SECURITY TARGET
FOR
ALACRIS® OCSP Client Professional Version 4.0.0 (EAL 2)

Prepared for:
Communications Security Establishment

Prepared by:
CGI Information Systems and Management Consultants Inc.

9 January 2004

Valid: 9 January 2004
CGI File number: CGI-ITSETF-ST-160603-01
CB File number: 383-4-21
Issue Number: 1.0
Page Count: 39

Document Change Log

ST Section	Change	Reason for Change	Date Changed
Initial Draft Version 0.1 - 2003-06-06			
All	Changed format of ST to make it more readable	TSFs, SFRs and SOs not well defined	2003-06-07
All	Updated document	QA performed	2003-06-07
Draft Version 0.2 - 2003-06-07			
All	Updated document	Match current TOE release	2003-06-13
All	Updated document	QA performed	2003-06-16
Draft Version 0.3 - 2003-06-16			
All	Updated document as per review	Evaluation performed	2003-06-17
Draft Version 0.4 - 2003-06-17			
All	Updated document as per review	Evaluation performed	2003-08-02
Draft Version 0.5 - 2003-08-02			
All	Updated document as per review		2003-08-20
Draft Version 0.6 - 2003-08-20			
All	Updated document as per review	QA performed	2003-9-19
Draft Version 0.7 - 2003-09-19			
5	F.Configure_Responder_Location was incorrectly repeated twice. The incorrect occurence was replaced with F.Security_Management.Configure_Responder_Validity_Options.	F.Configure_Responder_Location was incorrectly repeated twice.	2003-10-20
Draft Version 0.8 - 2003-10-20			
4.1.4.2	FPT_RPL.1.2 was modified to state that an error is returned to the calling application when replay detection is detected.	Corrected to reflect actual TOE implementation.	2003-10-22
Draft Version 0.9 - 2003-10-22			
4.1.2.6	FPT_ITI.1.2 was modified to state that an error is returned to the calling application when modifications are detected.	Corrected to reflect actual TOE implementation.	2003-10-22
Draft Version 0.10 - 2003-10-22			
2.3	Removed non-CAPI applications from evaluated configuration.	Updated to reflect discussions with Alacris.	2003-11-03

ST Section	Change	Reason for Change	Date Changed
All	Modifications following observation reports from evaluator and CSE Certification Board.		2003-11-03
Draft Version 0.11 - 2003-11-12			
3.3, 7.3.1.2	More clearly explained security relevance of auditing functions.	CSE Certification Board OR.	2003-11-30
	Proper use of copyright and trademark symbols.	CSE Certification Board OR.	2003-11-30
Draft Version 0.12 - 2003-11-30			
2.3	Updated supported OS platforms.		2003-12-08
7.4.1	Updated assurance measures.		2003-12-08
Draft Version 0.13 - 2003-12-08			
All	Performed QA	Evaluated Version.	2003-12-12
4.1.2.6	Add application note to clarify FPT_ITI.1.	CSE CB request.	2004-01-09
Version 1.0 - 2004-01-9			

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1 INTRODUCTION

1.1 Security Target Identification

Title: Security Target for Alacris® OCSP Client Professional Version 4.0.0.
Assurance Level: EAL2
Version: 1.0
Status: Evaluated Version
Release Date: January 9, 2004
Prepared By: CGI Information Systems and Management Consultants Inc.
Prepared For: Communications Security Establishment
CGI File Number: CGI-ITSETF-ST-160603-01
Page Count: 39
CB File Number: 383-4-21

1.2 Security Target Overview

The Target of Evaluation (TOE) is the Alacris® OCSP Client Professional Version 4.0.0. The Alacris® OCSP Client (AOC) provides an end user the ability to query the revocation status of an X.509 public key certificate using the On-line Certificate Status Protocol (OCSP) documented in RFC2560. The AOC communicates with the Alacris® OCSP Responder, or any responder compliant with RFC 2560, to query the revocation status of certificates in the context of a Public Key Infrastructure (PKI).

