and with payload formats shown in Table 12;**

c) **Operations: request, response**

].

Protocols	Mode	XG45	XI52	XB62	Conformance
HTTP	server and client (listens for requests and forwards)	✓	✓	✓	[RFC2616] with HTTP Basic Authentication (HTTP Digest Authentication is not supported).
HTTPS	server and client (listens for requests and forwards)	✓	✓	✓	[RFC2818] with HTTP Basic Authentication (HTTP Digest Authentication is not supported).
FTP	server and client (server listens for requests, client polls)	✓	✓	✓	[RFC0959], except the following FTP commands: REIN, APPE, ALLO, ABOR, SYST, HELP, NOOP.
FTP over SSL	server and client (server listens for requests, client polls)	✓	✓	✓	[RFC0959] and [RFC4217], except the following FTP commands: REIN, APPE, ALLO, ABOR, SYST, HELP, NOOP.
SFTP	server and client (server listens for requests, client polls)		✓	✓	[SFTP] except the following packet types: ● SSH_FXP_READLINK ● SSH_FXP_SYMLINK ● SSH_FXP_EXTENDED ● SSH_FXP_EXTENDED_REPLY ● SSH_FXF_APPEND flag in SSH_FXP_OPEN

Table 11: Protocols supported by the TOEs

Application Note: *HTTPS uses TLSv1.2; FTP may use TLSv1.2; SFTP uses SSH-2.*

Formats	XG45	XI52	XB62	References
JSON	✓	✓	✓	[RFC4627]
XML	✓	✓	✓	[W3CXML]
SOAP	✓	✓	✓	[W3CSOAP]
Others	✓	✓	✓	The payload is not transformed by the TOE.

Table 12: Message formats supported by the TOEs

6.1.3.4 Simple security attributes (FDP_IFF.1)

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

a) Subject security attributes:

- **requesting entities**

b) Information security attributes:

- **IP source address**
- **IP destination address**
- **TCP port**
- **request URL**
- **XML Schema Definition according to [W3CXSD]☝**
- **XML signature according to [W3CXMLSIG]☝**
- **Identity assertions:**
  - **FTP username and password conformant to [RFC0959]☝,**
  - **SFTP username/password and public key conformant to [SFTP]☝ and [RFC4252]☝,**
  - **credentials from HTTP Basic Authentication header conformant to [RFC2617]☝,**
  - **LTPA token from HTTP cookie conformant to [LTPA]☝,**
  - **SSL client certificate conformant to [RFC5280]☝ and [RFC5246]☝,**
  - **The following WS-Security tokens:**
    - **Username Token conformant to [OASIS-WSS]☝**
    - **X.509 Certificate Token conformant to [OASIS-WSS]☝**
    - **SAML v2.0 Token conformant to [OASIS-SAML20]☝**
- **message content with format according to Table 12**
- **size of message**

].

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

a) **Subjects on an internal network can cause information to flow through the TOE to another connected network if:**

- **all the information security attribute values are permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of information flow security attributes, created by authorized administrators according to the Domain Access Control Policy;**
- **the presumed address of the source subject, in the information, translates to an internal network address; and**
- **the presumed address of the destination subject, in the information, translates to an address on the other connected network.**

b) **Subjects on the external network can cause information to flow through the TOE to another connected network if:**

- **all the information security attribute values are permitted by the information flow security policy rules, where such rules may be composed from all possible combinations of the values of the information flow security attributes, created by authorized administrators according to the Domain Access Control Policy;**

- **the presumed address of the source subject, in the information, translates to an external network address; and**
- **the presumed address of the destination subject, in the information, translates to an address on the other connected network**

].

FDP_IFF.1.3 The TSF shall enforce the [**no additional information flow control SFP rules**].

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

a) **The TOE shall accept requests if the IP source address matches the list of allowed IP addresses.**

].

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

a) **The TOE shall reject requests for access or services where the information arrives on an external TOE interface, and the presumed address of the source subject is an external IT entity on an internal network.**

b) **The TOE shall reject requests for access or services where the information arrives on an internal TOE interface, and the presumed address of the source subject is an external IT entity on the external network.**

c) **The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on a broadcast network.**

d) **The TOE shall reject requests for access or services where the information arrives on either an internal or external TOE interface, and the presumed address of the source subject is an external IT entity on the loopback network.**

e) **The TOE shall reject requests if the IP source address matches the list of denied IP addresses.**

f) **For application protocols supported by the TOE according to Table 11, the TOE shall deny any access or service requests that do not conform to its associated published protocol specification or when authentication using the extracted identity assertion fails. This shall be accomplished through protocol filtering proxies that are designed for that purpose.**

g) **The TOE shall reject malformed JSON messages that do not conform to [RFC4627]☝.**

h) **The TOE shall reject malformed SOAP messages that do not conform to [W3CSOAP]☝.**

i) **The TOE shall reject malformed XML messages (wellformedness as well as schema validation).**

j) **The TOE shall reject messages with malicious XML (node size, element depth, attribute count, external reference handling).**

k) **The TOE shall reject messages with invalid XML signatures according to [W3CXMLSIG]☝, [W3CXMLC14N]☝ and [W3CXMLEXCC14N]☝.**

l) **The TOE shall reject messages received at a rate over an administrator-defined threshold (indicating DOS).**

m) **The TOE shall reject oversized messages.**

].

6.1.4 Identification and authentication (FIA)

6.1.4.1 Authentication failure handling (FIA_AFL.1)

FIA_AFL.1.1 The TSF shall detect when [**an administrator configurable positive integer within 1 to 64**] unsuccessful authentication attempts occur related to [**authorized user access**].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [**met, surpassed**], the TSF shall [

- **for the "admin" account, lock the account for 120 minutes or until it is re-enabled by another administrator with the privileged administrator role;**
- **for the rest of the accounts, lock the user account until it is re-enabled by an administrator with the privileged administrator role**

].

6.1.4.2 User attribute definition (FIA_ATD.1)

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual *administrative* users: [

a) **name**

b) **password**

c) **access level**

d) **membership to application domains**

].

Application Note: *The access level and the membership to application domains determine the role of the administrator. See application note in FMT_SMR.1 for more information.*

6.1.4.3 Verification of secrets (FIA_SOS.1)

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets *used to authenticate users* meet *the following metrics at a minimum:* [

- **be of 14 characters in length,**
- **have one lower case character and one upper case character,**
- **have one digit,**
- **have one special character,**
- **be different from the most recent N past passwords, where N is a configurable value that shall be greater or equal 3.**

].

6.1.4.4 User authentication before any action (FIA_UAU.2)

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

6.1.4.5 User identification before any action (FIA_UID.2)

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

6.1.4.6 User-subject binding (FIA_USB.1)

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: [**effective application domain**].

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [

a) If the subject is a privileged administrator, the TOE will set the effective application domain to the default application domain.

b) If the subject is a privileged domain administrator and member of exactly one application domain, the TOE will set the effective domain to that application domain.

c) If the subject is a privileged domain administrator and member of more than one application domain, the TOE will prompt the user to choose the effective application domain from the list of domains the user is a member of.

].

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [

a) If the subject is a privileged administrator, the TOE will allow the user to change the effective domain to any of the existing application domains in the TOE, including the "default" domain.

b) If the subject is a privileged domain administrator, the TOE will allow the user to change the effective domain to any of the application domains the subject is a member of.

].

6.1.5 Security management (FMT)

6.1.5.1 Management of security functions behaviour (Audit level) (FMT_MOF.1(AUD))

FMT_MOF.1.1 The TSF shall restrict the ability to [**modify the behaviour of**] the functions [

a) audit data generation

] to [**the privileged administrator role**].

Application note: *An administrator with the the privileged administrator role can set the audit level ("standard", "full") for audit data generation; see FAU_GEN.1 and FAU_SEL.1 for more information.*

6.1.5.2 Management of security attributes for the Domain Access Control Policy (FMT_MSA.1(DACP))

FMT_MSA.1.1 The TSF shall enforce the [**Domain Access Control Policy**] to restrict the ability to [**change_default, modify, delete, create**] the security attributes [**listed in FDP_ACF.1**] to [**the privileged administrator role**].

