DBsign for HTML Applications Version 4.0
Security Target

Release Date:	April 4, 2011
Version:	1.0
Prepared By:	Saffire Systems P.O. Box 3054 Champaign, IL 61826
Prepared For:	Gradkell Systems, Inc. 4910 University Square Suite 2 Huntsville, AL 35816

Table of Contents

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

List of Tables

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

List of Figures

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

1 Introduction

This section identifies the Security Target, Target of Evaluation (TOE), conformance claims, ST organization, document conventions, and terminology. It also includes an overview of the evaluated product.

1.1 ST Reference

This section will provide information necessary to identify and control the Security Target and the TOE.

ST Title	DBsign for HTML Applications Version 4.0 Security Target
Version:	1.0
Publication Date:	April 4, 2011
ST Author	Saffire Systems
Assurance Level:	EAL2 augmented with ALC_FLR.2

1.2 TOE Reference

The TOE claiming conformance to this ST is identified as:

DBsign for HTML Applications version 4.0

1.3 Document Terminology

Please refer to CC Part 1 Section 2.3 for definitions of commonly used CC terms.

Please refer to Appendix B, Glossary of the U.S. Government Basic Robustness Public Key-Enabled Applications (PKE) PP for definitions of terms relating to the PP.

1.3.1 ST Specific Terminology

DBS	Name of DBsign schema in which the system tables are stored

1.3.2 Acronyms

API	Application Programming Interface
CC	Common Criteria
DB	Database

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

EAL2	Evaluation Assurance Level 2
HTTPS	Secure Hyper-Text Transfer Protocol
IT	Information Technology
JRE	Java Runtime Environment
LDAP	Lightweight Directory Access Protocol
OSP	Organisational Security Policy
PKI	Public Key Infrastructure
PP	Protection Profile
RDBMS	Relational Database Management Systems
SFP	Security Function Policy
SFR	Security Functional Requirement
SOF	Strength of Function
ST	Security Target
TOE	Target of Evaluation
TOI	Time of Interest
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSP	TOE Security Policy

1.4 Overview

DBsign is a software only solution providing a digital signature system that supports cryptographic data integrity and non-repudiation for data stored in relational databases. DBsign supports digital signature operations for data stored within a database and other data provided by the application. A co-existing application can interface to DBsign using DBsign's API to perform digital signature operations for the given application. DBsign includes the following major components:

- Client-side signing component called the DBsign Universal Web Signer (DBsign UWS)
- Server-side component called the DBsign Server

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

- DBsign Administration Tools, a set of graphical administration tools used to administer DBsign configuration data

These components work together to make the integration of digital signatures into applications a quick and easy process.

The DBsign UWS includes a simple, high-level application programming interface (API) that minimizes changes to existing application code. The existing application can also interface with the DBsign Server to perform digital signature related operations through an API accessed via HTTP requests. No specialized cryptographic or digital signature knowledge is required of developers or users. The DBsign UWS provides an interface to DBsign for a co-existing application so that the co-existing application may integrate the digital signature security functionalities of DBsign without the need of having to integrate the actual source code of DBsign into the co-existing application. Therefore, DBsign may be programmatically integrated into a co-existing application without the capability of modifying the security functionalities incorporated by DBsign.

The DBsign Administration Tools is a Graphical User Interface (GUI) that allows for the DBsign Administrator to control the security and configuration parameters under which DBsign operates. The tools provide a means for the DBsign administrator to centrally configure and maintain the digital signature system. The DBsign Administration Tools may be used to configure and maintain multiple DBsign installations by connecting to different RDBMS databases when executing the tools.

DBsign relies upon FIPS 140 validated cryptographic modules in the IT environment to provide all of the cryptographic operations, including digital signature generation and verification.

DBsign accesses the FIPS 140 validated cryptographic modules via PKCS #11 and the Microsoft CryptoAPI. PKCS#11 and the Microsoft CryptoAPI are standardized APIs that provide access to cryptographic modules.

In the evaluated configuration, DBsign must be used with the following FIPS 140-2 validated cryptographic modules that are in the IT environment:

- Windows cryptographic modules accessible via the Microsoft Crypto API that are included with the Windows operating system
- Network Security Services (NSS) Cryptographic Module (software versions 3.2.2 & 3.11.4) accessed via PKCS #11
- Other FIPS 140-2 validated modules accessed via Microsoft CryptoAPI and PKCS #11
- FIPS 140-2 validated modules that execute within a MAC OS X operating system and are accessed via PKCS #11 or Apple Security Framework

In the evaluated configuration, DBsign must be used on the following Common Criteria validated operating systems that are installed and configured in the CC evaluated configuration:

- Microsoft Windows XP Professional and higher (32-bit and 64-bit)
- Microsoft Windows Server 2003 and higher (32-bit and 64-bit) (including Microsoft

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

Windows Server 2008)

- Red Hat Enterprise Linux 5 and higher (32-bit and 64-bit)
- Sun Solaris 8 and higher for SPARC platform (32-bit and 64-bit)
- Sun Solaris 10 and higher for INTEL platform (32-bit and 64-bit)
- Apple Mac OS X 10.6 and higher (32-bit and 64-bit)
- Oracle Enterprise Linux 5.1 and higher (32-bit and 64-bit)

In addition, the following products must be included on the DBsign platforms:

- Java: Sun JRE 1.5 or higher (32-bit and 64-bit as available)
- Browser:
  - Microsoft Internet Explorer (IE) 6 or higher (32-bit or 64-bit) or
  - Mozilla Firefox 3 and higher (32-bit and 64-bit) or
  - Apple Safari 3 and higher (32-bit and 64-bit)

1.5 TOE Description

1.5.1 Architecture Description

DBsign is a software only TOE. The client communicates with DBsign Server via the DBsign UWS, an applet downloaded to and executed within their web browser on the client machine. Therefore, the web browser is pointed to the web server hosting DBsign version 4.0 via HTTPS and the web server redirects the query to the application server in which DBsign Server resides. DBsign Server then communicates to a database to retrieve data to be signed by the client via a network protocol recognized by the database (i.e. SQL*Net for Oracle). DBsign supports most Relational Database Management Systems (RDBMS).

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

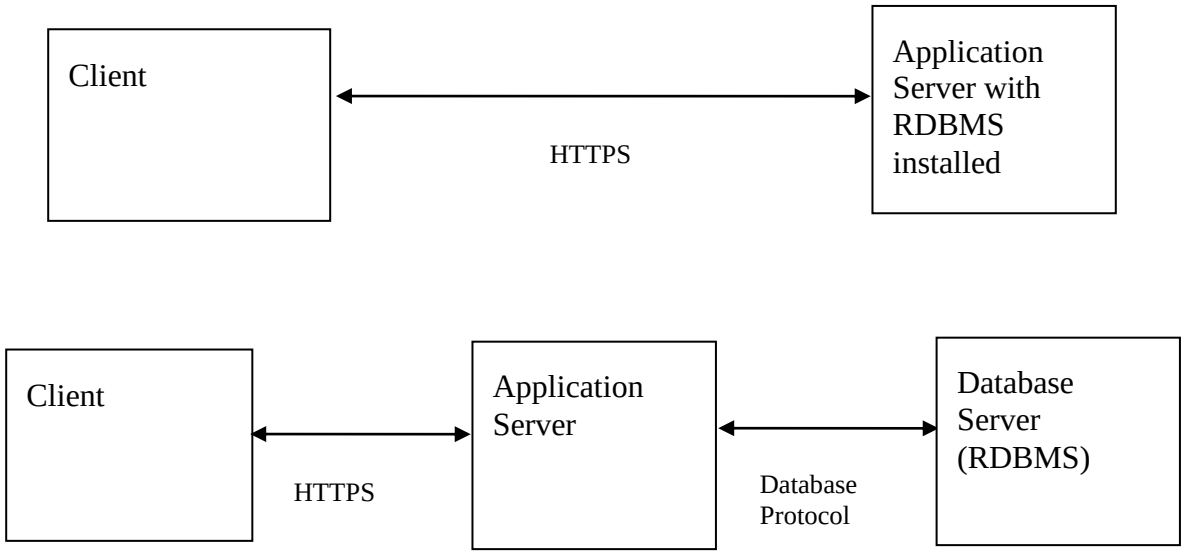

Figure 1: DBsign Configurations

DBsign additionally provides optional security features called the User Policy and Notary Signing features. The User Policy feature provides access control enforcement to digital signatures using templates. The Notary Signing feature provides server-side signing capability.

1.5.2 Physical Boundaries

This section identifies the hardware and software components of the product and denotes which are in the TOE and which are in the environment.

DBsign can be executed on a single physical computer, however in most cases the deployment consists of multiple physical computers. DBsign supports multiple clients to a server, however, at least one client, which could reside on the server, is required to support the full functionality of DBsign. The first computer is the client, which includes an operating system, a web browser client, and its underlying hardware. The DBsign UWS applet is downloaded to the client system and executed by the web browser's Java Virtual Machine (JVM). The second computer is the application server, which includes an operating system, web server, Java application server, application logic, the DBsign Administration Tools, the DBsign Server, and its underlying hardware. If there are only two computers, this second computer also includes the RDBMS. Otherwise, the third computer is the database server which includes an operating system, RDBMS, and its underlying hardware. The TOE also requires connectivity between the client and server to support the digital signature operations performed by DBsign.

Figure 2 depicts the physical architecture of DBsign at installation time (not during execution). The grayed rectangles labeled "DBsign Universal Web Signer", "DBsign Server", and "DBsign Admin Tools" including the API components included within the grayed rectangles represent the TOE components and boundaries in a physical aspect in relation to the non-TOE components.

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

(Note: the DBsign Universal Web Signer component is an applet that is downloaded to and executed on the web browser on the client.) The non-TOE components of the client include the operating system, web browser, and its underlying hardware. The non-TOE components of the server include the operating system, web server, Java application server, application logic, an RDBMS[1], and the underlying hardware. In addition, the HTTPS protocol used to communicate between the client and server is also a non-TOE component.

