Gilian G-Server Version 2.5 Security Target

July 30, 2003

Prepared for:

Gilian Technologies Inc.

1300 Island Drive, Suite 102
Redwood City, CA 94065

Prepared by:

Standards Institution of Israel

Author:	Nir Naaman
Audited by:	David Guttman
Last Edit Date:	July 30, 2003
Revision:	1.0
Document Name:	Gilian G-Server Version 2.5 Security Target.doc

Table of Contents

1. Introduction 7
1.1. ST Identification 7
1.2. ST Overview 7
1.3. Conformance Claims 7
1.4. Conventions 8
1.5. Terminology 12
1.5.1. Glossary 12
1.5.2. Common Abbreviations 16
1.6. Document Organization 17
2. TOE Description 18
2.1. Scope and Boundaries of the TOE 18
2.2. TOE Configuration 19
2.3. TOE Security Functions Scope of Control (TSC) 20
2.3.1. Subjects 20
2.3.2. User Data Objects 20
2.3.3. TSF Data Objects 20
2.4. TOE Security Functionality 21
2.4.1. ExitControl Functionality 21
2.4.2. EntryControl Functionality 23
2.4.3. Alerts 23
2.4.4. TOE Administration 23
2.4.5. Audit Functionality 24
2.4.6. Trusted Path/Channels 24
3. TOE Security Environment 25
3.1. Secure Usage Assumptions 25
3.2. Threats to Security 25
3.3. Organizational Security Policies 27
4. Security Objectives 28
4.1. Security Objectives for the TOE 28

4.2. Security Objectives for the Environment 30
5. IT Security Requirements 31
5.1. TOE Security Functional Requirements 31
5.1.1. Security Audit (FAU) 33
5.1.2. Cryptographic support (FCS) 38
5.1.3. User data protection (FDP) 39
5.1.4. Identification and authentication (FIA) 44
5.1.5. Security management (FMT) 44
5.1.6. Protection of the TOE Security Functions (FPT) 49
5.1.7. Resource utilisation (FRU) 50
5.1.8. TOE access (FTA) 50
5.1.9. Trusted path/channels (FTP) 50
5.2. TOE Security Assurance Requirements 52
5.2.1. Configuration management (ACM) 52
5.2.2. Delivery and operation (ADO) 52
5.2.3. Development (ADV) 53
5.2.4. Guidance documents (AGD) 54
5.2.5. Tests (ATE) 55
5.3. Security Requirements for the IT Environment 56
5.3.1. Trusted path/channels (FTP) 56
6. TOE Summary Specification 57
6.1. TSF Protection Function 57
6.1.1. Operating System 57
6.1.2. Transparency Envelope 57
6.1.3. SFR Mapping 59
6.2. ExitControl 59
6.2.1. HTTP Request/Response Processing for Static Resources 59
6.2.2. HTTP Request/Response Processing for Dynamic Resources 60
6.2.3. Request/Response Stripping 60
6.2.4. Resource Recovery 60
6.2.5. SFR Mapping 61
6.3. EntryControl 61

6.3.1. Limits and Constraints on HTTP Requests 61
6.3.2. Attack Signature Detection 62
6.3.3. SFR Mapping 62
6.4. Security Management Function 62
6.4.1. Roles 63
6.4.2. G-Server Administration 63
6.4.3. Resource Signatures Administration 65
6.4.4. Resource Integrity Verification 66
6.4.5. Pending Signatures 66
6.4.6. SFR Mapping 67
6.5. Audit Functions 68
6.5.1. System Log 68
6.5.2. Signing Logs 68
6.5.3. Verification Logs 68
6.5.4. Alert Log Viewing 68
6.5.5. SFR Mapping 68
6.6. Alerts 69
6.6.1. Email Alerts 69
6.6.2. SNMP Alerts 69
6.6.3. Execution of Preinstalled Executables 69
6.6.4. SFR Mapping 70
6.7. Trusted Path/Channel 70
6.7.1. Trusted Path 70
6.7.2. HTTPS Termination 70
6.7.3. HTTPS 70
6.7.4. TOE Access 70
6.7.5. SFR Mapping 71
6.8. TOE Assurance Measures 73
7. PP Claims 74
8. Rationale 75
8.1. Security Objectives Rationale 75
8.2. Security Requirements Rationale 83

8.2.1. Security Functional Requirements Rationale 83
8.2.2. Security Assurance Requirements Rationale 92
8.2.3. Extended Requirements Rationale 93
8.2.4. Dependency Rationale 96
8.2.5. Internal Consistency and Mutual Support 99
8.3. TOE Summary Specification Rationale 101

List of Tables

Table 1- Conventions for the use of formatting operations 10
Table 5.1 –Functional security components 31
Table 5.2 - Auditable Events 34
Table 5.3 -Management of security functions behaviour 45
Table 5.4- Management of site security attributes 45
Table 5.5- Management of administrator security attributes 46
Table 5.6- Management of TSF data 47
Table 5.7- Specification of Management Functions 48
Table 5.8- Assurance requirements: EAL1 52
Table 5.9 –Security Requirements for the IT Environment 56
Table 6.1- EntryControl Configurable Limits and Constraints 61
Table 6.2- G-Server Management Functions 64
Table 6.3- Resource Signature Management Functions 65
Table 6.4- Resource Integrity Verification Status Codes 66
Table 6.5- TOE Access Parameters 71
Table 6.6- Mapping of Assurance Requirements to TOE Assurance Measures 73
Table 8.1- TOE IT security objectives rationale 75
Table 8.2- Tracing of security objectives to the TOE security environment 76
Table 8.3- Security Objective to Functional Component Mapping 83
Table 8.4- Functional Component Grounding in Security Objectives 84
Table 8.5- Mapping of EAL 1 Assurance Components to Security Objectives 92
Table 8.6- Security Requirements Dependency Mapping 96

Table 8.7- TOE Summary Specification Rationale Mapping 101
Table 8.8- Mapping of Security Functions to SFRs 103

List of Figures

Figure 2.1 –The G-Server 200XL Appliance 18
Figure 2.2 –Traffic Mediation Architecture 19
Figure 2.3 –Integrity Validation Process 21
Figure 2.4 –Static Resource Validation 22
Figure 2.5 –Dynamic Resource Validation 22
Figure 6.1 –Transparency Envelope™ 58

1. Introduction

1.1. ST Identification

Title: Gilian G-Server Version 2.5 Security Target

ST Version: 1.0

ST Date: July 30, 2003

Authors: Nir Naaman

CC Version: Common Criteria for Information Technology Security Evaluation, Version 2.1, August 1999, ISO/IEC 15408, incorporated with interpretations as of 2002-02-28

Keywords: Web, HTTP, SSL, TLS, ExitControl, integrity

1.2. ST Overview

The Gilian G-Server is an appliance that is connected transparently in front of one or more HTTP (Web) servers. It examines all incoming and outgoing traffic for anomalies, and performs two main functions:

- **EntryControl** – protection against application-level attacks on the Web server;
- **ExitControl** – prevents maliciously modified Web resources from being sent out to end-users.

Web servers are notoriously vulnerable to compromise by outsiders. The G-Server is intended to mitigate the damage caused by a defacement attack by ensuring that fraudulent data cannot leave the Web server and reach the end-user. It achieves this objective by providing management tools for digitally signing authentic Web resources ahead of time, and performing real-time verification of data that is flowing out of the Web server using the signatures stored in its database.

1.3. Conformance Claims

The TOE is conformant with the following CC specifications:

- Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, Version 2.1, August 1999, ISO/IEC 15408-2, extended (Part 2 Extended)
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, Version 2.1, August 1999, ISO/IEC 15408-3, Evaluation Assurance Level (EAL) 1.

In this document where conformance to security standards is claimed, conformance is determined by the developer.

1.4. Conventions

The notation, formatting, and conventions used in this security target (ST) are consistent with version 2.1 of the Common Criteria for Information Technology Security Evaluation. Font style and clarifying information conventions were developed to aid the reader.

Naming convention for security environment considerations and for objectives is as follows:

- Assumptions are denoted by the prefix “A.”, e.g. “A.PEER”.

- Organizational Security Policy statements are denoted by the prefix “P.”, e.g. “P.Accountability”.

- Threats are denoted by the prefix “T.”, e.g. “T.Defacement”.

- Objectives for the IT TOE are denoted by the prefix “O.”, e.g. “O.I&A”.

- Objectives for the environment are denoted by the prefix “OE.”, e.g. “OE.PHYSICAL”.

The CC permits four functional and assurance requirement component operations: assignment, iteration, refinement, and selection. These operations are defined in the Common Criteria, Part 1, paragraph 4.4.1 as:

- Iteration: allows a component to be used more than once with varying operations;

- Assignment: allows the specification of parameters;

- Selection: allows the specification of one or more items from a list; and

- Refinement: allows the addition of details.

<u>Iteration</u>

Where necessary to cover different aspects of the same requirement (e.g. identification of more than one type of user), repetitive use of the same component to cover each aspect is permitted. Iteration is used together with assignment, selection, and refinement in order to specify the different iterations. In this document, iterations are identified with a number inside parentheses ("(#)"). These follow the short family name and allow components to be used more than once with varying operations. The component behaviour name includes information on the purpose of the specified iteration.

<u>Assignment</u>

Some components have elements that contain parameters that enable the ST author to specify a set of values for incorporation into the ST to meet a security objective. These elements clearly identify each parameter and constraint on values that may be assigned to that parameter. Any aspect of an element whose acceptable values can be unambiguously described or enumerated can be represented by a parameter. The parameter may be an attribute or rule that narrows the requirement to a specific value or range of values. For instance, based on a security objective, an element within a component may state that a

given operation should be performed a number of times. In this case, the assignment would provide the number, or range of numbers, to be used in the parameter.

Selection

This is the operation of picking one or more items from a list in order to narrow the scope of an element within a component.

Refinement

For all components, the ST author is permitted to limit the set of acceptable implementations by specifying additional detail in order to meet a security objective. Refinement of an element within a component consists of adding these technical details. In order for a change to a component to be considered a valid refinement, the change must satisfy all the following conditions:

- A TOE meeting the refined requirement would also meet the original requirement, as interpreted in the context of the ST;

- In cases where a refined requirement is iterated, it is permissible that each iteration address only a subset of the scope of the requirement; however, the sum of the iterations must together meet the entire scope of the original requirement;

- The refined requirement does not extend the scope of the original requirement; and

- The refined requirement does not alter the list of dependences of the original requirement.

Extended requirements are additional functional requirements defined in this ST that are not contained in Part 2 and/or additional assurance requirements not contained in Part 3. These requirements are used when security functionality is provided by the TOE that cannot be described by Part 2 or Part 3 requirements. A rationale for the usage of such extended requirements is given in section 8.2.3. Extended requirements receive names similar to existing Part 2 and Part 3 components, with an additional suffix of _EX which is appended to the component's short name. Alternatively, where an appropriate NIAP interpretation provides NIAP-style labeling, that labeling is used for the extended requirement.

Application Notes are used to clarify the author's intent for a given requirement. These are italicized and will appear following the component needing clarification.

These conventions are expressed by using combinations of bolded, italicized, and underlined text as specified in Table 1 below.

Table 1- Conventions for the use of formatting operations

Convention	Purpose	Operation
Boldface	Boldface text denotes completed component assignments. Example: *5.1.3.2. Protected authentication feedback (FIA_UAU.7)* FIA_UAU.7.1 The TSF shall provide only **obscured feedback** to the user while the authentication is in progress.	(completed) Assignment
<u>Underline</u>	Underlined text denotes completed component selections (out of a set of selection options provided in the original CC requirement). Example: FTP_ITC.1.2 The TSF shall permit <u>the TSF</u> to initiate communication via the trusted channel.	(completed) Selection
<u>Boldface Underline</u>	Underlined boldface text highlights component refinements. Example: *5.1.1.6. Selectable audit review [System Log] (FAU_SAR.3 (1))* FAU_SAR.3.1 The TSF shall provide the ability to perform <u>searches and sorting</u> of audit data **<u>in the System Log</u>** based on **the following criteria:** …	Refinement
Parentheses (iteration #)	Parentheses and an iteration number inform the reader that the requirement component will be used multiple times. Example: *5.1.1.6. Selectable audit review [System Log] (FAU_SAR.3 (1))* FAU_SAR.3.1 The TSF shall provide the ability to perform <u>searches and sorting</u> of audit data **<u>in the System Log</u>** based on **the following criteria:** … *5.1.1.8. Selectable audit review [Signing Log] (FAU_SAR.3 (3))* FAU_SAR.3.1 The TSF shall provide the ability to perform <u>searches and sorting</u> of audit data **<u>in the Signing Log</u>** based on **the following criteria:** …	Iteration 1 (FAU_SAR.3) Iteration 3 (FAU_SAR.3)

Convention	Purpose	Operation
Italics	Italics are used for application notes. Example: *Application Note:* *The default values are permissive in the sense that a resource that is not explicitly covered by an exception or verification rule, or a defined site that has not been specified as protected will default to an unprotected mode.*	Application Note
Extended Requirement (_EX)	The suffix "_EX" denotes an extended requirement that was not taken from Part 2 or Part 3 of the CC, but was defined specifically to provide security functionality that is relevant to this ST. An alternative notation is used for extended requirements taken from NIAP interpretations. Examples: *5.1.2.11. Inter-TSF user data monitoring (FDP_SDI_EX.1)* FDP_SDI_EX.1.1 The TSF shall provide a capability to monitor user data stored within a remote trusted IT product at the request of the authorised user. *5.1.1.2. Audit data generation (FAU_GEN.1-NIAP-0347)* FAU_GEN.1.1-NIAP-0347 The TSF shall be able to generate an audit record of the following auditable events:	Extended Requirement NIAP-style Extended Requirement

1.5. Terminology

In the Common Criteria, many terms are defined in Section 2.3 of Part 1. The following sections are a refined subset of those definitions, listed here to aid the user of this ST. The glossary is augmented with terms that are specific to the G-Server product.

1.5.1. Glossary

In the Common Criteria, many terms are defined in Section 2.3 of Part 1. The following are a subset of those definitions. They are listed here to aid the user of this ST.

Access Interaction between an entity and an object that results in the flow or modification of data.

Access Control Security service that controls the use of resources[1] and the disclosure and modification of data.[2]

Accountability Property that allows activities in an IT system to be traced to the entity responsible for the activity.

Administrator A user who has been specifically granted the authority to manage some portion or all of the TOE and whose actions may affect the TSP. Administrators may possess special privileges that provide capabilities to override portions of the TSP. G-Server administrators are identified users associated with the following G-Server roles:

- G-Master – user with full administrative rights.
- Signer and Viewer – users with limited administrative rights.

Assurance A measure of confidence that the security features of an IT system are sufficient to enforce its security policy.

Asymmetric Cryptographic System

A system involving two related transformations; one determined by a public key (the public transformation),and another determined by a private key (the private transformation) with the property that it is computationally infeasible to determine the private transformation (or the private key) from knowledge of the public transformation (and the public key).

Asymmetric Key The corresponding public/private key pair needed to determine the behaviour of the public/private transformations that comprise an asymmetric cryptographic system.

[1] Hardware and software.

[2] Stored or communicated.

Attack An intentional act attempting to violate the security policy of an IT system.

Authentication Security measure that verifies a claimed identity.

Authentication data Information used to verify a claimed identity.

Authorisation Permission, granted by an entity authorised to do so, to perform functions and access data.

Authorised user An authenticated user who may, in accordance with the TSP, perform an operation.

Availability Timely[3], reliable access to IT resources.

Compromise Violation of a security policy.

Confidentiality A security policy pertaining to disclosure of data.

Cryptographic key (key)

A parameter used in conjunction with a cryptographic algorithm that determines:

- the transformation of plaintext data into cipher text data,
- the transformation of cipher text data into plaintext data,
- a digital signature computed from data,
- the verification of a digital signature computed from data, or
- a digital authentication code computed from data.

Dynamic Resource A resource for which two distinct requests can provide different output information.

Discretionary Access Control

A means of restricting access to objects based on the identity of subjects and/or groups to which they belong. These controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission (perhaps indirectly) on to any other subject.

End-user A user that is not an administrator of the G-Server. End-users interact with the TOE by sending HTTP requests from the outside network that are routed through the TOE, and receiving responses from protected and unprotected sites on the inside network. End-users are not identified or authenticated by the TOE.

Entity A subject, object, user, or another IT device, which interacts with TOE objects, data, or resources.

[3] According to a defined metric.

ExitControl The access control service provided by the TOE ensuring that only genuine resources can exit into the outside network.

External IT entity Any trusted Information Technology (IT) product or system, outside of the TOE, which may, in accordance with the TSP, perform an operation.

Genuine resource A resource on a protected site that is verified by the TSF to be uncompromised.

G-Server The TOE.

Identity A representation (e.g., a string) uniquely identifying an authorised user, which can either be the full or abbreviated name of that user or a pseudonym.

Inside network A network to which all access is mediated by the TOE, hosting protected and unprotected sites.

Integrity A security policy pertaining to the corruption of data and TSF mechanisms.

Mandatory Access Control

A means of restricting access to objects based on subject and object sensitivity labels.[4]

Mandatory Integrity Control

A means of restricting access to objects based on subject and object integrity labels.

Named Object An object that exhibits all of the following characteristics:

- The object may be used to transfer information between subjects of differing user identities within the TSF.
- Subjects in the TOE must be able to request a specific instance of the object.
- The name used to refer to a specific instance of the object must exist in a context that potentially allows subjects with different user identities to request the same instance of the object.

Non-Repudiation A security policy pertaining to providing one or more of the following:

- To the sender of data, proof of delivery to the intended recipient,
- To the recipient of data, proof of the identity of the user who sent the data.

[4] The Bell-LaPadula model is an example of Mandatory Access Control.

Object	An entity that contains or receives information and upon which subjects perform operations.
Operating Environment	The total environment in which a TOE operates. It includes the physical facility and any physical, procedural, administrative and personnel controls.
Outside network	The network connected to the external interfaces of the TOE, through which end-users communicate with the TOE.
Peer TOEs	Mutually authenticated TOEs that interact to enforce a common security policy.
Public Object	An object for which the TSF unconditionally permits all entities "read" access. Only the TSF or authorised administrators may create, delete, or modify the public objects.
Resource	A named object on a protected site, identified via a URI.
Security attributes	TSF data associated with subjects, objects, and users that is used for the enforcement of the TSP.
Protected site	An HTTP server running on a host on the inside network, for which the G-Server is configured to provide resource integrity protection.
Static Resource	A resource for which generated outputs remain the same for an extended period of time, such as a day.
Subject	An entity within the TSC that causes operations to be performed. Subjects represented in the G-Server include protected sites, end-users, and administrators.
Symmetric key	A single, secret key used for both encryption and decryption in symmetric cryptographic algorithms.
Threat	Capabilities, intentions and attack methods of adversaries, or any circumstance or event, with the potential to violate the TOE security policy.
Threat Agent	Any human user or Information Technology (IT) product or system, which may attempt to violate the TSP and perform an unauthorised operation with the TOE.
Ungenuine resource	A resource on a protected site that is determined by the TSF as having been compromised.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.
Vulnerability	A weakness that can be exploited to violate the TOE security policy.

1.5.2. Common Abbreviations

The following abbreviations are used in this document:

CC Common Criteria
DAC Discretionary Access Control
EAL Evaluation Assurance Level
IT Information Technology
OSP Organisational Security Policy
SAR Security Assurance Requirement
SF Security Function
SFP Security Function Policy
SFR Security Functional Requirement
ST Security Target
TOE Target of Evaluation
TSC TSF Scope of Control
TSF TOE Security Functions
TSP TOE Security Policy
TSS TOE Summary Specification

1.6. Document Organization

Section 1 provides the introductory material for the security target.

Section 2 is the TOE description.

Section 3 describes the expected environment for the TOE. This section also defines the set of threats that are to be addressed by either the technical countermeasures implemented in the TOE or through environmental controls.

Section 4 defines the security objectives for both the TOE and the TOE environment.

Section 5 gives the functional and assurance requirements derived from the Common Criteria, Parts 2 and 3, respectively that must be satisfied by the TOE.