The AOC can be registered upon startup as a revocation provider for Microsoft® (MS) CryptoAPI (CAPI), providing OCSP revocation status checking for all CAPI enabled applications running on the host system. Alternatively, PKI applications can be programmed to interface directly with the Alacris® OCSP service, thereby providing the same OCSP revocation status checking to non-CAPI applications.

Alacris® OCSP Client configuration parameters are stored in the Windows® registry. Configuration parameters are managed through a graphical user interface (GUI) provided by the Microsoft® Management Console (MMC).

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 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® 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
MMC	Microsoft® Management Console
NIST	National Institute of Standards and Technology

TERM	DEFINITION
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, 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

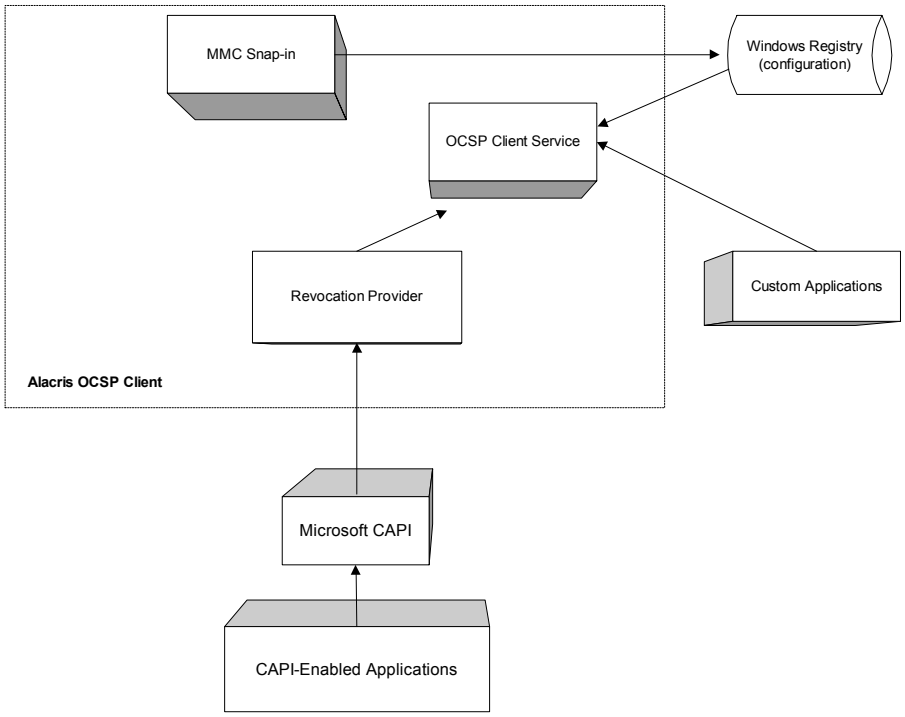

Figure 1 - TOE Components

The Target of Evaluation (TOE) is the Alacris® OCSP Client Professional Version 4.0.0, referred to in this ST as the AOC.

The AOC provides an end user the ability to query the revocation status of an X.509 public key certificate using the On-line Certificate Status Protocol (OCSP) documented in RFC2560. The AOC communicates with the Alacris® OCSP Server, or any responder compliant with RFC 2560, to query the revocation status of certificates in the context of a Public Key Infrastructure (PKI).

As shown in figure 1 above, the TOE boundary for this evaluation consists of the OCSP Client service, CAPI Revocation Provider Interface and the MMC snap-in provided for configuration of TOE parameters.

Outside of the TOE boundary is the Windows® operating system software platform that provides the IT security environment for the TOE. This IT environment includes the Windows® registry (used to store the configuration parameters for the TOE) and the FIPS-140-1 certified MS CAPI key and certificate container and MS CAPI libraries.

It should be explicitly noted that the AOC 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.

