SECURITY TARGET
FOR
ALACRIS® OCSP Server Professional Version 3.0.0 (EAL 2)

Prepared for:
Communications Security Establishment

Prepared by:
CGI Information Systems and Management Consultants Inc.

15 January 2004

Valid: 15 January 2004
CGI File number: CGI-ITSETF-ST-160603-03
CB File number: 383-4-22
Version: 1.6 Draft
Page Count: 44

Document Change Log

ST Section	Change	Reason for Change	Date Changed
Initial Draft Version 0.1 – 2003-06-06			
All	Applied standard formatting and performed QA.	Document format and structure was not consistent.	2003-07-07
Draft Version 1.0 – 2003-07-07			
All	Add in new features of TOE (configuration file access and verification)	Additional features of latest release of TOE.	2003-07-15
Draft Version 1.1 – 2003-07-15			
All	Revised to reflect comments of internal QA.	Internal QA	2003-09-29
Draft Version 1.2 – 2003-09-29			
4.1.4.1, 5, 7.4.1	Added security function for Freshness Proof.	Security functionality was previously omitted.	2003-10-28
5.1.16	F.Security_Management.Configure_OCSP_Server_Roles was incorrectly referred to as F.Security_Management.Configure_OCSP_Server_Permissions.	Fixed typo.	2003-10-28
Draft Version 1.3 – 2003-10-28			
All	Removed MetaData protection from evaluation scope.	Reflect discussions with Alacris® representatives.	2003-11-17
All	Fixed minor editorial errors.	Correct editorial errors.	2003-11-17
Draft Version 1.4 – 2003-11-17			
All	Addressed issues from evaluator observation reports.	Address observation reports.	2003-11-21
Draft Version 1.5 – 2003-11-21			
All	Addressed issues from CB observation report.	Address observation report issues.	2004-01-15
Draft Version 1.6 – 2004-01-15			

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION

1.1 Security Target Identification

Title: Security Target for Alacris® OCSP Server Professional Version 3.0.0.
Assurance Level: EAL2
Version: 1.6 Draft
Status: Draft
Release Date: January 15, 2004
Prepared By: CGI Information Systems and Management Consultants Inc.
Prepared For: Communications Security Establishment
CGI File Number: CGI-ITSETF-ST-160603-03
Page Count: 44
CB File Number: 383-4-22

1.2 Security Target Overview

The Alacris® OCSP Server (AOS), using the OCSP protocol defined in RFC2560, provides X.509 certificate status information to clients in a Public Key Infrastructure (PKI). The AOS accepts OCSP requests from the Alacris® OCSP Client, or any OCSP client implementation compliant with RFC2560, and returns the revocation status associated with the requested certificate in an OCSP response message conformant to RFC2560.

The AOS is made up of several components, including one or more responders. OCSP responders can be configured to use Certificate Revocation Lists to determine certificate status, or they can be configured to determine certificate status through relaying client requests to other third party responders using the OCSP protocol.

1.3 Definitions and Acronyms

1.3.1 Definitions

TERM	DESCRIPTION
Microsoft® CryptoAPI	FIPS-140-1 Certified certificate and keystore provided on Windows® platforms. Permits secure creation of private keypairs and certificate signing requests, secure storage of private keys, storage of X.509 certificates and public keys, provides the random seed and the crypto algorithms required for the creation of keys. Provides the secure interface through for applications that wish to use its functionality.
Microsoft® CAPI	Refers to Microsoft® CryptoAPI.
OCSP	Protocol that describes the structure of information within a communication package that enables the revocation status of an X.509 certificate to be checked without reference to a CRL.
MMC snap-in	A GUI framework plugin supported by the Windows®

TERM	DESCRIPTION
	platform. It provides easy access to configurable parameters of an application registered within its namespace. Has a Windows® look and feel and provides tab sheets for each set of configurable functions.
Secure Hyper Text Transfer Protocol	Protocol that transfers HTTP over SSL.
OCSP Responder	Service that on request checks the revocation status of a certificate and returns the result via OCSP protocol.
OCSP Requestor	Client that makes a request for revocation status checking of a certificate to a known OCSP service.
RFC 2560	The RFC that defines what is contained in the OCSP protocol and the constraints and requirements of this protocol.

Table 1 - Definitions

1.3.2 Acronyms

TERM	DEFINITION
API	Application Programming Interface
CC	Common Criteria
CRL	Certificate Revocation List
FIPS	Federal Information Standard (NIST)
HTTP	Hyper Text Transfer Protocol
HTTPS	Secure Hyper Text Transfer Protocol
IT	Information Technology
MS	Microsoft®
MMC	Microsoft® Management Console
DCOM	Distributed Component Object Model
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
SE	Security Environment
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SO	Security Objectives
SSL	Secure Sockets Layer
ST	Security Target
TOE	Target of Evaluation
TSS	TOE Summary Specifications

Table 2 - Acronyms

1.4 Common Criteria Conformance

This Security Target has been developed using Part 1, 2 and 3 of the Common Criteria for Information Technology Security Evaluation, Version 2.1, annotated with

interpretations as of 2002-10-25. The Target of Evaluation (TOE) has been developed to conform to the Evaluation Assurance Level 2 (EAL2) assurance level.

The TOE is conformant with:

- Common Criteria Version 2.1 Part 2 – extended.
- Common Criteria Version 2.1 Part 3 – EAL 2.

1.5 Related Standards and Documents

[ISO 15408] Information Technology - Security Techniques - Evaluation Criteria for IT Security (Hereafter referred to as Common Criteria or CC) Version 2.1 (ISO/IEC 15408 Evaluation Criteria for Information Technology Security; Part 1: Introduction and general model, Part 2: Security functional requirements, and Part 3: Security assurance requirements).

[CEM] Common Methodology for Information Security Evaluation, CEM-99/045, Part 2: Evaluation Methodology, Version 1.0, August 1999.

[RFC2560] Myers, M., Ankney, R., Malpani, A. and Galperin, S, "Internet X.509 Public Key Infrastructure Online Certificate Status Protocol", RFC 2560, June 1999.
Reference: http://www.faqs.org/rfcs/rfc2560.html

[RFC2459] Housley, R., Ford, W., Polk, W. and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", RFC 2459, January 1999.
Reference: http://www.ietf.org/rfc/rfc2459.txt?number=2459

[FIPS 140-1] National Institute of Standards and Technology, *Security Requirements for Cryptographic Modules*, January 4, 1994.
Reference: http://csrc.nist.gov/cryptval/140-1.htm

1.6 Related Protection Profiles

This ST is neither related to, nor claims conformance to any protection profile.

1.7 Security Target Organization

SECTION		CONTENTS DESCRIPTION
1	Introduction	Gives the definition of the ST that is being evaluated; identifies CC conformance claimed; identifies standards; gives an overview of the product.
2	TOE Description	Defines the TOE that is being evaluated; identifies the components that comprise the TOE (i.e. TOE Boundary), identifies all external interfaces to the TOE, and identifies the TOE security environment in which the TOE is intended to operate and the manner in which it is expected to be employed.
3	TOE Security Environment	Identifies: • Assumptions about the existing safeguards provided by the IT security environment that lie outside the TOE boundary; • Known threats to the secure operation of the TOE related to known vulnerabilities that can be exploited; • Required organizational security policies that the TOE must comply with; and • Security Objectives for the TOE. They are meant to counter identified threats to the TOE and provide conformance to organizational security policies. An objective counters a threat and/or is met by an assumption about the IT security environment. Security objectives for the TOE and the IT environment security are identified separately.
4	IT Security Requirements	Identifies and describes: • TOE security functional requirements (SFR) from CC; and • Required TOE security assurance requirements (SAR) from CC for EAL2.
5	TOE Summary Specifications	Provides: • A description of the TOE security functions (TSF) that meet the SFRs; and • The TOE assurance measures that meet the SARs.
6	Protection Profile Claims	There are no PP claims.
7	Rationale	Provides justification and evidence through correlation, that the ST is a complete and cohesive set of requirements. Consists of three main parts: • Security objectives rationale; • Security requirements rationale; and • TOE summary specification rationale