Section 6 describes the security functions and assurance measures provided by the TOE that address the security requirements.

Section 7 is a placeholder for a Protection Profile rationale. Because this ST does not claim conformance with any PP, this section is empty.

Section 8 provides a rationale to explicitly demonstrate that the TOE and environment security objectives satisfy the policies and threats. It provides Arguments for the coverage of each policy and threat. The section then explains how the set of requirements are complete relative to the objectives and how each security objective is addressed by one or more component requirements. It provides Arguments for the coverage of each objective. Next Section 8 provides arguments that address the use of extended requirements that are not taken from Part 2 of the CC, and a dependency analysis. Finally, the Summary Specification Rationale maps security requirements onto TOE security functions.

2. TOE Description

The Gilian G-Server is an appliance that is connected between one or more Web servers and the outside world, in order to detect and prevent invalid data from being sent out from these Web servers.

2.1. Scope and Boundaries of the TOE

The TOE consists of the following components:

- The **G-Server** appliance comes in a 2U rack-mountable form factor (see Figure 2.1) with processing and storage capabilities, as well as two Network Interfaces (NICs).

  The TOE is shipped as one of a set of *models* that differ amongst themselves in hardware capabilities and licensing limitations, while running the same software version (2.5 for this ST). The evaluated configuration contains the "G-Server 200XL" model.

Figure 2.1 –The G-Server 200XL Appliance

- Administration client software running on Microsoft Windows workstations, including two types of clients: **Administration Tool** and **Signing Tool**.
- **G-Agent** software that is installed on the Web server host. The G-Agent's role is to support the TOE in verifying the validity of scripts and programs that generate dynamic resources, and in providing support for sites requiring end-user authentication. G-Agent software is available for Windows, Solaris 8, and Linux operating systems, and Apache, IIS, iPlanet, and Netscape Enterprise Web servers.

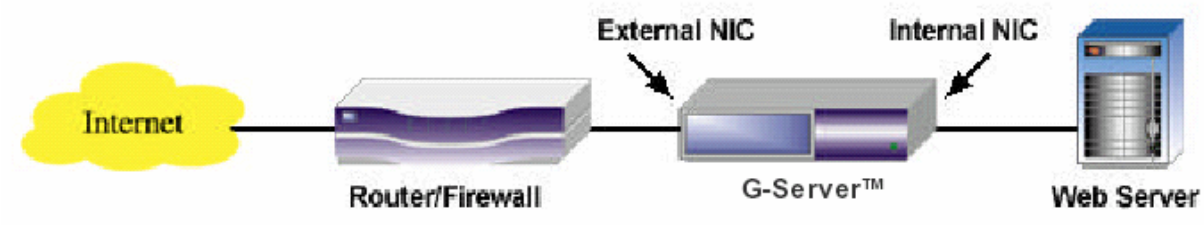
The evaluated configuration for the TOE includes the G-Server in Single Mode; no claims are made regarding High Availability configurations.

The TOE can be configured with an optional Bypass Card that provides fault-tolerance functionality. The Bypass Card is activated by a watchdog process on the TOE in order to maintain connectivity to the Web server in the event of a G-Server failure. The Bypass Card is <u>not</u> part of the evaluated configuration.

2.2. TOE Configuration

The TOE is connected via two NICs to the internal and external networks, respectively. Conceptually, the TOE mediates all traffic between the Web server(s) and the outside world, as described in Figure 2.2 below. In practice, the internal NIC might be connected to subnets containing multiple hosts. The G-Server 200XL model can support up to 50 protected sites, and can also route traffic to non-protected sites (fast forwarding).

Figure 2.2 –Traffic Mediation Architecture



This configuration allows the TOE to inspect all relevant packets sent from the Web server to the Internet. The TOE then processes these packets, while simply relaying onward any irrelevant packets such as ICMP pings and Web-server monitoring applications.

The G-Server is not assigned IP addresses for its NICs. A module of the TOE called the *Transparency Envelope*™ (TE) performs packet forwarding. The TOE advertises its external MAC address in response to ARP queries for IP addresses of protected and neighboring hosts connected on the internal NIC. The TE separates traffic mediated by the TOE into three streams, based on the source interface, IP addresses and ports:

- Protected HTTP and HTTPS traffic to and from protected sites;
- Fast-forwarded traffic that is flowing to and from IP addresses on the internal NIC but is not defined as protected traffic;
- Management sessions. Management traffic is identified by virtual IP addresses and ports pre-assigned by an authorised administrator.

Protected traffic is funneled through the TOE information flow control functions.

The TOE does not provide generalized firewall functionality. As depicted in Figure 2.2, it is intended to be deployed in a configuration where it is protected by a firewall from arbitrary external malicious network traffic, and communicates with internal hosts that are assumed to be non-malicious (see environmental assumption A.PEER). The TOE's purpose is to provide HTTP application-level information flow control.

2.3. TOE Security Functions Scope of Control (TSC)

2.3.1. Subjects

The following subjects are recognized by the TSF:

- **Protected sites** – hosts on the internal network that attempt to send resources out to end-users in response to incoming HTTP requests. Protected sites are subject to ExitControl information flow control;
- **End-users** – entities on the outside network that send HTTP requests to protected sites through the TOE. End-users are not authenticated by the TSF and are not subject to information flow control or access control;
- **Administrators** – users that interact directly with the administration tools of the TOE (Administration Tool and Signing Tool). Administrators are subject to access control, which defines the extent of each administrator's authorisations.

2.3.2. User Data Objects

The following user data objects are processed by the TOE:

- HTTP protocol requests and responses are mediated by the TOE between end-users and hosts on the internal network;
- Mirror copies of protected site resources are stored in the TOE's database in order to support resource Recovery when modified content is detected.

2.3.3. TSF Data Objects

The TOE contains various TSF data objects including the following types of objects:

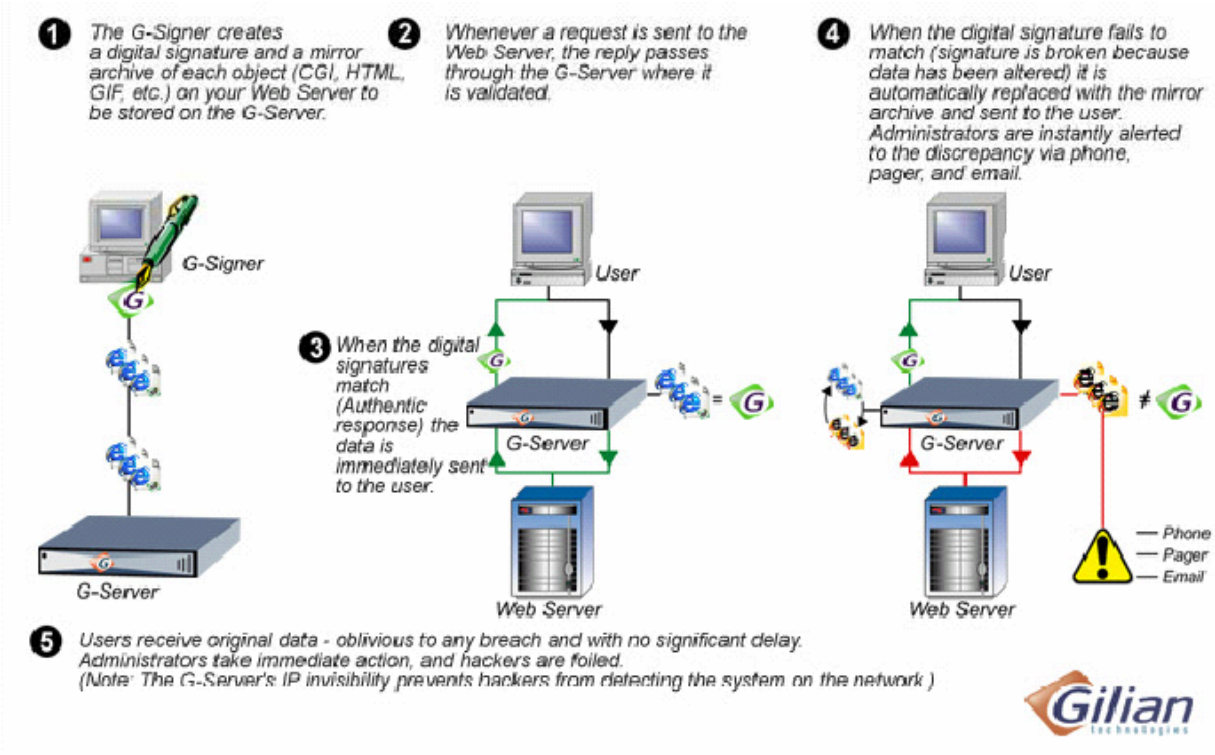
- Resource signatures in the TOE's database;
- Protected site properties and ExitControl information flow control rules;
- EntryControl event signature patterns;
- Administrator information including role assignments and user private and public keys;
- State cache containing outstanding HTTP requests;
- Audit logs.

2.4. TOE Security Functionality

2.4.1. ExitControl Functionality

Figure 2.3 below summarizes the process through which the TOE ensures that unauthorised modifications to Web resources are prevented from reaching end-users, thus countering Web defacement attacks.

Figure 2.3 –Integrity Validation Process

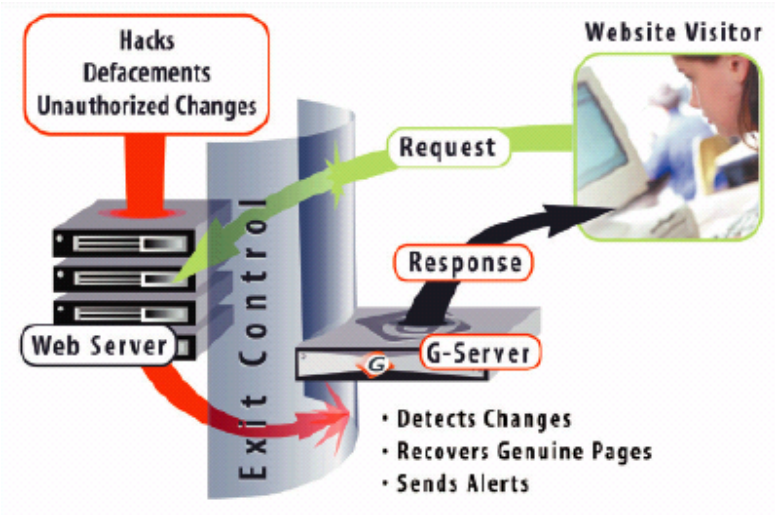


The TOE provides integrity validation services for two types of resources: static and dynamic. Static resources are defined as resources whose content remains the same over multiple requests for those resources. Dynamic resources are generated by scripts or programs, and yield different content for every invocation.

For static resources, integrity protection is provided by having an authorised administrator pre-sign a valid copy of the resource. The resource contents are hashed and digitally signed with the signer's private key. The signature is stored in the TOE's database along with a mirror of the resource contents.

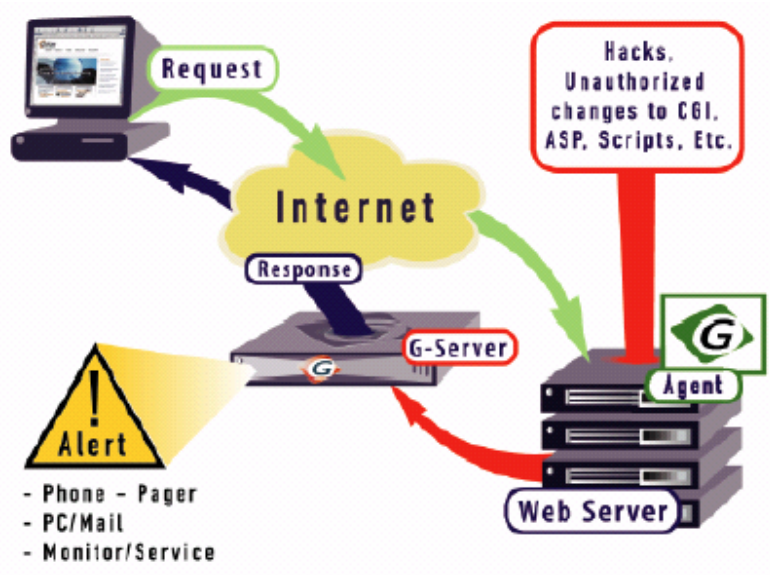
Whenever the TOE receives a request for a signed resource, it calculates a hash of the response and compares it to the signed hash; if the two do not match, the resource is identified as "ungenuine". The TOE can log the event, and can also replace the modified contents with a default Recovery Message. When a genuine mirror of the resource is stored in the database, the TOE can replace the modified contents with those of the mirror.

Figure 2.4 –Static Resource Validation



For dynamic resources, it is not possible to determine contents' validity by comparing them to a stored copy. For these resources, the validity of the script or program that generated them is inspected instead of the resource contents. This is achieved by requesting a hash of the generating script to be calculated by the G-Agent, and sent to the G-Server to be compared against a signed hash of the script. When the TOE determines that the script or program that generated the resource has been modified (and does not match the corresponding signature stored in the TOE's database), the TOE can replace the resource contents with those of a default Recovery Message.

Figure 2.5 –Dynamic Resource Validation



Although the TOE normally tests resource integrity when it is requested by an end-user, it also provides a capability for manual initiation of the integrity test for a given set of resources.

2.4.2. EntryControl Functionality

Although the main focus of the TSP is to control information flow from the Web server (protected site) to the end-user, the TOE can also provide protection against application-level attacks by matching HTTP requests to sets of constraints, limits, and patterns in order to detect potentially malicious requests. When an attack is detected, the connection is closed, and the TOE can optionally log the event and/or generate Alerts.

2.4.3. Alerts

When an integrity violation is detected, or when access is requested to selected resources, the TOE can be configured to generate appropriate Alerts. The TOE supports writing alerts to a log file, sending email over SMTP, generating SNMP traps to a Network Management System or pager, as well as executing application executables preinstalled on the G-Server.

As described in the User Guide, application executables that are triggered when an ungenuine resource is discovered must be installed on the G-Server by qualified Gilian personnel. These executables are outside the TOE and are not covered by the evaluated configuration.

2.4.4. TOE Administration

The TOE supports remote administration using two client software tools: the Administration Tool and the Signing Tool. The Administration Tool provides authorised administrators with all of the functions necessary for the administration of the TOE, including G-Server configuration, management of information flow control rules, etc. The Signing Tool is used to publish and update resource signatures, in coordination with Web content management.

Distributed administration is supported by providing a set of administration roles that support limiting authorised administrators' administrative authorisations. Access to the Administration Tool can be limited to read-only interaction (the Viewer role), as well as excluded altogether, by restricting the user to using the Signing Tool exclusively (the Signer role). In order to provide a capability for dividing content publishing authorisations among multiple content areas, signing scope can be restricted to specific sites and specified resource patterns.

The TOE supports a signature shift paradigm. When new resource contents are about to be published to the protected site, a signature of the updated contents is registered as a "sub-signature". The TOE will recognize both the old and new versions of the resource as valid, so that protection can be maintained before and after the new content is published to the site. A signature shift operation, either manual or automatic, invalidates the old signatures and activates the sub-signature as the authorised signature for the resource.

Although the TOE also supports an alternate method to Pending Signatures for signature updates, where protection is suspended while the new resource is being signed, this method is outside the evaluated configuration. Signing modified resources must be done using the Pending Signatures option in the evaluated configuration.

2.4.5. Audit Functionality

The TOE maintains a comprehensive audit trail composed of four different logs:

- The **System Log** contains events related to G-Server functionality and a record of TOE administration events;
- The **Signing Log** contains resource management events such as resource signing;
- The **Alerts Log** contains Alerts that were triggered by the ExitControl and EntryControl mechanisms;
- The **Verification Log** contains information flow events that were defined as being logged.

Logs can be exported to external files in order to maintain a permanent audit record.

2.4.6. Trusted Path/Channels

The TSF provides a trusted path for communication between administrators and the G-Server, via a combination of the SSL protocol, user authentication using the user's private key, and logical separation by the Transparency Envelope™ between administration and user data traffic.

The TOE supports SSL Web traffic by providing SSL trusted channel capabilities over both the channel to the end-user, and the channel to protected sites. The TOE effectively performs a Man in the Middle (MITM) interaction between the end-user and the site. The trusted channel can also be set up as HTTPS Termination Mode, in which the trusted channel terminates at the TOE, without establishment of a corresponding channel to the protected site, thus offloading the SSL processing from the Web server to the TOE.

3. TOE Security Environment

3.1. Secure Usage Assumptions

A.NETWORK_MEDIATION: Complete mediation of network traffic

The TOE environment is divided into an inside network that contains protected sites, and an outside network to which resources are sent. All communication between inside and outside is mediated by the TOE.

A.NO_EVIL_ADM: G-Server administrators are trusted not to abuse their authority

Administrators are non-hostile, appropriately trained and follow all administrator guidance.

A.NO_GENERAL_PURPOSE: No general purpose computing capabilities

TOE administrators will not install any general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) on the TOE.

A.PHYSICAL: Physical access

The TOE is located within controlled access facilities that prevent unauthorised physical access by outsiders.

A.PEER: Connectivity to other systems

It is assumed that TOE administrators will install the TOE in an environment protected by a security gateway or firewall from arbitrary external malicious network traffic. Protected sites as well as systems hosting administrative tools interacting with the TOE are assumed to be installed on the inside network, and to be under the same management control as the TOE. Systems hosting administrative tools interacting with the TOE are assumed to be non-malicious.

A.BROWSER: End-user software performs trusted channel verification

End-user software performs trusted channel verification to ensure that a trusted channel has been established that protects the user from Web spoofing attacks by entities outside of the TSC.

3.2. Threats to Security

T.Admin_Err_Commit: Administrative errors of commission

An administrator commits errors that directly compromise organizational security objectives or change the technical security policy enforced by the G-Server.

T.Admin_Err_Omit: Administrative errors of omission

The system administrator fails to perform some function essential to security.

T.Admin_Rogue: Hostile administrator modification of user or TSF data

An administrator maliciously obstructs organizational security objectives or modifies the system's configuration to allow security violations to occur.

T.Defacement: Malicious defacement of Web contents

A hacker maliciously modifies resources stored on a protected site in an attempt to deny access to valid Web resources, damage the organization's reputation, or otherwise provide misleading information in order to affect end-user experience and reactions.

T.Hack_AC: Hacker undetected system access

A hacker gains undetected access to the G-Server due to missing, weak and/or incorrectly implemented access control causing potential violations of integrity, confidentiality, or availability.

T.Hack_Avl_Resource: Hacker attempts resource denial of service

A hacker executes commands, sends data, or performs other operations that make system resources unavailable to system users. Resources that may be denied to users include bandwidth, processor time, memory, and data storage.

T.Hack_Comm_Eavesdrop: Hacker eavesdrops on user data communications

Hacker obtains end-user data by eavesdropping on communications lines.

T.Hack_Masq: Hacker masquerading as a legitimate user or as system process

A hacker masquerades as an authorised subject to perform operations that will be attributed to the authorised subject.

T.Hack_Msg_Data: Message content modification

A hacker modifies end-user data intercepted from a communication link between an end-user and a protected site before passing it on, thereby deceiving the intended recipient.

T.Hack_Site: Hacker crafts malicious Web request

An end-user crafts a malicious anomalous Web request to a protected site that results in a violation of the protected site's security policy.

T.Spoofing: Legitimate system services are spoofed

An attacker tricks end-users into interacting with spurious system services.

T.TSF_Compromise: Compromise of the TSF

An end-user, protected or unprotected site may send a specially crafted message through the TOE, thereby causing user data, TSF data or executable code to be inappropriately accessed (viewed, inserted, modified, or deleted).

T.Unattended_Session: A user takes over an unattended session

A user may gain unauthorised access to an unattended session.

3.3. Organizational Security Policies

P.Accountability: Individual accountability

Administrators shall be held accountable for their actions.

P.Availability: Information availability

Administrator-designated protected resources shall be maintained available to end-users regardless of the availability of the corresponding protected sites.

P.Integrity: Information content integrity

Protected resources shall retain their content integrity when requested by end-users.