2.1 TOE Software Components

The TOE's physical boundary includes:

- The OCSP Client service;
- The MMC snap-in; and
- The Revocation Provider.

2.1.1 OCSP Client service

The OCSP Client service is the component that sends OCSP requests and validates OCSP responses and provides logging functionality.

2.1.2 MMC Snap-in

The Microsoft® Management Console (MMC) snap-in is the component that provides an interface to the Alacris® OCSP client resource parameters stored in the Windows® registry.

2.1.3 Revocation Provider

The Revocation Provider is the component that integrates with Microsoft® CAPI to provide CAPI-enabled applications with on-line revocation checking capabilities.

2.2 Application Context

The security features in the Alacris® OCSP Client are:

- Availability through use of flexible OCSP Responder locations;
- Configurable confidentiality and integrity through SSL enabled HTTP connections -HTTPS;
- Non-repudiation through signing of OCSP Requests with a digital signature;
- Integrity through validated OCSP Responses;
- Accountability, non-repudiation and availability through logging and auditing;
- Integrity through certificate management for IT security environment certificates; and
- Availability through communication flow optimization.

2.2.1 Flexible OCSP Responder Locations

The AOC provides configurable parameters for:

- Specifying the OCSP Responder URL for particular Certificate Authority in the Issuer Certificates Mapping table;
- Populating the OCSP Responder URL with the AIA certificate extension; and
- Specifying a default URL for the OCSP Responder URL.

Since the OCSP Responder is discovered through a URL, proxy responders may be used.

2.2.2 Configurable SSL Connections

If configured to use SSL, the AOC initiates HTTPS with its registered OCSP Responders.

2.2.3 Signed OCSP Requests

The AOC provides non-repudiation through OCSP Requests that are digitally signed with an X.509 certificate. The signing certificate is included in the OCSP Requests. Private digital signing keys used for signature creation are stored in the Microsoft® CAPI or HSM according to organizational security policy.

2.2.4 Validated OCSP Responses

The AOC validates the values of the extensions in the OCSP Response against the rules configured in the AOC. The extensions are defined by RFC2560.

2.2.5 Logging and Auditing

The AOC performs logging to the Windows® Event Log and can also be configured to write detailed transaction information and binary dumps of OCSP requests and responses to operating system files.

2.2.6 Certificate Usage and Management

The AOC registers itself on start-up as a revocation provider for MS CAPI. When the AOC is shut down, the revocation provision for the MS CAPI is automatically un-registered.

2.2.7 Communication Flow Optimization

OCSP Responders can provide freshness proof that their certificate has not been revoked. The AOC can be configured to accept this proof in lieu of an additional revocation check, thereby optimizing communication between client and responder.

2.3 TOE Evaluated Configuration

Only CAPI enabled applications accessing the AOC through the CAPI Revocation Provider are supported in an evaluated configuration. Non-CAPI applications are not supported.

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

- MS Windows® 2000 Professional with Service Pack 3 and High Encryption Pack for Windows® 2000;
- MS Windows® XP, Service Pack 1; or
- MS Windows® 2003 Enterprise Edition.

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

- Nonces must be verified in an OCSP response;
- OCSP requests must be signed by the AOC client;
- All logging and auditing must be enabled; and
- SSL must be enabled between the AOC and the OCSP Responder.

2.4 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 stored in the Windows® registry;
- 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 have originated from within 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

The following threats countered by the TOE are:

[T.PACKET_SNIFFING] – An attacker may sniff the traffic between client and responder, gaining intelligence to be used as the basis for further attack. Subsequent threats address this issue in more detail;

[T.RESPONSE_REPLAY] – An attacker may replay a previously valid OCSP response obtained through traffic sniffing. This threat may allow the attacker to deceive a requestor into thinking the previously obtained certificate status is currently valid;

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

[T.UNAUTHORIZED_RESPONSE] – An attacker may reply to an OCSP request from the TOE, resulting in the TOE relying on an un-trusted source for revocation information; and

[T.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 the TOE and responder.