6.1.5.3 Management of security attributes for the Information Flow Control Policy (FMT_MSA.1(IFCP))

FMT_MSA.1.1 The TSF shall enforce the [**Domain Access Control Policy**] to restrict the ability to [**modify, delete, create**] the security attributes [**belonging to the Information Flow Control Policy and listed in FDP_IFF.1**] to [**authorized administrators according to the Domain Access Control Policy**].

6.1.5.4 Static attribute initialisation for the Domain Access Control Policy (FMT_MSA.3(DACP))

FMT_MSA.3.1 The TSF shall enforce the [**Domain Access Control Policy**] to provide [**permissive**] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [**the privileged administrator role**] to specify alternative initial values to override the default values when an object or information is created.

6.1.5.5 Static attribute initialisation for the Information Flow Control Policy (FMT_MSA.3(IFCP))

FMT_MSA.3.1 The TSF shall enforce the [**Domain Access Control Policy**] to provide [**restrictive**] default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the [**authorized administrators according to the Domain Access Control Policy**] to specify alternative initial values to override the default values when an object or information is created.

6.1.5.6 Management of TSF data (audit trail data) (FMT_MTD.1(AUD))

FMT_MTD.1.1 The TSF shall restrict the ability to [**perform management functions**] ~~the~~*on* [**audit trail data**] to [**the privileged administrator role**].

6.1.5.7 Management of TSF data (time and date) (FMT_MTD.1(TIME))

FMT_MTD.1.1 The TSF shall restrict the ability to [**set**] the [**time and date**] to [**the privileged administrator role**].

6.1.5.8 Management of TSF data (Domain Access Control Policy) (FMT_MTD.1(DACP))

FMT_MTD.1.1 The TSF shall restrict the ability to [**perform management functions**] ~~the~~*on* [

- **a) Application domains**
- **b) Users**

] to [**the privileged administrator role**].

6.1.5.9 Management of TSF data (Information Flow Control Policy) (FMT_MTD.1(IFCP))

FMT_MTD.1.1 The TSF shall restrict the ability to [**perform management functions**] ~~the~~*on* [**objects that comprise the Information Flow Control Policy**] to [**authorized administrators according to the Domain Access Control Policy**].

6.1.5.10 Management of TSF data (Cryptographic Material) (FMT_MTD.1(CRYPTO))

FMT_MTD.1.1 The TSF shall restrict the ability to [**perform management functions**] ~~the~~*on* [**cryptographic keys, digital certificates and certification revocation lists (CRL)**] to [**authorized administrators according to the Domain Access Control Policy**].

6.1.5.11 Management of limits on TSF data (FMT_MTD.2)

FMT_MTD.2.1 The TSF shall restrict the specification of the limits for [**number of authentication failures**] to [**the privileged administrator role** .

FMT_MTD.2.2 The TSF shall take the following actions, if the TSF data are at, or exceed, the indicated limits: [**none**].

6.1.5.12 Specification of Management Functions (FMT_SMF.1)

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

- **a) Management of the audit function**
- **b) Management of the audit trail data**
- **c) Management of application domains**
- **d) Management of users and application domain membership**
- **e) Management of password policy and login attempts threshold**
- **f) Management of the Information Flow Control Policy**
- **g) Management of the time and date**
- **h) Management of digital certificates and cryptographic keys**

].

6.1.5.13 Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles [

a) **privileged administrator**

b) **privileged domain administrator**

].

Application Note: *The role is defined by the access level of the user account ("privileged" for administrators) and its application domain membership: an administrator with one or more application domains assigned has the privileged domain administrator role (can only access to the authorized application domains); an administrator with no application domain associated has the privileged administrator role (can access to all application domains, including the "default' domain).*

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

6.1.6 Protection of the TSF (FPT)

6.1.6.1 Inter-TSF basic TSF data consistency (FPT_TDC.1)

FPT_TDC.1.1 The TSF shall provide the capability to consistently interpret [

a) **public keys**

b) **digital certificates**

c) **certificate revocation lists (CRLs),**

] when shared between the TSF and another trusted IT product.

FPT_TDC.1.2 The TSF shall use [

a) **the openssh-pubkey format as defined in [RFC4716],**

b) **the standard X.509 as defined in [RFC5280]; certificates of version 3 are supported (public key certificates),**

c) **the standard X.509 as defined in [RFC5280]; CRLs of version 2 are supported**

] when interpreting the TSF data from another trusted IT product.

6.1.6.2 Reliable time stamps (FPT_STM.1)

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps *by synchronizing the real time clock using the Network Time Protocol according to* [RFC2030].

Application Note: *The real time clock is in the environment and is assumed to be reliable. See OE.CLOCK. When used by the TOE, the Network Time Protocol servers are also assumed to be reliable. See OE.NTP.*

6.1.7 TOE access (FTA)

6.1.7.1 TOE session establishment (FTA_TSE.1)

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on [**a list of denied and allowed IP addresses associated with remote access to the command-line interface**].

6.1.8 Trusted path/channels (FTP)

6.1.8.1 Inter-TSF trusted channel (FTP_ITC.1)

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

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

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for [**polling FTP or SFTP servers and routing outgoing messages according to the Information Flow Control Policy**].

Application Note: *This SFR covers the HTTPS, SFTP and FTP over SSL protocols shown in Table 11 that can be part of the Information Flow Control Policy. The TSF uses the TLSv1.2 (HTTPS, FTP over SSL) and SSH-2 (SFTP) protocols for supporting the trusted channel.*
For the protection of the channel data from disclosure the processing of the protocol is part of the TOE and also the processing of the underlying AES encryption algorithm. However, the processing of the underlying AES encryption algorithm is supported by AES-NI instructions conformant to industrial standard [AESNI]☝*, which is not part of the TOE and therefore not evaluated.*

6.1.8.2 Trusted path (FTP_TRP.1)

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

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

FTP_TRP.1.3 The TSF shall require the use of the trusted path for [**initial user authentication, and security management functions performed by authorized administrators**].

Application Note: *This SFR covers the SSH protocol providing a trusted channel for remote sessions to administrators using the Command Line Interface (CLI).*

6.2 Security Functional Requirements Rationale

6.2.1 Coverage

The following table provides a mapping of SFR to the security objectives, showing that each security functional requirement addresses at least one security objective.

Security functional requirements	Objectives
FAU_GEN.1	O.ACCOUNT
FAU_SAR.1	O.AUDREC
FAU_SAR.3	O.AUDREC

Security functional requirements	Objectives
FAU_SEL.1	O.ACCOUNT
FAU_STG.1	O.AUDREC
FAU_STG.4	O.AUDREC
FCS_CKM.1	O.COMPROT, O.MSGPROT
FCS_CKM.2	O.COMPROT, O.MSGPROT
FCS_COP.1(ENC)	O.COMPROT, O.MSGPROT
FCS_COP.1(MAC)	O.COMPROT, O.MSGPROT
FCS_COP.1(MD)	O.COMPROT, O.MSGPROT
FCS_COP.1(SGN)	O.COMPROT, O.MSGPROT
FCS_RNG.1	O.MSGPROT
FDP_ACC.1	O.ACCESS
FDP_ACF.1	O.ACCESS
FDP_IFC.1	O.MEDIAT
FDP_IFF.1	O.MEDIAT
FIA_AFL.1	O.IDAUTH
FIA_ATD.1	O.IDAUTH
FIA_SOS.1	O.IDAUTH
FIA_UAU.2	O.IDAUTH
FIA_UID.2	O.IDAUTH
FIA_USB.1	O.IDAUTH
FMT_MOF.1(AUD)	O.ACCESS
FMT_MSA.1(DACP)	O.ACCESS
FMT_MSA.1(IFCP)	O.ACCESS
FMT_MSA.3(DACP)	O.ACCESS
FMT_MSA.3(IFCP)	O.ACCESS
FMT_MTD.1(AUD)	O.ACCESS