Table 3 – ST Structure

2 TOE DESCRIPTION

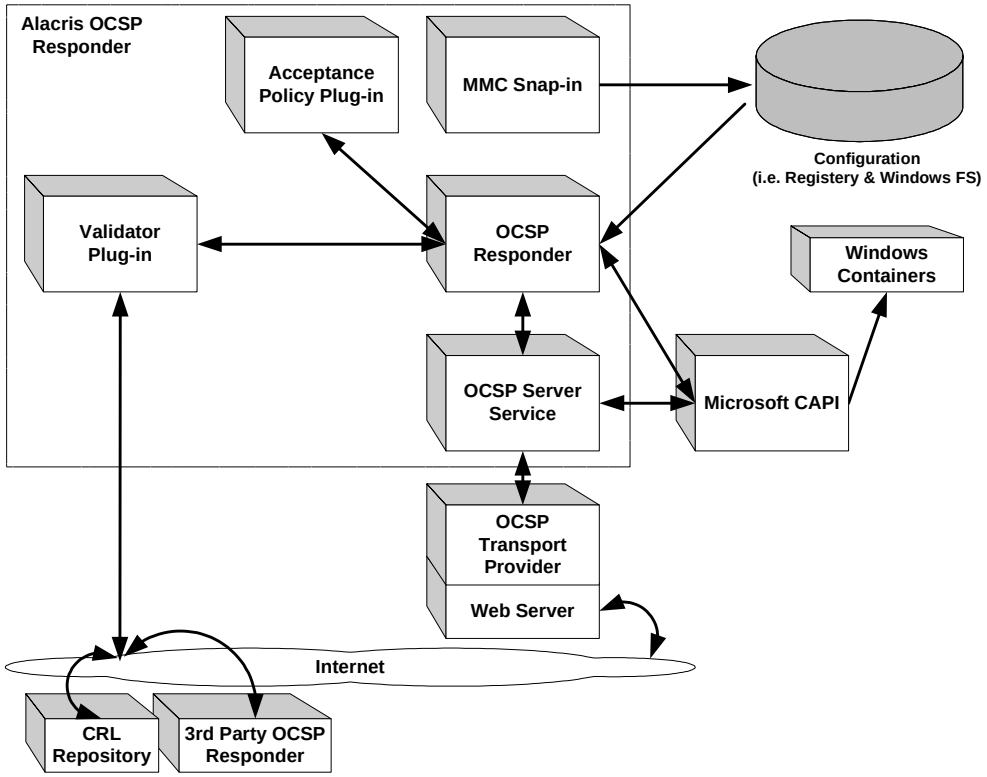

Figure 1 - TOE Components

The Target of Evaluation (TOE) is the Alacris® OCSP Server Version 3.0.0, referred to in this ST as the AOS.

The Alacris® OCSP Server (AOS), using the OCSP protocol defined in RFC2560, provides X.509 certificate status information to clients in a Public Key Infrastructure (PKI). The AOS accepts OCSP requests from the Alacris® OCSP Client, or any OCSP client implementation compliant with RFC2560, and returns the revocation status associated with the requested certificate in an OCSP response message conformant to RFC2560.

As indicated in the above diagram, the AOS consists of the following components:

- Configuration Information;
- MMC (Microsoft® Management Console) Snap-in;
- OCSP Server Service;
- Responder(s);
- Acceptance Policy-Plug-in;
- Validator Plug-in; and
- Transport Provider.

The following sections describe the AOS components in more detail and identify the TOE boundary.

2.1 Configuration Information

The AOS configuration information consists of the following:

- OCSP Service configuration;
- OCSP Server configuration; and
- OCSP Responder configuration.

The OCSP Service configuration is stored in the Windows® registry. The OCSP Server configuration and OCSP Responder configuration are stored in a Windows® file.

2.2 Management Console

The management console is implemented via an Alacris® provided Microsoft® Management Console (MMC) snap-in. Using the MMC snap-in, an administrator can access the OCSP Service, OCSP Server and OCSP Responder configuration.

2.3 OCSP Server Service

The OCSP Server service is the system that manages the configuration store, OCSP Responder registration, logging and auditing.

2.4 Responder(s)

OCSP Responders process OCSP requests from clients and produce OCSP responses on behalf of a particular Certificate Authority (CA). The AOS system can be configured to have one or more active responders.

2.5 Acceptance Policy Plug-in

The Acceptance Policy Plug-In is used by the Responder to determine whether a given OCSP request should be accepted or rejected. When a new request arrives, the Responder notifies the Acceptance Policy Plug-in that a new request has arrived. The plug-in processes the request and then returns to the Responder whether the request should be accepted.

The AOS is shipped with a Default Acceptance Policy Plug-In that allows requests to be accepted or rejected using common acceptance criteria such as client identity, digital signature validation, certificate extensions and number of certificate statuses requested. Additionally, the AOS exposes a programming interface that can be utilized to create custom Acceptance Policy Plug-ins.

2.6 Validator Plug-In

The Validator Plug-In is used by the Responder to obtain the revocation status of the requested certificate. Three types of Validator Plug-Ins are shipped with the AOS:

- CRL Pull Mode;

- CRL Push Mode; and
- OCSP Relying Participant.

The CRL Pull Mode and CRL Push Mode Validator Plug-Ins allow for the revocation information to be determined using remote or local CRL's. The OCSP Relying Participant Validator Plug-In allows the revocation status to be obtained through forwarding the OCSP request to a third party OCSP responder.

2.7 Transport Provider

The Transport Provider runs on a web server platform and is the interface point that allows OCSP requestors to connect to the OCSP server over a public network such as the Internet. The Transport Provider receives OCSP requests and forwards them to the OCSP Server service using an exposed DCOM (Distributed Component Object Model) interface. The Transport Provider receives the OCSP response from the OCSP Server service and returns it to the requesting client.

The AOS ships with Transport Providers for several platforms; however, custom Transport Providers can be built using a DCOM programming interface exposed by the OCSP Server Service.

2.8 TOE Boundary

As shown in the above diagram, the TOE boundary consists of the OCSP Server Service, OCSP Responder(s), Validator Plug-In, Acceptance Policy Plug-In and the administrative interface provided via the Alacris® MMC snap-in. In this document, these components together will be referred to as the TOE.

Outside of the TOE boundary is the Windows® operating system platform that provides the IT security environment for the TOE. This IT environment includes the Distributed Component Object Model (DCOM) framework and libraries, FIPS-140-1 certified MS CAPI key and certificate container and MS CAPI libraries.

The Transport Provider (including the web server platform it is hosted on) is not included in the TOE boundary. Also excluded from the TOE boundary are OCSP requestors, third party responders and remote repositories containing Certificate Revocation Lists (CRL's).

It should be explicitly noted that the AOS does not directly implement cryptography. Where cryptographic operations are performed within the TOE, they are accomplished by making calls to the appropriate functions within the MS CAPI libraries.

2.9 TOE Evaluated Configuration

An evaluated configuration of the AOS will use one of the Windows® Operating System platforms listed below:

- MS Windows® 2000 SP3; and
- MS Windows® 2003.

Although the AOS does provide the ability to create custom Validator and Acceptance Policy plug-ins, custom plug-ins are not included in an evaluated configuration. An evaluated configuration includes use of the following Alacris® provided plug-ins:

- Alacris® CRL Pull Mode Validator Plug-In;
- Alacris® Relying Participant Validator Plug-In; and
- Default Acceptance Policy Plug-In.

Additionally, the AOS has several configurable options. In an evaluated configuration, the following options must be configured:

- Kerberos or SChannel must be used for Server Authentication;
- Nonces must be verified in an OCSP response from a third party responder;
- OCSP requests sent by the TOE to a third party responder must be signed by the TOE;
- SSL/TLS must be used for communications between the TOE and third party responders;
- OCSP requests must be signed by the requesting client; and
- All logging and auditing must be enabled.

In addition to TOE configuration options, other environmental measures must exist in secure deployments of the TOE. The TOE must be deployed in an environment in which it is sufficiently protected against direct logical and physical attacks against both the TOE and the OS platform on which it resides. Subsequent sections of this document provide additional information on the security measures assumed to exit in the deployed environment.

2.10 Supported Standards

Supported standards:

- X.509 Certificates v.3 and CRLs v.2;
- HTTP/HTTPS; and
- OCSP v.1 (RFC2560).

3 TOE SECURITY ENVIRONMENT

The TOE security environment describes the security aspects of the environment in which the TOE is intended to be operated and the manner in which it is expected to be employed. This section will identify and list the assumptions made on the operational environment (including physical and procedural measures), the threats the product is designed to counter, and the organizational security policies with which the product is designed to comply.

3.1 Assumptions

The following security safeguards are assumed to exist in the operational environment:

[A.PHYS_SEC] - The host workstation for the TOE is assumed to be located within controlled access facilities that will prevent unauthorized physical access;

[A.LOGICAL_SEC] – The host workstation for the TOE is assumed to be protected from unauthorized logical access using appropriate logical access controls;

[A.NO_EVIL] –Administrators and operators are not careless or willfully negligent and will abide by the instructions provided in the administrative guidance supplied with the TOE; and

[A.MAINTENANCE] - The computer system, software and associated devices function correctly and are maintained at regular intervals. Maintenance will include the application of standard security hardening techniques for the operating system platform, application of security patches and archiving of audit logs so as not to exceed storage limitations.

3.2 Threats

3.2.1 IT Assets

The IT assets requiring protection are:

- TOE executable and Dynamic Link Library (DLL) components;
- TOE configuration data
- Audit and Log Data;
- OCSP requests and responses;
- MS CAPI key store; and
- All other platform operating system components used by the TOE.

3.2.2 Threat Agents

The Threat Agents can be classified as either:

- Threat Agents attempting to directly compromise the TOE or the OS platform on which the TOE and TSF data reside; and

- Threat Agents attempting to compromise the integrity of OCSP messages in transit from TOE to OCSP requestors or third party responders.