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;

[P.TRUSTED_RESPONDER] – The TOE must only interact with trusted OCSP responders; 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.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;

[O.REQUEST_VALIDITY] – When sending an OCSP request message to a 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.RESPONSE_VALIDITY] – The TOE must be able to authenticate an OCSP response as coming from a trusted responder and not having been altered in transmission;

[O. REPLAY_DETECTION] – The TOE must prevent and detect replay of old sessions between client and responders; and

[O.TRANSMISSION_CONFIDENTIALITY] – The TOE must be capable of ensuring that communications between the TOE and OCSP Responders are confidential.

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.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 *3.2.2 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 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.

4.1.2.1 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;
b) All auditable events for the [not specified] level of audit; and
c) [
    i.) [certificate status after processing;
    ii.) failure to initialize logging functions;
    iii.) service startup errors;
    iv.) OCSP request; and
    v.) OCSP response].

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.

4.1.2.2 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) [Information about certificate statuses received from a responder;
b) Information about the signer of OCSP responses;
c) Information about extensions included in OCSP responses;
d) Errors determining location of an OCSP responder;
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.

4.1.2.3 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 responder location;
b) Configure OCSP responder validity options as per RFC 2560;
c) Configure OCSP response validity options as per RFC2560;
d) Configure SSL parameters;
e) Configure client certificate to use when signing OCSP requests; and
f) Configure audit log parameters.]

4.1.2.4 FPT_RPL.1 Replay Detection

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

FPT_RPL.1.2 - The TSF shall [audit the replay detection event and return an error to the calling application] when replay is detected.

4.1.2.5 FPT_ITC.1 Inter-TSF Confidentiality During Transmission

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

4.1.2.6 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 hashing operations.

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 and returning an error to the calling application] if modifications are detected.

Application Note: The preceding three 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.

4.1.2.7 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.

4.1.3 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.

4.1.3.1 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.

4.1.3.2 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

4.1.3.3 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

4.1.3.4 FMT_MOF.1 Management of Security Functions Behavior

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

4.1.3.5 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 (i.e. Windows® registry)] to [system administrators].

Dependencies: FMT_SMF.1, FMT_SMR.1

4.1.3.6 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.

4.1.3.7 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

4.1.4 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 client (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_Responder_Location

This security function is used to configure responder locations to which OCSP requests are sent. The configuration is performed via the Alacris® MMC snap-in. The snap-in stores all TOE configuration information in the Windows® registry. Other security functions will subsequently access the configuration information from the Windows® registry.

Several options for determining responder locations are available:

1. Issuer Certificate Mapping. This option involves specifying the OCSP responder URL to be used for a particular Issuer Thumbprint (located in the X.509 certificate being validated). This thumbprint corresponds to the CA that issued the certificate whose validity is in question;
2. Authority Information Access (AIA) certificate extension. This option will use the responder URL that is specified in the AIA extension of the certificate whose validity is in question; and
3. Default URL. This option will use the specified responder URL in the event that the above two options are either not configured or not functional.

Note that the order indicated above implies the priority in which the options are processed (i.e. If the Issuer Certificate Mapping is enabled, it will always be checked before moving onto the AIA certificate extension, etc).

5.1.2 F.Security_Management.Configure_Responder_Validity_Options

This security function is used to configure the client policy for what constitutes a trusted responder. Some of these options determine explicit trust, the others determine the type of processing that is performed to validate a responder as trusted. The configuration is performed via the Alacris® MMC snap-in. The snap-in stores all TOE configuration information in the Windows® registry. Other security functions will subsequently access the configuration information from the Windows® registry.