4. Security Objectives

4.1. Security Objectives for the TOE

O.Admin_Guidance: Administrator guidance documentation

The TOE will deter administrator errors by providing adequate administrator guidance.

O.Admin_Role: Administrator roles

The TOE will provide administrator roles to isolate administrative actions.

O.Application_Protection: Protection against malicious Web requests

The TOE will provide protection against malicious Web requests that may cause a violation of a protected site's security policy.

O.Audit_Account: Auditing for accountability

The TOE will provide information about past subject behaviour to an authorised administrator through system mechanisms. Specifically, during any specified time interval, the TOE is able to report to an administrator selected auditable actions that an end-user, protected site, or administrator has performed.

O.Audit_Protect: Protect stored audit records

The TOE will protect audit records against unauthorised access, modification, or deletion to ensure accountability of subject actions.

O.I&A: Identify and authenticate each administrator

The TOE will uniquely identify and authenticate each administrator of the system.

O.Integrity: Integrity protection for protected resources

The TOE will prevent protected resources that have been modified in an unauthorised manner from flowing to end-users.

O.Limit_Sessions: Limit resources that can be allocated by outside users

The TOE will provide a capability for limiting the resources of the TOE that can be allocated to outside users accessing a given protected site or management function.

O.Manage: Administration of the TSF

The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE.

O.Redirection_Control: Control of authorised destinations for user redirection

The TOE will only permit redirection directives that redirect the end-user to a pre-authorised list of redirection directive destinations.

O.Resource_Recovery: Recovery of genuine resource contents

The TOE will provide to the end-user an archived copy of the genuine resource contents when unauthorised modification is detected.

O.Self_Protection: Protection of the TSF

The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorised disclosure.

O.TOE_Access: Control access to the TOE

The TOE will provide mechanisms that control a user's logical access to the TOE, and will terminate existing user sessions after a period of inactivity.

O.Trusted_Channel: Trusted channel for transmission of user data

The TOE will provide a trusted path for communication of user data between the TOE and remote users and trusted IT products that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

O.Trusted_Path: Provide a trusted path

The TOE will provide a trusted path between the user and the system. Execution of a user-requested action must be made via a trusted path with the following properties:

- The path is logically distinct from, and cannot be confused with, other communication paths (by either the user or the system).
- The path provides assured identification of its end points.

4.2. Security Objectives for the Environment

OE.PHYSICAL: Physical security

Those responsible for the TOE must ensure that the TOE is located in physically secure facilities where it is protected from physical attack that might compromise IT security objectives.

OE.MANAGED: Installation, management, and operation of the TOE

Those responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner that maintains IT security objectives.

OE.NETWORK_MEDIATION: Complete mediation of network traffic

Those responsible for the TOE shall ensure that the network is configured such that all information flows that are controlled by the TSP pass through the TOE.

OE.BROWSER_VERIFICATION: End-user software trusted channel verification

End-users shall ensure the validity of a trusted channel established with the TOE via manually-operated or automated end-user software mechanisms.

5. IT Security Requirements

5.1. TOE Security Functional Requirements

The functional security requirements for this ST consist of the following components from Part 2 with the addition of extended components (underlined), summarized in the following table.

The CC defined operations of assignment, selection, iteration, and refinement were applied as described in column 4 of Table 5.1 below to customize the components for this ST.

Table 5.1 –Functional security components

Functional Class	Functional Components		CC Operations
Security Audit	FAU_ARP.1	Security alarms	assignment
	FAU_GEN.1-NIAP-0347	Audit data generation	extended component: selection
	FAU_SAA.1	Potential violation analysis	assignment
	FAU_SAA.3	Simple attack heuristics	assignment
	FAU_SAR.1	Audit review	assignment
	FAU_SAR.3 (1) FAU_SAR.3 (2) FAU_SAR.3 (3) FAU_SAR.3 (4)	Selectable audit review	iteration, assignment, selection, refinement
	FAU_STG.2	Guarantees of audit data availability	assignment, selection
Cryptographic Support	FCS_CKM.1	Cryptographic key generation	iteration, assignment
	FCS_COP.1 (1) FCS_COP.1 (2) FCS_COP.1 (3)	Cryptographic operation	iteration, assignment
User Data Protection	FDP_ACC.1	Subset access control	assignment
	FDP_NIAP-0420-ATR.1	Security attribute management and inheritance	extended component: assignment
	FDP_DAU.2	Data authentication with identify of guarantor	assignment
	FDP_ETC.1	Export of user data without	assignment

Functional Class	Functional Components		CC Operations
		security attributes	
	FDP_IFC.1 (1) FDP_IFC.1 (2) FDP_IFC.1 (3)	Subset information flow control	iteration, assignment
	FDP_IFF.1 (1) FDP_IFF.1 (2) FDP_IFF.1 (3)	Simple security attributes	iteration, assignment
	FDP_ITC.1 (1) FDP_ITC.1 (2) FDP_ITC.1 (3)	Import of user data without security attributes	iteration, assignment
	FDP_SDI_EX.1	Inter-TSF user data monitoring	extended component: assignment, selection
Identification and Authentication	FIA_UAU.2	User authentication before any action	
	FIA_UAU.7	Protected authentication feedback	assignment
	FIA_UID.2	User identification before any action	
Security Management	FMT_MOF.1	Management of security functions behaviour	assignment, selection
	FMT_MSA.1 (1) FMT_MSA.1 (2)	Management of security attributes	iteration, assignment, selection
	FMT_MSA.2	Secure security attributes	
	FMT_MSA.3	Static attribute initialisation	assignment, selection
	FMT_MTD.1	Management of TSF data	assignment, selection
	FMT_REV.1 (1) FMT_REV.1 (2)	Revocation	iteration, assignment
	FMT_SMF.1	Specification of Management Functions	assignment
	FMT_SMR.1	Security roles	assignment
Protection of the TOE Security Functions	FPT_RVM.1	Non-bypassability of the TSP	
	FPT_SEP.1	TSF domain separation	
	FPT_SSP_EX.1	State transition control for	extended component:

Functional Class	Functional Components		CC Operations
		security attributes	assignment, selection
	FPT_STM.1	Reliable time stamps	
Resource Utilisation	FRU_RSA.1	Maximum quotas	assignment, selection
TOE Access	FTA_SSL.3	TSF-initiated termination	assignment
	FTA_TSE.1	TOE session establishment	assignment
Trusted path / channels	FTP_ITC.1 (1) FTP_ITC.1 (2)	Inter-TSF trusted channel	iteration, assignment, selection
	FTP_TRP.1	Trusted path	assignment, selection

5.1.1. Security Audit (FAU)

5.1.1.1. Security alarms (FAU_ARP.1)

FAU_ARP.1.1 The TSF shall take **action as follows** upon detection of a potential security violation:

a) If the potential security violation is signaled by the EntryControl mechanism (see FAU_SAA.3 below), closing the connection; and

b) Optionally (configured by the authorised administrator) triggering an Alert action that sends a message to any of the following destinations:

1) Sending an email to a list of administrator defined email addresses; and/or

2) Sending an SNMP trap message to an external device such as a Network Management System or a pager; and/or

3) Triggering one or more application executables preinstalled on the G-Server.

5.1.1.2. Audit data generation (FAU_GEN.1-NIAP-0347)

FAU_GEN.1.1-NIAP-0347 The TSF shall be able to generate an audit record of the following auditable events:

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

c[5]) Auditable events described in Table 5.2 below:

Table 5.2 - Auditable Events

Requirement	Auditable Events	Additional Information
FAU_ARP.1	Actions taken due to imminent security violations	Alert description
FAU_GEN.1	No Relevant Events	
FAU_SAA.1	Enabling and disabling of site protection	
	Logging of event indicated by information flow control rules	Event description
FAU_SAA.3	Enabling and disabling of Application Protection	
	Detection of potential attack	Event description
FAU_SAR.1	Reading of information from the audit records	
FAU_SAR.3 (1) FAU_SAR.3 (2) FAU_SAR.3 (3) FAU_SAR.3 (4)	No Relevant Events	
FAU_STG.2	No Relevant Events	
FCS_CKM.1	No Relevant Events	
FCS_COP.1 (1)	Success/Failure of signing operation	
FCS_COP.1 (2)	No Relevant Events	
FCS_COP.1 (3)	Success/failure of resource digest calculation	
FDP_ACC.1	No Relevant Events	
FDP_NIAP-0420-ATR.1	All access control decisions about establishing or modifying an object's security attributes	
FDP_DAU.2	Successful generation of validity evidence	resource URL
	Unsuccessful generation of validity evidence	

[5] Subsection b) of FAU_GEN.1.1-NIAP-0347 omitted as described in Part 2 Annex C for the 'not specified' level of audit: "if 'not specified' is selected, the PP/ST author should fill in all desired auditable events in FAU_GEN.1.1c, and this part of the element (item b) can be removed entirely."

Requirement	Auditable Events	Additional Information
	The identity of the subject that generated the evidence	
FDP_ETC.1	All attempts to export information	resource verification status (genuine/ungenuine)
FDP_IFC.1 (1) FDP_IFC.1 (2) FDP_IFC.1 (3)	No Relevant Events	
FDP_IFF.1 (1) FDP_IFF.1 (2)	All decisions on requests for information flow	resource verification status, recovery decision
FDP_IFF.1 (3)	No Relevant Events	
FDP_ITC.1 (1) FDP_ITC.1 (2)	All attempts to import user data	all security attributes
FDP_ITC.1 (3)	All imports of site SSL keys and certificates	site name
FDP_SDI_EX.1	All attempts to check resource integrity	results of integrity check
FIA_UAU.2	All use of the authentication mechanism	
FIA_UAU.7	No Relevant Events	
FIA_UID.2	All use of the user identification mechanism	
FMT_MOF.1	All modification in the behaviour of the functions in the TSF	
FMT_MSA.1 (1) FMT_MSA.1 (2)	All modifications of the values of security attributes	
FMT_MSA.2		
FMT_MSA.3	Modifications of the information flow control rules	
FMT_MTD.1	All modifications to the values of TSF data	
FMT_REV.1 (1) FMT_REV.1 (2)	Unsuccessful revocation of security attributes	
	All attempts to revoke security attributes	
FMT_SMF.1	Use of the management functions	
FMT_SMR.1	Modification to the group of administrators that are associated with a given role	
FPT_RVM.1	No Relevant Events	
FPT_SEP.1	No Relevant Events	
FPT_SSP_EX.1	All manual and automatic sub-signature and signature shift events	resource name
FPT_STM.1	Changes to the system time	

Requirement	Auditable Events	Additional Information
FRU_RSA.1	Rejection of allocation operation due to resource limits	
	All attempted uses of the resource allocation functions for resources that are under control of the TSF	
FTA_SSL.3	Termination of an interactive session by the session locking mechanism	
FTA_TSE.1	All attempts at establishment of a user session	
FTP_ITC.1 (1) FTP_ITC.1 (2)	Failure of the trusted channel functions	initiator and target of failed trusted channel functions
	All attempted uses of the trusted channel functions	initiator and target of all trusted channel functions
FTP_TRP.1	All attempted uses of the trusted path functions	user identification

FAU_GEN.1.2-NIAP-0347 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, other audit relevant information as given in column "Additional Information" of Table 5.2 above.

5.1.1.3. Potential violation analysis (FAU_SAA.1)

FAU_SAA.1.1 The TSF shall be able to apply a set of rules in monitoring the audited events and based upon these rules indicate a potential violation of the TSP.

FAU_SAA.1.2 The TSF shall enforce the following rules for monitoring audited events:

a) Accumulation or combination of **protected site responses that match corresponding ExitControl information flow control rules, for which an authorised administrator has determined that an alert should be generated,** known to indicate a potential security violation;

b) **No additional rules**.

5.1.1.4. Simple attack heuristics (FAU_SAA.3)

FAU_SAA.3.1 The TSF shall be able to maintain an internal representation of the following signature events**:**

a) **HTTP requests that fall outside a set of predefined limits or constraints on request properties;**

b) **HTTP requests that match a predefined set of attack signatures defined as string patterns that may appear in the request.**

that may indicate a violation of the TSP.

FAU_SAA.3.2 The TSF shall be able to compare the signature events against the record of system activity discernible from an examination of **traffic being forwarded by the TOE from the outside network to protected sites**.

FAU_SAA.3.3 The TSF shall be able to indicate an imminent violation of the TSP when a system event is found to match a signature event that indicates a potential violation of the TSP.

5.1.1.5. Audit review (FAU_SAR.1)

FAU_SAR.1.1 The TSF shall provide **identified administrators with the G-Master or Viewer roles** with the capability to read **System Log entries, site Alerts, site Verification Log and Signing Log entries** 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.

5.1.1.6. Selectable audit review [System Log] (FAU_SAR.3 (1))

FAU_SAR.3.1 The TSF shall provide the ability to perform searches and sorting of audit data **in the System Log** based on **the following criteria:**

a) **Date: The timestamp of the log.**

b) **Client IP: The IP address of the client.**

c) **User Name: The user who performed the operation.**

d) **Method: The event or operation that triggered the log entry.**

e) **Site Name: The target of the log entry.**

f) **Reply Status/Message: The reply status code and associated message describing the error, if reported.**

5.1.1.7. Selectable audit review [Verification Log] (FAU_SAR.3 (2))

FAU_SAR.3.1 The TSF shall provide the ability to perform searches and sorting of audit data **in the Verification Log** based on **the following criteria:**

a) **Date: The timestamp of the log.**

b) **Client IP: The IP address of the client who requested the resource.**

c) **Verification Result: Whether the resource is genuine or ungenuine.**

d) **Content Source: Whether the resource was from the Web server or from the recovery file.**

e) **Reply Status: The reply status code.**

f) **URL: The requested resource.**

g) **Message: Any associated messages.**

5.1.1.8. Selectable audit review [Signing Log] (FAU_SAR.3 (3))

FAU_SAR.3.1 The TSF shall provide the ability to perform searches and sorting of audit data **in the Signing Log** based on **the following criteria:**

a) **Date: The timestamp of the log.**

b) **Client IP: The IP address of the client who requested the resource.**

c) **User Name: The user who signed the resource.**

d) **Method: The method of signing.**

e) **URL: The resource that was signed.**

f) **Reply Status/Message: The reply status code and/or associated message.**

5.1.1.9. Selectable audit review [Alerts] (FAU_SAR.3 (4))

FAU_SAR.3.1 The TSF shall provide the ability to perform searches and sorting of audit data **Alerts** based on **the following criteria:**

a) **Number of occurrences**

b) **From Date**

c) **To Date**

5.1.1.10. Guarantees of audit data availability (FAU_STG.2)

FAU_STG.2.1 The TSF shall protect the stored audit records from unauthorised deletion.

FAU_STG.2.2 The TSF shall be able to prevent modifications to the audit records.

FAU_STG.2.3 The TSF shall ensure that **an administrator defined log size (default 1000 KB for system log, 10000KB for site Signing Log and site Verification Log) of** audit records will be maintained when the following conditions occur: audit storage exhaustion.

5.1.2. Cryptographic support (FCS)

5.1.2.1. 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 **RSA PKCS #1** and specified cryptographic key sizes **1024** that meet the following: **RSA PKCS#1**.

5.1.2.2. Cryptographic operation [Signing] (FCS_COP.1 (1))

FCS_COP.1.1 The TSF shall perform **signing of a server-generated authentication challenge, signing of resource hash** in accordance with a specified cryptographic algorithm **RSA** and cryptographic key sizes **1024** that meet the following: **RSA PKCS#1**.

5.1.2.3. Cryptographic operation [SSL Establishment] (FCS_COP.1 (2))

FCS_COP.1.1 The TSF shall perform **establishment of SSL/TLS Connections** in accordance with a specified cryptographic algorithm **RSA , triple-DES (in CBC mode), SHA-1, MD-5** and cryptographic key sizes **1024 (for RSA) and 168 (for triple-DES)** that meet the following: **IETF RFC 2246**.

5.1.2.4. Cryptographic operation [Hashing] (FCS_COP.1 (3))

FCS_COP.1.1 The TSF shall perform **hashing a resource** in accordance with a specified cryptographic algorithm **SHA-1** and cryptographic key sizes **None** that meet the following: **NIST FIPS 180-1**.

5.1.3. User data protection (FDP)

5.1.3.1. Subset access control (FDP_ACC.1)

FDP_ACC.1.1 The TSF shall enforce the **Resource Signing SFP** on

a) **Subjects: authenticated G-Server administrators;**

b) **Objects: G-Server representation of static and/or dynamic resources on protected sites;**

c) **Operations: signing a resource, entering the signature and optionally a mirror of the resource contents into the G-Server database.**

5.1.3.2. Security Attribute Management and Inheritance (FDP_NIAP-0420-ATR.1)

FDP_NIAP-0420-ATR.1.1. As part of the **Resource Signing SFP**, the TSF shall enforce the following policy rules with respect to security attribute establishment: **an authenticated user may create a signature in the G-Server database for a resource located in a protected site and cause a mirror of the resource to be stored in the database to support resource recovery, if and only if:**

a) **The user's G-Server administrator role is G-Master or Signer; or**

b) **The user's G-Server role is Viewer; and**

1) **The user's Advanced Properties maps the user as a Signer for the given site; and**

2) **If a scope is defined for the appropriate mapping, that scope contains the given resource.**

FDP_NIAP-0420-ATR.1.2. As part of the **Resource Signing SFP**, the TSF shall enforce the following policy rules with respect to security attribute modification: **as for security attribute establishment**.

5.1.3.3. Data authentication with identity of guarantor (FDP_DAU.2)

FDP_DAU.2.1 The TSF shall provide a capability to generate evidence that can be used as a guarantee of the validity of **static protected resources, and of dynamic resources whose validity is determined by the validity of the set of scripts and executables that generate the given resource**.

FDP_DAU.2.2 The TSF shall provide **the ExitControl mechanism as well as authorised identified administrator roles** with the ability to verify evidence of the validity of the indicated information and the identity of the user that generated the evidence.

5.1.3.4. Export of user data without security attributes (FDP_ETC.1)

FDP_ETC.1.1 The TSF shall enforce the **Static Resource SFP and Dynamic Resource SFP** when exporting user data, controlled under the SFP(s), outside of the TSC.

FDP_ETC.1.2 The TSF shall export the user data without the user data's associated security attributes.

5.1.3.5. Subset information flow control [Dynamic Resource] (FDP_IFC.1 (1))

FDP_IFC.1.1 The TSF shall enforce the **Dynamic Resource SFP** on **a protected site sending a dynamically generated resource in reply to an outstanding HTTP request**.

5.1.3.6. Subset information flow control [Static Resource] (FDP_IFC.1 (2))

FDP_IFC.1.1 The TSF shall enforce the **Static Resource SFP** on **a protected site sending a static resource in reply to an outstanding HTTP request**.

5.1.3.7. Subset information flow control [Import of SSL Keys] (FDP_IFC.1 (3))

FDP_IFC.1.1 The TSF shall enforce the **SSL Key Import SFP** on **an administrator importing SSL key files into the G-Server**.

5.1.3.8. Simple security attributes [Dynamic Resource] (FDP_IFF.1 (1))

FDP_IFF.1.1 The TSF shall enforce the **Dynamic Resource SFP** based on the following types of subject and information security attributes:

a) The following subject security attributes:

1) Protected site name;

b) The following information security attributes:

1) Resource name;

2) HTTP status code;

3) Verification status (genuine/ungenuine).

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

A resource shall be permitted to flow from a protected site to a remote browser if:

a) The resource is matched to an outstanding request to the given site; and:

b) Either the information flow control rules (determined by the authorised administrator) determine that the given resource is uncontrolled (not verified) for the given site; or

c) The resource is determined to be "genuine" by matching the hash of the script that generated the resource (as determined by the G-Agent on the protected site) to the stored hash for that script; or

d) The information flow control rules allow the given resource to pass even in an "ungenuine" state.

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

FDP_IFF.1.4 The TSF shall provide the following **additional capability: when a dynamic resource is determined to be "ungenuine", the TSF shall be able to send a default Recovery message in its place**.

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules: **if the authorised administrator has (temporarily) disabled protection for the protected site**.

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: **No explicit denial rules**.