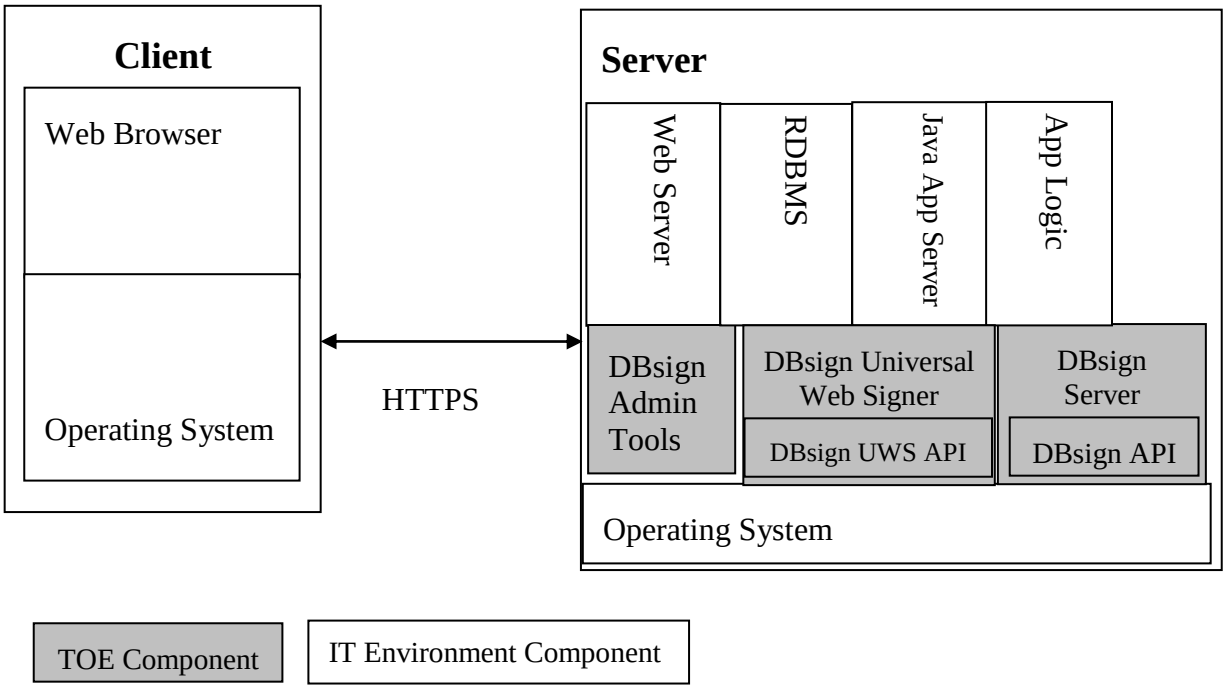

Figure 2: DBsign Physical Boundaries

HTML applications have a "thin-client" architecture. The user interface of the application executes on the client workstation. Most, if not all, of an application's business logic is executed in an application server. A current trend is to move some business logic in an application down to the browser in Javascript. HTML applications use DBsign to perform digital signature operations for data stored within a database and other data provided by the application. Figure 3 below depicts the location of the TOE components when they are executing. Note that the DBsign UWS applet is installed on the Server, but download to and executed on the Client. As shown in Figure 3, database-driven HTML applications can be composed of at least three tiers: (Note: It is possible to combine these platforms or to create additional tiers.)

Client Workstation	Executes the web browser to provide the user interface for the application
Application Server	Executes the application's business logic[2]

[1] The audit data and DBS tables reside in the RDBMS, which is in the TOE environment.

[2] Figure 3 depicts the web server, application server, and the DBsign Server executing on the same physical

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

Database Server Stores application data

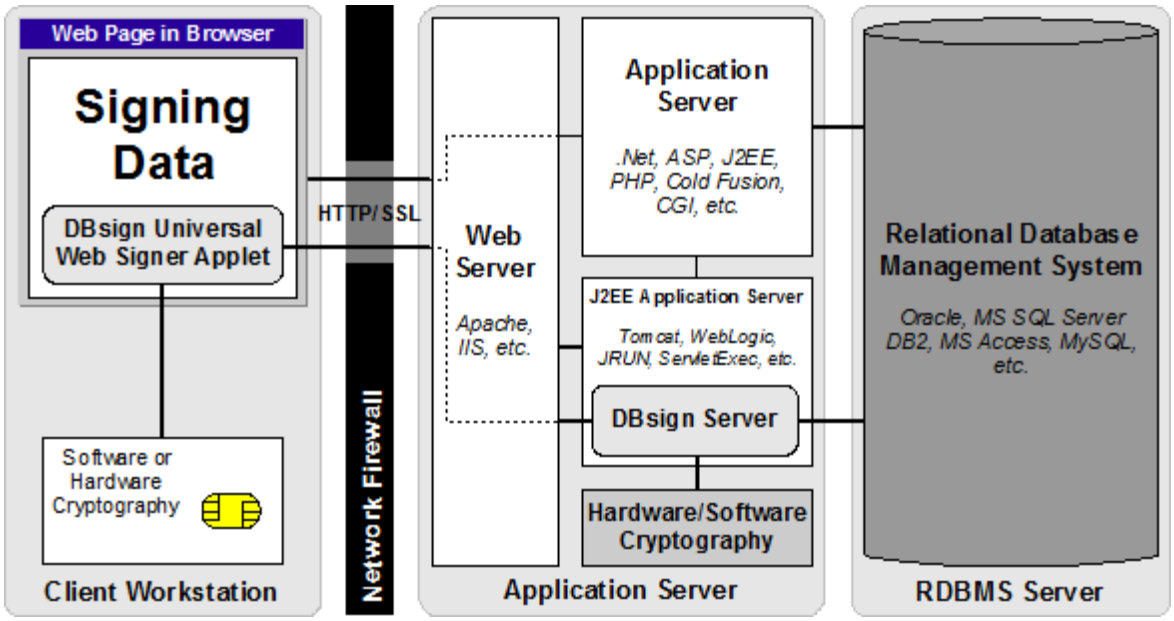

Figure 3: DBsign Execution Architecture

1.5.2.1 Hardware Components

The hardware components required for the TOE is the underlying hardware required for the operating system on which DBsign will be installed. Please refer to the minimum supported hardware requirements specified for the selected operating system.

1.5.2.2 Software Components

This table identifies software components and indicates whether or not each component is in the TOE.

TOE or Environment	Component	Description
TOE	DBsign Universal Web Signer	An applet installed on the Server and downloaded to/executed on the web browser on the client.
TOE	DBsign Servlet	DBsign application installed on the Server
TOE	DBsign Administration Tools	Administration tools installed on the Server.

platform. These three components can be on the same physical platform or multiple platforms.

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

TOE or Environment	Component	Description
Environment	Underlying Operating System	The following OSs that are CC validated at EAL2 or higher: ▪ Microsoft Windows XP Professional and higher (32-bit and 64-bit) ▪ Microsoft Windows Server 2003 and higher (32-bit and 64-bit) ▪ Red Hat Enterprise Linux (32-bit and 64-bit) ▪ Sun Solaris 8 and higher for SPARC platform (32-bit and 64-bit) ▪ Sun Solaris 10 and higher for INTEL platform (32-bit and 64-bit) ▪ Apple Mac OS X (32-bit and 64-bit)
Environment	Browser	▪ Microsoft Internet Explorer (IE) 6 or higher (32-bit or 64-bit) or ▪ Mozilla Firefox 3 and higher (32-bit and 64-bit) ▪ Apple Safari 3 and higher (32-bit and 64-bit)
Environment	Sun Java 1.5 (or higher) Java Runtime Environment (JRE)	Required for DBsign Administration Tools
Environment	RDBMS	Relational Database Management System installed on the Server

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

TOE or Environment	Component	Description
Environment	FIPS 140-2 validated cryptographic module	▪ Microsoft CryptoAPI Cryptographic Service Providers (CSPs) included with the Windows operating system ▪ Network Security Services (NSS) Cryptographic Module (software versions 3.2.2 & 3.11.4) accessed via PKCS #11 ▪ Any other FIPS 140-2 validated modules accessed via Microsoft CryptoAPI and PKCS #11 ▪ FIPS 140-2 validated modules that execute within a MAC OS X operating system and are accessed via PKCS #11 or Apple Security Framework

1.5.2.3 Guidance Documentation

The TOE includes the following administrative, installation, and application developer guidance:

DBsign Concepts Manual, Version 4.0, 2010

DBsign for HTML Applications: Integration Manual, Version 4.0, 2010

DBsign for HTML Applications Installation Manual, Version 4.0, 2010

DBsign Administration Tools Manual, Version 4.0, 2010

DBsign Configuration Editor Manual, Version 4.0, 2010

DBsign for HTML Applications Version 4.0 Release Notes, 2010

DBsign NIAP Configuration Manual, Version 4.0, 2010

1.5.3 Logical Boundaries

This section contains the product features and denotes which are in the TOE.

This section identifies the logical boundaries of the TOE in terms of the IT security features provided by the TOE. The IT security features include auditing and digital signature support. A description of each IT security feature identified is provided in the following subsections.

The TOE relies upon the underlying operating system, cryptographic module, and application to provide protection of the TSF and provide a mechanism for secure communication between the client and server.

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

1.5.3.1 Audit

The TOE provides auditing record generation capabilities for startup and shutdown of the audit functions, management functions, digitally signing data and verifying the digital signature of data. The auditing record generation capabilities of the TOE also report any integrity violations for verifications that are performed. It also identifies the specific data that has been modified. Audit record generation occurs on both the client and server system.

The audit records are stored in flat text files on the underlying operating systems. The TOE depends upon the IT environment to provide a mechanism (via a text viewer/editor) for viewing the events recorded in the audit log. The TOE also relies upon the underlying operating systems to protect the audit records.

1.5.3.2 User Policy

The TOE provides the optional ability to restrict access to the digital signing operations. By default, the User Policy system is disabled. The User Policy feature can be used to restrict:

- Who may digitally sign documents in the RDBMS
- Which certificates may be used to sign documents
- What types of documents individual users may sign

To support the User Policy feature, DBsign maintains a list of authorized users and associated certificates, but does not authenticate these users.