Descriptions of the various options are below:

1. **Trusted Responders** - Explicitly trust OCSP Responses signed by certificates whose thumbprints reside in the Trusted Responders List;
2. **Revocation Checking of Responders** - When an OCSP responder is not the issuing CA of the certificate whose status is in question, the certificate of the responder can itself be checked for revocation before the responder is trusted. The issuing CA can disable this revocation checking of the responder certificate by including the id-pkix-ocsp-nocheck extension in the certificate. The client policy can determine whether to disregard this extension and verify the certificate, accept the certificate without verification, or reject the response; and
3. **Freshness Proof** - In cases where the responder certificate status must be checked, the responder may submit a proof that their certificate is valid. This proof is signed and time stamped either by the CA that issued the responder certificate, or by another OCSP responder specified in the AIA certificate

extension of the responders certificate. An administrator can configure whether this freshness proof will be accepted, as well as the maximum time for which a freshness proof will be accepted.

5.1.3 F.Security_Management.Configure_OCSP_Response_Validity

This security function is used to configure various OCSP response processing options. The configuration is performed via the Alacris® MMC snap-in. The snap-in stores all TOE configuration information in the Windows® registry. Other security functions will subsequently access the configuration information from the Windows® registry.

Descriptions of the various options are below:

1. Nonce can be configured as mandatory in the transaction; and
2. "thisUpdate" and "nextUpdate" values from the OCSP response must be within the required parameters set by the administrator. These parameters are meant to compensate for unsynchronized time sources on the client and responder machines.

5.1.4 F.Security_Management.Configure_Client_Certificate

This security function allows an administrator to specify that all OCSP requests be signed with a client certificate, allowing the client to identify and authenticate itself to a responder. The configured certificate with private key must be present in the Local Machine or Alacris® OCSP Client Service certificate containers in the Windows® operating system. The configuration is performed via the Alacris® MMC snap-in. The snap-in stores all TOE configuration information in the Windows® registry. Other security functions will subsequently access the configuration information from the Windows® registry.

5.1.5 F.Security_Management.Configure_SSL_Parameters

This security function is used to configure SSL parameters. The configuration is performed via the Alacris® MMC snap-in. The snap-in stores all TOE configuration information in the Windows® registry. Other security functions will subsequently access the configuration information from the Windows® registry.

The following options are configurable:

1. Ignore errors that can be caused by the certificate host name of the server not matching the hostname in the request;
2. Ignore errors that can be caused by an expired server certificate;
3. Ignore errors caused by an unknown Certificate Authority; and
4. Ignore server certificate revocation problems.

5.1.6 F.Security_Management.Configure_Windows_Event_Log_Auditing

This security function allows the Windows® Event Log Auditing functions to be configured. The configuration is performed via the Alacris® MMC snap-in. The snap-in stores all TOE configuration information in the Windows® registry. Other security

functions will subsequently access the configuration information from the Windows® registry.

The audit functions can be configured to generate the following audit events that occur upon completion of OCSP response processing:

1. "Good" revocation status passed to CAPI is audited;
2. "Revoked" revocation status passed to CAPI is audited; and
3. "Unknown" revocation status passed to CAPI is audited.

5.1.7 F.Security_Management.Configure_OCSP_Binary_Dump_Logging

This security function allows for configuration of the functions responsible for OCSP Binary Dump Auditing. The configuration is performed via the Alacris® MMC snap-in. The snap-in stores all TOE configuration information in the Windows® registry. Other security functions will subsequently access the configuration information from the Windows® registry.

The following configuration options are possible within the Binary Dump Logging functions:

1. Operating system directory where the binary dumps should be stored;
2. Whether to log outgoing requests; and
3. Whether to log incoming responses.

Separate files are used for dumps corresponding to requests and those corresponding to responses. Separate files are used for each day. The log filenames are determined in the following fashion:

Request Logs:

<Admin Specified Directory>/Requests/YYYYMMDD/transaction.orq

Response Logs:

<Admin Specified Directory>/Responses/YYYYMMDD/transaction.ors

5.1.8 F.Security_Management.Configure_OCSP_Transaction_Log_Auditing

This security function allows an administrator to configure whether detailed transaction logs should be generated. The configuration is performed via the Alacris® MMC snap-in. The snap-in stores all TOE configuration information in the Windows® registry. Other security functions will subsequently access the configuration information from the Windows® registry.