5.1.3.9. Simple security attributes [Static Resource] (FDP_IFF.1 (2))

FDP_IFF.1.1 The TSF shall enforce the **Static Resource SFP** based on the following types of subject and information security attributes:

a) The following subject security attributes:

1) Protected site name;

b) The following information security attributes:

1) Resource name;

2) HTTP status code;

3) Verification status (genuine/ungenuine).

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

A resource shall be permitted to flow from a protected site to a remote browser if:

a) The resource is matched to an outstanding request to the given site; and:

b) Either the information flow control rules (determined by the authorised administrator) determine that the given resource is uncontrolled (not verified) for the given site; or

c) The resource is determined to be "genuine"; or

d) The information flow control rules allow the given resource to pass even in an "ungenuine" state.

FDP_IFF.1.3 The TSF shall enforce the **following information flow control SFP rules:**

For http responses with a redirection code of 301 "Moved Permanently" or 302 "Found", the TSF shall be able to verify the redirection directive against a list of authorised redirection destinations, predetermined by the authorised administrator.

FDP_IFF.1.4 The TSF shall provide the following **additional capabilities:**

When a resource is determined to be "ungenuine", the TSF shall be able to send in its place one of the following:

a) If a "genuine" mirror of the resource is available, the mirror is sent in its place; or

b) A default Recovery message predetermined by the authorised administrator is sent in place of the "ungenuine" resource.

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules: **if the authorised administrator has (temporarily) disabled protection for the protected site**.

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: **No explicit denial rules**.

5.1.3.10. Simple security attributes [SSL Key Files] (FDP_IFF.1 (3))

FDP_IFF.1.1 The TSF shall enforce the **SSL Key Import SFP** based on the following types of subject and information security attributes: **SSL key file and certificate file, protected site identification**.

FDP_IFF.1.2 The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: **the administrator is allowed to perform an import of the key file and certificate file and to associate them with a given protected site.**

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

FDP_IFF.1.4 The TSF shall provide the following **additional capabilities: no additional SFP capabilities**.

FDP_IFF.1.5 The TSF shall explicitly authorise an information flow based on the following rules: **no explicit authorisation rules**.

FDP_IFF.1.6 The TSF shall explicitly deny an information flow based on the following rules: **no explicit denial rules**.

5.1.3.11. Import of user data without security attributes [Dynamic Resource]

(FDP_ITC.1 (1))

FDP_ITC.1.1 The TSF shall enforce the **Dynamic Resource SFP** when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: **the TSF shall compute the Verification Status object security attribute as follows:**

a) **A hash is computed of the set of scripts or executables that have been determined by the authorised administrator to be involved in generating the given resource;**

b) **The hash is sent to the G-Server to be compared to a signed hash in the G-Server database;**

c) **The Verification Status is determined to be "genuine" if the hash matches the stored signature.**

5.1.3.12. Import of user data without security attributes [Static Resource]

(FDP_ITC.1 (2))

FDP_ITC.1.1 The TSF shall enforce the **Static Resource SFP** when importing user data, controlled under the SFP, from outside of the TSC.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the user data when imported from outside the TSC.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing user data controlled under the SFP from outside the TSC: **the TSF shall compute the Verification Status object security attribute as follows:**

a) **A hash is computed of the resource being received by the G-Server from the protected site;**

b) **The hash is compared to a signed hash in the G-Server database;**

c) **The Verification Status is determined to be "genuine" if a stored copy is found in the database and the computed hash matches the stored signature.**

5.1.3.13. Import of user data without security attributes [SSL Keys] (FDP_ITC.1 (1))

FDP_ITC.1.1 The TSF shall enforce the **SSL Key Import SFP** when importing **SSL keys and certificates**, controlled under the SFP, from outside of the TSC.

FDP_ITC.1.2 The TSF shall ignore any security attributes associated with the **SSL keys and certificates** when imported from outside the TSC.

FDP_ITC.1.3 The TSF shall enforce the following rules when importing **SSL keys and certificates** controlled under the SFP from outside the TSC: **no additional importation control rules**.

5.1.3.14. Inter-TSF user data monitoring (FDP_SDI_EX.1)

FDP_SDI_EX.1.1 The TSF shall provide a capability to monitor user data stored within a remote trusted IT product at the request of the authorised user.

FDP_SDI_EX.1.2 The TSF shall monitor **Web resources** for **unauthorised modification**, based on the following attributes: **resource contents**.

5.1.4. Identification and authentication (FIA)

5.1.4.1. 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.

5.1.4.2. Protected authentication feedback (FIA_UAU.7)

FIA_UAU.7.1 The TSF shall provide only **obscured feedback** to the user while the authentication is in progress.

5.1.4.3. User identification before any action (FIA_UID.2)

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

5.1.5. Security management (FMT)

5.1.5.1. Management of security functions behaviour (FMT_MOF.1)

FMT_MOF.1.1 The TSF shall restrict the ability to determine the behaviour of, disable, enable, or modify the behaviour of the functions **as specified in Table 5.3 below** to **authorised administrators assigned to the G-Master role**.

Table 5.3 -Management of security functions behaviour

Function	Action
Automatic actions taken by a G-Module when the G-Server detects a problem while logging activity	**determine the behaviour of, modify the behaviour of**
Specification of audit log size (default 1000 KB)	**determine the behaviour of, modify the behaviour of**
Display of recovery file when access is requested to a compromised resource for which no genuine copy can be recovered	**modify the behaviour of**
Rebooting the G-Server from the Administration Tool	**enable**
G-Server and site-related alerts	**purge**

5.1.5.2. Management of security attributes [Site Attributes] (FMT_MSA.1 (1))

FMT_MSA.1.1 The TSF shall enforce the **Static Resource SFP and Dynamic Resource SFP** to restrict the ability to query, modify, delete, **enable or disable** the security attributes **site properties: Domain Name, IP Address, Port, Protocol[6], and other properties, as well as site protection status** to **the authorised identified roles specified in Table 5.4 below**.

Table 5.4- Management of site security attributes

Security Attributes	G-Master role authorisations	Viewer role
Site properties	**query, modify, delete**	
G-Server protection for a given site	**query, enable, disable**	**query**
Automatic response settings for Alerts[7]	**query, modify**	
Site SSL keys and certificates	**modify**	

[6] Authorised administrator specification of the protocol security attribute for a given protected site, as a selection out of the values HTTP, HTTPS, and HTTPS termination, determines whether FTP_ITC.1 functionality will be provided for communication with the given site.

[7] Determines FAU_ARP.1 behaviour for the given site.

5.1.5.3. Management of security attributes [User Attributes] (FMT_MSA.1 (2))

FMT_MSA.1.1 The TSF shall enforce the **Resource Signing SFP** to restrict the ability to query, modify, or delete the security attributes **administrator security attributes: G-Server role, signing scope and authentication credentials** to **the authorised identified roles specified in Table 5.5 below**.

Table 5.5- Management of administrator security attributes

Security Attributes	Role	Authorisations
User's G-Server role and signing scope	**G-Master**	**query, modify, delete**
User's authentication credentials	**G-Master**	**set initial password, reset user key and password**
	User	**generate signing key and set new password**

5.1.5.4. Secure security attributes (FMT_MSA.2)

FMT_MSA.2.1 The TSF shall ensure that only secure values are accepted for security attributes.

5.1.5.5. Static attribute initialisation [Information Flow Rules] (FMT_MSA.3)

FMT_MSA.3.1 The TSF shall enforce the **Static Resource SFP and Dynamic Resource SFP** to provide permissive default values for security attributes that are used to enforce the SFP.

FMT_MSA.3.2 The TSF shall allow the **authorised administrators with the G-Master role** to specify alternative initial values to override the default values when an object or information is created.

Application Note:

The default values are permissive in the sense that a resource that is not explicitly covered by an exception or verification rule, or a defined site that has not been specified as protected will default to an unprotected mode.

The authorised administrator can override this default by specifying a resource pattern that covers all site resources and requires Recovery, as a first rule in the rules table.

5.1.5.6. Management of TSF data (FMT_MTD.1)

FMT_MTD.1.1 The TSF shall restrict the ability to query, modify, delete, clear**, or perform operations as specified in Table 5.6** the **TSF Data as specified in Table 5.6 below** to **the authorised identified roles specified in Table 5.6**.

Table 5.6- Management of TSF data

Security Attributes	Role	Action
Exception and verification information flow control rules	**G-Master**	**query, modify, delete**
Routing tables that determine access to hosts on the internal network	**G-Master**	**query, modify, clear**
	Viewer	**query**
Signature events defined for EntryControl Application Protection	**G-Master**	**query, modify, clear**
Quotas on the number of concurrent sessions	**G-Master**	**query, modify**
Authorized administrator IP addresses	**G-Master**	**query, modify**
G-Server configuration files[8]	**G-Master**	**export to and import from external files**
G-Server data files[9]	**G-Master**	**export to and import from external files**
G-Server log files[10]	**G-Master**	**export to external files**

5.1.5.7. Revocation [Resource Signatures] (FMT_REV.1 (1))

FMT_REV.1.1 The TSF shall restrict the ability to revoke security attributes associated with the **signed resources**[11] within the TSC to **the authorised identified roles defined by the Resource Signing SFP as authorised to sign a given resource**.

FMT_REV.1.2 The TSF shall enforce the rules **for resource signature revocation as follows: once a signature is revoked, the given resource is left in an unprotected state.**

5.1.5.8. Revocation [Users] (FMT_REV.1 (2))

FMT_REV.1.1 The TSF shall restrict the ability to revoke security attributes associated with the users within the TSC to **administrators with the G-Master role**.

---

[8] Includes site definitions, exception and verification rules, certificate and key files for HTTPS websites, user information and G-Server property definitions.

[9] Includes list of signed resources, the resources themselves and replacement and recovery files.

[10] Includes the System Log, Signing Log and Verification Log.

[11] FMT_REV.1 (1) is refined to treat the last term in the selection [selection: *users, subjects, objects, other additional resources*] as an assignment, in a similar fashion to the treatment of FMT_MSA.3 in NIAP I-0409.

FMT_REV.1.2 The TSF shall enforce the rules **for administrator user security attributes as follows:**

There are three different revocation methods:

a) **Locking a user temporarily revokes a user's authorisation to log on to the Administration Tool or the Signing Tool. If the user is connected to the G-Server when lock out is performed, it only takes effect when the user tries to log on again;**

b) **Resetting a user's key sets a new initial password for the user and forces him or her to create a new key and associated password the next time they log on to the Administration Tool. Because the authenticity of a resource is tied to the authenticity of the user who signed it, resetting a user key renders all the resources the user signed as Ungenuine, and therefore they must be signed again;**

c) **Deleting a user does not render all the resources signed by the user as Ungenuine.**

5.1.5.9. Specification of Management Functions (FMT_SMF.1)

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: **as specified in Table 5.7 below**.

Table 5.7- Specification of Management Functions

Component	Management Function
FMT_MOF.1	**Determination of automatic actions taken by a G-Module when the G-Server detects a problem while logging activity**
	Specification of the system audit log size
	Specification of recovery file to be returned to an end-user when a genuine copy of a resource cannot be recovered
	Rebooting the G-Server from the Administration Tool
	Purging G-Server and site-related alerts
FMT_MSA.1 (1)	**Management of site-related properties**
	Enabling and disabling G-Server protection for a given site
	Management of automatic response settings for Alerts
	Setting site SSL keys and certificates

Component	Management Function
FMT_MSA.1 (2)	**Management of administrators and their G-Server roles**
	Management of administrators' authentication credentials
FMT_MTD.1	**Management of information flow control rules**
	Management of routing tables on the G-Server that determine access to hosts on the internal network
	Management of signature events intercepted by EntryControl
	Export and import of G-Server configuration files, data files, and log files to and from external files
	Management of quotas on the number of concurrent sessions
	Management of authorized IP addresses for administrators

5.1.5.10. Security roles (FMT_SMR.1)

FMT_SMR.1.1 The TSF shall maintain the roles **G-Master, Signer, and Viewer**.

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

5.1.6. Protection of the TOE Security Functions (FPT)

5.1.6.1. Non-bypassability of the TSP (FPT_RVM.1)

FPT_RVM.1.1 The TSF shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

5.1.6.2. TSF domain separation (FPT_SEP.1)

FPT_SEP.1.1 The TSF shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP.1.2 The TSF shall enforce separation between the security domains of subjects in the TSC.

5.1.6.3. State transition control for security attributes (FPT_SSP_EX.1)

FPT_SSP_EX.1.1 The TSF shall support association of multiple versions up to **two versions** of object security attributes for **signed resources**.

FPT_SSP_EX.1.2 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and user data.

FPT_SSP_EX.1.3 The TSF shall periodically during normal operation and at the request of the authorised user invalidate previous versions of the security attributes within **all previous versions**.

5.1.6.4. Reliable time stamps (FPT_STM.1)

FPT_STM.1.1 The TSF shall be able to provide reliable time stamps for its own use.

5.1.7. Resource utilisation (FRU)

5.1.7.1. Maximum quotas (FRU_RSA.1)

FRU_RSA.1.1 The TSF shall enforce maximum quotas of the following resources: **maximum number of Web browser user requests that can be held in the request queue of each HTTP handler connection, maximum number of logged-in administrators** that defined group of users can use simultaneously.

5.1.8. TOE access (FTA)

5.1.8.1. TSF-initiated termination (FTA_SSL.3)

FTA_SSL.3.1 The TSF shall terminate an interactive session after an **administrator-defined time interval of user inactivity**.

5.1.8.2. TOE session establishment (FTA_TSE.1)

FTA_TSE.1.1 The TSF shall be able to deny session establishment based on **Administration Tool and Signing Tool presumed workstation IP addresses, and on the identified administrator's administrative role assignment**.

5.1.9. Trusted path/channels (FTP)

5.1.9.1. Inter-TSF trusted channel [From End-User to G-Server] (FTP_ITC.1 (1))

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

FTP_ITC.1.2 The TSF shall permit the remote trusted IT product to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **end-user sessions to protected sites that require the use of the Secure Sockets Layer**

(SSL) protocol or for which the authorised administrator has specified the HTTPS Termination protocol.

5.1.9.2. Inter-TSF trusted channel [From G-Server to Web Site] (FTP_ITC.1 (2))

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

FTP_ITC.1.2 The TSF shall permit the TSF to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for **communications with a site supporting the Secure Sockets Layer (SSL) protocol, for all sessions defined by the site as requiring the use of SSL**.

5.1.9.3. Trusted path (FTP_TRP.1)

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

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

FTP_TRP.1.3 The TSF shall require the use of the trusted path for initial user authentication and **administration sessions by authorised administrators using the Administration Tool and the Signing Tool**.

5.2. TOE Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level (EAL) 1 components as specified in Part 3 of the Common Criteria. No operations are applied to the assurance components.

Table 5.8- Assurance requirements: EAL1

Assurance Class	Assurance Components
Configuration Management (ACM)	ACM_CAP.1 Version numbers
Delivery and Operation (ADO)	ADO_IGS.1 Installation, generation, and start-up procedures
Development (ADV)	ADV_FSP.1 Informal functional specification
	ADV_RCR.1 Informal correspondence demonstration
Guidance Documents (AGD)	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
Tests (ATE)	ATE_IND.1 Independent testing - conformance

5.2.1. Configuration management (ACM)

5.2.1.1. Version numbers (ACM_CAP.1)

ACM_CAP.1.1D The developer shall provide a reference for the TOE.

ACM_CAP.1.1C The reference for the TOE shall be unique to each version of the TOE.

ACM_CAP.1.2C The TOE shall be labelled with its reference.

5.2.2. Delivery and operation (ADO)

5.2.2.1. Installation, generation, and start-up procedures (ADO_IGS.1)

ADO_IGS.1.1D The developer shall document procedures necessary for the secure installation, generation, and start-up of the TOE.

ADO_IGS.1.1C The installation, generation and start-up[12] documentation shall describe the steps necessary for secure installation, generation, and start-up of the TOE.

5.2.3. Development (ADV)

5.2.3.1. Informal functional specification (ADV_FSP.1)

ADV_FSP.1.1D The developer shall provide a functional specification.

ADV_FSP.1.1C The functional specification shall describe the TSF and its external interfaces using an informal style.

ADV_FSP.1.2C The functional specification shall be internally consistent.

ADV_FSP.1.3C The functional specification shall describe the purpose and method of use of all external TSF interfaces, providing details of effects, exceptions and error messages, as appropriate.

ADV_FSP.1.4C The functional specification shall completely represent the TSF.

5.2.3.2. Informal correspondence demonstration (ADV_RCR.1)

ADV_RCR.1.1D The developer shall provide an analysis of correspondence between all adjacent pairs of TSF representations that are provided.

ADV_RCR.1.1C For each adjacent pair of provided TSF representations, the analysis shall demonstrate that all relevant security functionality of the more abstract TSF representation is correctly and completely refined in the less abstract TSF representation.

[12] The specification of "installation, generation and start-up" in ADO_IGS.1.1C is added in order to comply with CCIMB Interpretation 051.

5.2.4. Guidance documents (AGD)

5.2.4.1. Administrator guidance (AGD_ADM.1)

AGD_ADM.1.1D The developer shall provide administrator guidance addressed to system administrative personnel.

AGD_ADM.1.1C The administrator guidance shall describe the administrative functions and interfaces available to the administrator of the TOE.

AGD_ADM.1.2C The administrator guidance shall describe how to administer the TOE in a secure manner.

AGD_ADM.1.3C The administrator guidance shall contain warnings about functions and privileges that should be controlled in a secure processing environment.

AGD_ADM.1.4C The administrator guidance shall describe all assumptions regarding user behaviour that are relevant to secure operation of the TOE.

AGD_ADM.1.5C The administrator guidance shall describe all security parameters under the control of the administrator, indicating secure values as appropriate.

AGD_ADM.1.6C The administrator guidance shall describe each type of security-relevant event relative to the administrative functions that need to be performed, including changing the security characteristics of entities under the control of the TSF.

AGD_ADM.1.7C The administrator guidance shall be consistent with all other documentation supplied for evaluation.

AGD_ADM.1.8C The administrator guidance shall describe all security requirements for the IT environment that are relevant to the administrator.

5.2.4.2. User guidance (AGD_USR.1)

AGD_USR.1.1D The developer shall provide user guidance.

AGD_USR.1.1C The user guidance shall describe the functions and interfaces available to the non-administrative users of the TOE.

AGD_USR.1.2C The user guidance shall describe the use of user-accessible security functions provided by the TOE.

AGD_USR.1.3C The user guidance shall contain warnings about user-accessible functions and privileges that should be controlled in a secure processing environment.

AGD_USR.1.4C The user guidance shall clearly present all user responsibilities necessary for secure operation of the TOE, including those related to assumptions regarding user behaviour found in the statement of TOE security environment.

AGD_USR.1.5C The user guidance shall be consistent with all other documentation supplied for evaluation.

AGD_USR.1.6C The user guidance shall describe all security requirements for the IT environment that are relevant to the user.

5.2.5. Tests (ATE)

5.2.5.1. Independent testing - conformance (ATE_IND.1)

ATE_IND.1.1D The developer shall provide the TOE for testing.

ATE_IND.1.1C The TOE shall be suitable for testing.

5.3. Security Requirements for the IT Environment

Objective OE.BROWSER_VERIFICATION is an objective for the IT environment. FTP_ITC.1 is iterated and refined to allocate this responsibility to the environment.

Table 5.9 –Security Requirements for the IT Environment

Functional Class	Functional Components		CC Operations
Trusted path/ channels	FTP_ITC.1 (3)	Inter-TSF trusted channel	iteration, assignment, refinement

5.3.1. Trusted path/channels (FTP)

5.3.1.1. Inter-TSF trusted channel [From browser to G-Server] (FTP_ITC.1 (3))

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

FTP_ITC.1.2 The **IT Environment** shall permit **the browser** to initiate communication via the trusted channel.

FTP_ITC.1.3 The **IT Environment** shall initiate communication via the trusted channel for **end-user sessions to protected sites that require the use of the Secure Sockets Layer (SSL) protocol or for which the authorised TOE administrator has specified the HTTPS Termination protocol**.