Threat agents attempting to directly compromise the TOE or the OS platform are assumed to originate from a well managed user community in a non-hostile working environment, and hence the TOE and IT environment protects against threats of inadvertent or casual attempts to breech the system security. The TOE is not intended to be applicable to circumstances in which protection is required against determined attempts by hostile and well-funded attackers.

Threat agents attempting to compromise the integrity of OCSP messages in transit may arise from public networks such as the Internet and therefore cannot be assumed to be part of a well-managed user community. For these types of threat agents, the TOE protects against threat agents with a moderate level of expertise and resources.

3.2.3 Motivation

For both types of threat agents discussed above, the motivation is to alter a PKI user's knowledge of the true revocation status of a public key certificate. Several reasons for wanting to alter a client's knowledge of the revocation status of a certificate exist and are application dependant; however, one general example is allowing a trusted transaction to complete with a revoked party.

3.2.4 Threats

[T.TRAFFIC_SNIFFING] – An attacker may sniff communications between the TOE and other entities that do not occur on private networks, gaining intelligence to be used as the basis for further attack. This issue is examined in further detail in subsequent threat descriptions;

[T.TOE_RESPONSE_REPLAY] - An attacker may replay a previously valid OCSP response, obtained through traffic sniffing, transmitted from the TOE to a requestor. This threat may allow the attacker to deceive a requestor into accepting the previous certificate status as currently valid;

[T.THIRD_PARTY_RESPONDER_RESPONSE_REPLAY] - An attacker may replay a previously valid OCSP response, obtained through traffic sniffing, sent from a third party responder to the TOE. This threat may allow the attacker to deceive the TOE into accepting the previous certificate status as currently valid;

[T.UNAUTHORIZED_CLIENT_REQUEST] – An attacker may spoof the identity of an authorized user and request certificate status from the TOE. This threat is particularly relevant in pay-per-use environments where an attacker could fraudulently affect billing to the legitimate user;

[T.UNAUTHORIZED_TOE_REQUEST] – An attacker may spoof the identity of the TOE and request certificate status from a third party responder. This threat is particularly

relevant in pay-per-use environments where an attacker could fraudulently affect billing to the TOE operator;

[T.UNAUTHORIZED_TOE_RESPONSE] - An attacker may reply to an OCSP request from a requestor, purporting to be the TOE, resulting in the requestor relying on an un-trusted source for revocation information;

[T.UNAUTHORIZED_THIRD_PARTY_RESPONDER_RESPONSE] – An attacker may reply to an OCSP request from the TOE, purporting to be a trusted third party responder, resulting in the TOE relying on an un-trusted source for revocation information;

[T.TOE_RESPONSE_INTEGRITY] – An attacker may affect the validity of certificate status information received by a requestor through modification of OCSP response data while in transit between the TOE and requestor.

[T.THIRD_PARTY_RESPONSE_INTEGRITY] – An attacker may affect the validity of certificate status information received by the TOE through modification of OCSP response data while in transit between a third party responder and the TOE.

[T.CRL_INTEGRITY] – An attacker may affect the validity of certificate status information received by the TOE through unauthorized CRL modification or creation.

3.3 Organizational Security Policies

The TOE must comply with the following organizational security policies:

[P.AUTHORIZED_ADMIN] - Only authorized administrators will administer the TOE and IT environment; and

[P.AUDIT] – The TOE must produce sufficient audit and logging information for diagnostic purposes and monitoring of security relevant events.

3.4 Security Objectives

3.4.1 Security Objectives for the TOE

The following are the security objectives for the TOE:

[O.TRANSMISSION_CONFIDENTIALITY] – The TOE must be capable of encrypting communications that do not occur on private networks;

[O.CLIENT_REQUEST_VALIDITY] – The TOE must be able to authenticate a requestor as being an authorized client of TOE services and verify that the request has not been altered in transit;

[O.TOE_REQUEST_VALIDITY] – When sending an OCSP request message to a trusted third party responder, the TOE must be able to authenticate itself to the responder and provide proof to the responder that the request message has not been altered in transit;

[O.TOE_RESPONSE_VALIDITY] - The TOE must be able to authenticate itself to a requestor as a trusted responder and provide proof to the requestor that the OCSP response has not been altered in transmission;

[O.THIRD_PARTY_RESPONSE_VALIDITY] – The TOE must be able to authenticate an OCSP response as coming from a trusted third party responder and not having been altered in transmission;

[O.TOE_RESPONSE_REPLAY_PREVENTION] - The TOE must be able to provide proof to a requestor that a previous OCSP response message from the TOE has not been replayed in response to a current request;

[O.THIRD_PARTY_RESPONSE_REPLAY_DETECTION] - The TOE must be able to prevent and detect replay of previous OCSP responses sent from a third party trusted responder to the TOE;

[O.CRL_INTEGRITY] – The TOE must be capable of verifying CRL's used to make decisions about certificate status as having been authorized by a trusted CA and not having been tampered with.

[O.AUDIT] – The TOE will provide the means of recording security relevant events so as to assist an administrator in the detection of potential attacks, or misconfiguration of the TOE security features, that would leave the TOE in an insecure state;

3.4.2 Security Objectives for the non-IT Environment

The following are the security objectives for the non-IT environment:

[OE.PHYS_SEC] – The host workstation for the TOE is located in a physically secure processing environment such that only authorized users have physical access;

[OE.PRIVATE_NETWORK] – Communication between components of the TOE not encrypted by secure protocols requires that the components be adequately isolated from public networks using appropriate environmental physical and logical security controls;

[OE.NO_EVIL] – Administrators and operators of the TOE will not be careless or willfully negligent and will abide by the instructions provided in the administrative guidance supplied with the TOE; and

[OE.MAINTENANCE] – Computer systems, software and associated devices function correctly and are maintained at regular intervals. Maintenance will include the application of standard security hardening techniques for the operating system platform,

application of security patches and archiving of audit logs so as not to exceed storage limitations.

3.4.3 Security Objectives for the IT Environment

The following are the security objectives for the IT environment, which will counter the threats noted in section *3.2.4 Threats*:

[OE.CRYPTO_SERVICES] – The IT environment will provide cryptographic services to the TOE;

[OE.ACCESS_CONTROL] – The IT environment will prevent users from gaining access to and performing operations on its resources until they have been properly identified and authenticated as authorized users;

[OE.AUTHORIZED_ADMIN] - The IT environment will ensure that only authorized administrators will be permitted to manage the security functionality of the TOE; and

[OE.TIMESTAMP] - The IT environment must provide reliable time stamps for use by the TOE audit functions.

4 IT SECURITY REQUIREMENTS

This section defines functional and assurance requirements for both the TOE and the IT environment.

The following conventions have been used to indicate operations that have been performed on the CC Part 2 functional components:

- Assignment and selection are indicated by [square brackets]; and
- Refinement is denoted using *italicized* text.

4.1 TOE Security Requirements

4.1.1 TOE Extended Security Functional Requirements

4.1.1.1 FPT_ AUTH.1 Inter-TSF Data Authentication

FPT_ AUTH.1.1 - The TSF shall provide a capability to authenticate the source of all TSF data that is received by the TSF from a remote trusted IT product.

FPT_AUTH.1.2 - The TSF shall provide a capability to provide evidence of the authenticity of all TSF data that is sent from the TSF to a remote trusted IT product.

4.1.1.2 FPT_RPLP.1 Replay Prevention

FPT_RPLP.1.1 - The TSF shall provide the evidence necessary for a remote trusted IT product to detect replay for the following entities when they are transmitted from the TOE to the remote trusted IT product: [assignment: list of entities].

4.1.1.3 FAU_ADG.1 Audit Data Generation

FAU_ADG 1.1 - The TSF shall be able to generate an audit record of the following auditable events: [assignment: list of auditable events].

FAU_ADG.1.2 - The TSF shall record within each audit record at least the following information: date and time of the event, type of event, and the outcome (success or failure) of the event.

Dependency: FPT_STM.1 Reliable Timestamps.

4.1.2 TOE Security Functional Requirements

Application Note: In this ST, OCSP messages are considered TSF data versus user data. This is consistent with the definitions contained in CC Part 2 (annotated with interpretations) dated 2002-10-25, par. 35, which states that user data is data stored in TOE resources upon which the TOE places no special meaning. Since OCSP messages do have special meaning to the TSF, in that they influence TSF outputs with respect to certificate status, they are considered TSF data.

4.1.3 FAU_GEN.1 Audit Data Generation

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

a) Startup and shutdown of the audit functions; and
b) All auditable events for the [not specified] level of audit:
    i.) [new CRL pushed;
    ii.) certificate configuration errors;
    iii.) responder/service initialization failures;
    iv.) internal errors;
    v.) freshness proof statuses; and
    vi.) configuration changes.]

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

a) Date and time of the event, type of event, subject identity, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [assignment: no other information].

Dependency: FPT_STM.1 Reliable Timestamps.