5.1.9 F.Verify_OCSP_Response

This security function verifies an OCSP response. In some cases, processing of the response is affected by parameters set by other security functions. The sequence of actions performed in OCSP response verification is described below:

1. Verify the responder as trusted using the parameters as set by the *F.Security_Management .Configure_Responder_Validity_Options* security function;
2. If the responder is not on the Trusted Responders List (determined by *F.Security_Management.Configure_Responder_Validity_Options*) then check whether required extensions are present in responder certificate (*specify exact extensions in accordance with RFC2560*);
3. Verify the digital signature on the response. For responders not on the Trusted Responders List, this will require path validation of the certificate to a certificate stored in the Trusted Root Certificate Authorities local client container;
4. Verify the response according to the parameters set by the *F.Security_Management.Configure_OCSP_Response_Validity_Options* security function; and
5. Verify the nonce included in the response as corresponding to the value in the request.

After the above processing has been performed, a certificate status of "good", "unkown" or "revoked" is returned to the calling application.

5.1.10 F.Sign_OCSP_Request

MS CAPI is used to sign the OCSP request using the client certificate configured via the *F.Security_Management.Configure_Client_Certificate* security function.

5.1.11 F.SSL_Session

The TOE will establish an SSL session for communications to a responder. Parameters for setting up the SSL session are configured by an administrator using the *F.Security_Management.Configure_SSL_Parameters* function. Note that it is the IT environment that provides the underlying SSL protocol, the TOE only makes function calls into the associated environmental libraries and allows configuration of the necessary protocol parameters.

5.1.12 F.Windows_Event_Log_Auditing

The Alacris® OCSP Client writes audits to the native Windows® Event Log supported on all Windows® systems.

The following audit events are always generated:

1. Alacris® OCSP Client service started;
2. Alacris® OCSP Client service stopped;
3. Errors related to starting the Alacris® OCSP Client service;
4. Errors related to starting the F.OCSP_Binary_Dump_Logging; and
5. Security problems.

In addition to the above, the following audits can be generated if configured by the administrator using *F.Security_Management.Configure_Windows_Event_Log_Auditing*:

1. "Good" revocation status passed to application;
2. "Revoked" revocation status passed to application; and
3. "Unknown" revocation status passed to application.

5.1.13 F.OCSP_Binary_Dump_Logging

The Alacris® OCSP Client can be configured to write binary dumps of all communications between the client and responder to a specified OS directory. If enabled, the transaction logs write the raw ASN.1 encoded OCSP requests made by the client and the OCSP responses returned by the Responder to the logs.

Configuration options are as specified in the *F.Security_Management.Configure_Binary_Dump_Logging* function:

1. Operating system directory where the transactions should be stored;
2. Whether to log outgoing requests; and
3. Whether to log incoming responses.

Separate files are used for binary dumps corresponding to requests and those corresponding to responses. Separate files are used for each day. The log filenames are determined in the following fashion:

Request Logs:

<Admin Specified Directory>/Requests/YYYYMMDD/transaction.orq

Response Logs:

<Admin Specified Directory>/Responses/YYYYMMDD/transaction.ors

5.1.14 F.OCSP_Transaction_Log_Auditing

The Alacris® OCSP Client can be configured to write detailed transaction logs for all OCSP requests and responses that are processed using the *F.Security_Management.Configure_OCSP_Transaction_Log_Auditing* function.

The following types of events are generated:

1. Information about certificate statuses received from a responder;
2. Information about the signer of OCSP responses;
3. Information about extensions included in OCSP responses;
4. Errors determining location of an OCSP responder;
5. OCSP errors returned by a responder as per RFC2560;
6. OCSP errors related to processing of extensions;
7. OCSP errors related to nonce processing;
8. OCSP errors related to freshness proof processing;
9. Errors relating to digital signature verification on OCSP response; and
10. Errors relating to validating the responder certificate.