6. TOE Summary Specification

This section describes the security functions of the TOE and the assurance measures taken to ensure correct implementation, and maps them to the security requirements.

The TOE includes the following security functions:

- TSF Protection Function
- ExitControl
- EntryControl
- Security Management Function
- Audit Function
- Alerts
- Trusted Path/Channel

6.1. TSF Protection Function

The TSF Protection security function provides:

- Domain Separation
- Network Traffic Mediation
- Secure Time Source

The TSF Protection security function is provided by the operating system, and by the Transparency Envelope, a proprietary networking solution that allows the G-Server to be transparently inserted between end-users and protected sites.

6.1.1. Operating System

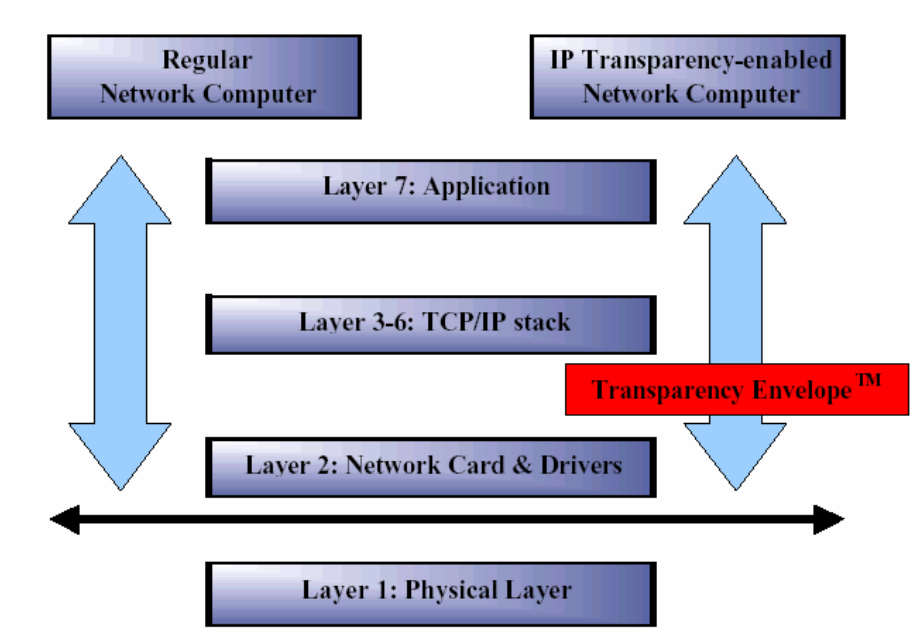
The G-Server is implemented as an application-level service running on a stripped-down Microsoft Windows 2000 Server SP3. In addition to the G-Server service, the other dedicated service running on the machine is the G-Watchdog, which performs availability tests on the G-Server application and restarts it or reboots the machine when an error is detected.

6.1.2. Transparency Envelope

The G-Server is installed between the Web server and the outside network. It does not perform IP routing, nor does it have IP addresses assigned to its two NICs (connected to the outside and inside networks).

The *Transparency Envelope*™ is a service that inserts itself above the network drivers and mediates every network packet entering the machine, as shown in Figure 6.1 below.

Figure 6.1 –Transparency Envelope™



The objectives of the Transparency Envelope are:

- To separate the different traffic categories in order to ensure mediation by the TOE of all mediated traffic, and to protect the TSF from tampering and interference attacks that might be attempted through user data communication channels;
- To make the G-Server platform harder to attack because it has no visible network interfaces (no IP address);
- To simplify installation of the G-Server between the outside and inside networks by transparently intercepting sessions to protected sites and funneling them through the information flow control and audit mechanisms; and
- To provide high-performance packet forwarding for fast-forwarded traffic.

The G-Server is configured by the administrator with routing tables that define the IP addresses of hosts residing on the inside network, for which the G-Server is supposed to perform packet forwarding. When an IP packet is received by the G-Server machine on the outside NIC, it is labeled as belonging to one of the following logical traffic categories:

- **Fast-Forwarded traffic** is traffic that is outside the TSC, i.e. non-HTTP traffic or traffic destined to IP addresses that have not been configured by an authorised G-Server administrator as protected sites. Fast-forwarded traffic is forwarded by the Transparency Envelope to the inside network with no further processing. It is not passed up to layer-3 IP route processing on the G-Server machine.

- **Mediated traffic** is HTTP (and HTTPS) traffic that is flowing to an IP address of a protected site. Such traffic is passed up by the Transparency Envelope to the G-Server service.
- **Administration traffic** is identified as traffic that has a destination IP address of one of the protected sites on the inside network, and a special management port that is reserved by the administrator for administration of the G-Server. When the Transparency Envelope detects a session initiation request to the reserved port, it performs session termination (in the sense of accepting the session and terminating it on the G-Server machine rather than forwarding it onward), and establishes a trusted path to the administration client. To the administration client, network configuration is performed as if this is a communication with the Web server itself.

6.1.3. SFR Mapping

The underlying platform satisfies or supports the following SFRs:

- **FPT_RVM.1** – All communications with protected sites are assumed to flow through the TOE. The TE labels all traffic according to its destination, and ensures that all traffic that in the TSC is mediated by the information flow control functions.
- **FPT_SEP.1** – The G-Server platform provides a security domain that is protected from interference and tampering by untrusted subjects. The G-Server is self-contained and does not rely on any external devices or services for authentication, naming, etc. All of the access control and information flow control security functions are implemented in the context of the G-Server appliance's hardware and software.

  Separation is enforced between the security domains of the subjects in the TSC via TE traffic labeling and separation.
- **FPT_STM.1** – Reliable time stamps are provided by the operating system.
- **FTP_ITC.1(1)** and **FTP_TRP.1** – The TE provides logical separation for Trusted Path and Trusted Channel establishment, performing traffic labeling and forwarding to the appropriate processing mechanism. This supports the Trusted Path/Channel security function described below.

6.2. ExitControl

The central security function provided by the G-Server is that of ExitControl, namely the control of information flow from protected sites on the inside network to end-users on the outside network.

6.2.1. HTTP Request/Response Processing for Static Resources

When an HTTP request to a protected site is intercepted by the Transparency Envelope, it is diverted to the G-Server application. The request is parsed and an outstanding request

record is created in the G-Server cache. The object's security attributes include the resource identifier (URL), its designation in the G-Server database as a static or dynamic resource, resource signatures (if any are registered), and audit and information flow rules and definitions. The request is then forwarded into the inside network.

Responses received from the inside network are matched to outstanding requests. When the information flow control rules specify that the resource is to be verified, the G-Server calculates an MD5 or SHA-1 hash of the response's content body, and attempts to match that to a pre-computed hash stored in the G-Server database. The first time a resource hash is brought into the in-memory cache from the database, the RSA or DSA digital signature (created by the authorised Signer that signed the resource) on the stored hash is verified as well.

If the G-Server determines that the resource is genuine, the HTTP response is released back to the Transparency Envelope to be forwarded to the end-user. Otherwise, depending on the information flow control rules and definitions, the G-Server performs an appropriate Recovery action for the resource.

The information flow control and audit rules can also trigger side-effects for a given request including Alert generation and logging of the request.

6.2.2. HTTP Request/Response Processing for Dynamic Resources

Resources determined to be dynamic resources are processed in a similar way. The request is parsed, and an outstanding request record is created in the G-Server cache.

For a resource that is determined to be dynamic, the G-Server sends a list of script or program identifiers that are involved in generating the resource. The list is piggybacked on the HTTP request forwarded to the Web server, as a special HTTP header. That header is intercepted by the G-Agent module installed on the protected site, which calculates a hash of each of the identified programs or scripts, and sends it back to the G-Server attached to the dynamically generated resource. The G-Server attempts to match the dynamic resource's hash in the same way as it does for static resources.

6.2.3. Request/Response Stripping

The security attributes used by the TSF to label requests and responses and to communicate object identifiers that need to be signed are internal to the TSF; the TSF strips them out of requests or responses that are imported from outside the TOE, and removes them when it is exporting the response back to the end-user.

6.2.4. Resource Recovery

When a resource is received from a protected site for which the information flow control rules and definitions require Recovery, the G-Server searches its database for a genuine mirror copy of the resource contents. If one is found, it is used to replace the contents received from the protected site. If none is found, an administrator-defined default Recovery message is sent instead. This last is always the case for dynamic resources; the G-Server does not support mirroring of dynamic resources.

6.2.5. SFR Mapping

The ExitControl security function satisfies or supports the following SFRs:

- **FDP_DAU.2** – The ExitControl security function performs validity verification on protected resources using the evidence provided by resource signatures, generated by the Security Management Function. Resource validity is determined by comparing the hash stored in the G-Server database with the hash computed for the protected resource. The identity of the user that generated the evidence is determined and verified via the signature associated with the resource hash in the database.
- **FDP_ETC.1** – Resources are exported back to end-users without their associated security attributes; thus the end-user does not perceive any difference in resource contents even when the resource has been defaced and been recovered by the G-Server.
- **FDP_IFC.1(1)** and **FDP_IFF.1(1)** – Dynamic resource information flow control is performed by the ExitControl security function.
- **FDP_IFC.1(2)** and **FDP_IFF.1(2)** – Static resource information flow control is performed by the ExitControl security function. An additional capability is Resource Recovery.
- **FDP_ITC.1(1)** and **FDP_ITC.1(2)** – HTTP Request/Response Processing security functions control user data import from end-users and protected sites.

6.3. EntryControl

In addition to the ExitControl mechanism, the G-Server provides an optional Application Protection facility called EntryControl. When an HTTP request is received by the G-Server for a protected site, it can be tested against a set of predefined signature patterns. When an anomalous request is detected, the connection is closed, and a log entry and/or Alert optionally generated. This security function is intended to provide protection against known HTTP application-level attacks with known signature patterns, as well as unknown attacks that can be distinguished by anomalous request characteristics.

6.3.1. Limits and Constraints on HTTP Requests

An administrator can define a set of predefined limits or constraints on request properties, on a per-site basis, detailed in Table 6.1 below. When EntryControl is enabled, the default limits apply unless modified by the administrator.

Table 6.1- EntryControl Configurable Limits and Constraints

Limit or Constraint	Description
Maximum URL length	maximum length of the URL before the query
Maximum query length	maximum length of the query
Maximum parameters in query	maximum number of parameters in the query

Maximum query parameter length	maximum length of each parameter in the query (name and value)
Maximum number of headers	maximum number of headers in the HTTP request
Maximum length of a header	maximum length of each HTTP header (name and value)
Maximum content length	maximum length of the content part of the request
Maximum parameters in content	maximum number of parameters in the content if it is a submitted form
Maximum content parameter length	maximum length of each parameter in the content if it is a submitted form (name and value)
Maximum http method length	maximum length of the HTTP method
Maximum chunks in content	maximum number of chunks in the content
Maximum characters in HTTP version	maximum length of the HTTP version
Range of characters that may appear in request headers (ASCII values)	
Range of characters that may appear in request content (ASCII values)	
Permitted HTTP methods (GET, POST, etc.)	
Whether to allow fragments in URL	

6.3.2. Attack Signature Detection

The EntryControl mechanism can also perform a surface analysis on the request, looking for predefined attack signatures coded as strings. These patterns can be matched to HTTP headers, the query, the content part of the HTTP request, the URL, and/or a normalized version of the URL.

This security function provides the capability to detect known attacks that can be characterized by a recurring string pattern in the request.

6.3.3. SFR Mapping

The EntryControl security function satisfies the following SFRs:

- **FAU_ARP.1** – EntryControl generates Alerts based on FAU_SAA.3 heuristics.
- **FAU_SAA.3** – Simple attack heuristics are provided by the EntryControl security function by setting limits and constraints on http requests and detecting attack signatures.

6.4. Security Management Function

G-Server administration is performed via three user interfaces: the Maintenance Tool is a command line console interface that is available on the G-Server console, and is used for

initial and low-level configuration and system startup and shutdown tasks. The Administration Tool is a GUI based client/server tool that provides a remote administration capability for most administrator tasks. The Signing Tool is a similar tool that is used for management of resource signatures.

6.4.1. Roles

The G-Server provides support for administrative roles by associating administrators with a role attribute, which is used to determine administrative privileges. Roles include G-Master, which has full administrative privileges, Viewer, with read-only privileges to administration data, and Signer, which is limited to management of resources and resource signatures in the G-Server database.

For further granularity, a user with the Viewer role can be assigned further Signer privileges for a set of selected sites.

6.4.2. G-Server Administration

Basic G-Server administration is performed using the Administration Tool. Management functions are: configuration, management of exception rules and verification rules, user management, and monitoring of audit trails, as summarized below in Table 6.2.

The G-Server restricts access to these management functions to appropriate user roles. This is supported through the definition of a read-only role (Viewer) that is permitted to view some of the configuration information as an aid to troubleshooting and resource management.

The G-Server further restricts content administrators (Signers) from performing restricted security management functions by providing a limited alternate administration interface, the Signing Tool. Users assigned to the Signer role are not permitted to access the G-Server through the Administration Tool interface.

Table 6.2- G-Server Management Functions

Category	Management Function	Description
G-Server management	G-Server configuration	General properties, error reporting, cache parameters, networking properties, Alert destinations, and setting the default Recovery file.
	G-Server maintenance	Rebooting, synchronization, and performing backup and recovery.
Site Management	Site properties	Definition of new sites, site properties update, deleting a site, and enabling or disabling protection.
	SSL Key Management	Installation of SSL keys, certificates.
	Alerts management	Specification of Alert destinations.
	Application Protection	Configuration of the EntryControl signature event patterns.
	Redirection Validation	Specification of authorized redirection destinations.
	Log Management	Setting lmits on per-site logs.
	Information Flow Control Rules	Management of exception rules and of verification rules.
User Management	User Account Management	Adding users, updating user properties (e.g. roles), deleting a user
	Revocation and Suspension	Locking a user from accessing the TOE, performing key reset.
System Monitoring	Diagnostics	Performing connectivity diagnostics.
	Database Monitoring	Viewing signed resources.
	Log Review	Report generation, exporting to external files, and purging of Alerts, System Log, and site Verification Log and Signing Logs.
	Resource Monitoring	Verifying resources stored on a protected site.

6.4.3. Resource Signatures Administration

Resource signature management functions are used by content administrators to manage resources and signatures stored in the G-Server database. These functions are separated from the Administration Tool and provided by the Signing Tool, so that they can be allocated to multiple content owners, each with his or her own area of responsibility. Content owners sign updated content when it becomes available for publishing on the protected site. They are typically associated with the Signer role, which does not have authorization to use the Administration Tool.

Resource signing is performed by the Signing Tool, using a locally-stored administrator private key. Either the Signing Tool or the Administration Tool create the user's key when the user account is established, and use it for both resource signing and for user authentication.

The signed hash of the resource is then stored on the G-Server, with the signature serving to bind the identity of the administrator that signed the resource to the resource hash.

Table 6.3- Resource Signature Management Functions

Management Function	Description
Signing List Management	selection of resources on protected sites that are to be signed
Resource Signing	signing by the administrator that the contents of the selected resources are genuine, storing a mirror copy on the G-Server
Dependency Management	definition of clusters of resources on a protected site that work together to generate a dynamic resource

6.4.4. Resource Integrity Verification

Both the Administration and the Signing Tools provide a capability for requesting a status report to be generated for all or a subset of the resources that have been registered in the G-Server database. This capability involves requesting these resources from the protected sites and verifying their validity. Resource status is displayed as described in Table 6.4 below.

Table 6.4- Resource Integrity Verification Status Codes

Status	Icon	Status Description	Meaning
Genuine		None	The resource is genuine
Ungenuine		Resource not found on the Web Server	The server returns status code 404
		Unauthorized change to resource	The resource does not match its digital signature
		Error status code returned from the Web Server	The server returns a status code other than 200 or 404
Unknown		Resource Not Signed	The resource is not signed
		Communication problem with the Web Server	The server does not reply, or sends an illegal HTTP reply (parsing errors)
		Resource Unprotected	The resource is disabled (presigned)
		Pending Signature only	The resource only has a pending signature and is not fully signed

6.4.5. Pending Signatures

Resources are content stored on a Web server. This content is signed by a G-Server administrator, and thereafter is verified by the G-Server for integrity errors whenever it is accessed by an end-user.

When a resource is updated by an authorized content manager, there are two objects that must be updated before the new content is considered valid: the resource contents on the Web server, and the resource signature on the G-Server. Any mismatch between the two might lead to the G-Server considering the resource as ungenuine.

The solution is to perform the update in two steps. In the first step, the resources are given a pending signature while still located on a staging server, or any other server that you use to collect content before moving it to the protected Web server. These pending signatures are held in reserve by the G-Server until the resources are uploaded to the Web server and a signature shift is performed.

At this point, the G-Server holds two signatures per resource, the current signature and the pending one. When the G-Server verifies the URL, it first checks it against the signature. If the results do not match, it verifies the URL against the pending signature.

Only if this result is ungenuine as well does the G-Server consider the URL to be ungenuine.

The second step involves performing the signature shift after the resources are on the Web server, which removes the old signatures and converts the pending signatures into the new signatures for the resources. These shifts can either be scheduled ahead of time using the Administration Tool or performed on demand.

6.4.6. SFR Mapping

The Security Management security function satisfies the following SFRs:

- **FCS_CKM.1** - user keys are generated by the Admin Toolkit.
- **FCS_COP.1 (3)** and **FCS_COP.1 (1)** - resource hashing and signing (respectively) are performed when an administrator signs a resource.
- **FDP_ACC.1** and **FDP_NIAP-0420-ATR.1** – Only an authorized administrator can manage resource signatures and mirror copies in the G-Server database.
- **FDP_DAU.2 –** Authorized administrators can sign resource contents, and can view resource validity status information, including the identity of the administrator that signed the given resource.
- **FDP_ITC.1 (3), FDP_IFC.1 (3),** and **FDP_IFF.1 (3)** - the G-Server supports the secure import of protected site SSL keys and certificates.
- **FDP_SDI_EX.1** – The G-Server provides an administrator-initiated resource integrity verification security function.
- **FMT_MOF.1** – Only the authorised administrator may manage security function behaviour.
- **FMT_MSA.1(1)** and **FMT_MSA.1(2)** – Only an authorised administrator may manage site and administrator security attributes.
- **FMT_MSA.2** - the TSF creates only secure cryptographic keys.
- **FMT_MSA.3** – The G-Server Security Management function ensures that only an authorised administrator may override the default values for security attributes that are used for information flow control.
- **FMT_MTD.1** – Only an authorised administrator may manage information flow control rules, routing tables, EntryControl Application Protection rules, and may export and import G-Server configuration, data, and log files.
- **FMT_REV.1(1)** – Only an authorised administrator may revoke resource signatures.
- **FMT_REV.1(2)** – Only an authorised administrator may revoke user security attributes.
- **FMT_SMF.1** – The TOE provides the listed security management functions.
- **FMT_SMR.1** – The G-Server provides administrator roles.

- **FPT_SSP_EX.1** – Pending Signatures provide a mechanism for resource signature state transition control.

6.5. Audit Functions

The G-Server maintains a comprehensive audit trail composed of four different logs:

- The **System Log** contains events related to G-Server functionality and a record of TOE administration events;
- Site **Signing Log**s contain resource management events such as resource signing;
- Site **Verification Log**s contain information flow events that match administrator-defined event logging patterns.
- The **Alerts Log** contains Alerts that were triggered by the ExitControl and EntryControl mechanisms;

The logs can be viewed, filtered, and sorted. The administrator can export the log to an external file, and can purge the log. Log sizes are configurable by the administrator.

6.5.1. System Log

The system log is a cyclic log containing a comprehensive record of G-Server activities, including user authentications and administrative activities, as well as a detailed list of system errors. When the log reaches capacity, old entries are deleted automatically in order to make room for new ones.

6.5.2. Signing Logs

The signing log contains details about every signing action performed on a selected site, including the following events: signing and unsigning resources, enabling and disabling resource protection, adding and removing dependencies, creating sub-signatures, performing signature shifts, performing signature verification on protected resources.

6.5.3. Verification Logs

The verification log contains the details of resource retrievals from the selected site, including the verification result obtained by the G-Server.