Security functional requirements	Objectives
FMT_MTD.1(TIME)	O.ACCESS
FMT_MTD.1(DACP)	O.ACCESS
FMT_MTD.1(IFCP)	O.ACCESS
FMT_MTD.1(CRYPTO)	O.ACCESS
FMT_MTD.2	O.ACCESS
FMT_SMF.1	O.ACCESS
FMT_SMR.1	O.ACCESS
FPT_TDC.1	O.MSGPROT
FPT_STM.1	O.AUDREC, O.COMPROT
FTA_TSE.1	O.IDAUTH
FTP_ITC.1	O.MSGPROT
FTP_TRP.1	O.COMPROT

Table 13: Mapping of security functional requirements to security objectives

6.2.2 Sufficiency

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

Security objectives	Rationale
O.ACCOUNT	The objective: "*The TOE must provide accountability for information flow through the TOE and user accountability for the use of security management functions by administrators.*" is satisfied by: ● FAU_GEN.1: specifying the audit events generated by the TOE. ● FAU_SEL.1: selecting the audit events generated by the TOE based on the audit level.
O.AUDREC	The objective: "*The TOE must provide a means to record a readable audit trail of information flows through the TOE and for authorized administrator use of security functions related to audit, with accurate dates and times, and a means to search and sort the audit trail based on relevant attributes. Also, the TOE must prevent unauthorized users from accessing the audit trail.*"

Security objectives	Rationale
	is satisfied by: ● FAU_SAR.1: specifying a mechanism for authorized users to review all audit records. ● FAU_SAR.3: specifying that authorized users are able to search and sort audit data. ● FAU_STG.1: specifying that the audit records cannot be deleted or modified by unauthorized users. ● FAU_STG.4: specifying how the audit functionality responds when the audit trail is full. ● FPT_STM.1: specifying the reliability of timestamps for auditing.
O.COMPROT	The objective: "*The TOE must protect information transmitted between a remotely located authorized administrator and the TOE against disclosure and modification.*" is satisfied by: ● FCS_CKM.1: specifying cryptographic key generation for trusted channel establishment. ● FCS_CKM.2: specifying cryptographic key distribution for trusted channel establishment. ● FCS_COP.1(ENC): specifying the symmetric and asymmetric encryption and decryption algorithms for trusted channel establishment. ● FCS_COP.1(MAC): specifying the message authentication code algorithms for trusted channel establishment. ● FCS_COP.1(MD): specifying the message digest algorithms for trusted channel establishment. ● FCS_COP.1(SGN): specifying the digital signature generation and verification algorithms for trusted establishment. ● FCS_RNG.1: specifying random number generation used for creating cryptographic keys and master secrets. ● FTP_ITC.1: specifying that a trusted channel is enforced between the TOE and another trusted IT product. ● FTP_TRP.1: specifying that a trusted channel is enforced between the TOE and a remote administrator. ● FPT_STM.1: specifying the reliability of timestamps for certificate validation.
O.MSGPROT	The objective: "*The TOE must provide cryptographic means including generation and validation of digital signatures, generation and validation of XML signatures, XML payload encryption and decryption, and encryption and decryption of messages during processing of information flow control.*" is satisfied by: ● FCS_CKM.1: specifying cryptographic key generation for trusted channel establishment and policy processing.

Security objectives	Rationale
	- FCS_CKM.2: specifying cryptographic key distribution for trusted channel establishment and policy processing. - FCS_COP.1(ENC): specifying the symmetric and asymmetric encryption and decryption algorithms for trusted channel establishment and policy processing. - FCS_COP.1(MAC): specifying the message authentication code algorithms for trusted channel establishment and policy processing - FCS_COP.1(MD): specifying the message digest algorithms for policy processing. - FCS_COP.1(SGN): specifying the digital signature generation and verification algorithms for policy processing - FCS_RNG.1: specifying random number generation used for creating cryptographic keys and master secrets. - FPT_TDC.1: specifying that the TOE must consistently interpret digital certificates and certificate revocation lists. - FTP_ITC.1: specifying that a trusted channel is enforced between the TOE and another trusted IT product.
O.IDAUTH	The objective: "*The TOE must uniquely identify and authenticate the claimed identity of all TOE users, before granting a user access to the TOE and the TOE management functions in the effective application domain*" is satisfied by: - FIA_AFL.1: specifying that an account is locked after a specified number of unsuccessful authentication attempts on the account. - FIA_ATD.1: specifying the user security attributes associated with a TOE user. - FIA_SOS.1: specifying the quality metrics that the password of a user account must meet. - FIA_UAU.2: specifying the authentication of TOE administrators. - FIA_UID.2: specifying the identification of TOE administrators. - FIA_USB.1: specifying the assignment of the effective application domain where the administrator is switched to.
O.ACCESS	The objective: "*The TOE must control access to administrative resources as well as administrative operations based on the role an administrator is assigned to. The TOE must allow authorized administrators to specify the access rights of administrators to resources.*" is satisfied by: - FDP_ACC.1 and FDP_ACF.1: specifying the Domain Access Control Policy. - FMT_MOF.1(AUD): specifying the management of the audit trail and audit trail data. - FMT_MSA.1(DACP) and FMT_MSA.3(DACP): specifying how the Domain Access Control Policy's security attributes are managed by the identified role(s).

Security objectives	Rationale
	● FMT_MSA.1(IFCP) and FMT_MSA.3(IFCP): specifying how the Information Flow Control Policy's security attributes are managed by the identified role(s). ● FMT_MTD.1(AUD): specifying how the audit level is managed by the identified role(s). ● FMT_MTD.1(TIME): specifying how time and date are managed by the identified role(s). ● FMT_MTD.1(DACP): specifying how the Domain Access Control Policy is managed by the identified role(s). ● FMT_MTD.1(IFCP): specifying how the Information Flow Control Policy is managed by the identified role(s). ● FMT_MTD.1(CRYPTO): specifying how cryptographic material is managed by the identified role(s). ● FMT_MTD.2: specifying how unsuccessful authentication attempts are managed by the identified role(s). ● FMT_SMF.1: specifying the management of audit function, authentication data, and the information flow control policy. ● FMT_SMR.1: specifying the user roles supported by the TOE.
O.MEDIAT	The objective: "*The TOE must mediate the flow of all information between clients and servers located on internal and external networks governed by the TOE*" is satisfied by: ● FDP_IFC.1: specifying the Information Flow Security Function Policy components for information flow control. ● FDP_IFF.1: specifying the Information Flow Security Function Policy rules for information flow control.

Table 14: Security objectives for the TOE rationale

6.2.3 Security requirements dependency analysis

The following table demonstrates the dependencies of SFRs modeled in CC Part 2 and how the SFRs for the TOE resolve those dependencies.

Security functional requirement	Dependencies	Resolution
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_SEL.1	FAU_GEN.1	FAU_GEN.1
	FMT_MTD.1	FMT_MTD.1(AUD)

Security functional requirement	Dependencies	Resolution
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.4	FAU_STG.1	FAU_STG.1
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1]	FCS_COP.1(ENC)
	FCS_CKM.4	This dependency is unresolved. The generated keys are not formally destroyed. The object reuse mechanisms in the runtime environment prevent their use except for the intended context.
FCS_CKM.2	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
	FCS_CKM.4	This dependency is unresolved. The generated keys are not formally destroyed. The object reuse mechanisms in the runtime environment prevent their use except for the intended context.
FCS_COP.1(ENC)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
	FCS_CKM.4	This dependency is unresolved. The keys used for encryption, decryption, and data authentication are not formally destroyed. The object reuse mechanisms in the runtime environment prevent their use except for the intended context.
FCS_COP.1(MAC)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
	FCS_CKM.4	This dependency is unresolved. The keys used for encryption, decryption, and data authentication are not formally destroyed. The object reuse mechanisms in the runtime environment prevent their use except for the intended context.
FCS_COP.1(MD)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	This dependency is unresolved. Message digests do not use keys.
	FCS_CKM.4	This dependency is unresolved. Message digests do not use keys.
FCS_COP.1(SGN)	[FDP_ITC.1 or FDP_ITC.2 or FCS_CKM.1]	FCS_CKM.1
	FCS_CKM.4	This dependency is unresolved. The keys used for message signing and verification are not formally destroyed. The object reuse mechanisms in the runtime environment prevent their use except for the intended context.