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 Organizational Security Policies	O.AUDIT	O.REQUEST_VALIDITY	O.RESPONSE_VALIDITY	O. REPLAY_DETECTION	O.TRANSMIISSION_CONFIDENTIALITY
T.PACKET_SNIFFING					X
T.RESPONSE_REPLAY				X	
T.UNAUTHORIZED_REQUEST		X			X
T.UNAUTHORIZED_RESPONSE			X		
T.RESPONSE_INTEGRITY			X		
P.TRUSTED_RESPONDER			X	X	
P.AUDIT	X				

Table 6 – Mapping of Objectives to Threats and Policies

T.PACKET_SNIFFING – This threat is directly countered by the O.TRANSMISSION_CONFIDENTIALITY objective, which states that the TOE must be capable of encrypting communications.

T.RESPONSE_REPLAY – The O.REPLAY_DETECTION objective directly counters this threat.

T.UNAUTHORIZED_REQUEST – O.REQUEST_VALIDITY directly supports mitigation of this threat by requiring that the TOE be capable of authenticating OCSP messages sent to an OCSP responder. O.TRANSMISSION_CONFIDENTIALITY works in conjunction with O.REQUEST_VALIDITY to ensure that an attacker cannot capture previously valid OCSP requests and replay them to a responder.

T.UNAUTHORIZED_RESPONSE – O.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.

T.RESPONSE_INTEGRITY – O.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 trusted responder.

P.TRUSTED_RESPONDER – O.RESPONSE_VALIDITY and O.REPLAY_DETECTION allow implementation of this OSP by requiring that the TOE be capable of authenticating OCSP responses as coming from a trusted responder as well as not being the product of an attacker replaying previous communication between the TOE and a trusted responder.

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

7.2 Security Objectives for Environment Rationale

	Security Objectives						
Threats, Organizational Security Policies and Assumptions	OE.ACCESS_CONTROL	OE.AUTHORIZED_ADMIN	OE.TIMESTAMP	OE.CRYPTO_SERVICES	OE.PHYS_SEC	OE.NO_EVIL	OE.MAINTENACE
P.AUTHORIZED_ADMIN		X					
P.AUDIT			X				
A.PHYS_SEC					X		
A.LOGICAL_SEC	X						
A.NO_EVIL						X	
A.MAINTENANCE							X
T.PACKET_SNIFFING				X			
T.RESPONSE_REPLAY				X			
T.UNAUTHORIZED_REQUEST				X			
T.UNAUTHORIZED_RESPONSE				X			
T.RESPONSE_INTEGRITY				X			

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

P.AUTHORIZED_ADMIN – OE.AUTHORIZED_ADMIN directly supports implementation of this OSP 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.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.

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

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

T.PACKET_SNIFFING – OE.CRYPTO_SERVICES contributes to the mitigation of this threat by providing the TOE with the cryptographic services required to prevent packet sniffing.

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

T.UNAUTHORIZED_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_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.RESPONSE_INTEGRITY – OE.CRYPTO_SERVICES contributes to the mitigation of this threat by providing the TOE with the cryptographic services required to verify the integrity of responses.

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.REQUEST_VALIDITY	FMT_SMF.1, FPT_AUTH.1
O.RESPONSE_VALIDITY	FMT_SMF.1, FPT_ITI.1, FPT_AUTH.1
O.REPLAY_DETECTION	FPT_RPL.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 SFRs are required to meet at least one security objective. The rationale for selection of these SFRs 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.REQUEST_VALIDITY – FPT_AUTH.1 provides the ability for the client to authenticate OCSP messages sent to a responder. FMT_SMF.1 provides a mechanism for configuring client side certificate options in support of FPT_AUTH.1.