6.5.4. Alert Log Viewing

The alert log contains a record for each alert that was generated.

6.5.5. SFR Mapping

The Audit security function satisfies the following SFRs:

- **FAU_GEN.1-NIAP-0347** – The TOE Audit security function provides a capability for generating the audit event records indicated in Table 5.2.

- **FAU_SAA.1** – The Alerts Log can be set to trigger external notification functions.
- **FAU_SAR.1** – Authorised administrators are provided with a capability for reading the audit logs.
- **FAU_SAR.3 (1-4)** – The System Log, Verification Log, Signing Log, and Alerts Log can all be searched and sorted by the authorised administrator.
- **FAU_STG.2** – The TOE does not provide any capability for performing modifications to the audit records. Only Authorised administrators may purge the logs. The System Log, Verification Log, and Signing Log are stored in cyclical file**s,** where file size can be set by the administrator. The Alerts Log will not overwrite old records when storage is exhausted; new Alert records are then discarded until an authorised administrator purges the log.

6.6. Alerts

The Administration Tool enables you to manage two levels of alerts: G-Server alerts, such as requested attempts to log in with a bad password, and site alerts, such as notifications about ungenuine content. G-Server alerts include errors related to problems in the system itself.

The three types of Alert G-Modules, described in the following sections, are executed by the G-Server according to the exception and verification rules. If a requested resource matches a rule that triggers alerts, the G-Server issues an alert in the Alert log, and triggers those Alert G-Modules that have been configured.

The administrator can limit the frequency of alerts sent for the same ungenuine data.

6.6.1. Email Alerts

The E-mail G-Module sends an e-mail alert to a predefined list of recipients when an ungenuine resource is detected.

The Quantity limit field determines the interval between e-mail alerts for a particular ungenuine resource, as measured by the number of requests for that resource. This prevents the G-Server from flooding the administrator and e-mail recipients with multiple alerts for the same ungenuine resource.

6.6.2. SNMP Alerts

The SNMP (Simple Network Management Protocol) G-Module sends alert messages to an external device, such as a Network Management System or a pager, when ungenuine resources are detected. The administrator can specify SNMP traps that trigger the alerts on a site-by-site basis.

6.6.3. Execution of Preinstalled Executables

The Executables G-Module triggers commands in other applications installed on the G-Server, such as an audible alarm or an instant messaging program, when an ungenuine

resource is detected. This is determined by the exception and verification rules for the site.

6.6.4. SFR Mapping

The Alerts security function satisfies the following SFRs:

- **FAU_ARP.1** – The TOE is capable of generating Alerts to a set of administrator-defined destinations.

6.7. Trusted Path/Channel

6.7.1. Trusted Path

When an administrator accesses the G-Server using the Administration Tool or the Signing Tool, the G-Server sets up a trusted channel between the client and the server. Integrity and confidentiality protection are achieved using the Secure Sockets Layer (SSL) protocol. Once the session has been established, the client signs a server challenge using the administrator's password protected private key, authenticating the administrator.

Administrative sessions are logically separated from user data traffic by the Transparency Envelope, as described above.

6.7.2. HTTPS Termination

The G-Server provides an SSL Termination capability for end-user HTTPS sessions. A set of SSL certificates (and associated private keys) corresponding to the protected sites on the inside network is installed on the G-Server. The G-Server detects an HTTPS session initiation request going to the protected site, and establishes an SSL-based trusted channel with the end-user on the protected site's behalf.

6.7.3. HTTPS

For protected sites that support the SSL protocol, the G-Server establishes the G-Server to protected site trusted channel as an SSL client, as well as performing HTTPS Termination in order to establish the trusted channel to the end-user's browser. In this scenario, the G-Server is performing a Man in the Middle (MitM) interaction between the end-user and the protected site, in order to guarantee the integrity of the resource contents being returned to the end-user.

6.7.4. TOE Access

The G-Server enforces session termination after a period of user inactivity for both Web browser sessions and for administrators using the Administration Tool or the Signing Tool.

It provides capabilities for limiting the number of users accessing the system simultaneously, and for limiting administrators to specified IP addresses.

The TOE access capabilities are summarized below in Table 6.5.

Table 6.5- TOE Access Parameters

Parameter Name	Description
HTTP Request Timeout (sec)	number of seconds that the system should wait for data before closing a browser connection.
Max Idle Time (sec)	maximum number of seconds that the G-Server will wait for activity from the Administration Tool or the Signing Tool. After this time elapses, the G-Server logs the user out of the tool, forcing them to log in again.
Concurrent Connections	minimum and maximum number of HTTP handlers that will be available to deal with requests from site visitors.
Max. requests per http handler	maximum number of user requests that can be held in the request queue of each connection.
Authorized IP Addresses	blocks unauthorized users from logging in to the G-Server by specifying a list of specific, authorized IP addresses for Administration Tool and Signing Tool logins.

6.7.5. SFR Mapping

The Trusted Path/Channel security function satisfies the following SFRs:

- **FCS_COP.1 (1)** - the client signs a server challenge using the administrator's private key, authenticating the administrator.
- **FCS_COP.1 (2)** - SSL session establishment is performed by the Trusted Path/Channel security functions.
- **FIA_UAU.2** – Administrators are authenticated before they are allowed to perform any action in the TOE.
- **FIA_UAU.7** – The TOE obscures user input when entering a password.
- **FIA_UID.2** – Administrators are identified before they are allowed to perform any action in the TOE.
- **FTP_ITC.1 (1)** – A Trusted Channel can be established between the end-user and the G-Server, using the Secure Sockets Layer (SSL) protocol. SSL is used automatically when the protected site is providing its content over SSL; it can also be configured for a given protected site even when it is serving content over HTTP (HTTPS Termination).
- **FTP_ITC.1 (2)** – When a protected site is providing its content over SSL, the G-Server will establish a Trusted Channel to the site over HTTPS (HTTP over SSL).
- **FTP_TRP.1** – Administration Tool and Signing Tool administrative sessions are provided with a communication path that is logically distinguished from other communication paths by the TE, and protected from modification or disclosure by

establishing a Trusted Path using the SSL protocol, with the user being further authenticated using a challenge-response protocol based on the user's private key.

- **FRU_RSA.1** – The TOE Access security function limits the number of concurrent sessions for both end-users and administrators.
- **FTA_SSL.3** – The TOE Access security function terminates inactive sessions after an administrator-defined time interval, for both end-users and administrators.
- **FTA_TSE.1** – The authorised administrator can set up a TOE Access condition based on a set of authorised IP addresses. Access to the Administration Tool functionality is further dependent on the user's administrative role.

6.8. TOE Assurance Measures

The assurance requirements of EAL1 are met by the TOE documentation described in Table 6.6 below, as well as by providing the TOE to the evaluator for independent testing.

Table 6.6- Mapping of Assurance Requirements to TOE Assurance Measures

SAR	Description	Assurance Measures
ACM_CAP.1	Version numbers	The TOE implements ACM_CAP.1 by including a version number on both the product container and the media (CD-ROM) provided with it. Additionally, the TOE software has an "about" option which lists both the version and the Build Number (for further granularity). The TOE automatically verifies that the versions of the G-Server and that of the Administration and Signing Tools are consistent.
ADO_IGS.1	Installation, generation, and start-up procedures	*G-Server Installation and Getting Started Guide, Version 2.5* provides the content and presentation needed to meet ADO_IGS.1.
ADV_FSP.1	Informal functional specification	*Introduction, Version 1.02* describes the set of documents that detail the TOE's external interfaces.
ADV_RCR.1	Informal correspondence demonstration	Each functional specification document provides a mapping of module interfaces to the relevant TOE security functions. *Correspondence Mapping.xls* demonstrates this correspondence in tabular format.
AGD_ADM.1	Administrator guidance	*G-Server User Guide, Version 2.*5 provides the content and presentation needed to meet AGD_ADM.1 and AGD_USR.1.
AGD_USR.1	User guidance	
ATE_IND.1	Independent testing - conformance	The vendor shall provide the TOE to the evaluator for testing.

7. PP Claims

This Security Target was not written to conform to any Protection Profile.

8. Rationale

8.1. Security Objectives Rationale

This section shows that all threats, secure usage assumptions, and organizational security policies are completely covered by security objectives. In addition, each objective counters or addresses at least one assumption, organizational security policy, or threat.

Table 8.1 and Table 8.2 present the mapping of objectives to the security environment; this is then followed by explanatory text of how this mapping was derived for each environmental consideration.

Table 8.1- TOE IT security objectives rationale

Policy/Threats/Assumptions	Objectives
T.Admin_Err_Commit	O.Admin_Guidance, O.Admin_Role, O.Audit_Account, O.I&A, O.Manage, OE.MANAGED
T.Admin_Err_Omit	O.Admin_Guidance, OE.MANAGED
T.Admin_Rogue	O.Admin_Role, O.Audit_Account, O.Audit_Protect, O.I&A, O.TOE_Access
T.Defacement	O.Integrity, O.Manage, O.Resource_Recovery, O.Redirection_Control
T.Hack_AC	O.I&A, O.Self_Protection, O.TOE_Access, O.Trusted_Path
T.Hack_Avl_Resource	O.Limit_Sessions
T.Hack_Comm_Eavesdrop	O.Trusted_Channel
T.Hack_Masq	O.I&A, O.Audit_Account, O.Audit_Protect, O.TOE_Access, O.Trusted_Path
T.Hack_Msg_Data	O.Trusted_Channel
T.Hack_Site	O.Application_Protection, O.Audit_Account, O.Manage
T.Spoofing	O.Trusted_Channel, O.Redirection_Control, OE.BROWSER_VERIFICATION
T.TSF_Compromise	O.Self_Protection
T.Unattended_Session	O.TOE_Access
P.Accountability	O.Audit_Account, O.Audit_Protect, O.I&A, O.Trusted_Path

Policy/Threats/Assumptions	Objectives
P.Availability	O.Limit_Sessions, O.Resource_Recovery
P.Integrity	O.Integrity, O.Trusted_Channel
A.NETWORK_MEDIATION	OE.NETWORK_MEDIATION
A.NO_EVIL_ADM	OE.MANAGED
A.NO_GENERAL_PURPOSE	OE.MANAGED
A.PHYSICAL	OE.PHYSICAL
A.PEER	OE.MANAGED
A.BROWSER	OE.BROWSER_VERIFICATION

Table 8.2- Tracing of security objectives to the TOE security environment

Objectives	Policy/Threats/Assumptions
O.Admin_Guidance	T.Admin_Err_Commit, T.Admin_Err_Omit
O.Admin_Role	T.Admin_Err_Commit, T.Admin_Rogue
O.Application_Protection	T.Hack_Site
O.Audit_Account	P.Accountability, T.Admin_Err_Commit, T.Admin_Rogue, T.Hack_Masq, T.Hack_Site
O.Audit_Protect	P.Accountability , T.Admin_Rogue, T.Hack_Masq
O.I&A	P.Accountability, T.Admin_Err_Commit, T.Admin_Rogue, T.Hack_AC, T.Hack_Masq
O.Integrity	P.Integrity, T.Defacement
O.Limit_Sessions	P.Availability, T.Hack_Avl_Resource
O.Manage	T.Admin_Err_Commit, T.Defacement, T.Hack_Site
O.Redirection_Control	T.Defacement, T.Spoofing
O.Resource_Recovery	P.Availability, T.Defacement
O.Self_Protection	T.Hack_AC, T.TSF_Compromise
O.TOE_Access	T.Admin_Rogue, T.Hack_AC, T.Hack_Masq, T.Unattended_Session
O.Trusted_Channel	P.Integrity, T.Hack_Comm_Eavesdrop, T.Hack_Msg_Data, T.Spoofing
O.Trusted_Path	P.Accountability, T.Hack_AC, T.Hack_Masq
OE.PHYSICAL	A.PHYSICAL

Objectives	Policy/Threats/Assumptions
OE.MANAGED	A.NO_EVIL_ADM, A.NO_GENERAL_PURPOSE, A.PEER, T.Admin_Err_Commit, T.Admin_Err_Omit
OE.NETWORK_MEDIATION	A.NETWORK_MEDIATION
OE.BROWSER_VERIFICATION	A.BROWSER, T.Spoofing

T.Admin_Err_Commit: Administrative errors of commission

An administrator commits errors that directly compromise organizational security objectives or change the technical security policy enforced by the G-Server.

O.Manage ensures that the TOE provides the necessary administrator support in order to mitigate this threat. O.Admin_Guidance supports this objective by providing adequate administrator guidance.

O.Admin_Role provides administrative roles that can isolate the amount of damage an authorised administrator can perform. O.I&A and O.Audit_Account support recovery after an administrator error has occurred by providing identifying information regarding the erring administrator and the modifications performed.

OE.MANAGED requires those responsible for the TOE to ensure that the TOE is delivered, installed, managed, and operated in a manner that maintains IT security objectives, including providing appropriate training and supervision for administrators.

T.Admin_Err_Omit: Administrative errors of omission

The system administrator fails to perform some function essential to security.

O.Admin_Guidance provides adequate administrator guidance to ensure that no essential functions are missed by the administrator.

OE.MANAGED requires those responsible for the TOE to ensure that the TOE is delivered, installed, managed, and operated in a manner that maintains IT security objectives, including providing appropriate training and supervision for administrators.

T.Admin_Rogue: Hostile administrator modification of user or TSF data

An administrator maliciously obstructs organizational security objectives or modifies the system's configuration to allow security violations to occur.

O.Admin_Role provides administrative roles that can isolate the amount of damage an authorised administrator can perform. O.I&A ensures that administrators are identified and authenticated before they are given access to the TOE. O.TOE_Access restricts administrators' access to the Administration tool. O.Audit_Account ensures that any

modifications are recorded, in order to provide deterence against malicious administrator actions. O.Audit_Protect ensures accountability by protecting these audit records against modification or unauthorised deletion by a malicious administrator.

T.Defacement: Malicious defacement of Web contents

A hacker maliciously modifies resources stored on a protected site in an attempt to deny access to valid Web resources, damage the organization's reputation, or otherwise provide misleading information in order to affect end-user experience and reactions.

O.Integrity prevents protected resources that have been modified in an unauthorised manner from flowing to end-users. O.Resource_Recovery can replace the modified resource with an archived copy of the genuine resource contents, if a mirror copy of the resource was stored in the G-Server database. O.Manage supports these objectives by providing the functions and facilities necessary to sign protected resources and to manage the ExitControl rules.

O.Redirection_Control prevents a hacker from inserting a redirection directive that causes end-users to be redirected to an inappropriate site or location, thereby bypassing the TSF's enforcement mechanisms.

T.Hack_AC: Hacker undetected system access

A hacker gains undetected access to the G-Server due to missing, weak and/or incorrectly implemented access control causing potential violations of integrity, confidentiality, or availability.

O.I&A ensures that each administrator is identified and authenticated before receiving access to the G-Server. O.TOE_Access limits access to TOE administration according to workstation address and user roles, thereby preventing an unauthorised outsider from attempting access to the system. O.Trusted_Path ensures that administrator sessions are logically distinct from, and cannot be confused with, other communication paths (e.g. end-user to protected site interaction). It also provides assured identification of the session end-point, preventing the hacker from interfering with an authorised user's administrative session.

O.Self_Protection protects the TSF's execution domain and its resources from external interference, tampering, or unauthorised disclosure.

T.Hack_Avl_Resource: Hacker attempts resource denial of service

A hacker executes commands, sends data, or performs other operations that make system resources unavailable to system users. Resources that may be denied to users include bandwidth, processor time, memory, and data storage.

O.Limit_Sessions provides administrator-configurable limits to the number of sessions available at any given time to end-users accessing a given protected site, as well as to the number of concurrently active administrators. This allows the administrator to ensure that bandwidth allocation, processor time allocation, memory allocation, and data storage resources, which are a function of the number of concurrent sessions, stay within system limits. It also ensures continued service for protected sites that are not under attack.

T.Hack_Comm_Eavesdrop: Hacker eavesdrops on user data communications

Hacker obtains end-user data by eavesdropping on communications lines.

O.Trusted_Channel provides a trusted path for end-user data flowing between the TOE and remote users and trusted IT products that is logically distinct from other communication channels, protecting the data from modification or disclosure.

T.Hack_Masq: Hacker masquerading as a legitimate user or as system process

A hacker masquerades as an authorised subject to perform operations that will be attributed to the authorised subject.

O.I&A requires unique user identification and authentication. O.TOE_Access limits user access using additional attributes such as workstation IP address and user role.

O.Audit_Account provides a deterrent to masquerade threats by recording user activity, including user identity, source IP address, access timestamp and other information. O.Audit_Protect prevents an administrator from modifying or deleting audit records in an attempt to remove traces of unauthorised or anomalous activity.

O.Trusted_Path ensures that a trusted path will be established between the user and the system, providing assured identification of its end points, and protecting session data from modification and disclosure. This protection can also prevent session hijacking attacks that can be used as a form of masquerade.

T.Hack_Msg_Data: Message content modification

A hacker modifies end-user data intercepted from a communication link between an end-user and a protected site before passing it on, thereby deceiving the intended recipient.

O.Trusted_Channel provides a trusted path for end-user data flowing between the TOE and remote users and trusted IT products that is logically distinct from other communication channels, protecting the data from modification or disclosure.

T.Hack_Site: Hacker crafts malicious Web request

An end-user crafts a malicious anomalous Web request to a protected site that results in a violation of the protected site's security policy.

O.Application_Protection provides protection against malicious Web requests that may cause a violation of a protected site's security policy. O.Manage provides the authorised administrator with the functions and facilities needed to manage the EntryControl rules.

O.Audit_Account provides the capability for logging Web requests as an aid to detection of and recovery from site compromise attacks; an attacker that compromises the protected site might tamper with audit trails stored on the compromised site, whereas the G-Server audit trail can still be used for attack forensics procedures.

T.Spoofing: Legitimate system services are spoofed

An attacker tricks end-users into interacting with spurious system services.

O.Trusted_Channel provides assured identification of its end points. In order to fully counter this threat, the environment must apply OE.BROWSER_VERIFICATION in order to verify the TOE-provided identification information.

O.Redirection_Control prevents a hacker from inserting a redirection directive that causes end-users to be covertly redirected to an inappropriate site or location.

T.TSF_Compromise: Compromise of the TSF

An end-user, protected or unprotected site may send a specially crafted message through the TOE, thereby causing user data, TSF data or executable code to be inappropriately accessed (viewed, inserted, modified, or deleted).

O.Self_Protection ensures that the TSF maintains a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorised disclosure.

T.Unattended_Session: A user takes over an unattended session

A user may gain unauthorised access to an unattended session.

O.TOE_Access controls a user’s logical access to the TOE, initiating session termination after a period of user inactivity.

P.Accountability: Individual accountability

Administrators shall be held accountable for their actions.

O.Audit_Account provides a capability to generate reports on past user activity. O.Audit_Protect ensures that this capability is protected against unauthorised modifica-

tion and deletion. O.I&A provides the TSF with a unique identification of all administrators of the TSF.

O.Trusted_Path prevents users from hijacking authorised users' sessions in an attempt to usurp their identity.

P.Availability: Information availability

Administrator-designated protected resources shall be maintained available to end-users regardless of the availability of the corresponding protected sites.

O.Resource_Recovery ensures that critical user data on a protected site is available to end-users even in the face of an attack that compromises the information stored on the site, by providing to the end-user an archived copy of the genuine resource contents.

O.Limit_Sessions diminishes the effect of possible denial of service attacks by allowing an administrator to limit the number of concurrent sessions, thereby preventing an attacker from consuming all available bandwidth, CPU, memory, and/or storage resources. This ensures continued service for protected sites that are not under attack.

P.Integrity: Information content integrity

Protected resources shall retain their content integrity when requested by end-users.

O.Integrity ensures that protected resources that have been modified in an unauthorised manner are prevented from flowing to end-users.

O.Trusted_Channel protects user data from modification in transit, maintaining its integrity while it travels over the network.

A.NETWORK_MEDIATION: Complete mediation of network traffic

The TOE environment is divided into an inside network that contains protected sites, and an outside network to which resources are sent. All communication between inside and outside is mediated by the TOE.