4.1.4 FAU_ADG.1 Audit Data Generation

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

a) [Method/component used to service status request;
b) Certificate status returned to client for particular serial number;
c) Requestor identity for OCSP request;
d) Request forwarding/routing information;
e) OCSP errors related to processing of extensions;
f) OCSP errors related to nonce processing;
g) OCSP errors related to freshness proof processing;

h) Errors relating to digital signature verification on OCSP response; and
i) Errors relating to validating the responder certificate].

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

a) Date and time of the event, type of event, and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definition of the functional components included in the PP/ST, [assignment: No other information].

Dependency: FPT_STM.1 Reliable Timestamps.

4.1.4.1 FMT_SMF.1 Specification of Management Functions

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

a) [Configure OCSP server authentication method;
b) Configure OCSP server permissions for the following:
   i. Start/Stop a responder;
   ii. Request certificate status;
   iii. Push CRL;
   iv. Modify server permissions;
   v. Modify ownership of object containing permissions;
c) Configure local compromised authorities list;
d) Configure certificates for digital signature operations;
e) Configure unknown status behavior;
f) Enable CRL push mode;
g) Enable CRL pull mode;
h) Configure CRL pull mode options:
   i. Specify CRL Distribution Point;
   ii. Specify polling interval;
i) Configure Relying Participant Validator options:
   i. Configure OCSP responder location;
   ii. Configure OCSP responder validity options as per RFC 2560;
   iii. Configure OCSP response validity options as per RFC2560;
j) Configure SSL/TLS parameters;
k) Configure audit logging parameters;
l) Configure restrictions on valid OCSP requestors;
m) Configure options for obtaining freshness proof;
   i. Configure freshness proof polling interval;
   ii. Enable responder location for obtaining freshness proof.]

4.1.4.2 FPT_RPL.1 Replay Detection

FPT_RPL.1.1 - The TSF shall detect replay for the following entities: [OCSP response messages from third party responders].

FPT_RPL.1.2 - The TSF shall [audit the replay detection event] when replay is detected.

4.1.4.3 FPT_RPLP.1 Replay Prevention

FPT_RPLP.1.1 - The TSF shall provide the evidence necessary for a remote trusted IT product to detect replay for the following entities when they are transmitted from the TOE to the remote trusted IT product: [OCSP response messages].

4.1.4.4 FPT_ITI.1 Inter-TSF Detection of Modification

FPT_ITI.1.1 - The TSF shall provide the capability to detect modification of all TSF data during transmission between the TSF and a remote trusted IT product within the following metric: [assignment: modifications detected by a standard cryptographic hash function (MD5, SHA1, SHA2, etc.]

Application Note: Although the TOE performs an integrity verification function, the hashing algorithm used in the verification is not directly implemented in the TOE. The TOE makes use of the environmental cryptographic libraries to perform this function.

FPT_ITI.1.2 - The TSF shall provide the capability to verify the integrity of all TSF data transmitted between the TSF and a remote trusted IT product and perform [assignment: logging of the event] if modifications are detected.

Application Note: The preceding two SFR's encapsulate the requirements for confidentiality and integrity of OCSP messages as well as detection of replay of valid OCSP messages. The requirement for authentication of the OCSP responder and OCSP client is encapsulated via the extended SFR specified in the following section.

4.1.4.5 FPT_ AUTH.1 Inter-TSF Data Authentication

FPT_ AUTH.1.1 - The TSF shall provide a capability to authenticate the source of all TSF data that is received by the TSF from a remote trusted IT product.

FPT_AUTH.1.2 - The TSF shall provide a capability to provide evidence of the authenticity of all TSF data that is sent from the TSF to a remote trusted IT product.

4.1.4.6 FPT_ITC.1 Inter-TSF Confidentiality During Transmission

FPT_ITC.1.1 - The TOE shall protect all TSF data transmitted from the TSF to a remote trusted IT product from unauthorized disclosure during transmission.

4.1.4.7 FMT_SMR.1 Security Roles

FMT_SMR.1.1 - The TOE shall maintain the roles [users that can control responder, users that can request status, users that can push CRL, users that can modify roles].

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

Application Note: Although the TOE associates users with roles, it relies on the OS to identify and authenticate users. The TOE roles are based on operating system identities.

Dependency: FIA_UID.1

4.1.5 IT Environment Security Functional Requirements

Application Note: The TOE requires that the underlying Windows® operating system provide sufficient logical protection for the TSF and TSF data through access control to the workstation hosting the TOE, as well as restricting access to the MMC configuration tool to authenticated administrators (as defined by the operating system policies in effect). Additionally, the IT environment must ensure that this access control and security roles are not bypassed. The SFR's stated below are aimed at providing this protection for the TSF and TSF data through the IT environment.

4.1.5.1 FIA_UID.2 Timing of Identification

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

4.1.5.2 FIA_UAU.2 Timing of Authentication

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

Dependency: FIA_UID.1

4.1.5.3 FMT_SMR.1 Security Roles

FMT_SMR.1.1 - The *IT environment* shall maintain the roles [user and system administrator].

FMT_SMR.1.2 – The *IT environment* shall be able to associate users with roles.

Dependency: FIA_UID.1

4.1.5.4 FMT_MOF.1 Management of Security Functions Behaviour

FMT_MOF.1.1 - The *IT environment* shall restrict the ability to [modify the behavior of] the functions [all TSF security management functions] to [system administrators].

Dependencies: FMT_SMF.1, FMT_SMR.1

4.1.5.5 FMT_MTD.1 Management of TSF Data

FMT_MTD.1.1 - The *IT environment* shall restrict the ability to [view or modify] the [all TSF data used for configuration of the TSF] to [system administrators].

Dependencies: FMT_SMF.1, FMT_SMR.1

4.1.5.6 FPT_STM.1 Reliable Time Stamps

FPT_STM.1.1 - The *IT environment* shall be able to provide reliable time stamps for its own use.

4.1.5.7 FCS_COP.1 Cryptographic Operation

FCS_COP.1.1 - The *IT environment* shall perform [SSL v3, digital signature generation and verification] in accordance with the [algorithms listed in table 4] and cryptographic key sizes [cryptographic key sizes listed in table 4] that meet the following: [list of standards listed in table 4].

Dependencies: FCS_CKM.1, FMT_MSA.2 and FCS_CKM.4

Algorithm	Key Size (bits)	Standards
RSA Key Generation	512, 1024, 2048	X9.31
RSA Encryption/Digital Signature Verification	512, 1024, 2048	FIPS 186-2, X9.31
DSA Key Generation	512, 1024, 2048	X9.30
DSA Digital Signature Verification	512, 1024, 2048	FIPS 186-2, X9.30
SHA-1 Hash Function	Not Applicable	FIPS 180-1
MD5 Hash Function	Not Applicable	RFC1321

Algorithm	Key Size (bits)	Standards
SSL v3	128	INTERNET-DRAFT SSL 3.0, November 18, 1996

Table 4 - Cryptographic Operations

4.1.6 Security Assurance Requirements for the TOE

The assurance requirements for the TOE taken from Part 3 of the CC is EAL 2 level of assurance as described in Part 3 of the CC. The assurance components are summarized in the following table.

ASSURANCE CLASS	ASSURANCE COMPONENTS	ASSURANCE COMPONENT
Class ACM: Configuration Management	ACM_CAP.2	Configuration items
Class ADO: Delivery and Operation	ADO_DEL.1	Delivery procedures
	ADO_IGS.1	Installation, generation and startup procedures
Class ADV: Development	ADV_FSP.1	Informal functional specification
	ADV_HLD.1	Descriptive high-level design
	ADV_RCR.1	Informal correspondence demonstration
Class AGD: Guidance Documents	AGD_ADM.1	Administrator guidance
	AGD_USR.1	User guidance
Class ATE: Tests	ATE_FUN.1	Functional testing
	ATE_COV.1	Evidence of coverage
	ATE_IND.2	Independent testing - sample
Class AVA: Vulnerability Assessment	AVA_SOF.1	Strength of TOE security function evaluation
	AVA_VLA.1	Developer vulnerability analysis

Table 5 - Security Assurance Requirements

5 TOE SUMMARY SPECIFICATION

A listing of the TOE security functions and their summary specifications are provided below.

5.1 TOE Security Functions

This section describes the security functions implemented by the TOE to meet the security requirements for the Alacris® OCSP Responder (stated within section 4 of this ST). A mapping of the security functions identified and their related security requirements can be found within Table 7 in section 7.3.2 of this ST.

5.1.1 F.Security_Management.Configure_Server_Authentication

This security function is used to allow an administrator to specify the OS authentication service that should be used to authenticate clients attempting to access the OCSP server.

The supported authentication service options are:

1. NTLMSSP**;**
2. Kerberos; and
3. SChannel.

5.1.2 F.Security_Management.Configure_OCSP_Server_Roles

This security function allows an administrator to configure the permissions that users should have on the OCSP server. Permissions are implemented using roles based on existing Windows® users and groups. The following roles are assignable to users and groups:

1. **Control Responder** – User can start/stop a responder;
2. **Request Status** –Remote user can make an OCSP request. In an evaluated configuration, only the Transport Provider user should be granted this permission;
3. **Push CRL** – User can push a CRL to the responder;
4. **Modify Permissions** – User can modify roles;
5. **Modify Ownership** – User can modify ownership of the security object storing the permissions.