1.5.3.3 Security Management

The TOE includes multiple graphical user interfaces which are available for the DBsign administrator to manage the TOE. (The DBsign administrator is defined by the DB. The DB administrator creates and manages the DBsign administrator account in the DB.) These management features include the following:

- Manage the DBsign signature templates which are used to define how DBsign operates on data in the RDBMS
- Modify the descriptions of the DBsign security levels
- Configure the DBsign User Policy feature (enable, disable, define/query/edit DBsign user definition, specify user's certificates)
- Configure the list of certificate authorities DBsign trusts to issue certificates to end users
- Configure the audit log settings
- Manage the certificates and CRLs that DBsign stores in the RDBMS
- Configure the list of OCSP responders DBsign trusts to provide certificate revocation status information
- Create and populate the DBsign System Tables with initial data

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

All of the TSF configuration data is stored in the RDBMS: The DBsign Administration tools communicate directly with the RDBMS using a JDBC driver as required by the RDBMS. The RDBMS defines the communication protocol that be used to connect to it. The DBsign server communicates directly with the RDBMS to obtain the TSF configuration data. The DBsign Administration tools that communicate directly with the RDBMS require users to identify and authenticate themselves to the RDBMS prior to performing TSF-mediated administrative functions.

An additional tool is provided for creating a new DBsign configuration file. This tool does not install or activate the new DBsign configuration file. An administrative user on the DBsign server must install the new DBsign configuration file for it to be used. This tool does not require users to identify or authenticate themselves as the functionality provided by the tool does not impact the security functionality of the system until it is installed by an operating system administrator.

1.5.3.4 Digital Signature Support

The TOE provides the capability to request digital signature operations of the FIPS 140-2 validated cryptographic module which is in the IT environment. The digital signatures operations include digitally signing data and verifying digitally signed data. The TOE utilizes the defined digital signature operations to integrate with third-party applications that require the use of the digital signature operations that the TOE provides.

The TOE user data includes the data passed to and from DBsign as well as the certificates, CRLs, OCSP requests and OCSP responses.

The TSF data includes the list of trust anchors which is managed by the DBsign administrator and signed for protection.

1.5.3.4.1 Certification Path Validation

The TOE provides for all X.509 validation checks, including both certification path development and certification path validation. Certification path validation consists of validating certificates starting with one certified by a trust anchor and ending with the one issue to the subscriber of interest.

Public key certificates in a certification path can be categorized in three types for the purpose of certification path validation:

- Trust Anchors: The trust anchors can be in the form of self-signed certificates. The trust anchor is used to obtain the Distinguished Name (DN), public key, algorithm identifier, and the public key parameters (if applicable). DBsign permits validation of trust anchor if it is in the form of a self-signed certificate, including validating signature and verifying that the self-signed certificate validity period has not expired.
- Intermediate certificates: These are the certificates issued to the CAs. All certificates in a certification path are intermediate certificates, except the last one.
- End certificate: This is the last certificate in the certification path and is issued to the

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

subscriber of interest. This is typically an end-entity (i.e., not a CA) certificate. However, this package permits this certificate to be a CA certificate also.

The certification path validation provided by the TOE includes processes for the following security related certificate extenstions checks: no-check, keyUsage, extendedKeyUsage, basicConstraints, certificatePolicies, PolicyMapping, inhibitAnyPolicy, policyConstraints, nameConstraints.

1.5.3.4.2 PKI Signature Generation

The TOE performs the following functions on behalf of the requesting applications:

- Select the appropriate private key;
- Invoke a signature generation function using the selected private key; and
- Generate and include signature information that identifies the signer and is useful in efficient signature verification.

1.5.3.4.3 PKI Signature Verification

The TOE performs the following functions on behalf of the requesting applications:

- Process the signature information, e.g. the PKCS 7 blob;
- Invoke a signature verification function with the public key obtained from certification path validation; and
- Verify the signature information.

1.5.3.4.4 Online Certificate Status Protocol Client

The TOE performs the following functions to determine the revocation state of public key certificates at the request of the application:

- Generate Online Certificate Status Protocol (OCSP) requests
- Validate OCSP responses

1.5.3.4.5 Certificate Revocation List (CRL) Validation

The TOE provides the ability to determine the revocation state of public key certificates using a CRL.

1.5.3.5 Self Protection

The TOE provides protection mechanisms for its security functions. One of the protection mechanisms is that the TSF requires the administrative users to be authenticated by the IT environment before any administrative operations can be performed, whether those functions are related to the management of user accounts, configuration of the User Policy or the configuration of cryptographic operations.

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

The TOE relies upon the IT environment to protect the confidentiality of all data being transmitted between IT entities sending information through the TOE (via HTTPS). All functions of the TOE are confined to the TOE itself. There is no concept of a non-administrative user session with the TOE. External entities request an operation from the TOE and the TOE responds with the requested output. All external TSF interfaces are well defined. In this way, the TOE is self-contained and maintains its own execution domain which further protects it from interference and tampering by untrusted subjects.

1.5.4 Items Excluded from the TOE

There are no items excluded from the TOE.

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

2 Conformance Claims

2.1 CC Conformance Claims

This ST was developed to Common Criteria (CC) for Information Technology Security Evaluation – September, 2006 Version 3.1, Revision 3, CCMB-2006-09-001

The ST claims to be

CC Version 3.1 Part 1 conformant

CC Version 3.1 Part 2 extended

CC Version 3.1 Part 3 conformant

2.2 PP and Package Claims

The ST claims to be Evaluation Assurance Level 2 with augmentation.

The PP to which this ST conforms is defined in terms of packages. The ST claims conformance to the following Protection Profile (PP):

U.S. Government Basic Robustness Public Key-Enabled Applications (PKE) PP with the following packages

1. Certification Path Validation (CPV) – Basic
2. CPV – Basic Policy
3. CPV - Policy Mapping
4. CPV – Name Constraints
5. PKI Signature Generation
6. PKI Signature Verification
7. Online Certificate Status Protocol (OCSP) Client
8. Certificate Revocation List (CRL) Validation
9. Audit

at Basic Robustness Assurance, Version 2.8, May 1, 2007.

The ST claims conformance to the following packages defined in the PKE PP as noted in the following table.

Package	**Conformance Claim**
CPV – Basic	Conformant
CPV – Basic Policy	Conformant
CPV - Policy Mapping	Conformant
CPV – Name Constraints	Conformant
PKI Signature Generation	Conformant

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

Package	Conformance Claim
PKI Signature Verification	Conformant
OCSP Client	Conformant
CRL Validation	Conformant
Audit	Conformant

2.3 Conformance Claim Rationale

The PKE PP requires demonstrable conformance. This section demonstrates the following:

1. The statement of the security problem definition of the ST is equivalent or more restrictive than the statement of the security problem definition in the PP.
2. The statement of security objectives of the ST is equivalent or more restrictive than the statement of security objectives in the PP.
3. The statement of security requirements of the ST is equivalent or more restrictive than the statement of security requirements in the PP.

2.3.1 Security Problem Definition Conformance Rationale

The statements of threats, policies, and assumptions have been copied verbatim from the PKE PP. No additional threats, policies, or assumptions have been added.

2.3.2 Security Objectives Conformance Rationale

The statement of security objectives and the corresponding rationale have been copied verbatim from the PKE PP.

The ST includes two additional TOE security objectives: O.ACCESS and O.MANAGE. These security objectives define additional TOE functionality that does not interfere with the functionality provided in the TOE security objectives from the PKE PP.

2.3.3 Security Requirements Conformance Rationale

The statement of IT environment SFRs and the corresponding rationale have been copied verbatim from the PKE PP, except that the security requirement operations left uncompleted in the PKE PP have been completed in this ST and a few of the SFRs have been iterated since they are used more than once in the ST. The operations completed in this ST are denoted as described in Section 6.1.

The statement of TOE SFRs and the corresponding rationale have been copied verbatim from the PKE PP, except for the following

a) The security requirement operations left uncompleted in the PKE PP have been completed in this ST. The operations completed in this ST are denoted as described in

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

Section 6.1.

b) The PKE PP assumed reverse certification path building. The TOE implements forward certification path building. Functionally, both methods accurately and adequately build and verify the certification path. The following SFR elements was refined to reflect the functionality provided by the TSF:

- FDP_CPD_(EXT).1.1

c) DBsign supports both CRL and OCSP revocation checking. If one of the checks pass, the other is not performed. This was clarified by refining the following SFR element and adding an ST Application Note:

- FDP_DAU_CPV_(EXT).1.4

d) The PKE PP assumes that certification path output is requested by the users of the TOE. For DBsign, the users requesting digital signing services are not interested in receiving certification path output, instead this information is used between internal components of the TSF. Functionally, the TSF does process and provide the certification path output for its own use as requested by the application. The following SFRs were refined to reflect the functionality provided by the TSF:

- FDP_DAU_CPO_(EXT).1
- FDP_DAU_CPO_(EXT).2
- FDP_DAU_CPO_(EXT).3

e) The following SFRS copied verbatim from the PKE PP have been iterated since this ST used these components more than once:

- FDP_ACC.1 iterated to FDP_ACC.1:1
- FMT_MOF.1 iterated to FMT_MOF.1:1
- FMT_MSA.1 iterated to FMT_MSA.1:1
- FMT_SMF.1 iterated to FMT_SMF.1:1

f) Some of the functionality provided by DBsign is not always performed, but can be performed if configured or enabled by an administrator. The following SFRs were refined to describe this capability:

- FDP_ETC_SIG_(EXT).1
- FDP_ITS_SIG_(EXT).1
- FDP_DAU_OCS_(EXT).1

The ST includes eight additional TOE SFRs, identified below. These SFRs have either been copied from CC Part 2 with the appropriate operations performed or are defined in Section 5. These SFRs define additional TOE functionality that increase the functionality restrictions required by the TOE.