OE.NETWORK_MEDIATION upholds this assumption by requiring those responsible for the TOE to ensure that the network is configured such that all information flows that are controlled by the TSP pass through the TOE.

A.NO_EVIL_ADM: G-Server administrators are trusted not to abuse their authority

Administrators, and especially users assigned to the G-Master role, are non-hostile, appropriately trained and follow all administrator guidance.

OE.MANAGED upholds this assumption by requiring those responsible for the TOE to ensure that the TOE is delivered, installed, managed, and operated in a manner which maintains IT security objectives.

A.NO_GENERAL_PURPOSE: No general purpose computing capabilities

TOE administrators will not install any general-purpose computing or storage repository capabilities (e.g., compilers, editors, or user applications) in the TOE.

OE.MANAGED upholds this assumption by requiring those responsible for the TOE to ensure that the TOE is delivered, installed, managed, and operated in a manner which maintains IT security objectives.

A.PHYSICAL: Physical access

The TOE is located with controlled access facilities that prevent unauthorised physical access by outsiders.

A.PHYSICAL upholds this assumption by requiring those responsible for the TOE to ensure that the TOE is located in physically secure facilities where it is protected from physical attack which might compromise IT security objectives.

A.PEER: Connectivity to other systems

It is assumed that TOE administrators will install the TOE in an environment protected by a security gateway or firewall from arbitrary external malicious network traffic. Protected sites as well as systems hosting administrative tools interacting with the TOE are assumed to be installed on the inside network, and to be under the same management control as the TOE. Systems hosting administrative tools interacting with the TOE are assumed to be non-malicious.

OE.MANAGED upholds this assumption by requiring those responsible for the TOE to ensure that the TOE is delivered, installed, managed, and operated in a manner which maintains IT security objectives. This includes installation and operation of the TOE, workstations used for administrating the TOE, as well as protected sites, in an environment that is under the same management control and operating under the security policy constraints assumed by A.PEER.

A.BROWSER: End-user software performs trusted channel verification

End-user software performs trusted channel verification to ensure that a trusted channel has been established that protects the user from Web spoofing attacks by entities outside of the TSC.

OE.BROWSER_VERIFICATION upholds this assumption by requiring end-users to ensure that the validity of the trusted channel is verified by end-user software.

8.2. Security Requirements Rationale

This section provides a rationale for the completeness and internal consistency of the security requirements in meeting the identified security objectives.

8.2.1. Security Functional Requirements Rationale

Table 8.3 maps the set of specified SFRs to security objectives specified in Section 4, showing how each security objective is met by one or more SFRs.

Table 8.4 provides evidence that each SFR is necessary. This is followed by appropriate explanatory text.

Table 8.3- Security Objective to Functional Component Mapping

Objectives	Requirements
O.Admin_Role	FAU_SAR.1, FDP_ACC.1, FDP_NIAP-0420-ATR.1, FMT_MOF.1, FMT_MSA.1(1), FMT_MSA.1(2), FMT_MTD.1, FMT_REV.1(2), FMT_SMR.1
O.Application_Protection	FAU_ARP.1, FAU_GEN.1-NIAP-0347, FAU_SAA.3, FAU_SAR.1, FAU_SAR.3(2), FAU_SAR.3(4)
O.Audit_Account	FAU_GEN.1-NIAP-0347, FAU_SAR.1, FAU_SAR.3(1), FAU_SAR.3(3), FCS_COP.1(1), FDP_DAU.2, FPT_STM.1
O.Audit_Protect	FAU_SAR.1, FAU_STG.2
O.I&A	FIA_UAU.2, FIA_UAU.7, FIA_UID.2, FMT_REV.1(2)
O.Integrity	FAU_ARP.1, FAU_GEN.1-NIAP-0347, FAU_SAA.1, FAU_SAR.1, FAU_SAR.3(2), FAU_SAR.3(4), FCS_COP.1 (1), FCS_COP.1 (3), FDP_DAU.2, FDP_ETC.1, FDP_IFC.1(1), FDP_IFC.1(2), FDP_IFF.1(1), FDP_IFF.1(2), FDP_ITC.1(1), FDP_ITC.1(2), FDP_SDI_EX.1, FMT_REV.1(2), FPT_SSP_EX.1
O.Limit_Sessions	FRU_RSA.1

O.Manage	FAU_ARP.1, FAU_SAA.1, FAU_SAA.3, FCS_CKM.1, FCS_COP.1(1), FCS_COP.1(3), FDP_DAU.2, FDP_IFC.1(1), FDP_IFC.1(2), FDP_IFC.1(3), FDP_IFF.1(1), FDP_IFF.1(2), FDP_IFF.1(3), FDP_ITC.1 (3), FMT_MSA.2, FMT_MSA.3, FMT_REV.1(1), FMT_REV.1(2), FMT_SMF.1, FPT_SSP_EX.1
O.Redirection_Control	FDP_IFC.1(2), FDP_IFF.1(2)
O.Resource_Recovery	FDP_IFF.1(2)
O.Self_Protection	FPT_RVM.1, FPT_SEP.1
O.TOE_Access	FMT_REV.1(2), FTA_SSL.3, FTA_TSE.1
O.Trusted_Channel	FCS_COP.1 (2), FTP_ITC.1(1), FTP_ITC.1(2)
O.Trusted_Path	FCS_CKM.1(2), FCS_COP.1(1), FCS_COP.1(2), FTP_TRP.1
OE.BROWSER_VERIFICATION	FTP_ITC.1(3)

Table 8.4- Functional Component Grounding in Security Objectives

	O.Admin_Role	O.Application_Protection	O.Audit_Account	O.Audit_Protect	O.I&A	O.Integrity	O.Limit_Sessions	O.Manage	O.Redirection_Control	O.Resource_Recovery	O.Self_Protection	O.TOE_Access	O.Trusted_Channel	O.Trusted_Path	OE.BROWSER_VERIFICATION
FAU_ARP.1		✓				✓		✓							
FAU_GEN.1-NIAP-0347		✓	✓			✓									
FAU_SAA.1						✓		✓							
FAU_SAA.3		✓						✓							
FAU_SAR.1	✓	✓	✓	✓		✓									
FAU_SAR.3(1)			✓												
FAU_SAR.3(2)		✓				✓									
FAU_SAR.3(3)			✓												

	O.Admin_Role	O.Application_Protection	O.Audit_Account	O.Audit_Protect	O.I&A	O.Integrity	O.Limit_Sessions	O.Manage	O.Redirection_Control	O.Resource_Recovery	O.Self_Protection	O.TOE_Access	O.Trusted_Channel	O.Trusted_Path	OE.BROWSER_VERIFICATION
FAU_SAR.3(4)		✓				✓									
FAU_STG.2				✓											
FCS_CKM.1								✓							
FCS_COP.1(1)			✓			✓		✓						✓	
FCS_COP.1(2)													✓	✓	
FCS_COP.1(3)						✓		✓							
FDP_ACC.1	✓														
FDP_NIAP-0420-ATR.1	✓														
FDP_DAU.2			✓			✓		✓							
FDP_ETC.1						✓									
FDP_IFC.1(1)						✓		✓							
FDP_IFC.1(2)						✓		✓	✓						
FDP_IFC.1(3)								✓							
FDP_IFF.1(1)						✓		✓							
FDP_IFF.1(2)						✓		✓	✓	✓					
FDP_IFF.1(3)								✓							
FDP_ITC.1(1)						✓									
FDP_ITC.1(2)						✓									
FDP_ITC.1(3)								✓							
FDP_SDI_EX.1						✓									
FIA_UAU.2					✓										
FIA_UAU.7					✓										
FIA_UID.2					✓										

	O.Admin_Role	O.Application_Protection	O.Audit_Account	O.Audit_Protect	O.I&A	O.Integrity	O.Limit_Sessions	O.Manage	O.Redirection_Control	O.Resource_Recovery	O.Self_Protection	O.TOE_Access	O.Trusted_Channel	O.Trusted_Path	OE.BROWSER_VERIFICATION
FMT_MOF.1	✓														
FMT_MSA.1(1)	✓														
FMT_MSA.1(2)	✓														
FMT_MSA.2								✓							
FMT_MSA.3								✓							
FMT_MTD.1	✓														
FMT_REV.1(1)								✓							
FMT_REV.1(2)	✓				✓	✓		✓				✓			
FMT_SMF.1								✓							
FMT_SMR.1	✓														
FPT_RVM.1											✓				
FPT_SEP.1											✓				
FPT_SSP_EX.1						✓		✓							
FPT_STM.1			✓												
FRU_RSA.1							✓								
FTA_SSL.3												✓			
FTA_TSE.1												✓			
FTP_ITC.1(1)													✓		
FTP_ITC.1(2)													✓		
FTP_TRP.1														✓	
FTP_ITC.1(3)															✓

O.Admin_Role: Administrator roles

The TOE will provide administrator roles to isolate administrative actions.

FMT_SMR.1 defines the administrative roles that can be assigned to users. The following SFRs restrict management actions to specified administrative roles:

- FAU_SAR.1 restricts audit review
- FDP_ACC.1 and FDP_NIAP-0420-ATR.1 restrict resource signing.
- FMT_MOF.1 restricts execution of management functions.
- FMT_MSA.1(1) restricts management of site attributes, FMT_MSA.1(2) restricts management of user attributes, and FMT_MTD.1 restricts management of TSF data.
- FMT_REV.1(2) restricts user revocation to authorised identified roles.

O.Application_Protection: Protection against malicious Web requests

The TOE will provide protection against malicious Web requests that may cause a violation of a protected site's security policy.

FAU_SAA.3 defines a set of signature event patterns that are matched against incoming traffic to detect potential violations of the TSP. FAU_ARP.1 provides an automatic response to these events by closing the connection and optionally generating an alert.

FAU_GEN.1-NIAP-0347 requires a capability for generating audit records when a potential attack is detected. FAU_SAR.1 provides the authorised identified administrator with the capabilities needed to review the audit trail. FAU_SAR.3(2) and FAU_SAR.3(4) provide additional capabilities for performing searches and sorting on the Verification log and Alerts log, respectively.

O.Audit_Account: Auditing for accountability

The TOE will provide information about past subject behaviour to an authorised administrator through system mechanisms. Specifically, during any specified time interval, the TOE is able to report to an administrator selected auditable actions that an end-user, protected site, or administrator has performed.

FAU_GEN.1-NIAP-0347 requires that the TSF be able to generate an audit record of auditable events, including identifying information such as subject identity. FPT_STM.1 supports this objective by providing secure time stamps for the audit records. FAU_SAR.1 provides a requirement that the TSF shall provide the capability of reading the audit records in a manner suitable for the identified user roles to interpret the information. FAU_SAR.3(1) and FAU_SAR.3(3) provide additional capabilities for searching and sorting of the audit data based on identifying criteria.

FDP_DAU.2 requires that authorised identified administrator roles be provided with the capability to verify the identity of the user that generated a given resource signature, together with its validity.

O.Audit_Protect: Protect stored audit records

The TOE will protect audit records against unauthorised access, modification, or deletion to ensure accountability of subject actions.

FAU_STG.2 requires that audit records be protected from unauthorised deletion and that modifications can be prevented by the TSF. In addition, it provides guarantees for audit data availability in the event of audit storage exhaustion.

FAU_SAR.1 defines the administrator roles that are authorised to access the audit records.

O.I&A: Identify and authenticate each administrator

The TOE will uniquely identify and authenticate each administrator of the system.

FIA_UID.2 and FIA_UAU.2 require users to be successfully identified and authenticated before allowing any other TSF-mediated actions on behalf of those users.

FMT_REV.1 (2) defines capabilities for user revocation and suspension, in order to maintain the uniqueness of the identification mechanism in the face of suspected compromise of authentication credentials.

FIA_UAU.7 ensures that only obscured feedback is provided to the user while the authentication is in progress, protecting against leakage of authentication credentials.

O.Integrity: Integrity protection for protected resources

The TOE will prevent protected resources that have been modified in an unauthorised manner from flowing to end-users.

FDP_ITC.1(1) and FDP_ITC.1(2) require that a resource will be validated when it is received by the G-Server from the protected site. The validation is performed against the resource signature stored in the G-Server database, created using FDP_DAU.2. This validation attribute is removed by FDP_ETC.1 when the resource is finally released back to the end-user.

FCS_COP.1(1) and FCS_COP.1(3) provide the cryptographic implementation for FDP_DAU.2, requiring support for signing and hashing, respectively.

FDP_IFC.1(1) and FDP_IFF.1(1), FDP_IFC.1(2) and FDP_IFF.1(2) deal with performing information flow control on resources in order to prevent modified resources from flowing to end users in an unauthorised manner.

FDP_SDI_EX.1 provides the capability to verify resource integrity manually, in order to detect and correct integrity errors before the user has a chance to ask for the resources.

FMT_REV.1(2) supports the integrity objective in the face of compromise of administrator authentication credentials by providing the capability of resetting a user's key, thereby automatically invalidating the resource signatures signed by that key.

FPT_SSP_EX.1 provides a Pending Signatures paradigm that ensures that integrity is maintained at all times, even when resources are being modified in an authorised manner.

FAU_GEN.1-NIAP-0347 can be configured to generate audit records when modified resources are detected, whereas FAU_ARP.1 (supported by FAU_SAA.1) can generate Alerts to administrators. FAU_SAR.1 is the requirement that supports authorised administrators in reading the audit trail.

FAU_SAR.3(2) and FAU_SAR.3(4) support the administrator acting in the auditor role by offering sort and search capabilities on the Verification and Alerts logs.

O.Limit_Sessions: Limit sessions to outside users

The TOE will limit the resources of the TOE that can be allocated at any given time to outside users.

FRU_RSA.1 enforces administrator-defined maximum quotas for the number of concurrent user sessions, thereby limiting the resources that can be allocated by outside users.

O.Manage: Administration of the TSF

The TOE will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE.

FMT_SMF.1 defines the set of security management functions required for the TOE.

FAU_ARP.1 provides a capability for the authorised administrator to configure Alert notification destinations, including email, SNMP, and triggering preinstalled executables on the G-Server.

FAU_SAA.1 requires a facility for the authorised administrator to be able to specify Alert generation for a given ExitControl information flow control rule.

FAU_SAA.3 provides an administrator facility for defining EntryControl signature event patterns for detecting HTTP application-level attacks on a protected site.

FDP_DAU.2 provides resource signing and verification facilities and functions for authorised administrators. FPT_SSP_EX.1 enhances this capability by supporting administrator-controlled Pending Signatures and signature shifts. FMT_REV.1 (1) provides signature revocation capabilities, as well as FMT_REV.1 (2) for administrator revocation.

FDP_COP.1(3) and FDP_COP.1(1) provide the cryptographic implementation for FDP_DAU.2, requiring support for signing and hashing, respectively.

FDP_IFC.1(1), FDP_IFC.1(2), FDP_IFF.1(1), and FDP_IFF.1(2) provide ExitControl management functions for administration of exception and verification rules for information flow control. FMT_MSA.3 defines default security attribute behaviour for the information flow control rules, and the capability for an authorised administrator to specify alternative initial values.

FCS_CKM.1 generates user authentication and signing keys. FMT_MSA.2 ensures that only secure keys are generated by the system.

FDP_ITC.1(3), FDP_IFC.1(3), and FDP_IFF.1(3) provide a capability for importing SSL keys and certificates and associating them with a given protected site.

O.Redirection_Control: Control of authorised destinations for user redirection

The TOE will only permit redirection directives that redirect the end-user to a pre-authorised list of redirection directive destinations.

FDP_IFC.1(2) and FDP_IFF.1(2) provide an additional capability for validating redirection directives coming back from Web server against a list of authorised redirection destinations.

O.Resource_Recovery: Recovery of genuine resource contents

The TOE will provide to the end-user an archived copy of the genuine resource contents when unauthorised modification is detected.

FDP_IFF.1(2) provides an additional capability for replacing a modified copy of the resource with a “genuine” mirror copy.

O.Self_Protection: Protection of the TSF

The TSF will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorised disclosure.

FPT_RVM.1 together with FPT_SEP.1 ensure non-bypassability and domain separation for the TOE.

O.TOE_Access: Control access to the TOE

The TOE will provide mechanisms that control a user’s logical access to the TOE.

FTA_SSL.3 provides for session termination after an administrator-defined time interval in order to counter masquerade, hijacking and spoofing threats. FTA_TSE.1 provides the

TSF with a capability for testing user attributes such as IP address as a condition for permitting session establishment.

FMT_REV.1(2) provides a capability for suspending a user, which means that he cannot login until his access restrictions are removed.

O.Trusted_Channel: Trusted channel for transmission of user data

The TOE will provide a trusted path for communication of user data between the TOE and remote users and trusted IT products that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from modification or disclosure.

FTP_ITC.1(1) provides a trusted channel between the TOE and an end-user. FTP_ITC.1(2) provides a capability for extending that channel by forming a similar channel from the TOE to a protected site.

FCS_COP.1(2) provides cryptographic support for SSL session establishment.

O.Trusted_Path: Provide a trusted path

The TOE will provide a trusted path between the user and the system. Execution of a user-requested action must be made via a trusted path with the following properties:

- *The path is logically distinct from, and cannot be confused with, other communication paths (by either the user or the system).*
- *The path provides assured identification of its end points.*

FTP_TRP.1 provides a trusted path between the administrator and the G-Server.

FCS_COP.1(2) provides cryptographic support for SSL session establishment. FCS_COP.1(1) provides an administrator signature on a server challenge that authenticates the administrator to the G-Server as part of the Trusted Path establishment.

OE.BROWSER_VERIFICATION: End-user software trusted channel verification

End-users shall ensure the validity of a trusted channel established with the TOE via manually-operated or automated end-user software mechanisms.

The FTP_ITC.1(3) requirement for the IT environment provides a trusted channel between the browser and the TOE that corresponds to the channel required by FTP_ITC.1(1). This requirement for the IT environment supports the end-user in ensuring the validity of the trusted channel established with the TOE.

8.2.2. Security Assurance Requirements Rationale

The level of assurance chosen for this ST is that of Evaluation Assurance Level (EAL) 1, as defined in Part 3 of the Common Criteria.

EAL1 is considered an appropriate assurance level for the TOE because, as described in Part 3, it provides a meaningful increase in assurance over an unevaluated IT product and is appropriate for low-threat environments.

The TOE is designed as a second-level defense. Attackers must still penetrate firewall and Web server defenses, in addition to the TOE itself, in order to violate the integrity policy enforced by the TSF. Furthermore, the TOE itself has no general purpose storage capabilities (A.NO_GENERAL_PURPOSE), and is not designed to store confidential information. Thus there is no great motivation to compromise the TOE as a means to achieving access to information stored on the TOE.

Assumption A.PEER asserts that the TOE will be installed and operated in an environment that is protected by a security gateway or firewall from arbitrary external malicious network traffic. Protected sites as well as systems hosting administrative tools interacting with the TOE are assumed to be installed on the inside network, and to be under the same management control as the TOE. Systems hosting administrative tools interacting with the TOE are assumed to be non-malicious. The TOE itself is located within controlled access facilities that prevent physical access by unauthorised outsiders (A.PHYSICAL). Administrators are assumed to be non-hostile (A.NO_EVIL_ADM). Therefore the threat level is considered low.

Table 8.5 below describes the mapping of the EAL1 assurance components to security objectives for the TOE.

Table 8.5- Mapping of EAL 1 Assurance Components to Security Objectives

Objectives	Requirements
O.Admin_Guidance	ADO_IGS.1, AGD_ADM.1, AGD_USR.1
Other (EAL1)	ACM_CAP.1, ADV_FSP.1, ADV_RCR.1, ATE_IND.1

O.Admin_Guidance: Administrator guidance documentation

The TOE will deter administrator errors by providing adequate administrator guidance.

ADO_IGS.1, AGD_ADM.1, and AGD_USR.1 ensure the adequacy of the installation and generation guidance, administration guidance, and user guidance, respectively.

8.2.3. Extended Requirements Rationale

8.2.3.1. Audit data generation (FAU_NIAP-0347-GEN.1)

FAU_NIAP-0347-GEN.1 is a variation on FAU_GEN.1 that adds the modifier "(if applicable)" to the requirement of recording the subject identity in audit records.