Security functional requirement	Dependencies	Resolution
FCS_RNG.1	No dependencies.	
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1	FDP_ACC.1
	FMT_MSA.3	FMT_MSA.3(DACP)
FDP_IFC.1	FDP_IFF.1	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1	FDP_IFC.1
	FMT_MSA.3	FMT_MSA.3(IFCP)
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_ATD.1	No dependencies.	
FIA_SOS.1	No dependencies.	
FIA_UAU.2	FIA_UID.1	FIA_UID.2
FIA_UID.2	No dependencies.	
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_MOF.1(AUD)	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.1(DACP)	[FDP_ACC.1 or FDP_IFC.1]	FDP_ACC.1
	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.1(IFCP)	[FDP_ACC.1 or FDP_IFC.1]	FDP_IFC.1
	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MSA.3(DACP)	FMT_MSA.1	FMT_MSA.1(DACP)
	FMT_SMR.1	FMT_SMR.1
FMT_MSA.3(IFCP)	FMT_MSA.1	FMT_MSA.1(IFCP)
	FMT_SMR.1	FMT_SMR.1
FMT_MTD.1(AUD)	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1

Security functional requirement	Dependencies	Resolution
FMT_MTD.1(TIME)	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MTD.1(DACP)	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MTD.1(IFCP)	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MTD.1(CRYPTO)	FMT_SMR.1	FMT_SMR.1
	FMT_SMF.1	FMT_SMF.1
FMT_MTD.2	FMT_MTD.1	FMT_MTD.1(DACP)
	FMT_SMR.1	FMT_SMR.1
FMT_SMF.1	No dependencies.	
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FPT_TDC.1	No dependencies.	
FPT_STM.1	No dependencies.	
FTA_TSE.1	No dependencies.	
FTP_ITC.1	No dependencies.	
FTP_TRP.1	No dependencies.	

Table 15: TOE SFR dependency analysis

6.3 Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 4 components as specified in [CC] part 3, augmented by ALC_FLR.3.

The following table shows the security assurance requirements (SARs), and the operations performed on the components according to CC part 3: iteration (Iter.), refinement (Ref.), assignment (Ass.) and selection (Sel.).

Security assurance class	Security assurance requirement	Source	Operations			
			Iter.	Ref.	Ass.	Sel.
ADV Development	ADV_ARC.1 Security architecture description	CC Part 3	No	No	No	No
	ADV_FSP.4 Complete functional specification	CC Part 3	No	No	No	No

Security assurance class	Security assurance requirement	Source	Operations			
			Iter.	Ref.	Ass.	Sel.
	ADV_IMP.1 Implementation representation of the TSF	CC Part 3	No	No	No	No
	ADV_TDS.3 Basic modular design	CC Part 3	No	No	No	No
AGD Guidance documents	AGD_OPE.1 Operational user guidance	CC Part 3	No	No	No	No
	AGD_PRE.1 Preparative procedures	CC Part 3	No	No	No	No
ALC Life-cycle support	ALC_CMC.4 Production support, acceptance proce dures and automation	CC Part 3	No	No	No	No
	ALC_CMS.4 Problem tracking CM coverage	CC Part 3	No	No	No	No
	ALC_DEL.1 Delivery procedures	CC Part 3	No	No	No	No
	ALC_DVS.1 Identification of security measures	CC Part 3	No	No	No	No
	ALC_FLR.3 Systematic flaw remediation	CC Part 3	No	No	No	No
	ALC_LCD.1 Developer defined life-cycle model	CC Part 3	No	No	No	No
	ALC_TAT.1 Well-defined development tools	CC Part 3	No	No	No	No
ASE Security Target evaluation	ASE_INT.1 ST introduction	CC Part 3	No	No	No	No
	ASE_CCL.1 Conformance claims	CC Part 3	No	No	No	No
	ASE_SPD.1 Security problem definition	CC Part 3	No	No	No	No
	ASE_OBJ.2 Security objectives	CC Part 3	No	No	No	No
	ASE_ECD.1 Extended components definition	CC Part 3	No	No	No	No
	ASE_REQ.2 Derived security requirements	CC Part 3	No	No	No	No
	ASE_TSS.1 TOE summary specification	CC Part 3	No	No	No	No
ATE Tests	ATE_COV.2 Analysis of coverage	CC Part 3	No	No	No	No
	ATE_DPT.1 Testing: basic design	CC Part 3	No	No	No	No
	ATE_FUN.1 Functional testing	CC Part 3	No	No	No	No
	ATE_IND.2 Independent testing - sample	CC Part 3	No	No	No	No
AVA Vulnerability assessment	AVA_VAN.3 Focused vulnerability analysis	CC Part 3	No	No	No	No

Table 16: Security assurance requirements (SARs)

6.4 Security Assurance Requirements Rationale

The evaluation assurance level has been chosen to match an Enhanced-Basic attack potential commensurate with the threat environment that is experienced by typical consumers of the TOE. In addition, the evaluation assurance level has been augmented with ALC_FLR.3 commensurate with the augmented flaw remediation capabilities offered by the developer beyond those required by the evaluation assurance level.

7 TOE Summary Specification

7.1 TOE Security Functionality

7.1.1 Security audit

The audit facility records a specific set of events including all required TOE auditable events. Audit records are stored on the network appliance's flash memory and hence are stable across reboots. The TOE generates audit records of the following event types:

- system events (start and stop of the audit function, configuration and management of the audit functions, shutdown and restart, etc);
- authentication events (use of the identification mechanism, use of the authentication mechanism, reaching of the threshold for unsuccessful authentication attempts);
- management events (application domains, files and directories, administrator accounts and roles, changes to the time); and
- requests and decisions for information flow.

When the TOE generates an audit record, it contains at least the following:

- Timestamp: date and time of the audit event,
- Event Type: the type of event that is audited,
- Identity: subject identity associated with the audited event, and
- Event Status: success or failure.

The DataPower CLI provides commands for reviewing the audit log. The audit records can be searched or sorted based on user identity, presumed subject address, ranges of dates, ranges of times, and ranges of addresses.

The TOE provides authorized administrators with the functions necessary to start, stop, configure, and manage the audit function, including selecting the level of audit (full or standard). The TOE also allows the authorized administrator to observe, search, and sort the set of audited events.

The level of audit determines whether information flow requests and decisions are audited (full) or not (standard); all other audited events are always generated regardless of the audit level chosen.

An authorized administrator can read the audit records; however, only the TOE can write to the audit log, and it is not directly modifiable by administrators. In other words, there are no means for administrators to manually edit the audit log on the TOE.

In order to prevent audit data loss, the Router sets aside filesystem space at boot time. The Router splits the specified "reserve space" into a "hard reserve" and a "soft limit". When an audit entry is about to be written to persistent storage, the Router checks how much free space is available. If the amount free is below the soft limit value, the Router will shutdown all data-processing activities.

In addition to shutting down data-processing activities, the Router will free up the hard reserve space. This will let an administrator login, move older audit files off-host, and delete moved audit files to free up space, auditing all the activities performed by the administrator. Once space is freed up, the network appliance will resume data processing.

The Security Audit function is designed to satisfy the following security functional requirements:

- FAU_GEN.1: the TOE fulfills this requirement by generating all the required events and including all necessary parameters in the audit records.