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

- FIA_UAU_ENV_(EXT).1
- FIA_UAU_ENV_(EXT).1
- FDP_ACC.1:2
- FDP_ACF.1
- FMT_MOF.1:2
- FMT_MSA.1:2
- FMT_MSA.3
- FMT_SMF.1:2

The statement of SARs is EAL2 augmented with ALC_FLR.2, which corresponds exactly with the Basic Robustness assurance package defined in the PKE PP.

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

3 Security Problem Definition

This section contains assumptions regarding the security environment and the intended usage of the TOE and threats on the TOE and the TOE environment.

3.1 Relationship between Basic Robustness Level and the formation of applicable assumptions, threats and the policies of the TSE

Basic robustness TOEs falls in the upper left area of the robustness figures discussed in Appendix D of the PKE PP. A Basic Robustness TOE is considered sufficient for low threat environments or where compromise of protected information will not have a significant impact on mission objectives. This implies that the motivation of the threat agents will be low in environments that are suitable for TOEs of this robustness. In general, basic robustness results in "good commercial practices" that counter threats based in casual and accidental disclosure or compromise of data protected by the TOE.

Threat agent motivation can be considered in a variety of ways. One possibility is that the value of the data process or protected by the TOE will generally be seen as of little value to the adversary (i.e., compromise will have little or no impact on mission objectives). Another possibility, (where higher value data is processed or protected by the TOE) is that procuring organizations will provide other controls or safeguards (i.e., controls that the TOE itself does not enforce) in the fielded system in order to increase the threat agent motivation level for compromise beyond a level of what is considered reasonable or expected to be applied.

3.2 Assumptions

This section identifies Secure Usage Assumptions for the IT environment.

A.Configuration	The TOE will be properly installed and configured.
A.Basic	The attack potential on the TOE is assumed to be "Basic".
A.NO_EVIL	Administrators are non-hostile, appropriately trained and follow all administrator guidance.
A.PHYSICAL	It is assumed that the environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.

3.3 Threats

The threats identified in this section may be addressed by the TOE. The asset under attack is the information transiting the TOE. In general, the threat agent includes, but is not limited to: 1) people with TOE access who are expected to possess "average" expertise, few resources, and moderate motivation, or 2) failure of the TOE.

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

T.AUDIT_COMPROMISE A user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action.

T.CHANGE_TIME An unauthorized user may change the TSF notion of time resulting in accepting old revocation information or expired certificates.

T.CRYPTO_COMPROMISE A user or process may cause key, data, or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified, or deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms.

T.MASQUERADE A user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources.

T.POOR_TEST Lack of or insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may result in incorrect TOE behavior being undiscovered thereby causing potential security vulnerabilities.

T.RESIDUAL_DATA A user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another.

T.TSF_COMPROMISE A user or process may cause, through an unsophisticated attack, TSF data, security attributes, or executable code to be inappropriately accessed (viewed, modified, or deleted).

T.UNATTENDED_SESSION A user may gain unauthorized access to an unattended session.

T.UNAUTHORIZED_ACCESS A user may gain access to user data for which they are not authorized according to the TOE security policy.

T.UNIDENTIFIED_ACTIONS The administrator may not have the ability to notice potential security violations, thus limiting the administrator's ability to identify and take action against a possible security breach.

3.3.1 Threats for CPV - Basic Package

T.Certificate_Modi An untrusted user may modify a certificate resulting in using a wrong public key.

T.DOS_CPV_Basic The revocation information or access to revocation information could be made unavailable, resulting in loss of system availability.

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

T.Expired_Certificate An expired (and possibly revoked) certificate as of TOI could be used for signature verification.

T.Untrusted_CA An untrusted entity (Certification Authority (CA)) may issue certificates to bogus entities, permitting those entities to assume identity of other legitimate users.

T.No_Crypto The user public key and related information may not be available to carry out the cryptographic function.

T.Path_Not_Found A valid certification path is not found due to lack of system functionality.

T.Revoked_Certificate A revoked certificate could be used as valid, resulting in security compromise

T.User_CA A user could act as a CA, issuing unauthorized certificates.

3.3.2 Threats for CPV – Basic Policy Package

T.Unknown_Policies The user may not know the policies under which a certificate was issued.

3.3.3 Threats for CPV –Policy Mapping Package

T.Mapping The user may accept unacceptable certificates or reject acceptable certificates due to improper certificate policy mapping.

T.Wrong_Policy_Dec The user may accept certificates that were not generated with the diligence and security acceptable to the user. The user may reject certificates that were generated with the diligence and security acceptable to the user.

3.3.4 Threats for CPV – Name Constraints Package

T.Name_Collision The user may accept certificates from CA where the CA's understanding and the user's understanding of the names differ, i.e., user and CA associate different identity with the same name.

3.3.5 Threats for PKI Signature Generation Package

T.Clueless_PKI_Sig The user may try only inappropriate certificates for signature verification because the signature does not include a hint.

3.3.6 Threats for PKI Signature Verification Package

T.Assumed_Identity_PKI_Ver A user may assume the identity of another user in order to verify a PKI signature.

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

T.Clueless_PKI_Ver The user may try only inappropriate certificates for signature verification because hints in the signature are ignored.

3.3.7 Threats for Online Certificate Status Protocol (OCSP) Client Package

T.DOS_OCSP The OCSP response of access to the OCSP response could be made unavailable, resulting in loss of system availability.

T.Replay_OCSP_Info The user may accept an OCSP response from well before TOI resulting in accepting a revoked certificate.

T.Wrong_OCSP_Info The user may accept a revoked certificate or reject a valid certificate due to a wrong OCSP response.

3.3.8 Threats for Certificate Revocation List (CRL) Validation Package

T.DOS_CRL The CRL or access to CRL could be made unavailable, resulting in loss of system availability.

T.Replay_Revoc_Info_CRL The user may accept a CRL issued well before TOI resulting in accepting a revoked certificate.

T.Wrong_Revoc_Info_CRL The user may accept a revoked certificate or reject a valid certificate due to a wrong CRL.

3.3.9 Threats for Audit Package

T.PKE_Accountability The PKE related audit events cannot be linked to individual actions.

3.4 Organisational Security Policies

The environment must include and comply with the following organizational security policies.

P.ACCESS_BANNER The IT Environment shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.

P.ACCOUNTABILITY The authorized users of the TOE shall be held accountable for their actions within the TOE.

P.CRYPTOGRAPHY Only NIST FIPS validated cryptography (methods and implementations) are acceptable for key management (i.e., generation, access, distribution, destruction, handling, and storage of keys) and

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

cryptographic services (i.e., encryption, decryption, signature, hashing, key exchange, and random number generation services).

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

4 Security Objectives

This chapter describes the security objectives for the TOE and the TOE's IT environment. The security objectives are divided between TOE Security Objectives (i.e., security objectives addressed directly by the TOE) and Security Objectives for the Environment (i.e., security objectives addressed by the IT domain or by non-technical or procedural means).

4.1 IT Security Objectives For The Environment

The following IT security objectives for the environment are to be addressed by the TOE environment by technical means.

OE.AUDIT_GENERATION The IT Environment will provide the capability to detect and create records of security-relevant events associated with users.

OE.AUDIT_PROTECTION The IT Environment will provide the capability to protect audit information.

OE.AUDIT_REVIEW The IT environment will provide the capability to selectively view audit information.

OE.CORRECT_TSF_OPERATION The IT Environment will provide the capability to test the TSF to ensure the correct operation of the TSF at a customer's site.

OE.CRYPTOGRAPHY The TOE shall use NIST FIPS 140-2 validated cryptographic services provided by the IT Environment.

OE.DISPLAY_BANNER The IT Environment will display an advisory warning regarding use of the TOE.

OE.MANAGE The IT Environment will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use.

OE.MEDIATE The IT Environment will protect user data in accordance with its security policy.

OE.RESIDUAL_INFORMATION The IT Environment will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated.

OE.SELF_PROTECTION The IT Environment will maintain a domain for its own execution that protects it and its resources from external interference, tampering, or unauthorized disclosure.

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

OE.TIME_STAMPS	The IT Environment will provide reliable time stamps and the capability for the administrator to set the time used for these time stamps.
OE.TIME_TOE	The IT Environment will provide reliable time for the TOE use.
OE.TOE_ACCESS	The IT Environment will provide mechanisms that control a user's logical access to the TOE.
OE.TOE_PROTECTION	The IT Environment will protect the TOE and TOE resources from external interference, tampering, or unauthorized disclosure and modification.

4.2 Non-IT Security Objectives For The Environment

The non-IT security objectives for the environment listed below are to be satisfied without imposing technical requirements on the TOE. Thus, they will be satisfied through application of procedural or administrative measures.

OE.Basic	The TOE will be designed and implemented for a minimum attack potential of "Basic" as validated by the vulnerability analysis.
OE.Configuration	The TOE will be installed and configured properly for starting up the TOE in a secure state.
OE.NO_EVIL	Sites using the TOE will ensure that administrators are non-hostile, appropriately trained and follow all administrator guidance.
OE.PHYSICAL	The non-IT environment will provide an acceptable level of physical security so that the TOE cannot be tampered with or be subject to side channel attacks such as the various forms of power analysis and timing analysis.

4.3 Security Objectives For The TOE

This section defines the IT security objectives that are to be addressed by the TOE.

4.3.1 Security Objectives for CPV - Basic Package

O.Availability	The TSF shall continue to provide security services even if revocation information is not available.
O.Correct_Temporal	The TSF shall provide accurate temporal validation results.
O.Current_Certificate	The TSF shall only accept certificates that are not expired as of TOI.

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

O.Get_KeyInfo	The TSF shall provide the user public key and related information in order to carry out cryptographic functions.
O.Path_Find	The TSF shall be able to find a certification path from a trust anchor to the subscriber.
O.Trusted_Keys	The TSF shall use trusted public keys in certification path validation.
O.User	The TSF shall only accept certificates issued by a CA.
O.Verified_Certificate	The TSF shall only accept certificates with verifiable signatures.
O.Valid_Certificate	The TSF shall use certificates that are valid, i.e., not revoked.