O.RESPONSE_VALIDITY – FMT_SMF.1 provides a mechanism for configuring the options for processing of OCSP requests and controlling what constitutes a valid request. FPT_ITI.1 and FPT_AUTH.1 provide integrity and authentication for the TSF data transmitted between TOE and responder.

O.REPLAY_DETECTION – FPT_RPL.1 supports replay detection for OCSP responses messages.

O.TRANSMISSION_CONFIDENTIALITY – FPT_ITC.1 provides for confidentiality of TSF data between the responder and the TOE.

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 SFRs: 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 SFRs for data authentication are concerned with user data, no such SFRs 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 a 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.

7.3.2 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

Security Functional Requirement	Dependencies	Dependency Satisfied? (Y/N)
FPT_RPL.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 (CSPs) 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 CSPs 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 (CSPs) 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 CSPs 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 Client 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.

ASSURANCE REQUIREMENTS MET BY ASSURANCE MEASURES		ASSURANCE MEASURES (ALACRIS® DOCUMENTATION)
	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.
	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.

ASSURANCE REQUIREMENTS MET BY ASSURANCE MEASURES		ASSURANCE MEASURES (ALACRIS® DOCUMENTATION)
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_ITC.1	FPT_ITI.1	FPT_AUTH.1
F.Verify OCSP_Response				X		X	X
F.Sign OCSP_Request						X	X
F.SSL_Session					X		
F.Windows_Event_Log_Auditing	X						
F.OCSP_Binary_Dump_Logging		X					
F.OCSP_Transaction_Log_Auditing		X					
F.Security_Management.Configure_Responder_Location			X				
F.Security_Management.Configure_Responder_Validity_Options			X				
F.Security_Management.Configure_OCSP_Response_Validity			X				
F.Security_Management.Configure_Client_Certificate			X				
F.Security_Management.Configure_SSL_Parameters			X				
F.Security_Management.Configure_Windows Event_Log_Auditing			X				
F.Security_Management.Configure_OCSP_Binary_Dump_Logging			X				
F.Security_Management.Configure_OCSP_Transaction_Log_Auditing			X				

Table 11 – Mapping of Objectives to Threats, Policies and Assumptions

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.OCSP_Transaction_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 transmitted between TOE and responder.

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

- F.Security_Management.Configure_Responder_Location;
- F.Security_Management.Configure_Responder_Validity_Options;
- F.Security_Management.Configure_OCSP_Response_Validity;
- F.Security_Management.Configure_Client_Certificate;
- F.Security_Management.Configure_SSL_Parameters;
- F.Security_Management.Configure_Windows_Event_Log_Auditing;
- F.Security_Management.Configure_OCSP_Binary_Dump_Logging; and
- F.Security_Management .Configure_OCSP_Transaction_Log_Auditing.

FPT_RPL.1 – F.Verify_OCSP_Response includes the ability (configured via F.Security_Management.Configure_OCSP_Response_Validity) to verify nonces in OCSP responses, thus providing protection against replayed responses.

FPT_ITC.1 – F.SSL_Session establishes an SSL session between the TOE and responder, satisfying the confidentiality requirements for transfer of TSF Data (OCSP messages) between TOE and responder.

FPT_AUTH.1 – F.Sign_OCSP_Request allows the TOE to sign OCSP requests using a digital certificate. This meets requirements for data authentication of request messages from TOE to Responder. F.Verify_OCSP_Response verifies the digital signature on the OCSP response sent from the responder to TOE, satisfying data authentication requirements from responder to TOE.

FPT_ITI.1 – F.Sign_OCSP_Request allows the TOE to sign OCSP requests using a digital certificate. This meets requirements for data integrity of request messages from TOE to Responder. F.Verify_OCSP_Response verifies the digital signature on the OCSP response sent from the responder to TOE, satisfying data integrity requirements from responder to TOE.

7.6 PP Claims Rationale

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