- FAU_SAR.1: the TOE fulfills this requirement by providing CLI commands for reviewing the audit log.
- FAU_SAR.3: the TOE fulfills this requirement by providing CLI commands to search and sort the audit log based on the options specified in this requirement.
- FAU_SEL.1: the TOE fulfills this requirement by selecting the audit events to be generated based on the audit level.
- FAU_STG.1 and FAU_STG.4: the TOE fulfills these requirements by restricting access to the audit log to the authorized administrator and by providing a mechanism to control loss of audit records if the audit log becomes full.
- FPT_STM.1: the TOE fulfills this requirement by providing timestamps for all audit event records. The TOE uses the SNTP protocol to maintain a reliable time.

7.1.2 Cryptographic support

The TOE provides cryptographic support for the following security functionality:

- Secure communication between the TOE and application endpoints through the establishment of TLS version 1.2 and SSH version 2 sessions. The secure transport layer used depends on the upper protocol (e.g. HTTPS uses TLS, SFTP uses SSH).
- Secure remote access to the command-line interface by administrators and from the command-line interface to remote computers through the establishment of SSH version 2 sessions.
- Digital signing and verification of XML payloads.
- Encryption and decryption of XML payloads.

The cryptographic support functionality is designed to satisfy the following security functional requirements:

- FCS_CKM.1: the TOE fulfills this requirement by generating cryptographic keys.
- FCS_CKM.2: the TOE fulfills this requirement by establishing cryptographic keys.
- FCS_COP.1(ENC): the TOE fulfills this requirement by performing both symmetric and asymmetric encryption and decryption.
- FCS_COP.1(MAC): the TOE fulfills this requirement by generating HMAC and MAC message authentication codes.
- FCS_COP.1(MD): the TOE fulfills this requirement by generating multiple message digests.
- FCS_COP.1(SGN): the TOE fulfills this requirement by performing digital signature generation and verification.
- FPT_TDC.1: the TOE fulfills this requirement by consistently interpreting digital certificates and certificate revocation lists (CRLs).
- FPT_STM.1: the TOE fulfills this requirement by providing timestamps for certificate validation. The TOE uses the SNTP protocol to maintain a reliable time.

The following sections describe the cryptographic algorithms and sizes that the TOE provides for the functionality mentioned above.

7.1.2.1 TLS version 1.2

The TLS version 1.2 protocol is implemented according to [RFC5246]☝ and [RFC5746]☝. The protocol allows the establishment of a secure session for the HTTPS and FTP over TLS protocols.

TLSv1.2 provides server authentication and client authentication (optional) using digital certificates; for that purpose the TOE also supports certificate validation and the use of certificate revocation lists according to [RFC5280] (see section 7.1.2.5).

The following cipher suites are supported:

- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

Cryptographic keys for the following algorithms with respective key sizes are generated:

- AES keys with 128 and 256 bits
- Triple-DES keys with 168 bits
- HMAC keys with 160 and 256 bits

Encryption algorithms supported:

- RSAES-PKCS1-v1_5 with key sizes 1024, 2048, and 4096 bits
- AES (CBC mode) with key sizes 128 and 256 bits
- Triple-DES (CBC mode) with key size 168 bits

Message Authentication Code (MAC) algorithms supported:

- MAC-SHA-1 and HMAC-SHA-1 (160 bits)
- MAC-SHA-256 and HMAC-SHA-256 (256 bits)

Digital signature verification and generation algorithms, and key sizes supported:

- RSASSA-PKCS1-v1_5 with SHA-1 and SHA-256; 1024, 2048, and 4096 bits

7.1.2.2 SSH version 2

The SSH version 2 protocol is implemented according to [RFC4253]. The protocol allows the establishment of a secure session for SFTP server and poller handlers, SCP commands invoked from the command-line interface, and remote sessions started by administrators.

SSH-2 provides server authentication using a host private key. When SSH-2 is used in the context of an SFTP connection, password and public-key authentication is supported either in client or server mode. DSA and RSA key pairs are supported for public-key authentication.

In remote administration sessions, only password authentication is supported for SSH clients.

Cryptographic keys for the following algorithms with respective key sizes are generated:

- AES keys with 128, 192, and 256 bits
- Triple-DES keys with 168 bits
- HMAC keys with 160 bits

Encryption algorithms supported:

- AES (CBC and CTR modes) with key sizes 128, 192, and 256 bits
- Triple-DES (CBC mode) with key size 168 bits

Message Authentication Code (MAC) algorithms supported:

- HMAC-SHA-1 (160 bits)

Digital signature verification and generation algorithms, and key sizes supported:

- DSA with SHA-1 (L = 1024 bits, N = 160 bits)
- RSASSA-PKCS1-v1_5 with SHA-1; 1024, 2048, and 4096 bits

7.1.2.3 XML signature

The TOE implements digital signature generation and verification of XML messages according to [W3CXMLSIG].

MAC (Message Authentication Code) algorithms supported:

- HMAC-SHA-1 (160 bits)

Digital signature verification and generation algorithms, and key sizes supported:

- HMAC-SHA-1 (160 bits, minimum 80 bits)
- DSA with SHA-1: L = 1024 bits, N = 160 bits
- RSASSA-PKCS1-v1_5 with SHA-1, SHA-256, SHA-384, and SHA512; 1024, 2048, and 4096 bits

7.1.2.4 XML encryption

The TOE implements encryption and decryption of XML payloads according to [W3CXMLENC].

Encryption algorithms and key sizes supported:

- AES: 128, 192, and 256 bits
- Triple-DES: 168 bits

Key transport and wrapping algorithms, and key sizes supported:

- RSAES-PKCS1-v1_5 and RSAES-OEAP: 1024, 2048, and 4096 bits
- AES: 128, 192, and 256 bits
- Triple-DES: 168 bits

7.1.2.5 Certificate validation

The TOE supports validation of X.509 digital certificates according to [RFC5280]. The TOE performs full certificate chain checking using Public Key Infraestructure X.509 (PKIX), verifies the expiration of the certificate (assuming a reliable time provided by the TOE), and verifies its revocation using Certificate Revocation Lists (LDAP or HTTP protocol).

The following extensions for CA certificates can be marked as critical; a certificate containing any other critical extension causes the certificate to be rejected.

- Key Usage (not required): if present, it must indicate that the key is suitable for certificate signing.
- Subject Alternative Name (not used): regardless of its criticality, validation does not reject a certificate if it contains the extension.
- Basic Constraints: fully implemented in accordance to [RFC5280].
- Certificate Policies: fully implemented in accordance to [RFC5280].
- Authority Information Access: only used for the Online Certificate Status Protocol (OCSP). Not supported in the evaluated configuration.
- Policy Constraints: fully implemented in accordance to [RFC5280].
- Inhibit Any-Policy: fully implemented in accordance to [RFC5280].

Other non-critical extensions are ignored.

Failure in certificate validation implies that the digital certificate cannot be trusted and therefore the cryptographic operation using the certificate (digital verification, authentication, etc.) fails.

Digital certificates must be imported into the TOE; although the TOE supports the generation of certificate signing requests, this functionality is not allowed in the evaluated configuration.

Additionally, the TOE assumes that the security strength of the private key and the hashing algorithm used in the certificate is sufficient and does not provoke any weakness).

7.1.2.6 Random number generation

The TOE includes a Deterministic Random Number Generator (DRNG) used to create master secrets and symmetric keys for the communication protocols. The DRNG is seeded with random data provided by the blocking version of the Random Number Generator (RNG) implemented in the underlying operating system (/dev/random).

In case the seed source does not have enough entropy, the TOE uses the unblocking version of the RNG implemented in the underlying operating system (/dev/urandom) as a fallback mechanism for creating master secrets and symmetric keys.