4.3.2 Security Objectives for CPV – Basic Policy Package

O.Provide_Policy_Info	The TSF shall provide certificate policies for which the certification path is valid.

4.3.3 Security Objectives for CPV –Policy Mapping Package

O.Map_Policies	The TSF shall map certificate policies in accordance with user and CA constraints.
O.Policy_Enforce	The TSF shall validate a certification path in accordance with certificate policies acceptable to the user.

4.3.4 Security Objectives for CPV – Name Constraints Package

O.Authorised_Names	The TSF shall validate a certificate only if the CA is authorized to issue a certificate to the subject.

4.3.5 Security Objectives for PKI Signature Generation Package

O.Give_Sig_Hints	The TSF shall provide hints for selecting correct certificate for signature verification.

4.3.6 Security Objectives for PKI Signature Verification Package

O.Use_Sig_Hints	The TSF shall use hints for selecting correct certificates for signature verification.
O.Linkage_Sig_Ver	The TSF shall use the correct user public key for signature verification.

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

4.3.7 Security Objectives for Online Certificate Status Protocol (OCSP) Client Package

O.Accurate_OCSP_Info The TSF shall accept only accurate OCSP responses.

O.Auth_OCSP_Info The TSF shall accept the revocation information from an authorized source for OCSP transactions.

O.Current_OCSP_Info The TSF accept only OCSP responses current as of TOI.

O.User_Override_Time_OCSP The TSF shall permit the user to override the time checks on the OCSP response.

4.3.8 Security Objectives for Certificate Revocation List (CRL) Validation Package

O.Accurate_Rev_Info The TSF shall accept only accurate revocation information.

O.Auth_Rev_Info The TSF shall accept the revocation information from an authorized source for CRL.

O.Current_Rev_Info The TSF shall accept only CRL that are current as of TOI.

O.User_Override_Time_CRL The TSF shall permit the user to override the time checks on the CRL.

4.3.9 Security Objectives for Audit Package

O.PKE_Audit The TSF shall audit security relevant PKE events.

4.3.9.1 Security Objectives for DBsign features

O.ACCESS The TSF shall provide the ability to restrict access to the digital signing operations.

O.MANAGE The TSF will provide all the functions and facilities necessary to manage and configure the security of the TOE and restrict these functions and facilities from unauthorized use.

4.4 Security Objectives Rationale

4.4.1 Environmental Security Objectives Rationale

Table 1 maps base assumptions, OSPs, and threats to objectives, demonstrating that all assumptions, OSPs, and threats are mapped to at least one objective. Table 2 maps base objectives to threats, OSPs, and assumptions, demonstrating that all objectives are mapped to at least one threat, OSP, or assumption.

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

Table 1: Mapping the TOE Base Assumptions, Threats, and OSPs to Objectives

Assumption/OSP/Threat	Objectives
A.Configuration	OE.Configuration
A.Basic	OE.Basic
A.NO_EVIL	OE.NO_EVIL
A.PHYSICAL	OE.PHYSICAL
P.ACCESS_BANNER	OE.DISPLAY_BANNER
P.ACCOUNTABILITY	OE.AUDIT_GENERATION OE.TIME_STAMPS OE.TOE_ACCESS OE.TIME_TOE
P.CRYPTOGRAPHY	OE.CRYPTOGRAPHY
T.AUDIT_COMPROMISE	OE.AUDIT_PROTECTION OE.RESIDUAL_INFORMATION OE.SELF_PROTECTION OE.TOE_PROTECTION
T.CHANGE_TIME	OE.TIME_TOE
T.CRYPTO_COMPROMISE	OE.CRYPTOGRAPHY OE.PHYSICAL
T.MASQUERADE	OE.TOE_ACCESS
T.POOR_TEST	OE.CORRECT_TSF_OPERATION
T.RESIDUAL_DATA	OE.RESIDUAL_INFORMATION
T.TSF_COMPROMISE	OE.RESIDUAL_INFORMATION OE.SELF_PROTECTION OE.TOE_PROTECTION OE.MANAGE
T.UNATTENDED_SESSION	OE.TOE_ACCESS
T.UNAUTHORIZED_ACCESS	OE.MEDIATE
T.UNIDENTIFIED_ACTIONS	OE.AUDIT_REVIEW OE.AUDIT_GENERATION OE.TIME_STAMPS OE.TIME_TOE

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

A.NO_EVIL states that administrators are non-hostile, appropriately trained and follow all administrator guidance. This assumption is mapped to:

- **OE.NO_EVIL**, which states that sites using the TOE will ensure that administrators are non-hostile, appropriately trained and follow all administrator guidance.

A.PHYSICAL states that environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.. This assumption is mapped to:

- **OE.PHYSICAL**, which states that the non-IT environment will provide an acceptable level of physical security so that the TOE cannot be tampered with or be subject to side channel attacks such as the various forms of power analysis and timing analysis.

A.Configuration states that the TOE will be properly installed and configured. This assumption is mapped to:

- **OE.Configuration**, which states that the TOE shall be installed and configured properly for starting up the TOE in a secure state.

A.Basic states that the attack potential on the TOE is assumed to be ”Basic”. A.Basic is mapped to:

- **OE.Basic,** which states that the TOE will be designed for a minimum attack potential of “Basic” as validated by the vulnerability analysis.

P.ACCESS_BANNER states that the IT Environment shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system. This policy is mapped to:

- **OE.DISPLAY_BANNER** which states that the IT Environment will display an advisory warning regarding use of the TOE. **OE.DISPLAY_BANNER** satisfies this policy by ensuring that the TOE displays an administrator configurable banner that provides all interactive users with a warning about the unauthorized use of the TOE

P.ACCOUNTABILITY states that the authorized users of the TOE shall be held accountable for their actions within the TOE. This policy is mapped to:

- **OE.AUDIT_GENERATION** which states that the IT Environment will provide the capability to detect and create records of security-relevant events associated with users. **OE.AUDIT_GENERATION** addresses this policy by providing the administrator with the capability of configuring the audit mechanism to record the actions of a specific user, or review the audit trail based on the identity of the user. Additionally, the administrator’s ID is recorded when any security relevant change is made (e.g. access rule modification, start-stop of the audit mechanism, establishment of a trusted channel, etc.).
- **OE.TIME_STAMPS** which states that the IT Environment will provide reliable time stamps and the capability for the administrator to set the time used for these time stamps. **OE.TIME_STAMPS** plays a role in supporting this policy by requiring the IT Environment to provide a reliable time stamp (configured locally by the Security

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

Administrator or via an external NTP server). The audit mechanism is required to include the current date and time in each audit record. All audit records that include the user ID, will also include the date and time that the event occurred.

- **OE.TIME_TOE** which states that the IT Environment will provide reliable time for the TOE use. **OE.TIME_STAMPS** plays a role in supporting this policy by permitting the TOE to provide reliable time on audit records generated by the TOE.
- **OE.TOE_ACCESS** which states that the IT Environment will provide mechanisms that control a user's logical access to the TOE. **OE.TOE_ACCESS** supports this policy by requiring the IT Environment to identify and authenticate all authorized users prior to allowing any TOE access or any TOE mediated access on behalf of those users.

P.CRYPTOGRAPHY states that only NIST FIPS validated cryptography (methods and implementations) are acceptable for key management (i.e.; generation, access, distribution, destruction, handling, and storage of keys) and cryptographic services (i.e.; encryption, decryption, signature, hashing, key exchange, and random number generation services). This policy is mapped to:

- **OE.CRYPTOGRAPHY** which states The TOE shall use NIST FIPS 140-2 validated cryptographic services provided by the IT Environment. **OE.CRYPTOGRAPHY** satisfies this policy by requiring the IT Environment to implement NIST FIPS validated cryptographic services. These services will provide confidentiality and integrity services as required by the IT Environment and the TOE.

T.AUDIT_COMPROMISE states that a user or process may view audit records, cause audit records to be lost or modified, or prevent future audit records from being recorded, thus masking a user's action. This threat is mapped to:

- **OE.AUDIT_PROTECTION** which states that the IT Environment will provide the capability to protect audit information. **OE.AUDIT_PROTECT** contributes to mitigating this threat by controlling access to the audit trail. Only an administrator is allowed to read the audit trail, no one is allowed to modify audit records, the administrator is the only one allowed to delete the audit trail, and the IT Environment has the capability to prevent auditable actions from occurring if the audit trail is full.
- **OE.RESIDUAL_INFORMATION** which states that the IT Environment will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated. **OE.RESIDUAL_INFORMATION** prevents a user not authorized to read the audit trail from access to audit information that might otherwise be persistent in a resource (e.g., memory). By ensuring the IT Environment prevents residual information in a resource, audit information will not become available to any user or process except those explicitly authorized for that data.
- **OE.SELF_PROTECTION** which states that the IT Environment will maintain a domain for its own execution that protects it and its resources from external interference, tampering, or unauthorized disclosure. **OE.SELF_PROTECTION** contributes to countering this threat by ensuring that the IT Environment can protect itself from users. If the IT Environment could not maintain and control its domain of

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

execution, it could not be trusted to control access to the resources under its control, which includes the audit trail which are always invoked is also critical to the migration of this threat.

- **OE.TOE_PROTECTION** which states The IT Environment will protect the TOE and TOE resources from external interference, tampering, or unauthorized disclosure and modification. **OE.TOE_PROTECTION** contributes to countering this threat by ensuring that the IT Environment can protect TOE. If the TOE could not be protected, it could not be trusted to provide accurate audit information.

T.CHANGE_TIME states that an unauthorized user may change the TSF notion of time resulting in accepting old revocation information or expired certificates. This threat is mapped to:

- **OE.TIME_TOE** which states that the IT Environment will provide reliable time for the TOE use. **OE.TIME_TOE** protects against this threat by ensuring that the IT Environment does not permit users to change the time.