These parameters are used by the *F.OCSP_Server_Roles* function.

5.1.3 F.Security_Management.Configure_Compromised_Authorities_List

This security function allows an administrator to specify certificate authorities for which issued certificates should always have a revoked status returned. The certificate authority is placed on the Compromised Authorities List using the thumbprint of the issuer certificate. The information that should be returned in addition to the revoked status can also be specified.

5.1.4 F.Security_Management.Configure_Session_Certificate

The TOE will allow an administrator to configure the certificate that is to be used for SSL/TLS sessions. The certificate configured by this function is used by the *F.Secure_Session* security function.

5.1.5 F.Security_Management.Configure_OCSP_Signing_Certificate

This security function allows an administrator to specify the digital certificate that will be used to sign OCSP responses.

5.1.6 F.Security_Management.Configure_Unknown_Status

This security function allows an administrator to specify that unknown statuses will not be returned to requestors. This function allows configuration of the error message and return code that should be returned to requestors instead of the unknown status.

5.1.7 F.Security_Management.Configure_CRL_Options

An administrator can configure the TOE to obtain revocation information using CRL's.

Two modes are possible:

1. **Pull Mode** – The distribution point can be configured as well as the polling interval. The following options are configurable using Pull Mode:
    a. CRL Distribution Point (ldap, http, file);
    b. Polling Interval; and
2. **Push Mode** – The local container is searched for the CRL. The searching is instantaneously triggered by an event when the container holding the CRL is updated.

5.1.8 F.Security_Management.Configure_Relying_Participant_Validator

This security function allows the TOE to be configured to relay OCSP requests to another responder, validate the response from that responder, re-sign the response and send it back to the original requestor.

Several options are configurable:

1. URL of OCSP Responder to which requests should be relayed;
2. Require TOE to sign relayed requests and digital certificate to be used to sign the request;
3. Specification of Trusted Responders. Trusted Responders are specified by adding the thumbprint (SHA1 hash) of the responder certificate to the Trusted Responders List maintained by the TOE;
4. Revocation Checking. There are 3 options for revocation checking of an OCSP Responder that does not have a certificate containing the id-pkix-ocsp-nocheck extension:
    a. Verify revocation;
    b. Accept response; and
    c. Reject response.
5. Response Validity Options. The following options are available:
    a. Require nonce verification; and
    b. "thisUpdate" and "nextUpdate" values from the OCSP response must be within the required parameters set by an administrator. These parameters are meant to compensate for unsynchronized time sources between the tow responders.

5.1.9 F.Security_Management.Configure_Default_Acceptance_Policy_Plugin

This security function allows an administrator to configure acceptance criteria for OCSP requests. The configurable options are discussed below:

1. Reject requests for status of more than one certificate;

The following options require that an administrator enable the option to only accept signed OCSP Requests:

1. Certificate chain inclusion requirements:
    a. Require that signed requests include signer's entire certificate path;
    b. Require that signed requests include certificate path excluding root CA certificate;
    c. Require that signed requests include only signer's end certificate;
    d. No restrictions on signer's certificate path applied;
2. Maximum number of certificates in requestor's certificate chain;
3. Revocation checking of requestor's certificate;
    a. No revocation checking;
    b. Revocation checking only on end certificate;
    c. Revocation checking on all certificates in chain;
    d. Revocation checking on every certificate in chain except the root CA certificate;
4. Restrictions on signer's certificate;
    a. Accept OCSP request only if certificate is present on certificate thumbprint list;
    b. Accept OCSP request only if certificate extensions present in list are present in signer's certificate and/or the indicated certificate in the certificate chain;

5.1.10 F.Security_Management.Configure_Detailed_Server_Log_Auditing

This security function allows an administrator to configure whether detailed transaction logs should be generated.

5.1.11 F.Security_Management.Configure_Binary_Dump_Logging

This security function allows an administrator to configure the security functions responsible for binary dump logging.

The following options are configurable:

1. Save incoming requests;
2. Save outgoing responses; and
3. Save responses for routed requests.

5.1.12 F.Security_Management.Configure_Freshness_Proof

This security function allows an administrator to enable freshness proof as well as configure options related to how the freshness proof is obtained.

The following options are configurable:

1. Enable/Disable Freshness Proof;
2. Enable the Issuer Certificates Mapping for obtaining responder location
3. Enable AIA for obtaining responder location; and
4. Enable Default OCSP Responder URL for obtaining responder location.

Note that the order of precedence regarding which option to use for determining the responder location is as specified in the above list.

5.1.13 F.OCSP_Server_Roles

The TOE provides access control to the OCSP server through the use of the authentication and authorization.

The TOE will authenticate clients of the OCSP server using the OS authentication service configured in *F.Security_Management.Configure_OCSP_Server_Authentication*. Once authenticated, the TOE will verify the user as authorized to perform the action as determined by the permissions set by the *F.Security_Management.Configure_OCSP_Server_Roles* security function.

5.1.14 F.Secure_Session

The TOE will use the certificate configured by the *F.Security_Management.Configure_Session_Certificate* security function to establish an SSL/TLS session with third party responders. Note that it is the IT environment that provides the underlying SSL/TLS protocol, the TOE only makes function calls into the associated environmental libraries and allows configuration of the necessary protocol parameters.

5.1.15 F.Process_CRL

This security function allows the TOE to process CRL's according to the parameters set using the *F.Security_Management.Configure_CRL_Options*. If Pull Mode is enabled, this function will retrieve the CRL to be processed using the specified location and at the specified time intervals. If Push Mode is enabled, the *F.Process_CRL* function is called through an event from the IT environment indicating that a CRL has been updated in the local container.

In both cases, digital signature verification of the CRL occurs to verify the authenticity and integrity of the CRL as coming from a trusted CA and not having been altered in transit.

5.1.16 F.Process_OCSP_Request

When an OCSP request is received, the following actions take place:

1. The request is validated for RFC2560 conformance;
2. The Compromised Authorities List is checked. If the issuing CA of the certificate being queried is found, then a "revoked" status is returned by the *F.Create_OCSP_Response* security function;
3. Attempt to locate an appropriate responder is made. If an appropriate responder cannot be located, an "unknown" status is returned by the *F.Create_OCSP_Response* security function;
4. The OCSP request is processed using the rules configured in *F.Security_Management.Configure_Default_Acceptance_Policy_Plugin* to determine whether the request is valid. If the request is not valid, an error is returned to the client by the *F.Create_OCSP_Response* security function;
5. If the responder that is configured is a local one, then the appropriate local CRL information is consulted to determine revocation status. Revocation status returned in *F.Create_OCSP_Response* is "Good" or "Revoked".
6. If the responder that is configured is a remote one, then the TOE creates an OCSP request and sends it to a remote responder and processes the response using the *F.Relying_Participant_Validator* security function. The certificate status derived by *F.Relying_Participant_Validator* is returned in a digitally signed OCSP message by the *F.Create_OCSP_Response* security function.

5.1.17 F.Relying_Participant_Validator

If the responder is configured for Relying Participant Validator, this security function allows the TOE to relay an OCSP request, in accordance with the rules defined in RFC2560, to a third party responder and verify the response. Third party responders are located using the parameters specified by *F.Security_Management.Configure_Relying_Participant_Validator*. Options to include in the request and the digital certificate to use for signing the request are also determined by the parameters set by *F.Security_Management.Configure_Relying_Participant_Validator*.

When the response from the third party responder is received, the TOE verifies the digital signature, nonces and other options in accordance with the settings of *F.Security_Management.Configure_Relying_Participant_Validator*.

5.1.18 F.Create_OCSP_Response

This security function will use the certificate status determined by the *F.Process_OCSP_Request* function and create and sign an RFC2560 conformant OCSP response using the certificate configured by the *F.Security_Management.Configure_OCSP_Signing_Certificate* security function. If the client requestor included nonces in their original request, the nonces are inserted into the OCSP response to enable replay detection by the requestor.

5.1.19 F.Windows_Event_Log_Auditing

The TOE writes audits to the native Windows® Event Log supported on all Windows® systems.

The following audit events are always generated:

1. Alacris® OCSP service started;
2. Alacris® OCSP service stopped;
3. Unsuccessful server access attempts;
4. Bad service requests;
5. Responder startup failure; and
6. Configuration changes.

5.1.20 F.OCSP_Binary_Dump_Logging

The TOE can be configured to write binary dumps of all communications between the TOE and OCSP clients, as well as between the TOE and other responders, to a specified OS directory. If enabled, the raw ASN.1 encoded OCSP transactions are written to the logs.

This security function uses the parameters set by the *F.Security_Management.Configure_OCSP_Binary_Dump_Logging* to determine which OCSP transactions to log.

5.1.21 F.OCSP_Detailed_Server_Log_Auditing

The Alacris® OCSP Server can be configured to write detailed transaction logs of all OCSP processing that occurs on the responder. This logging must be enabled via the F.Security_Management.Configure_Detailed_Server_Log_Auditing security function.