7.1.3 User data protection

All traffic through the TOE is subject to the information flow policies. The TOE allows the definition of rules that filter traffic based on the following information:

- IP source address
- IP destination address
- TCP port
- Request URL
- Message content
- XML Schema Definition
- XML signature
- Identity assertion obtained from XML standards-based messages or transport layer information (see definition in FDP_IFF.1)
- Protocol header (HTTP, HTTPS, FTP, FTP over SSL, SFTP) attributes
- Size of message

The authorized administrator has the ability to establish the information flow control policy through an internal data model consisting of the following object groups:

- Services: Multi-Protocol Gateway, Web Service Proxy, and XML Firewall.
- Front side protocol handlers: HTTP, HTTPS, FTP, SFTP.
- Access Control Lists: allows or denies IP addresses.
- Authentication, Authorization and Auditing policies.
- Application Security and Processing Policies: Matching Rules, Web Request and Web Respond Profiles, Processing Rules, URL Rewrite Policies.
- Cryptography: SSL Proxy Profiles, Crypto Profiles, Identification Credentials, Certificate and Key Aliases, digital certificates, and private keys.

Not all services are supported in all appliance models. The following table shows the differences between the three models supported in this evaluation.

Object	XG45	XI52	XB62
SFTP Poller Front Side Handler		✓	✓
SFTP Server Front Side Handler		✓	✓
XML Firewall Service	✓	✓	

Table 17: Information flow control policy object support (only differences)

Administrators configure information flow control policies to allow or deny traffic flow using a combination of objects belonging to these groups and their related attributes. By default, no traffic is permitted to flow.

For application protocols supported by the TOE (HTTP, HTTPS, FTP, FTP over SSL, SFTP), the TOE denies any access or service requests that do not conform to its associated published protocol specification (e.g., RFC). The TOE can also verifies well-formed JSON, XML, and SOAP messages according to the corresponding specification. The TOE also does not accept oversized messages

The TOE can reject XML and SOAP messages based on schema validation. The TOE can also reject messages with external references, or potentially malicious XML messages based on exceeding certain threshold values (node size, element depth, attribute count).

The TOE can also perform XML signature generation and validation, XML encryption, and XML canonicalization according to [W3CXMLSIG], [W3CXMLENC], [W3CXMLC14N], and [W3CXMLEXCC14N]. XML files are canonicalized before signatures are generated.

Only XML well-formedness and conformance to XML related standards are subject to evaluation; not the prevention of XML based attacks (e.g. XSW).

The TOE can also extract identity assertions from the transport protocol messages (e.g. HTTP Basic Authentication header) and XML messages and perform authentication and authorization. The TOE uses the AAA framework (Authentication, Authorization and Audit) to support several authentication and authorization mechanisms, which can be internally implemented (e.g., validation of an SSL client certificate) or through requests to authentication and/or authorization systems located in the operational environment. Both authentication and authorization are rules in the information flow control policy: any failure in these steps causes the incoming message to be rejected.

The TOE also enforces the Domain Access Control Policy based on application domains. An application domain is a set of directories and files used for the creation and maintenance of the information flow control policy, so the TOE itself can be partitioned in different application environments. Access control is enforced in both ways: by allowing domain administrators to switch only to those domains that they are allowed, administrators can only configure the information flow control policy the authorized domains; by controlling access to objects through file permissions (predefined in all directories and configurable in the local: directory), administrators can perform files and directory operations in only the authorized domains and directories.

A global domain known as the "default" domain consists of directories used for specific purposes (e.g. the audit: directory allocates the audit logs), some are shared to the rest of the domains (pubcerts: and sharedcerts; directories) while some others are not visible from other domains. The administrator performs global security management functions and operations on files and directories belonging to this domain; only administrators with the privileged administrator role can access the "default' domain.

An application domain is created for a given set of backend services. The application domain has a predefined directory structure, and each directory has predefined file permissions; the only exception is the local: directory whose file permissions can be configured by an administrator with the privileged administrator role. Application domains can be configured to have visibility to other domains, in that case, the application domain can access objects under the local: directory of application domains, and the store: directory of the "defined" domain.

The User data protection function is designed to satisfy the following security functional requirements:

- FDP_ACC.1: the TOE enforces the Domain Access Control Policy on all traffic flows.
- FDP_ACF.1: the TOE permits the authorized administrator to establish access control rules based on all attributes specified in the requirement.
- FDP_IFC.1: the TOE enforces the Information Flow Control Policy on all traffic flows.
- FDP_IFF.1: the TOE permits the authorized administrator to establish traffic flow rules based on all attributes specified in the requirement. By default, no traffic flows are permitted.

7.1.4 Identification and authentication

When an administrator attempts to access the TOE through the CLI administrator interface, the administrator must provide a user name and password at the login dialog. Only authorized administrators may log into the TOE. Access is only allowed after the TOE verifies the administrator name and password provided against the account database that it maintains. The TOE is configured so that it locks a user account after a number of unsuccessful attempts (i.e., failed login attempts) defined by an authorized administrator. The threshold range is between 1 to 64, and the default login failure threshold is 3. Once that number is reached, the administrator cannot login until an administrator with the privileged administrator role resets the locked administrator account. The "admin" account (which is hardcoded) is the only account that is not locked permanently: if it is not reset by another administrator, the account is unlocked after 120 minutes.

When an administrator attempts to access the TOE through the CLI administrator interface using remote connection (SSH), the TOE enforces the information flow control policy on that connection before the user is authenticated. For example, the TOE can verify whether the SSH connection is established from a IP address that matches the access control list associated with the SSH service.

The TOE maintains the following information of the administrator:

- User account
- Password
- Access level
- Application domains

The TOE also keeps the effective application domain where the administrator switches to after authentication and during the session in the command-line interface (CLI). After a successful login, the TOE allows the administrator to choose one of the application domains to which is member, and set it as the effective application domain; a similar behavior occurs when the administrator switches to another application domain with the "switch domain" command. If the administrator has only one application domain assigned, the TOE automatically switches to that application domain.

The Identification and Authentication function is designed to satisfy the following security functional requirements:

- FIA_AFL.1: the TOE fulfills this requirement by preventing login of administrators who have reached a defined threshold of unsuccessful authentication attempt.

- FIA_ATD.1: the TOE fulfills this requirement by maintaining administrator accounts that contains administrator user identity (i.e., user name) and role information for individual administrators.
- FIA_UID.2: the TOE fulfills this requirement by preventing administrator access to the TOE until the administrator is successfully identified and authenticated.
- FIA_UAU.2: the TOE fulfills this requirement by preventing administrator access to the TOE until the administrator is successfully identified and authenticated. Incoming and outgoing messages to the security management interface is permitted before user is authenticated but subject to the information flow policies.
- FIA_USB.1: the TOE fulfills this requirement by assigning the effective application domain from the list of application domains allowed to the administrator.
- FTA_TSE.1: the TOE fulfills this requirement by denying remote administrative access based on a list of allowed and denied IP addresses.

7.1.5 Security management

The TOE provides system wide and domain-specific management functions through a command-line interface (CLI) to users with the following roles:

- Privileged administrator role: has access to all application domains, including the "default" domain, and all TOE security functionality.
- Privileged domain administrator role: has access to functions only on the application domain the administrator has access to. Administrators with this role do not have access to the "default" domain.

In terms of security management, an application domain is a unit of administration and works as an environment: when an administrator switches into an application domain, the administrator performs security management functions in that application domain exclusively.

The table below shows the security management functions available, their scope of application (system wide, domain specific) and the roles that can perform them.