T.CRYPTO_COMPROMISE states that a user or process may cause key, data or executable code associated with the cryptographic functionality to be inappropriately accessed (viewed, modified, or deleted), thus compromising the cryptographic mechanisms and the data protected by those mechanisms. This threat is mapped to:

- **OE.CRYPTOGRAPHY** which states that the TOE shall use NIST FIPS 140-2 validated cryptographic services provided by the IT Environment. **OE.CRYPTOGRAPHY** protects against this threat by ensuring that the cryptography used is sound and has been validated.
- **OE.PHYSICAL** which states that the non-IT environment will provide an acceptable level of physical security so that the TOE cannot be tampered with or be subject to side channel attacks such as the various forms of power analysis and timing analysis. **OE.PHYSICAL** contributes to protection against this threat by providing physical protection from side channel attacks protects against the attempts to compromise the cryptographic mechanisms.

T.MASQUERADE states that a user or process may masquerade as another entity in order to gain unauthorized access to data or TOE resources. This threat is mapped to:

- **OE.TOE_ACCESS** which states that the IT Environment will provide mechanisms that control a user's logical access to the TOE. **OE.TOE_ACCESS** mitigates this threat by controlling the logical access to the TOE and its resources. By constraining how and when authorized users can access the TOE, and by mandating the type and strength of the authentication mechanism this objective helps mitigate the possibility of a user attempting to login and masquerade as an authorized user. In addition, this objective provides the administrator the means to control the number of failed login attempts a user can generate before an account is locked out, further reducing the possibility of a user gaining unauthorized access to the TOE.

T.POOR_TEST states that lack of or insufficient tests to demonstrate that all TOE security functions operate correctly (including in a fielded TOE) may result in incorrect TOE behavior being undiscovered thereby causing potential security vulnerabilities. This threat is mapped to:

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

- **OE.CORRECT_TSF_OPERATION** which states that the IT Environment will provide the capability to test the TSF to ensure the correct operation of the TSF at a customer's site. **OE.CORRECT_TSF_OPERATION** ensures that once the TOE is installed at a customer's location, the capability exists that the integrity of the TSF (hardware and software) can be demonstrated, and thus providing end users the confidence that the TOE's security policies continue to be enforced.

T.RESIDUAL_DATA states that a user or process may gain unauthorized access to data through reallocation of TOE resources from one user or process to another. This threat is mapped to:

- **OE.RESIDUAL_INFORMATION** which states that the IT Environment will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated. **OE.RESIDUAL_INFORMATION** counters this threat by ensuring that TSF data and user data is not persistent when resources are released by one user/process and allocated to another user/process.

T.TSF_COMPROMISE states that a user or process may cause, through an unsophisticated attack, TSF data, security attributes, or executable code to be inappropriately accessed (viewed, modified, or deleted). This threat is mapped to:

- **OE.RESIDUAL_INFORMATION** which states that the IT Environment will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated. **OE.RESIDUAL_INFORMATION** is necessary to mitigate this threat, because even if the security mechanisms do not allow a user to explicitly view TSF data, if TSF data were to inappropriately reside in a resource that was made available to a user, that user would be able to inappropriately view the TSF data
- **OE.SELF_PROTECTION** which states that the IT Environment will maintain a domain for its own execution that protects it and its resources from external interference, tampering, or unauthorized disclosure. **OE.SELF_PROTECTION** is necessary to mitigate this threat to provide the TOE a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure through its own interfaces. This feature in turn ensures that other processes can not interfere with the IT Environment and defeat the IT Environment mechanisms.
- **OE.TOE_PROTECTION** which states that the IT Environment will protect the TOE and TOE resources from external interference, tampering, or unauthorized disclosure and modification. **OE.TOE_PROTECTION** is necessary to mitigate this threat by ensuring that the IT Environment will protect the TOE. This feature ensures that other processes can not defeat the TOE protection mechanisms.
- **OE.MANAGE** which states that the IT Environment will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use. **OE.MANAGE** is necessary because an access control policy is not specified to control access to TSF data and the TSF relies upon the RDBMS to protect, maintain

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

and store the TSF data. This objective is used to dictate who is able to view and modify TSF data, as well as the behavior of TSF functions

T.UNATTENDED_SESSION states that a user may gain unauthorized access to an unattended session. This threat is mapped to:

- **OE.TOE_ACCESS** which states that the IT Environment will provide mechanisms that control a user's logical access to the TOE. **OE.TOE_ACCESS** helps to mitigate this threat by including mechanisms that place controls on user's sessions. User and administrator's sessions are locked. Locking the session reduces the opportunity of someone gaining unauthorized access the session when the console is unattended.

T.UNAUTHORIZED_ACCESS states that a user may gain access to user data for which they are not authorized according to the TOE security policy. This threat is mapped to:

- **OE.MEDIATE** which states that the IT Environment will protect user data in accordance with its security policy. **OE.MEDIATE** ensures that all accesses to user data are subject to mediation, unless said data has been specifically identified as public data**.** The TOE requires successful authentication prior to gaining access to any controlled-access content. By implementing strong authentication to gain access to these services, an attacker's opportunity to successfully conduct a man-in-the-middle and/or password guessing attack is greatly reduced. Lastly, the IT Environment will ensure that all configured enforcement functions (authentication, access control rules, etc.) must be invoked prior to allowing a user to gain access to TOE or TOE mediated services. The IT Environment restricts the ability to modify the security attributes associated with access control rules, access to authenticated and unauthenticated services, etc to the Administrator. This feature ensures that no other user can modify the information flow policy to bypass the intended TOE security policy.

T.UNIDENTIFIED_ACTIONS states that the administrator may not have the ability to notice potential security violations, thus limiting the administrator's ability to identify and take action against a possible security breach. This threat is mapped to:

- **OE.AUDIT_REVIEW** which states that the IT Environment will provide the capability to selectively view audit information. **OE.AUDIT_REVIEW** helps to mitigate this threat by providing the Administrator with a required minimum set of configurable audit events that could indicate a potential security violation. By configuring these auditable events, the IT Environment and TOE monitors the occurrences of these events (e.g. set number of authentication failures, set number of information policy flow failures, self-test failures, etc.).
- **OE.AUDIT_GENERATION** which states that the IT Environment will provide the capability to detect and create records of security-relevant events associated with users. **OE.AUDIT_GENERATION** helps to mitigate this threat by recording actions for later review
- **OE.TIME_STAMPS** which states that the IT Environment will provide reliable time stamps and the capability for the administrator to set the time used for these time stamps. **OE.TIME_STAMPS** helps to mitigate this threat by ensuring that audit records have correct timestamps.

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

- **OE.TIME_TOE** which states that the IT Environment will provide reliable time for the TOE use. **OE.TIME_STAMPS** plays a role in supporting this policy by permitting the TOE to provide reliable time on audit records generated by the TOE.

In Table 2, the Base Objectives are mapped back to threats and assumptions, thereby demonstrating that every objective is mapped to a threat or assumption. Explanation of the mapping is defined above and is not repeated following Table 2. Note, once again, these threats, assumption, OSPs, and objectives are included in every PP in this PP family.

Table 2: Mapping the Base Objectives to Threats, Assumptions or OSPs

Objectives	**Assumption/OSP/Threat**
OE.AUDIT_GENERATION	P.ACCOUNTABILITY T.UNIDENTIFIED_ACTIONS
OE.AUDIT_PROTECTION	T.AUDIT_COMPROMISE
OE.AUDIT_REVIEW	T.UNIDENTIFIED_ACTIONS
OE.Configuration	A.Configuration
OE.CORRECT_TSF_OPERATION	T.POOR_TEST
OE.CRYPTOGRAPHY	P.CRYPTOGRAPHY T.CRYPTO_COMPROMISE
OE.DISPLAY_BANNER	P.ACCESS_BANNER
OE.Basic	A.Basic
OE.MANAGE	T.TSF_COMPROMISE
OE.MEDIATE	T.UNAUTHORIZED_ACCESS
OE.NO_EVIL	A.NO_EVIL
OE.PHYSICAL	A.PHYSICAL T.CRYPTO_COMPROMISE
OE.RESIDUAL_INFORMATION	T.AUDIT_COMPROMISE T.RESIDUAL_DATA T.TSF_COMPROMISE
OE.SELF_PROTECTION	T.AUDIT_COMPROMISE T.TSF_COMPROMISE
OE.TIME_STAMPS	P.ACCOUNTABILITY T.UNIDENTIFIED_ACTIONS
OE.TIME_TOE	P.ACCOUNTABILITY T.CHANGE_TIME

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

Objectives	Assumption/OSP/Threat
	T.UNIDENTIFIED_ACTIONS
OE.TOE_ACCESS	P.ACCOUNTABILITY T.MASQUERADE T.UNATTENDED_SESSION
OE.TOE_PROTECTION	T.AUDIT_COMPROMISE T.TSF_COMPROMISE

4.4.2 Security Objectives Rationale for Packages

The following subsections provide the mapping and rationale for the security objectives and threats associated with each individual package.

4.4.2.1 Security Objectives Rationale for CPV - Basic Package

The following tables demonstrate the mapping of threats to objectives and objectives to threats for the CPV – Basic Package. Explanatory text is provided below the tables to support the mappings.

Table 3: Mapping of Threats to Objectives for CPV – Basic Package

Threat	Objectives
T.Certificate_Modi	O.Verified_Certificate
T.DOS_CPV_Basic	O.Availability
T.Expired_Certificate	O.Correct_Temporal O.Current_Certificate
T.Untrusted_CA	O.Trusted_Keys
T.No_Crypto	O.Get_KeyInfo
T.Path_Not_Found	O.Path_Find
T.Revoked_Certificate	O.Valid_Certificate
T.User_CA	O.User

T.Certificate_Modi states that an untrusted user may modify a certificate resulting in using a wrong public key. This threat is mapped to:

- **O.Verified_Certificate**, which states that the TSF shall only accept certificates with verifiable signatures.

T.DOS_CPV_Basic states that the revocation information or access to revocation information could be made unavailable, resulting in loss of system availability. This threat is mapped to:

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

- **O.Availability**, which states that the TSF shall continue to provide security services even if revocation information is not available.