The following types of events are generated:

1. Local responder to be used to service a request;
2. Returned status for certificate serial number;
3. Forwarding information for requests;
4. Identification of requestors;
5. No local responder available;
6. Forwarding failed;
7. Compromised authority;
8. Signing errors;
9. Validator plug-in errors;
10. Policy plug-in errors;
11. Exceptions; and
12. Internal errors.

5.1.22 F.Freshness_Proof

Obtain freshness proof as configured using the parameters defined by F.Security_Management.Configure_Freshness_Proof.

6 PROTECTION PROFILE CLAIMS

6.1 PP Reference

There are no relevant Protection Profiles for a TOE whose objective is to perform OCSP requests.

7 RATIONALE

7.1 Security Objectives for TOE Rationale

The following table maps Security Objectives for the TOE to aspects of the identified threats to be countered by the TOE as well as aspects of the Organizational Security Policies to be met by the TOE.

	Security Objectives								
Threats and Policies	O.TRANSMISSION_CONFIDENTIALITY	O.CLIENT_REQUEST_VALIDITY	O.TOE_REQUEST_VALIDITY	O.TOE_RESPONSE_VALIDITY	O.THIRD_PARTY_RESPONSE_VALIDITY	O.TOE_RESPONE_REPLAY_PREVENTION	O.THIRD_PARTY_RESPONSE_REPLAY_DETECTION	O.CRL_INTEGRITY	O.AUDIT
T.TRAFFIC_SNIFFING	X								
T.TOE_RESPONSE_REPLAY						X			
T.THIRD_PARTY_RESPONDER_RESPONSE_REPLAY							X		
T.UNAUTHORIZED_CLIENT_REQUEST	X	X							
T.UNAUTHORIZED_TOE_REQUEST	X		X						
T.UNAUTHORIZED_TOE_RESPONSE				X					
T.UNAUTHORIZED_THIRD_PARTY_RESPONDER_RESPONSE					X				
T.TOE_RESPONSE_INTEGRITY				X					
T.THIRD_PARTY_RESPONSE_INTEGRITY					X				
T.CRL_INTEGRITY								X	
P.AUDIT									X

Table 6 – Mapping of Objectives to Threats and Policies

T.TRAFFIC_SNIFFING – This threat is directly countered by the O.TRANSMISSION_CONFIDENTIALITY objective, which states that the TOE must be capable of encrypting communications that do not occur on private networks.

T.TOE_RESPONSE_REPLAY – The O.TOE_RESPONSE_REPLAY_PREVENTION objective directly counters this threat.

T.THIRD_PARTY_RESPONDER_RESPONSE_REPLAY – The O.THIRD_PARTY_RESPONSE_REPLAY_DETECTION objective directly supports mitigation of this threat.

T.UNAUTHORIZED_CLIENT_REQUEST - O.CLIENT_REQUEST_VALIDITY directly supports mitigation of this threat by requiring that the TOE be capable of authenticating a requestor as being an authorized client of TOE services. O.TRANSMISSION_CONFIDENTIALITY works in conjunction with O.CLIENT_REQUEST_VALIDITY to ensure that an attacker cannot capture previously valid OCSP requests and replay them to a responder.

T.UNAUTHORIZED_TOE_REQUEST – O.TOE_REQUEST_VALIDITY directly supports mitigation of this threat by requiring that the TOE be capable of authenticating itself as an authorized client of third party responder services. O.TRANSMISSION_CONFIDENTIALITY works in conjunction with O.TOE_REQUEST_VALIDITY to ensure that an attacker cannot capture previously valid OCSP requests from the TOE and replay them to a third party responder.

T.UNAUTHORIZED_TOE_RESPONSE – O.TOE_RESPONSE_VALIDITY directly supports mitigation of this threat by requiring that the TOE be capable of authenticating itself to an OCSP requestor as a trusted responder and provide proof to the requestor that the OCSP response has not been altered in transit.

T.UNAUTHORIZED_THIRD_PARTY_RESPONDER_RESPONSE – O.THIRD_PARTY_RESPONSE_VALIDITY directly supports mitigation of this threat by requiring that the TOE be capable of authenticating OCSP response messages as coming from a trusted responder third party responder.

T.TOE_RESPONSE_INTEGRITY – O.TOE_RESPONSE_VALIDITY directly supports mitigation of this threat by requiring that the TOE be capable of authenticating itself to an OCSP requestor as a trusted responder and provide proof to the requestor that the OCSP response has not been altered in transit.

T.THIRD_PARTY_RESPONSE_INTEGRITY – O.THIRD_PARTY_RESPONSE_VALIDITY directly supports mitigation of this threat by requiring that the TOE be capable of verifying the integrity of OCSP response messages sent from a third party trusted responder.

T.CRL_INTEGRITY – O.CRL_INTEGRITY directly supports this threat by requiring that the TOE be capable of verifying CRL's as having been authorized by a trusted CA and not having been tampered with.

P.AUDIT – This OSP is directly supported by O.AUDIT. It is also supported by various environmental security objectives as discussed in the following section.

7.2 Security Objectives for IT Environment Rationale

	Security Objectives							
Threats, Policies and Assumptions	OE.PHYS_SEC	OE.CRYPTO_SERVICES	OE.PRIVATE_NETWORK	OE.NO_EVIL	OE.MAINTENANCE	OE.ACCESS_CONTROL	OE.AUTHORIZED_ADMIN	OE.TIMESTAMP
T.UNAUTHORIZED_CLIENT_REQUEST		X						
T.UNAUTHORIZED_TOE_REQUEST		X						
T.UNAUTHORIZED_TOE_RESPONSE		X						
T.UNAUTHORIZED_THIRD_PARTY_RESPONDER_RESPONSE		X						
T.TOE_RESPONSE_INTEGRITY		X						
T.THIRD_PARTY_RESPONSE_INTEGRITY		X						
T.CRL_INTEGRITY		X						
T.TRAFFIC_SNIFFING		X	X					
P.AUDIT								X
P.AUTHORIZED_ADMIN							X	
A.PHYS_SEC	X							
A.MAINTENANCE					X			
A.NO_EVIL				X				
A.LOGICAL_SEC						X		

Table 7 – Mapping of Objectives to Threats, Policies and Assumptions

T.UNAUTHORIZED_CLIENT_REQUEST - OE.CRYPTO_SERVICES contributes to the mitigation of this threat by providing the TOE with the cryptographic services required to authenticate valid clients.

T.UNAUTHORIZED_TOE_REQUEST – OE.CRYPTO_SERVICES contributes to the mitigation of this threat by providing the TOE with the cryptographic services required to prevent unauthorized requests.

T.UNAUTHORIZED_TOE_RESPONSE – OE.CRYPTO_SERVICES contributes to the mitigation of this threat by providing the TOE with the cryptographic services required to prevent unauthorized responses.

T.UNAUTHORIZED_THIRD_PARTY_RESPONDER_RESPONSE – OE.CRYPTO_SERVICES contributes to the mitigation of this threat by providing the TOE with the cryptographic services required to authenticate third party responses as authorized.

T.TOE_RESPONSE_INTEGRITY – OE.CRYPTO_SERVICES contributes to the mitigation of this threat by providing the TOE with the cryptographic services required to prevent undetected response modification.

T.THIRD_PARTY_RESPONSE_INTEGRITY – OE.CRYPTO_SERVICES contributes to the mitigation of this threat by providing the TOE with the cryptographic services required to prevent undetected response modification.

T.CRL_INTEGRITY – OE.CRYPTO_SERVICES contributes to the mitigation of this threat by providing the TOE with the cryptographic services required to authenticate CRL's as having been issued by a trusted CA and not having been tampered with.

T.TRAFFIC_SNIFFING –OE.PRIVATE_NETWORK supports mitigation of traffic sniffing threats by requiring that when communications occur that are not encrypted by secure protocols, the components involved in the communication must be adequately isolated from public networks using appropriate physical and logical security controls. OE.CRYPTO_SERVICES contributes to the mitigation of this threat by providing the TOE with the cryptographic services required to prevent packet sniffing when communications do not occur on private networks.

P.AUTHORIZED_ADMIN – OE.AUTHORIZED_ADMIN directly supports mitigation of this threat by requiring that the IT environment ensure that only authorized administrators be permitted to manage the security functionality of the TOE.

P.AUDIT – OE.TIMESTAMP, in addition to the TOE security objectives discussed in the previous section, supports implementation of this OSP by ensuring that the TOE has a reliable source of time to use when generating audit events.

A.PHYS_SEC – OE.PHYS_SEC directly satisfies this assumption.

A.NO_EVIL - OE.NO_EVIL directly satisfies this assumption.

A.MAINTENANCE – OE.MAINTENANCE directly satisfies this assumption.

A.LOGICAL_SEC – OE.ACCESS_CONTROL directly satisfies this assumption by requiring that the IT environment identify and authenticate users as authorized before granting them access to resources.