Security Management Function	System wide	Domain	Privileged Administrator Role	Privileged Domain Administrator Role
Set the audit level of the TOE	✓		✓	
Create, modify, and delete application domains, change default values of application domain properties	✓		✓	
Create, modify, and delete users, change default values of user properties (access level and application domain membership)	✓		✓	
Reset user accounts that have been locked	✓		✓	
Specify the password policy to be enforced when an administrator account is created or the administrator password is changed	✓		✓	
Specify the threshold for the number of authentication attempt failures	✓		✓	

Security Management Function	System wide	Domain	Privileged Administrator Role	Privileged Domain Administrator Role
Create, modify, and delete objects comprising the Information Flow Control Policy	✓	✓	✓	Allowed domains
Set the time and date used to form the timestamps included in the audit records and perform certificate validation (the timestamp is provided by the operational environment, but the administrator can set the time and date from the TOE)	✓		✓	
Manage digital certificates (import, export) and cryptographic keys (import, export)	✓	✓	✓	Allowed domains

Table 18: Security Management Functions by administrator role

The TOE provides permissive values to the Domain Access Control Policy: when an administrator with the administrator privileged role creates a user, the TOE assigns by default an access level of "user" and leaves the user with no application domain assigned. The administrator then changes the access level to "privileged" and sets the proper role assigning the corresponding application domains or none.

Similarly, when an administrator creates an application domain the TOE assigns full access for the local: directory; the administrator then can change the file permissions to restrict the different operations that can be performed on directories and files according to the Domain Access Control Policy specified in FDP_ACF.1.

The TOE provides restrictive values to the Information Flow Control Policy: by default, the TOE does not accept network traffic until the administrator creates system wide or application domain specific objects to configure the different services, protocol handlers, and processing rules.

The Security Management function is designed to satisfy the following security functional requirements:

- FIA_SOS.1: the TOE fulfills this requirement by ensuring that a new password meet a minimum quality metric when a user is created or a password is changed by an authorized administrator.
- FMT_MOF.1(AUD): the TOE fulfills this requirement by restricting management of the audit function to authorized administrators.
- FMT_MSA.1(DACP): the TOE fulfills this requirement by allowing only authorized administrators to modify security attributes used by the Domain Access Control Policy.
- FMT_MSA.1(IFCP): the TOE fulfills this requirement by allowing only authorized administrators to create and modify the security attributes used by the Information Flow Control Policy.
- FMT_MSA.3(DACP): the TOE fulfills this requirement by providing permissive default values for security attributes for the Domain Access Control Policy and allowing only authorized administrators to specify alternate initial values.
- FMT_MSA.3(IFCP): the TOE fulfills this requirement by providing restrictive default values for security attributes for the Information Flow Control Policy and allowing only authorized administrators to specify alternate initial values.

- FMT_MTD.1(AUD): the TOE fulfills this requirement by restricting the management of the audit trail data to authorized administrators.
- FMT_MTD.1(TIME): the TOE fulfills this requirement by restricting time-setting functions to authorized administrators.
- FMT_MTD.1(DACP): the TOE fulfills this requirement by restricting security management functions on users and application domains to authorized administrators.
- FMT_MTD.1(IFCP): the TOE fulfills this requirement by restricting security management functions on objects comprising the information control security policy to authorized administrators.
- FMT_MTD.1(CRYPTO): the TOE fulfills this requirement by restricting security management functions on cryptographic material to authorized administrators.
- FMT_MTD.2: For FMT_MTD.2.1, the TOE fulfills this requirement by allowing the configuration of the login failure threshold only to authorized administrators. For FMT_MTD.2.2, the TOE fulfills this requirement by locking out an administrator who has exceeded the login failure threshold until the account is reset by an authorized administrator.
- FMT_SMF.1: the TOE fulfills this requirement by allowing only authorized administrators to access and administrate the claimed security functions.
- FMT_SMR.1: the TOE fulfills this requirement by maintaining administrator roles, and associating administrators with the role.

7.1.6 Protection of the TOE security functionality

The TOE provides protected communications between the TOE and another trusted IT product (e.g., clients, other devices) via the SSH version 2 and TLS version 1.2 protocols.

For the TLS protocol, the TOE provides certificate validation interpreting public key certificates and certificate revocation lists according to [RFC5280].

For the SSH protocol, the TOE verifiies the signature generated by the SSH client according to the Public Key authentication method defined in [RFC4252].

Additionally, the TOE synchronizes the real time clock and provides reliable timestamps using the Network Time Protocol according to [RFC2030]. Timestamps are used for certificate validation as well as the generation of audit records.

The cryptographic support function is designed to satisfy the following security functional requirements:

- FPT_TDC.1: the TOE fulfills this requirement by consistently interpreting public keys, digital certificates, and certificate revocation lists (CRLs).
- FPT_STM.1: the TOE fulfills this requirement by providing timestamps for audit generation and certificate validation. The TOE uses the SNTP protocol to maintain a reliable time.

7.1.7 Trusted channel

The TOE establishes a trusted channel with IT entities for incoming and outgoing messages when the information flow control policy enforces the use of one of the following protocols:

- HTTPS according to [RFC2818],
- SFTP according to [SFTP], and
- FTP according to [RFC4217].

The TOE also establishes a trusted channel for administrative communication between itself and a remote administrator using an SSH client. This SSH client initiates the communication by contacting the TOE.

For both purposes, the TOE establishes trusted channels with the following protocols in the evaluated configuration:

- SSH version 2 [RFC4253]☝ (used by the SSH daemon that serves remote administrator sessions, the SCP command supported by the CLI, and the SFTP protocol), and
- TLS version 1.2 [RFC5246]☝ and [RFC5747]☝ (used by the HTTPS and FTP protocols).

For more information on the cryptography, see section 7.1.2.

This function is designed to satisfy the following security functional requirement:

- FTP_ITC.1: the TOE fulfills this requirement by providing secure channels (via TLS and SSH) when the TOE receives or polls messages from a trusted IT product, or sends messages to another trusted IT product.
- FTP_TRP.1: the TOE fulfills this requirement by providing secure channels (via SSH) when a remote administrator communicates with the TOE.

8 Abbreviations, Terminology and References

8.1 Abbreviations

AES
Advanced Encryption Standard

B2B
Business to Business

BST
Binary Security Token

CBC
Cipher Block Chaining

CLI
Command Line Interface

CRL
Certificate Revocation List

CTR
Counter

DNS
Domain Name System

DMZ
Demilitarized Zone

DRNG
Deterministic Random Number Generator

DSA
Digital Signature Algorithm

ebMS
Electronic Business Messaging Service

ESB
Enterprise Service Bus

FIPS
Federal information Processing Standard

FTP
File Transfer Protocol

GbE
Gigabit Ethernet

HMAC
Hash-based MAC

HTTP
Hyper Text Transfer Protocol

HTTPS
Hyper Text Transfer Protocol Secure

IP
Internet Protocol

JSON
JavaScript Object Notation

JMS
Java Message Service

LDAP
Lightweight Directory Access Protocol

LAN
Local Area Network

LCD
Liquid Crystal Display

LED
Light Emitting Diode

LTPA
Lightweight Third Party Authentication

MAC
Message Authentication Code

MQ
Message Queue

NIC
Network Interface Card

OAEP
Optimal Asymmetric Encryption Padding

PKIX
Public Key Infraestructure (X.509)

RADIUS
Remote Authentication Dial In User Service

RAID
Redundant Array of Independent Disks

RNG
Random Number Generator

RSA
Ron Rivest, Adi Shamir, and Leonard Adleman

SAML
Security Assertion Markup Language

SCP
Secure Copy

SDK
Software Development Kit

SFTP
Secure File Transfer Protocol

SHA
Secure Hash Algorithm

SMTP
Simple Mail Transfer Protocol

SNMP
Simple Network Management Pro tocol

SOA
Service-Oriented Architecture

SOAP
Simple Object Access Protocol

SSH
Secure Shell

SSH-2
SSH version 2

SSL
Secure Sockets Layer

TDEA
Triple Data Encryption Algorithm

TLS
Transport Layer Security

TPM
Trusted Platform Module

URL
Uniform Resource Locator

USB
Universal Serial Bus

WebGUI
Web-based Graphical User Interface

WSS
Web Service Security

XPath
XML Path Language

XML
Extensible Markup Language

XSLT
XML Stylesheet Language Tranformations

8.2 Terminology

This section contains definitions of technical terms that are used with a meaning specific to this document. Terms defined in the [CC] are not reiterated here, unless stated otherwise.