T.Expired_Certificate states that an expired (and possibly revoked) certificate as of TOI could be used for signature verification. This threat is mapped to:

- **O.Correct_Temporal**, which states that the TSF shall provide accurate temporal validation results.
- **O.Current_Certificate**, which states that the TSF shall only accept certificates that are not expired as of TOI.

T.Untrusted_CA states that an untrusted entity (Certification Authority (CA)) may issue certificates to bogus entities, permitting those entities to assume identity of other legitimate users. This threat is mapped to:

- **O.Trusted_Keys**, which states that the TSF shall use trusted public keys in certification path validation.

T.No_Crypto states that the user public key and related information may not be available to carry out the cryptographic function. This threat is mapped to:

- **O.Get_KeyInfo**, which states that the TSF shall provide the user public key and related information in order to carry out cryptographic functions.

T.Path_Not_Found states that a valid certification path is not found due to lack of system functionality. This threat is mapped to:

- **O.Path_Find**, which states that the TSF shall be able to find a certification path from a trust anchor to the subscriber.

T.Revoked_Certificate states that a revoked certificate could be used as valid, resulting in security compromise. This threat is mapped to:

- **O.Valid_Certificate**, which states that the TSF shall use certificates that are valid, i.e., not revoked.

T.User_CA states that a user could act as a CA, issuing unauthorized certificates. This threat is mapped to:

- **O.User**, which states that the TSF shall only accept certificates issued by a CA.

Table 4 maps objectives for the CPV – Basic Package to threats, demonstrating that every objective is mapped to a threat. The mapping is described in the text above and is not repeated following Table 4.

Table 4: Mapping of Objectives to Threats for CPV – Basic Package

Objectives	**Threat**
O.Availability	T.DOS_CPV_Basic
O.Correct_Temporal	T.Expired_Certificate
O.Current_Certificate	T.Expired_Certificate

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

Objectives	Threat
O.Get_KeyInfo	T.No_Crypto
O.Path_Find	T.Path_Not_Found
O.Trusted_Keys	T.Untrusted_CA
O.User	T.User_CA
O.Valid_Certificate	T.Revoked_Certificate
O.Verified_Certificate	T.Certificate_Modi

4.4.2.2 Security Objectives Rationale for CPV – Basic Policy Package

The mapping of threats to objectives for the CPV – Basic Policy package is shown in Table 5. Text that further supports the mapping is provided following Table 5.

Table 5: Mapping of Threats to Objectives for CPV – Basic Policy Package

Threat	Objectives
T.Unknown_Policies	O.Provide_Policy_Info

T.Unknown_Policies states that the user may not know the policies under which a certificate was issued. This threat is mapped to:

- **O.Provide_Policy_Info**, which states that the TSF shall provide certificate policies for which the certification path is valid.

Table 6 maps objectives for the CPV – Basic Policy package to threats, demonstrating that every objective is mapped to a threat. The mapping is described in the text above and is not repeated following Table 6.

Table 6: Mapping of Objectives to Threats for CPV – Basic Package

Objectives	Threat
O.Provide_Policy_Info	T.Unknown_Policies

4.4.2.3 Security Objectives Rationale for CPV –Policy Mapping Package

The mapping of threats to objectives for the CPV –Policy Mapping package is shown in Table 7. Text that further supports the mapping is provided following Table 7.

Table 7: Mapping of Threats to Objectives for CPV –Policy Mapping Package

Threat	Objectives
T.Mapping	O.Map_Policies
T.Wrong_Policy_Dec	O.Policy_Enforce

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

T.Mapping states that the user may accept unacceptable certificates or reject acceptable certificates due to improper certificate policy mapping. This threat is addressed by:

- **O.Map_Policies**, which states that the TSF shall map certificate policies in accordance with user and CA constraints.

T.Wrong_Policy_Dec states that the user may accept certificates that were not generated with the diligence and security acceptable to the user. The user may reject certificates that were generated with the diligence and security acceptable to the user. This threat is addressed by:

- **O.Policy_Enforce**, which states that the TSF shall validate a certification path in accordance with certificate policies acceptable to the user.

Table 8 maps objectives for the CPV – Policy Mapping package to threats, demonstrating that every objective is mapped to a threat. The mapping is described in the text above and is not repeated following Table 8.

Table 8: Mapping of Objectives to Threats for CPV –Policy Mapping Package

Objectives	**Threat**
O.Map_Policies	T.Mapping
O.Policy_Enforce	T.Wrong_Policy_Dec

4.4.2.4 Security Objectives Rationale for CPV – Name Constraints Package

The mapping of threats to objectives for the CPV –Name Constraints package is shown in Table 9. Text that further supports the mapping is provided following Table 9.

Table 9: Mapping of Threats to Objectives for CPV –Name Constraints Package

Threat	**Objectives**
T.Name_Collision	O.Authorised_Names

T.Name_Collision states that the user may accept certificates from CA where the CA's understanding and the user's understanding of the names differ, i.e., user and CA associate different identity with the same name. This threat is addressed by:

- **O.Authorised_Names**, which states that the TSF shall validate a certificate only if the CA is authorized to issue a certificate to the subject.

Table 10 maps objectives for the CPV – Name Constraints Package to threats, demonstrating that every objective is mapped to a threat. The mapping is described in the text above and is not repeated following Table 10.

Table 10: Mapping of Objectives to Threats for CPV – Name Constraints Package

Objectives	**Threat**
O.Authorised_Names	T.Name_Collision

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

4.4.2.5 Security Objectives Rationale for PKI Signature Generation Package

The mapping of threats to objectives for the PKI Signature Generation package is shown in Table 11. Text that further supports the mapping is provided following Table 11.

Table 11: Mapping of Threats to Objectives for PKI Signature Generation Package

Threat	Objectives
T.Clueless_PKI	O.Give_Sig_Hints

T.Clueless_PKI_Sig states that the user may try only inappropriate certificates for PKI signature verification because the signature does not include a hint. This threat is addressed by:

- **O.Give_Sig_Hints**, which states that the TSF shall give hints for selecting correct certificates or keys for PKI signature.

Table 12 maps objectives for the PKI Signature Generation package to threats, demonstrating that every objective is mapped to a threat. The mapping is described in the text above and is not repeated following Table 12.

Table 12: Mapping of Objectives to Threats for PKI Signature Generation Package

Objectives	Threat
O.Give_Sig_Hints	T.Clueless_PKI

4.4.2.6 Security Objectives Rationale for PKI Signature Verification Package

The mapping of threats to objectives for the PKI Signature Verification package is shown in Table 13. Text that further supports the mapping is provided following Table 13.

Table 13: Mapping of Threats to Objectives for PKI Signature Verification Package

Threat	Objectives
T.Assumed_Identity_PKI_Ver	O.Linkage_Sig_Ver
T.Clueless_PKI_Ver	O.Use_Sig_Hints

T.Assumed_Identity_PKI_Ver states that a user may assume the identity of another user for PKI signature verification. This threat is addressed by:

- **O.Linkage_Sig_Ver**, which states that the TSF shall use the correct user public key for signature verification.

T.Clueless_PKI_Ver states that the user may try only inappropriate certificates for PKI signature verification by ignoring hints in the signature. This threat is addressed by:

- **O.Use_Sig_Hints**, which states that the TSF shall provide hints for selecting correct certificates or keys for signature verification.

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

Table 14 maps objectives The PKI Signature Verification package to threats, demonstrating that every objective is mapped to a threat. The mapping is described in the text above and is not repeated following Table 14.

Table 14: Mapping of Objectives to Threats for PKI Signature Verification Package

Objectives	Threat
O.Linkage_Sig_Ver	T.Assumed_Identity_PKI_Ver
O.Use_Sig_Hints	T.Clueless_PKI_Ver

4.4.2.7 Security Objectives Rationale for Online Certificate Status Protocol (OCSP) Client Package

The mapping of threats to objectives for the OCSP Client package is shown in Table 19. Text that further supports the mapping is provided following Table 19.

Table 15: Mapping of Threats to Objectives for OCSP Client Package

Threat	Objectives
T.DOS_OCSP	O.User_Override_Time_OCSP
T.Right_OCSP_Info	O.Current_OCSP_Info
T.Wrong_OCSP_Info	O.Accurate_OCSP_Info O.Auth_OCSP_Info

T.DOS_OSCP states that the OCSP response or access to the OCSP response could be made unavailable, resulting in loss of system availability. This threat is mapped to:

- **O.User_Override_Time_OCSP**, which states that the TSF shall permit the user to override the time checks on the OCSP response.

T.Replay_OCSP_Info states that the user may accept revocation information from well before TOI resulting in accepting revoked certificate for OCSP transactions. This threat is mapped to:

- **O.Current_OCSP_Info**, which states that the TSF accept only OCSP responses current as of TOI .

T.Wrong_OCSP_Info states that the user may accept a revoked certificate or reject a valid certificate due to wrong revocation information. This threat is mapped to:

- **O.Accurate_OCSP_Info**, which states that the TSF shall accept only accurate OCSP responses.
- **O.Auth_OCSP_Info**, which states that the TSF shall accept the OCSP response from an authorized source.

Table 16 maps objectives for the OCSP Client package to threats, demonstrating that every objective is mapped to a threat. The mapping is described in the text above and is not repeated following Table 16.

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

Table 16: Mapping of Objectives to Threats for OCSP Client Package

Objectives	Threat
O.Accurate_OCSP_Info	T.Wrong_OCSP_Info
O.Auth_OCSP_Info	T.Wrong_OCSP_Info
O.Current_OCSP_Info	T.Right_OCSP_Info
O.User_Override_Time_OCSP	T.DOS_OCSP

4.4.2.8 Security Objectives Rationale for Certificate Revocation List (CRL) Validation Package

The mapping of threats to objectives for the CRL Validation package is shown in Table 17. Text that further supports the mapping is provided following Table 17.