7.3 Security Functional Requirements Rationale

Objective	Security Functional Requirement
O.AUDIT	FAU_ADG.1, FAU_GEN.1, FPT_STM.1, FMT_SMF.1
O.CLIENT_REQUEST_VALIDITY	FMT_SMF.1, FPT_ITI.1, FPT_AUTH.1
O.TOE_REQUEST_VALIDITY	FMT_SMF.1, FPT_AUTH.1, FPT_ITI.1
O.TOE_RESPONSE_VALIDITY	FMT_SMF.1, FPT_AUTH.1, FPT_ITI.1
O.THIRD_PARTY_RESPONSE_VALIDITY	FMT_SMF.1, FPT_ITI.1, FPT_AUTH.1
O.TOE_RESPONSE_REPLAY_PREVENTION	FPT_RPLP.1
O.THIRD_PARTY_RESPONSE_REPLAY_DETECTION	FPT_RPL.1
O.CRL_INTEGRITY	FPT_ITI.1, FPT_AUTH.1
O.TRANSMISSION_CONFIDENTIALITY	FPT_ITC.1
OE.ACCESS_CONTROL	FIA_UID.2, FIA_UAU.2
OE.AUTHORIZED_ADMIN	FIA_UID.2, FIA_UAU.2, FMT_SMR.1, FMT_MOF.1, FMT_MTD.1
OE.TIMESTAMP	FPT_STM.1
OE.CRYPTO_SERVICES	FCS_COP.1

Table 8 – Mapping of Objectives to Security Functional Requirements

The table above shows the mapping of security objectives to Security Functional Requirements (SFR). All objectives are satisfied by at least one SFR and all SFR's are required to meet at least one security objective. The rationale for selection of these SFR's to meet the objectives is given below.

O.AUDIT – FAU_ADG.1 and FAU_GEN.1 both require that the TOE generate audit information in support of the O.AUDIT objective. FPT_STM.1 ensures that the audit functions have a trusted time source with which to time stamp the audit events. FMT_SMF.1 allows an administrator to configure specific audit functionality.

O.CLIENT_REQUEST_VALIDITY – FMT_SMF.1 allows an administrator to set acceptance criteria for what constitutes a valid client request. FPT_ITI.1 and FPT_AUTH.1 provide the ability to authenticate a request as coming from an authorized user and not having been altered in transit.

O.TOE_REQUEST_VALIDITY – FPT_AUTH.1 and FPT_ITI.1 provide the ability for the TOE to authenticate OCSP requests sent to a third party responder. FMT_SMF.1 provides a mechanism for configuring digital signing certificate options in support of FPT_AUTH.1 and FPT_ITI.1.

O.TOE_RESPONSE_VALIDITY – FPT_AUTH.1 and FPT_ITI.1 provide the ability for the TOE to authenticate OCSP responses sent to a requestor as coming from an authorized responder and not having been altered in transit. FMT_SMF.1 provides a mechanism for configuring digital signing certificate options in support of FPT_AUTH.1 and FPT_ITI.1.

O.THIRD_PARTY_RESPONSE_VALIDITY – FMT_SMF.1 allows an administrator to set acceptance criteria for what constitutes a valid response from a third party OCSP responder. FPT_ITI.1 and FPT_AUTH.1 provide integrity and authentication for the TSF data transmitted between TOE and third party responder.

O.TOE_RESPONSE_REPLAY_PREVENTION – FPT_RPLP.1 requires the TOE to support replay prevention for messages sent to requestors.

O.THIRD_PARTY_RESPONSE_REPLAY_DETECTION - FPT_RPL.1 supports replay detection for OCSP responses messages.

O.CRL_INTEGRITY – FPT_ITI.1 and FPT_AUTH.1 provide the ability for the TOE to authenticate CRL's as coming from an authorized CA and not having been maliciously altered.

O.TRANSMISSION_CONFIDENTIALITY – FPT_ITC.1 provides for confidentiality of TSF data between the TOE and other entities that do not occur on private networks.

OE.ACCESS_CONTROL – FIA_UID.2 and FIA_UAU.2 combine to require that a user be authenticated before allowing access to the workstation hosting the TOE.

OE.AUTHORIZED_ADMIN – FMT_SMR.1 requires that the IT environment provide role separation between users of the TOE and administrators of the TOE. FIA_UAU.2 and FIA_UID.2 combine to provide the ability for the IT environment to identify and authenticate individuals before the determination is made as to their role. FMT_MOF.1 and FMT_MTD.1 restrict the ability to manage the TSF and TSF data to individuals the IT environment has authenticated as administrators of the TOE.

OE.TIMESTAMP – FPT_STM.1 requires that the IT environment provide a source of reliable timestamps to the TOE to meet this objective.
OE.CRYPTO_SERVICES – FCS_COP.1 provides the required cryptographic services. Note that these cryptographic services are in support of the following TOE SFR's: FPT_AUTH.1, FPT_ITI.1 and FPT_ITC.1.

7.3.1 Explicitly Stated Security Functional Requirements Rationale

This section justifies the use of explicitly stated requirements for the TOE.

7.3.1.1 FPT_ AUTH.1 Inter-TSF Data Authentication

The existing CC Part 2 SFR's for data authentication are concerned with user data, no such SFR's are present for TSF data. OCSP messages are TSF Data as per the application note in the section titled "TOE Security Functional Requirements". Since the OCSP client and responder exchange digitally signed data, it is necessary to add an extended security functional requirement to encapsulate this required functionality.

7.3.1.2 FAU_ADG.1 Audit Data Generation

The TOE contains a detailed logging function in addition to the auditing functions that write events to the Windows® event log. This logging function is implemented in such a way as to provide a method for monitoring security relevant events, such as the receipt of OCSP messages that have been invalidated through modification on the network, digital signature errors, nonce processing errors, etc. It does not include an event for specifying the start-up and shutdown of audit functions, nor does it include the subject identity in each audit record as required by FAU_GEN.1.1.; hence, an extended functional requirement was added to include this functionality in the scope of evaluation.

7.3.1.3 FPT_RPLP.1 Replay Prevention

The TOE provides a mechanism for inserting nonces into the OCSP messages sent to clients. These nonces allow the clients to detect replay of previously valid OCSP messages. However, from the perspective of the TOE, the TOE is enabling the prevention of replay. The current CC Part 2 SFR (FPT_RPL.1) only addresses replay detection, not prevention. Hence, an extended security functional requirement was added to address replay prevention aspects of the TOE.

7.3.2 Rationale for Satisfying All Dependencies

The table below illustrates the Security Functional Requirements and their dependencies. It also indicates whether the ST satisfies each dependency. Where dependencies have not been satisfied, an appropriate rationale is provided following the table.

Security Functional Requirement	Dependencies	Dependency Satisfied? (Y/N)
FAU_GEN.1	FPT_STM.1	Y
FAU_ADG.1	FPT_STM.1	Y
FMT_SMF.1	None	Y
FPT_RPL.1	None	Y
FPT_RPLP.1	None	Y
FPT_ITC.1	None	Y
FPT_ITI.1	None	Y
FPT_AUTH.1	None	Y
FIA_UID.2	None	Y
FIA_UAU.2	FIA_UID.1	Y
FMT_SMR.1	FIA_UID.1	Y
FMT_MOF.1	FMT_SMF.1, FMT_SMR.1	Y
FMT_MTD.1	FMT_SMF.1, FMT_SMR.1	Y
FPT_STM.1	None	Y
FCS_COP.1	FDP_ITC.1 or FCS_CKM.1, FMT_MSA.2, FCS_CKM.4	N

Table 9 – Dependency Rationale

From the above table, the only dependencies not satisfied are for the FCS_COP.1 requirements. A rationale for non-inclusion of the dependencies follows.

The TOE has been designed to rely on the IT environment for cryptographic services. In particular, it makes use of the MS CAPI on Windows® platforms. MS CAPI is designed to support an architecture where different Cryptographic Service Providers (CSP's) can be plugged into the MS CAPI framework in a manner that is seamless to the applications using MS CAPI. Therefore, specification of such implementation details such as key generation (FCS_CKM.1) and key destruction (FCS_CKM.4) is not possible, as the TOE could make use of different CSP's in the context of a deployed system. These parameters must be decided on by local policy at the site of deployment.

For the FCS_COP.1 requirement, the CC identifies the following dependencies:

- FDP_ITC.1; or
- FCS_CKM.1, FCS_CKM.4, and FMT_MSA.2.