FAU_GEN.1.1-NIAP-0347 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 [selection: *choose one of: minimum, basic, detailed, not specified*] level of audit; and

c) [selection: [assignment: *other specifically defined auditable events*], *"no additional events"*].

FAU_GEN.1.2-NIAP-0347 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, [selection: [assignment: *other audit relevant information]*, "*no other information*"]

8.2.3.2. Security Attribute Management and Inheritance (FDP_NIAP-0420-ATR.1)

FDP_NIAP-0420-ATR.1 is defined in NIAP Interpretation I-0420, and is also equivalent to the SFR defined in CCIMB RI # 107 – "Attribute Inheritance/ Modification Rules Need to be Included in Policy."

FDP_NIAP-0420-ATR.1 Security Attribute Management and Inheritance addresses the policy rules to be enforced during the establishment and modification of security attributes.

As described in the interpretation: "FMT_MSA.1.1 only allows the specification of the roles permitted to make selected security attribute modifications. However, the FMT_MSA component provides no ability to specify policies related to security attribute modification, such as how new objects inherit security attributes from creating subjects, or ancillary rules that control security attribute modification. For example, one cannot use FMT_MSA to specify a rule that a Mandatory Access Control SFPs policy must be satisfied in order to set security attributes controlled under a Discretionary Access Control policy.

One might think that such rules could be specified under FDP_ACF or FDP_ICF. However, those families allow specification of rules related to access of objects, not how

security attributes obtain values. Providing a place to specify such rules appears to be an omission in the CC."

FDP_NIAP-0420-ATR.1.1. As part of the [assignment: *access control SFP, information flow control SFP*], the TSF shall enforce the following policy rules with respect to security attribute establishment: [selection: *[assignment: list of rules governing security attribute inheritance], "none"*].

FDP_NIAP-0420-ATR.1.2. As part of the [assignment: *access control SFP, information flow control SFP*], the TSF shall enforce the following policy rules with respect to security attribute modification: [selection: *[assignment: list of rules governing security attribute modification], "none"*].

Hierarchical To: No Components

Dependencies: [FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control]

8.2.3.3. Inter-TSF user data monitoring (FDP_SDI_EX.1)

The G-Server provides the capability to perform integrity monitoring for user data that is stored outside of the TSC, through an inter-TSF trusted channel. This is similar to functionality provided by other integrity scanning tools available on the market. FDP_SDI cannot support this functionality claim because of two reasons: it deals solely with user data stored within the TSC, and it doesn't support manual operation or activation of this capability.

The instantiated SFR is derived from the following extended SFR:

FDP_SDI_EX.1.1 The TSF shall provide a capability to monitor user data stored within a remote trusted IT product [selection: *during initial start-up, periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which self test should occur]*].

FDP_SDI_EX.1.2 The TSF shall monitor [assignment: *list of objects or information types*] for [assignment: *integrity errors*], based on the following attributes: [assignment: *user data attributes*].

Hierarchical to: No other components.

Dependencies: No dependencies.

8.2.3.4. State transition control for security attributes (FPT_SSP_EX.1)

In distributed systems, it is often necessary to maintain multiple versions of object security attributes that correspond to user data objects whose updates are being propagated through the system.

FPT_SSP.1 and FPT_SSP.2 deal with state synchrony between separate parts of the TOE. They are not intended to provide synchronization with Remote Trusted IT Products. Furthermore, they model a simplistic requirement where each part of the TOE has only one concurrent version of the TSF data, and that state is being synchronized between the parts. This is insufficient to provide common functionality such as key versioning.

Although FPT_TDC.1 provides a capability for consistent interpretation of TSF data when shared between the TSF and another trusted IT product, the component was deemed inappropriate for this purpose because the TSF data in question is not synchronized between the TOE and the remote IT product; rather the TOE computes the TSF data from user data received from the remote IT product.

The instantiated SFR is derived from the following extended SFR:

FPT_SSP_EX.1.1 The TSF shall support association of multiple versions up to [assignment: *number of versions*] of object security attributes for [assignment: *list of objects or information types*].

FPT_SSP_EX.1.2 The TSF shall ensure that the protocol used provides for the unambiguous association between the security attributes and user data.

FPT_SSP_EX.1.3 The TSF shall [selection: *periodically during normal operation, at the request of the authorised user, at the conditions [assignment: conditions under which version invalidation should occur]*] invalidate previous versions of the security attributes within [assignment: *rules for determining invalidated versions*].

Hierarchical to: No other components.

Dependencies: No dependencies.

8.2.4. Dependency Rationale

Table 8.6 depicts the satisfaction of all security requirement dependencies. For each security requirement included in the ST, the CC dependencies are identified in the column "CC dependency", and the satisfied dependencies are identified in the "ST dependency" column. Iterated components are identified to help determine exactly which specific iteration is dependent on which SFR or SAR. Requirements that do not have defined dependencies are not listed in the table.

For explicitly stated requirements, the CC dependencies identified for similar requirements were used as guidance to identify their dependencies.

Dependencies that are satisfied by a hierarchically higher component are given in **boldface**. Dependencies that are satisfied by alternative components are in **underlined boldface** and are explained in the "Dependency description" column.

Table 8.6- Security Requirements Dependency Mapping

SFR	CC dependency	ST dependency	Dependency description
FAU_ARP.1	FAU_SAA.1	FAU_SAA.1, FAU_SAA.3	Automatic response to EntryControl and ExitControl potential violation indication
FAU_GEN.1-NIAP-0347	FPT_STM.1	FPT_STM.1	Audit depends on secure time
FAU_SAA.1	FAU_GEN.1	**FAU_GEN.1-NIAP-0347**	Equivalent to FAU_GEN.1
FAU_SAR.1	FAU_GEN.1	**FAU_GEN.1-NIAP-0347**	Equivalent to FAU_GEN.1
FAU_SAR.3 (1)	FAU_SAR.1	FAU_SAR.1	Selectable audit review (4 iterations) dependency on audit review security functionality
FAU_SAR.3 (2)			
FAU_SAR.3 (3)			
FAU_SAR.3 (4)			
FAU_STG.2	FAU_GEN.1	**FAU_GEN.1-NIAP-0347**	Equivalent to FAU_GEN.1
FCS_CKM.1	[FCS_CKM.2 or FCS_COP.1], FCS_CKM.4, FMT_MSA.2	FCS_COP.1 (1), FMT_MSA.2	Key destruction is not an issue because keys are used for authentication, and are irrelevant after user record is removed from the G-Server database.

SFR	CC dependency	ST dependency	Dependency description
FCS_COP.1(1)	[FDP_ITC.1 or FCS_CKM.1], FCS_CKM.4, FMT_MSA.2	FDP_CKM.1, FMT_MSA.2	See FCS_CKM.4 exclusion rationale as for FCS_CKM.1.
FCS_COP.1(2)		FDP_ITC.1(3), FMT_MSA.2	
FCS_COP.1(3)		None	Hashing function is not based on a cryptographic key
FDP_ACC.1	FDP_ACF.1	**FDP_NIAP-0420-ATR.1**	FDP_NIAP-0420-ATR.1 describes a requirement for access control to security attributes, rather than user data as in FDP_ACF
FDP_NIAP-0420-ATR.1	FDP_ACC.1 or FDP_IFC.1	FDP_ACC.1	Security attribute management and inheritance SFR
FDP_DAU.2	FIA_UID.1	**FIA_UID.2**	FIA_UID.2 is hierarchical to FIA_UID.1 so it can be used to satisfy the dependency
FDP_ETC.1	FDP_ACC.1 or FDP_IFC.1	FDP_IFC.1 (1), FDP_IFC.1 (2)	Export of user data including dynamic and static resources
FDP_IFC.1 (1)	FDP_IFF.1	FDP_IFF.1 (1)	Dynamic Resource SFP
FDP_IFC.1 (2)	FDP_IFF.1	FDP_IFF.1 (2)	Static Resource SFP
FDP_IFC.1 (3)	FDP_IFF.1	FDP_IFF.1 (3)	SSL Key Import SFP
FDP_IFF.1 (1)	FDP_IFC.1, FMT_MSA.3	FDP_IFC.1 (1), FMT_MSA.3	Dynamic Resource SFP
FDP_IFF.1 (2)	FDP_IFC.1, FMT_MSA.3	FDP_IFC.1 (2), FMT_MSA.3	Static Resource SFP
FDP_IFF.1 (3)	FDP_IFC.1, FMT_MSA.3	FDP_IFC.1 (3), FMT_MSA.3	SSL Key Import SFP
FDP_ITC.1 (1)	[FDP_ACC.1 or FDP_IFC.1], FMT_MSA.3	FDP_IFC.1 (1), FMT_MSA.3	Import of user data without security attributes under the Dynamic Resource SFP
FDP_ITC.1 (2)	[FDP_ACC.1 or FDP_IFC.1], FMT_MSA.3	FDP_IFC.1 (2), FMT_MSA.3	Import of user data without security attributes under the Static Resource SFP
FDP_ITC.1 (3)	[FDP_ACC.1 or FDP_IFC.1], FMT_MSA.3	FDP_IFC.1 (3), FMT_MSA.3	Import of cryptographic keys under the SSL Key Import SFP
FIA_UAU.2	FIA_UID.1	**FIA_UID.2**	FIA_UID.2 is hierarchical to

SFR	CC dependency	ST dependency	Dependency description
			FIA_UID.1 so it can be used to satisfy the dependency
FIA_UAU.7	FIA_UAU.1	**FIA_UAU.2**	FIA_UAU.2 is hierarchical to FIA_UAU.1 so it can be used to satisfy the dependency for obscuring feedback provided during user authentication
FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1	
FMT_MSA.1 (1)	[FDP_ACC.1 or FDP_IFC.1], FMT_SMF.1, FMT_SMR.1	FDP_IFC.1 (1), FDP_IFC.1 (2), FMT_SMF.1, FMT_SMR.1	Management of site attributes in the context of both the Dynamic Resource SFP and the Static Resource SFP
FMT_MSA.1 (2)	[FDP_ACC.1 or FDP_IFC.1], FMT_SMF.1, FMT_SMR.1	FDP_ACC.1 FMT_SMF.1, FMT_SMR.1	Management of user attributes
FMT_MSA.2	ADV_SPM.1, [FDP_ACC.1 or FDP_IFC.1], FMT_MSA.1, FMT_SMR.1	FDP_IFC.1 (3), FMT_MSA.1, FMT_SMR.1	The dependency on ADV_SPM.1 is not justifiable for EAL1. The ST describes the relevant security policy model as “secure crypto-graphic keys”.
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1, FMT_SMR.1	Initial attributes
FMT_MTD.1	FMT_SMF.1, FMT_SMR.1	FMT_SMF.1, FMT_SMR.1	Management of TSF data
FMT_REV.1 (1)	FMT_SMR.1	FMT_SMR.1	
FMT_REV.1 (2)	FMT_SMR.1	FMT_SMR.1	
FMT_SMR.1	FIA_UID.1	**FIA_UID.2**	FIA_UID.2 is hierarchical to FIA_UID.1 so it can be used to satisfy the dependency
ADO_IGS.1	AGD_ADM.1	AGD_ADM.1	
ADV_FSP.1	ADV_RCR.1	ADV_RCR.1	
AGD_ADM.1	ADV_FSP.1	ADV_FSP.1	
AGD_USR.1	ADV_FSP.1	ADV_FSP.1	
ATE_IND.1	ADV_FSP.1,	ADV_FSP.1,	

SFR	CC dependency	ST dependency	Dependency description
	AGD_ADM.1, AGD_USR.1	AGD_ADM.1, AGD_USR.1	

8.2.5. Internal Consistency and Mutual Support

This section demonstrates that the stated security requirements together form a mutually supportive and internally consistent whole.

Mutual support is shown through consideration of the interactions between and among the SFRs. This also builds on the dependency analysis addressed by the previous section, because if functional requirement A has a dependency on functional requirement B, B supports A by definition.

The security requirements work mutually so that each primary SFR is protected against bypassing, tampering, and deactivation by other SFRs.

The primary SFRs are the requirements that address the primary objectives, namely O.Integrity, O.Application_Protection, and O.Resource_Recovery. The SFRs directly addressing these objectives are described above in the Security Functional Requirements Rationale.

8.2.5.1. Prevention of Bypass of SFRs

FPT_RVM.1 ensures that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed, thereby preventing bypass of the information flow control SFRs.

FIA_UID.2 and FIA_UAU.2 ensure that administrators are identified and authenticated before they can perform any TSF-mediated action. FIA_UAU.7 and FTA_SSL.3 support the O.I&A objective by countering shoulder surfing, and access to an administrator's workstation.

FTP_TRP.1 ensures that administrators' sessions are protected against hijacking and other network based attacks. FTA_TSE.1 further supports this objective by restricting the source addresses from which administrators can access the TOE.

FTP_ITC.1 (1) and FTP_ITC.1 (2) prevent bypass of the TSF through modification of the user session data or by spoofing attacks.

FPT_SSP_EX.1 ensures that resource integrity protection cannot be bypassed during resource content updates.

8.2.5.2. Prevention of Tampering with SFRs

FPT_SEP.1 requires that the TSF maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects. Separation is enforced between the security domains of subjects in the TSC.

FPT_STM.1 provides reliable time stamps for the TSF.

FAU_STG.2 prevents modifications and unauthorized deletion of the audit records.

FRU_RSA.1 caps the number of concurrent user sessions, countering tampering attacks that involve overwhelming the TSF with a large number of access requests.

8.2.5.3. Prevention of De-activation of SFRs

The security management SFRs, including FMT_MOF.1, FMT_MSA.1 (1) and FMT_MSA.1 (2), FMT_MTD.1, as well as FMT_REV.1 (1) and FMT_REV.1 (2) all restrict the modification of TSF data and functions to authorised personnel.

FDP_ACC.1 and FDP_NIAP-0420-ATR.1 restrict the management of resource signatures to authorised administrators, preventing other subjects from deactivating resource integrity protection by overwriting resource signatures stored in the G-Server database.

8.2.5.4. Detection of attacks on other SFRs

The components belonging to the FAU class ensure that audit records are generated and that appropriate audit management and review capabilities are provided to support an authorised administrator of the TOE in detecting attacks against other SFRs.

FDP_SDI_EX.1 supports FDP_DAU.2 by providing a capability for an authorised administrator to proactively verify resource integrity on protected sites.

8.2.5.5. Cryptographic support

FCS_CKM.1 provides key generation support for administrator keys.

FDP_ITC.1(3), FDP_IFC.1(3), and FDP_IFF.1(3) support the management and trusted path/channel security functions by supporting import of protected site SSL keys and certificates.

FCS_COP.1(1), FCS_COP.1(2), and FCS_COP.1(3) provide cryptographic support for the integrity, trusted path and channel, and management security functions.

8.3. TOE Summary Specification Rationale

This section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security functional requirements (SFRs). The collection of security functions work together to provide all of the security requirements as indicated in Table 8.7, and detailed in Table 8.8. It is also evident from an inspection of the tables that the security functions described in the TSS are all necessary to address the required security functionality of the TSF.

The assurance measures that correspond to the security assurance requirements (SARs) are demonstrated in Section 6, and in particular in Table 6.6.

Table 8.7- TOE Summary Specification Rationale Mapping

	TSF Prot.	ExitControl	EntryControl	Mgmt	Audit	Alerts	Channels
FAU_ARP.1			✓			✓	
FAU_GEN.1-NIAP-0347					✓		
FAU_SAA.1					✓		
FAU_SAA.3			✓				
FAU_SAR.1					✓		
FAU_SAR.3(1)					✓		
FAU_SAR.3(2)					✓		
FAU_SAR.3(3)					✓		
FAU_SAR.3(4)					✓		
FAU_STG.2					✓		
FCS_CKM.1				✓			
FCS_COP.1(1)				✓			✓
FCS_COP.1(2)							✓
FCS_COP.1(3)				✓			
FDP_ACC.1				✓			
FDP_NIAP-0420-ATR.1				✓			
FDP_DAU.2		✓		✓			
FDP_ETC.1		✓					
FDP_IFC.1(1)		✓					
FDP_IFC.1(2)		✓					
FDP_IFC.1(3)				✓			

	TSF Prot.	ExitControl	EntryControl	Mgmt	Audit	Alerts	Channels
FDP_IFF.1(1)		✓					
FDP_IFF.1(2)		✓					
FDP_IFF.1(3)				✓			
FDP_ITC.1(1)		✓					
FDP_ITC.1(2)		✓					
FDP_ITC.1(3)				✓			
FDP_SDI_EX.1				✓			
FIA_UAU.2							✓
FIA_UAU.7							✓
FIA_UID.2							✓
FMT_MOF.1				✓			
FMT_MSA.1(1)				✓			
FMT_MSA.1(2)				✓			
FMT_MSA.2				✓			
FMT_MSA.3				✓			
FMT_MTD.1				✓			
FMT_REV.1(1)				✓			
FMT_REV.1(2)				✓			
FMT_SMF.1				✓			
FMT_SMR.1				✓			
FPT_RVM.1	✓						
FPT_SEP.1	✓						
FPT_SSP_EX.1				✓			
FPT_STM.1	✓						
FRU_RSA.1							✓
FTA_SSL.3							✓
FTA_TSE.1							✓
FTP_ITC.1(1)	✓						✓
FTP_ITC.1(2)							✓
FTP_TRP.1	✓						✓

Table 8.8- Mapping of Security Functions to SFRs

Security Function	Subsection	SFRs
TSF Protection Function	Operating System	FPT_RVM.1, FPT_SEP.1, FPT_STM.1
	Transparency Envelope	FPT_RVM.1, FPT_SEP.1, FTP_ITC.1(1), FTP_TRP.1
ExitControl	Processing for Static	FDP_DAU.2, FDP_IFC.1(2), FDP_IFF.1(2), FDP_ITC.1(2)
	Processing for Dynamic	FDP_DAU.2, FDP_IFC.1(1), FDP_IFF.1(1), FDP_ITC.1(1)
	Request/Response Stripping	FDP_ETC.1, FDP_ITC.1(1), FDP_ITC.1(2)
	Resource Recovery	FDP_IFF.1(2)
EntryControl	Limits and Constraints	FAU_ARP.1, FAU_SAA.3
	Attack Signature Detection	FAU_ARP.1, FAU_SAA.3
Security Management Function	Roles	FMT_SMR.1
	G-Server Administration	FCS_CKM.1, FDP_IFC.1(3), FDP_IFF.1(3), FDP_ITC.1(3), FMT_MOF.1, FMT_MSA.1(1), FMT_MSA.1(2), FMT_MSA.3, FMT_MTD.1, FMT_REV.1(2), FMT_SMF.1
	Resource Signatures Administration	FCS_COP.1(1), FCS_COP.1(3), FDP_ACC.1, FDP_NIAP-0420-ATR.1, FDP_DAU.2, FMT_REV.1(1)
	Resource Integrity Verification	FDP_SDI_EX.1
	Pending Signatures	FDP_DAU.2, FPT_SSP_EX.1
Audit	System Log	FAU_GEN.1-NIAP-0347, FAU_SAR.1, FAU_SAR.3(1), FAU_STG.2
	Verification Log	FAU_GEN.1-NIAP-0347, FAU_SAR.1, FAU_SAR.3(2), FAU_STG.2
	Signing Log	FAU_GEN.1-NIAP-0347, FAU_SAR.1, FAU_SAR.3(3), FAU_STG.2
	Alerts Log	FAU_GEN.1-NIAP-0347, FAU_SAA.1, FAU_SAR.1, FAU_SAR.3(4), FAU_STG.2

Security Function	Subsection	SFRs
Alerts	Alert Generation	FAU_ARP.1
Channels	Trusted Path	FCS_COP.1(1), FCS_COP.1(2), FIA_UAU.2, FIA_UAU.7, FIA_UID.2, FTP_TRP.1
	HTTPS Termination	FCS_COP.1(2), FTP_ITC.1(1)
	HTTPS	FCS_COP.1(2), FTP_ITC.1(2)
	TOE Access	FRU_RSA.1, FTA_SSL.3, FTA_TSE.1