External IT entity
An IT entity that interacts with the TOE from outside of the TOE boundary.

External Network
Network connected to the TOE from outside the DMZ. It can be the Internet or a network within the organization.

External TOE interface
TOE interface (i.e. Ethernet port) that is physically connected to the External Network

Internal Network
Network connected to the TOE, located behind the DMZ and whose access to data and services from external IT entities are protected by the TOE.

Internal TOE interface
TOE interface (i.e. Ethernet port) that is physically connected to the Internal Network.

Presumed source address
The client IP address.

Requesting application
Refers to an application or client (e.g., web service, an enterprise application, or a web browser) that are requesting information flow through/from the TOE.

User
Humans or machines interacting with the TOE via the provided user and programmatic interfaces. The term user in this document includes administrators of the TOE unless a specific distinction is made in the text.

User identity
A name that uniquely identifies a user in the TOE.

8.3 References

AESNI **Intel® Advanced Encryption Standard (Intel® AES) Instructions Set**
Version Rev 3.01
Date September 22, 2012
Location https://software.intel.com/sites/default/files/article/165683/aes-wp-2012-09-22-v01.pdf

AIS20 **Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren (Functionality Classes and Evaluation Methodology for Deterministic RNGs)**
Version 3
Date 2013-05-15

AIS31 **Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren (Functionality Classes and Evaluation Methodology for Physical RNGs)**
Version 3
Date 2013-05-15

CC **Common Criteria for Information Technology Security Evaluation**
Version 3.1R4
Date September 2012
Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R4.pdf
Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R4.pdf
Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R4.pdf

DPKC **IBM WebSphere DataPower version 6.0.2 Knowledge Center**
Date received 2015-02-16
Location TBD

FIPS180-4 **SECURE HASH STANDARD (SHS)**
Version FIPS 180-4
Date March 2012
Location http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf

FIPS197 **Specification for the ADVANCED ENCRYPTION STANDARD (AES)**
Version FIPS PUB 197
Date November 26, 2001
Location http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

LTPA **Understanding LTPA**
Date January 2009
Location ftp://public.dhe.ibm.com/software/integration/datapower/library/prod_docs/Misc/UnderstandingLTPA-v1.pdf

OASIS-SAML20 **Security Assertion Markup Language (SAML) v2.0**
Date March 2005
Location https://www.oasis-open.org/standards#samlv2.0

OASIS-WSS **Web Services Security (WSS) v1.1**
Date February 2006
Location https://www.oasis-open.org/standards#wssv1.1

RFC0959 **File Transfer Protocol**
Author(s) J. Postel, J. Reynolds
Date 1985-10-01
Location http://www.ietf.org/rfc/rfc0959.txt

RFC2030 **Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI**
Author(s) D. Mills
Date 1996-10-01
Location http://www.ietf.org/rfc/rfc2030.txt

RFC2104 **HMAC: Keyed-Hashing for Message Authentication**
Author(s) H. Krawczyk, M. Bellare, R. Canetti
Date 1997-02-01
Location http://www.ietf.org/rfc/rfc2104.txt

RFC2616 **Hypertext Transfer Protocol -- HTTP/1.1**
Author(s) R. Fielding, J. Gettys, J. Mogul, H. Frystyk, L. Masinter, P. Leach, T. Berners-Lee
Date 1999-06-01
Location http://www.ietf.org/rfc/rfc2616.txt

RFC2617 **HTTP Authentication: Basic and Digest Access Authentication**
Author(s) J. Franks, P. Hallam-Baker, J. Hostetler, S. Lawrence, P. Leach, A. Luotonen, L. Stewart
Date 1999-06-01
Location http://www.ietf.org/rfc/rfc2617.txt

RFC2818 **HTTP Over TLS**
Author(s) E. Rescorla
Date 2000-05-01
Location http://www.ietf.org/rfc/rfc2818.txt

RFC3447 **Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1**
Author(s) J. Jonsson, B. Kaliski
Date 2003-02-01
Location http://www.ietf.org/rfc/rfc3447.txt

RFC4217 **Securing FTP with TLS**
Author(s) P. Ford-Hutchinson
Date 2005-10-01
Location http://www.ietf.org/rfc/rfc4217.txt

RFC4252 **The Secure Shell (SSH) Authentication Protocol**
Author(s) T. Ylonen, C. Lonvick
Date 2006-01-01
Location http://www.ietf.org/rfc/rfc4252.txt

RFC4253 **The Secure Shell (SSH) Transport Layer Protocol**
Author(s) T. Ylonen, C. Lonvick
Date 2006-01-01
Location http://www.ietf.org/rfc/rfc4253.txt

RFC4344 **The Secure Shell (SSH) Transport Layer Encryption Modes**
Author(s) M. Bellare, T. Kohno, C. Namprempre
Date 2006-01-01
Location http://www.ietf.org/rfc/rfc4344.txt

RFC4627 **The application/json Media Type for JavaScript Object Notation (JSON)**
Author(s) D. Crockford
Date 2006-07-01
Location http://www.ietf.org/rfc/rfc4627.txt

RFC4716 **The Secure Shell (SSH) Public Key File Format**
Author(s) J. Galbraith, R. Thayer
Date 2006-11-01
Location http://www.ietf.org/rfc/rfc4716.txt

RFC5246 **The Transport Layer Security (TLS) Protocol Version 1.2**
Author(s) T. Dierks, E. Rescorla
Date 2008-08-01
Location http://www.ietf.org/rfc/rfc5246.txt

RFC5280 **Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile**
Author(s) D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, W. Polk
Date 2008-05-01
Location http://www.ietf.org/rfc/rfc5280.txt

RFC5746 **Transport Layer Security (TLS) Renegotiation Indication Extension**
Author(s) E. Rescorla, M. Ray, S. Dispensa, N. Oskov
Date 2010-02-01
Location http://www.ietf.org/rfc/rfc5746.txt

RFC5747 **4over6 Transit Solution Using IP Encapsulation and MP-BGP Extensions**
Author(s) J. Wu, Y. Cui, X. Li, M. Xu, C. Metz
Date 2010-03-01
Location http://www.ietf.org/rfc/rfc5747.txt

SFTP **SSH File Transfer Protocol**
Date April 1, 2002
Location http://tools.ietf.org/html/draft-ietf-secsh-filexfer-02

SP800-38A **Recommendation for Block Cipher Modes of Operation: Methods and Techniques**
Version NIST Special Publication 800-38A 2001 Edition
Date December 2001
Location http://csrc.nist.gov/publications/nistpubs/800-38a/sp800-38a.pdf

SP800-67 **Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher**
Version Revision 1
Date January 2012
Location http://csrc.nist.gov/publications/nistpubs/800-67-Rev1/SP-800-67-Rev1.pdf

W3CSOAP **SOAP Version 1.2 Part 1: Messaging Framework (Second Edition)**
Date April 27, 2007
Location http://www.w3.org/TR/soap12-part1/

W3CXML **Extensible Markup Language (XML) 1.0 (Fifth Edition)**
Date November 26, 2008
Location http://www.w3.org/TR/REC-xml/

W3CXMLC14N **Canonical XML Version 1.0**
Date March 15, 2001
Location http://www.w3.org/TR/2001/REC-xml-c14n-20010315

W3CXMLENC **XML Encryption Syntax and Processing**
Date December 10, 2002
Location http://www.w3.org/TR/2002/REC-xmlenc-core-20021210/

W3CXMLEXCC14N **Exclusive XML Canonicalization Version 1.0**
Date July 18, 2002
Location http://www.w3.org/TR/2002/REC-xml-exc-c14n-20020718/

W3CXMLSIG **XML Signature Syntax and Processing (Second Edition)**
Date 10 June 2008
Location http://www.w3.org/TR/2008/REC-xmldsig-core-20080610/

W3CXSD **W3C XML Schema Definition Language (XSD) 1.1 Part 1: Structures**
Date February 2006
Location http://www.w3.org/TR/xmlschema11-1/