The dependencies for this requirement are not applicable and the rationale is as follows:

- FDP_ITC.1: this requirement applies to user data that is imported from outside of the TSF Scope of Control (TSC) and concerned with applying rules to the imported data. There is no user data within the TOE that is imported from outside the TSC and, therefore, this requirement is not applicable;
- FCS_CKM.1 and FCS_CKM.4: these requirements are concerned with key generation (FCS_CKM.1) and key destruction (FCS_CKM.4) and are applicable to cryptographic operations that rely upon the secure management of keys. The TOE has been designed to rely on the IT environment for cryptographic services. In particular, it makes use of the MS CAPI on Windows® platforms. MS CAPI is designed to support an architecture where different Cryptographic Service Providers (CSP's) can be plugged into the MS CAPI framework in a manner that is seamless to the applications using MS CAPI. Therefore, specification of such implementation details such as key generation (FCS_CKM.1) and key destruction (FCS_CKM.4) is not possible, as the TOE could make use of different CSP's in the context of a deployed system. These parameters must be decided by local policy at the site of deployment and an appropriate CSP can be installed.
- FMT_MSA.2: this requirement is concerned with ensuring that only secure values are accepted for security attributes. There are no security attributes entered within the context of the operations specified by FCS_COP.1, therefore, FMT_MSA.2 (including its dependencies) is not applicable.

7.4 Assurance Requirements Rationale

The Alacris® OCSP Server is intended for use in environments where threat agents have a low to moderate level of expertise and resources; therefore, an assurance level of EAL 2, structurally tested, was chosen for this evaluation.

7.4.1 Assurance Measures Satisfy Assurance Requirements

The table below provides a tracing of the assurance measures used to meet each assurance requirement. From this table, it is seen that all assurance requirements trace to at least one assurance measure. The assurance requirements identified in the table are those required to meet the CC assurance level, EAL2. As all assurance requirements are traced to at least one of the assurance measures, the identified assurance measures are sufficient to meet the assurance requirements.

ASSURANCE REQUIREMENTS MET BY ASSURANCE MEASURES		ASSURANCE MEASURES (ALACRIS® DOCUMENTATION)
Configuration Management	ACM_CAP.2	Alacris® provided CM documentation which documents the CM processes followed during development of the TOE and also provides a configuration list for the TOE. The TOE is labeled with a unique version number that appears on the CDROM on which it is provided to the consumer. This version number is also available from within the TOE software.
Delivery and Operation	ADO_DEL.1	Alacris® provided delivery documentation that describes how the TOE is securely delivered to consumers.
	ADO_IGS.1	The TOE is shipped with appropriate installation, generation and startup documentation in electronic format.
Development	ADV_FSP.1	Development documents provided by Alacris® included a functional specification and high level design that documented functionality, subsystems and interfaces. Additionally, a correspondence mapping was provided between the TSF and the development documents.
	ADV_HLD.1	
	ADV_RCR.1	
Guidance Documents	AGD_ADM.1	The TOE is shipped with appropriate user and guidance documentation in electronic format.
	AGD_USR.1	
Tests	ATE_FUN.1	Alacris® provided formal test documentation including test plans, test cases, expected results and actual test results.

ASSURANCE REQUIREMENTS MET BY ASSURANCE MEASURES		ASSURANCE MEASURES (ALACRIS® DOCUMENTATION)
	ATE_COV.1	The test documentation provided a correspondence mapping between the vendor executed tests and the TSF, which allowed the evaluators to determine that appropriate test coverage has been achieved during vendor testing.
	ATE_IND.2	The TOE was formally tested by the CCEF to ensure that the TSF functions as described in the evaluation deliverables. Testing consisted of executing a sample of the vendor tests as well as a series of independent tests created by CCEF evaluators.
Vulnerability Assessment	AVA_SOF.1	No strength of function claim is made for the TOE.
	AVA_VLA.1	Alacris® provided a vulnerability assessment report that demonstrates the TOE's resistance to exploitation of obvious vulnerabilities by attackers with a "low" attack potential.

Table 10 - Mapping of Assurance Measures to EAL2 Requirements

7.5 TOE Summary Specification Rationale

7.5.1 TOE Security Functions Rationale

The table below provides a mapping of Security Functions to Security Functional Requirements. Following the table is a description of how each Security Functional Requirement is addressed by the corresponding Security Function.

	TOE Security Functional Requirements								
Security Functions	FAU_GEN.1	FAU_ADG.1	FMT_SMF.1	FPT_RPL.1	FPT_RPLP.1	FPT_ITI.1	FPT_AUTH.1	FPT_ITC.1	FMT_SMR.1
F.Security_Management.Configure_Server_Authentication			X						
F.Security_Management.Configure_OCSP_Server_Roles			X						
F.Security_Management.Configure_Compromised_Authorities_List			X						
F.Security_Management.Configure_Session_Certificate			X						
F.Security_Management.Configure_OCSP_Signing_Certificate			X						
F.Security_Management.Confgure_Unknown_Status			X						

	TOE Security Functional Requirements								
Security Functions	FAU_GEN.1	FAU_ADG.1	FMT_SMF.1	FPT_RPL.1	FPT_RPLP.1	FPT_ITI.1	FPT_AUTH.1	FPT_ITC.1	FMT_SMR.1
F.Security_Management.Configure_CRL_Options			X						
F.Security_Management.Configure_Relying_Participant_Validator			X						
F.Security_Management.Configure_Default_Acceptance_Policy_Plugin			X						
F.Security_Management.Configure_Detailed_Server_Log_Auditing			X						
F.Security_Management.Configure_Binary_Dump_Logging			X						
F.Security_Management.Configure_Freshness_Proof			X						
F.OCSP_Server_Roles									X
F.Secure_Session								X	
F.Process_OCSP_Request						X	X		
F.Create_OCSP_Response					X	X	X		
F.Windows_Event_Log_Auditing	X								
F.OCSP_Binary_Dump_Logging		X							
F.OCSP_Detailed_Server_Log_Auditing		X							
F.Relying_Participant_Validator				X		X	X		
F.Process_CRL						X	X		
F.Freshness_Proof							X		

Table 11 – Mapping of Security Functions to Security Functional Requirements

FAU_GEN.1 – F.Windows_Event_Log_Auditing satisfies the requirement to generate the specified events.

FAU_ADG.1 – F.OCSP_Binary_Dump_Logging and F.Detailed_Server_Log_Auditing satisfy the requirement to generate the specified events.
F.OCSP_Transaction_Log_Auditing provides a readable log of the events, while F.OCSP_Binary_Dump_Logging provides a log of the raw OCSP data communicated between TOE and responder.

FMT_SMF.1 – The specified security management functions are implemented with the following:

- F.Security_Management.Configure_Server_Authentication;
- F.Security_Management.Configure_OCSP_Server_Roles;
- F.Security_Management.Configure_Compromised_Authorities_List;
- F.Security_Management.Configure_Session_Certificate;
- F.Security_Management.Configure_OCSP_Signing_Certificate;
- F.Security_Management.Configure_Unknown_Status;
- F.Security_Management.Configure_CRL_Options;
- F.Security_Management.Configure_Relying_Participant_Validator;
- F.Security_Management.Configure_Default_Acceptance_Policy_Plugin;

- F.Security_Management.Configure_Detailed_Server_Log_Auditing;
- F.Security_Management.Configure_Binary_Dump_Logging; and
- F.Security_Management.Configure_Freshness_Proof.

FPT_RPL.1 – F.Relying_Participant_Validator allows for the enabling of nonces in OCSP requests sent to third party responders. This allows for the detection of previously valid responses from third party responders.

FPT_RPLP.1 – F.Create_OCSP_Response allows for the insertion of nonces into responses sent to an OCSP requestor. The use of nonces allows the client requestor to detect replay of previously valid responses sent by the TOE.

FPT_ITI.1 – F.Create_OCSP_Response digitally signs all OCSP response messages sent to a requestor, allowing the requestor to verify the integrity of the response message. F.Process_OCSP_Request a for verifying the integrity of requests sent to the TOE through digital signature validation on the request. F.Relying_Participant_Validator allows for the use of a certificate for digital signing of requests sent by the TOE to third party responders. This allows the third party responders to verify the integrity of requests from the TOE. F.Process_OCSP_Request verifies the integrity of responses from third party responders that are used to satisfy client requests through validation of the digital signature. F.Process_CRL verifies that CRL's have been signed by a trusted CA and have not been altered.

FPT_AUTH.1 – F.Create_OCSP_Response digitally signs all OCSP response messages sent to a requestor. F.Freshness_Proof allows the responder to present proof to the requestor that the responder's certificate is not revoked. F.Process_OCSP_Request validates the digital signature on requests received by the TOE. These two functions together meet requirements for data authentication between the requestor and TOE. F.Relying_Participant_Validator allows for the use of digital signatures when forwarding a request to a third party responder. F.Process_OCSP_Request verifies the authenticity of responses from third party responders that are used to satisfy client requests through validation of the digital signature. These latter two functions meet the requirements for data authentication between the requestor and TOE. F.Process_CRL verifies that CRL's have been signed by a trusted CA and have not been altered.

FPT_ITC.1 – F.Secure_Session establishes an SSL/TLS session between the TOE and third party responders, satisfying the confidentiality requirements for transfer of TSF Data (OCSP messages) between TOE and third party responders. All other communication channels are secured using environmental security controls.

FMT_SMR.1 – F.OCSP_Server_Roles implements roles as per the configuration specified by F.Security_Management.Configure_OCSP_Server_Roles.

7.6 PP Claims Rationale

There are no PP compliance issues, as there are no relevant PPs for this TOE.