Table 17: Mapping of Threats to Objectives for OCSP Client Package

Threat	Objectives
T.DOS_CRL	O.User_Override_Time_CRL
T.Replay_Revoc_Info_CRL	O.Current_Rev_Info
T.Wrong_Revoc_Info_CRL	O.Accurate_Rev_Info O.Auth_Rev_Info

T.DOS_CRL states that the CRL or access to the CRL could be made unavailable, resulting in loss of system availability. This threat is mapped to:

- **O.User_Override_Time_CRL**, which states that the TSF shall permit the user to override the time checks on the CRL.

T.Replay_Revoc_Info_CRL states that the user may accept a CRL issued well before TOI resulting in accepting currently revoked certificate. This threat is mapped to:

- **O.Current_Rev_Info**, which states that the TSF shall accept only CRL that are current as TOI.

T.Wrong_Revoc_Info_CRL states that the user may accept a revoked certificate or reject a valid certificate due to wrong revocation information. This threat is mapped to:

- **O.Accurate_Rev_Info**, which states that the TSF shall accept only accurate revocation information.
- **O.Auth_Rev_Info**, which states that the TSF shall accept the revocation information from an authorized source for CRL.

Table 18 maps objectives for the CRL Validation package to threats, demonstrating that every objective is mapped to a threat. The mapping is described in the text above and is not repeated following Table 18.

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

Table 18: Mapping of Objectives to Threats for OCSP Client Package

Objectives	Threat
O.Accurate_Rev_Info	T.Wrong_Revoc_Info_CRL
O.Auth_Rev_Info	T.Wrong_Revoc_Info_CRL
O.Current_Rev_Info	T.Replay_Revoc_Info_CRL
O.User_Override_Time_CRL	T.DOS_CRL

4.4.2.9 Security Objectives Rationale for Audit Package

The mapping of threats to objectives for the Audit package is shown in Table 19. Text that further supports the mapping is provided following Table 19.

Table 19: Mapping of Threats to Objectives for PKI Signature Generation Package

Threat	Objectives
T.PKE_Accountability	O.PKE_Audit

T.PKE_Accountability states that the PKE related audit events cannot be linked to individual actions. This threat is mapped to:

- **O.PKE_Audit**, which states that the TSF shall audit security relevant PKE events. This coupled with the base audit functions provided by the IT Environment mitigate this threat.

Table 20 maps objectives for the Audit package to threats, demonstrating that every objective is mapped to a threat. The mapping is described in the text above and is not repeated following Table 20.

Table 20: Mapping of Objectives to Threats for PKI Signature Generation Package

Objectives	Threat
O.PKE_Audit	T.PKE_Accountability

4.4.2.10 Security Objectives Rationale for DBsign additional features

The mapping of threats to objectives for the additional DBsign features is shown in Table 21. Text that further supports the mapping is provided following Table 21.

Table 21: Mapping of Threats to Objectives for DBsign additional features

Threat	Objectives
T.UNAUTHORIZED_ACCESS	O.ACCESS
T.TSF_COMPROMISE	O.MANAGE

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

T.TSF_COMPROMISE states that a user or process may cause, through an unsophisticated attack, TSF data, security attributes, or executable code to be inappropriately accessed (viewed, modified, or deleted). This threat is mapped to:

- **O.MANAGE** which states that the TSF will provide all the functions and facilities necessary to manage and configure the security of the TOE, and restrict these functions and facilities from unauthorized use. This objective is used to dictate who is able to view and modify TSF data, as well as the behavior of TSF functions

T.UNAUTHORIZED_ACCESS states that a user may gain access to user data for which they are not authorized according to the TOE security policy. This threat is mapped to:

- **O.ACCESS** which states that the TSF shall provide the ability to restrict access to the digital signing operations. **O.ACCESS** provides the ability to control which users can access certificates used to digitally sign RDBMS data**.**

Table 22 maps objectives for the additional DBsign features to threats, demonstrating that every objective is mapped to a threat. The mapping is described in the text above and is not repeated following Table 22.

Table 22: Mapping of Objectives to Threats for DBsign additional features

Objectives	**Threat**
O.ACCESS	T.UNAUTHORIZED_ACCESS
O.MANAGE	T.TSF_COMPROMISE

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

5 Extended Components Definition

This section defines the newly defined components (also known as extended components) used to define the security requirements for this ST. The extended components used in this ST are members of existing CC Part 2 families and are based on the existing CC Part 2 SFRs.

Extended components are denoted by their name ending with "_(EXT)" or a NIAP interpretation tag, such as “-NIAP-0407”.

The following extended components used in this ST are defined in the PKE PP:

- FAU_GEN.1-NIAP-0407:1 Audit data generation
- FAU_GEN.2-NIAP-0410:1 User identity association
- FAU_SEL.1-NIAP-0407 Selective audit
- FAU_STG.1-NIAP-0429 Protected audit trail storage
- FAU_STG.NIAP-0429-1 Protected audit trail storage
- FCS_CRM_FPS_(EXT).1 FIPS compliant cryptographic module
- FDP_ACF.1-NIAP-0407 Security attribute based access control – PKI Credential Management
- FMT_MSA.3-NIAP-0429 Static attribute initialization
- FPT_TST_SOF_(EXT).1 TSF testing for Software only TOEs
- FDP_CPD_(EXT).1 Certification path development
- FDP_DAU_CPI_(EXT).1 Certification path initialization – basic
- FDP_DAU_CPV_(EXT).1 Certificate processing – basic
- FDP_DAU_CPV_(EXT).2 Intermediate certificate processing – basic
- FDP_DAU_CPO_(EXT).1 Certification path output – basic
- FDP_DAU_CPI_(EXT).2 Certification path initialization – basic policy
- FDP_DAU_CPO_(EXT).2 Certification path output – basic policy
- FDP_DAU_CPI_(EXT).3 Certification path initialization –policy mapping
- FDP_DAU_CPV_(EXT).3 Intermediate certificate processing – policy mapping
- FDP_DAU_CPO_(EXT).3 Certification path output – policy mapping
- FDP_DAU_CPI_(EXT).4 Certification path initialization –names
- FDP_DAU_CPV_(EXT).4 Certificate processing – name constraints
- FDP_DAU_CPV_(EXT).5 Intermediate certificate processing – name constraints
- FDP_ETC_SIG_(EXT).1 Export of PKI Signature
- FDP_ITC_SIG_(EXT).1 Import of PKI Signature
- FDP_DAU_SIG_(EXT).1 Signature Blob Verification
- FDP_DAU_OCS_(EXT).1 Basic OCSP Client
- FDP_DAU_CRL_(EXT).1 Basic CRL Checking
- FAU_GEN.1-NIAP-0407:2 Audit data generation - TOE
- FAU_GEN.2-NIAP-0410:2 User identity association - TOE

5.1 FIA Identification and Authentication

The FIA class is extended to include 2 additional components.

The FIA class addresses the requirements to verify a claimed user identity. The extended components defined in this section require the TOE to ensure that claimed user identities are

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

verified by the IT environment.

5.1.1 FIA_UAU_ENV_(EXT).1 Timing of authentication with a third party

FIA_UAU_ENV_(EXT).1 is a member of the FIA_UAU family. This extended requirement is necessary since a CC Part 2 SFR does not exist that allows for the authentication to be performed by the IT environment, but required by the TOE. This extended SFR is based on CC Part 2 FIA_UAU.1.

Management: FIA_UAU_ENV_(EXT).1

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

- Managing the list of actions that can be taken before the user is authenticated.

Audit: FIA_UAU_ENV_(EXT).1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Unsuccessful use of the authentication mechanism;
- Basic: All use of the authentication mechanism;
- Detailed: All TSF mediated actions performed before authentication of the user.

Hierarchical to: No other components.

Dependencies: FIA_UID.1 Timing of identification or
FIA_UID_ENV_(EXT).1 Time of identification with a third party.

FIA_UAU_ENV_(EXT).1.1 The TSF shall allow [assignment: list of TSF mediated actions] on behalf of the user to be performed before the user is authenticated by the IT environment.

FIA_UAU_ENV_(EXT).1.2 The TSF shall require each user to be successfully authenticated by the IT environment before allowing any other TSF-mediated actions on behalf of that user.

5.1.2 FIA_UID_TRD.1 Timing of identification with a third party

FIA_UID_ENV_(EXT).1 is a member of the FIA_UID family. This extended requirement is necessary since a CC Part 2 SFR does not exist that allows for the identification to be performed by the IT environment, but required by the TOE. This extended SFR is based on CC Part 2 FIA_UID.1.

Management: FIA_UID_ENV_(EXT).1

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

- If an authorized administrator can change the actions allowed before identification, the managing of the action lists.

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

Audit: FIA_UID_ENV_(EXT).1

The following actions should be auditable if FAU_GEN Security audit data generation is included in the PP/ST:

- Minimal: Unsuccessful use of the user identification mechanism, including the user identity provided;
- Basic: All use of the user identification mechanism, including the user identity provided.

Hierarchical to: No other components.

Dependencies: None

FIA_UID_ENV_(EXT).1.1 The TSF shall allow [assignment: list of TSF mediated actions] on behalf of the user to be performed before the user is identified by the IT environment.

FIA_UID_ENV_(EXT).1.2 The TSF shall require each user to be successfully identified by the IT environment before allowing any other TSF-mediated actions on behalf of that user.

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

6 Security Requirements

The security requirements that are levied on the TOE are specified in this section of the ST.

6.1 Conventions

The CC defines four operations on security functional requirements. The conventions below define the conventions used in this ST to identify the operations completed in the PP and the operations completed in this ST by the ST author. All operations completed in the PP are surrounded by square brackets ([operation]). When NIAP Interpretations are included in requirements, the additions from the interpretations are displayed as refinements.

Assignment made in PP:	**[indicated with bold text]**
Selection made in PP:	[indicated with underlined text]
Refinement made in PP:	[***additions indicated with bold text and italics***]
	[***deletions indicated with strike-through ~~bold text and italics~~***]
Iteration made in PP:	[indicated with typical CC requirement naming followed by a colon and number for each iteration (e.g., FMT_MSA.1:1)]
Assignment made in ST:	**indicated with bold text**
Selection made in ST:	indicated with underlined text
Refinement made in ST:	***additions indicated with bold text and italics***
	deletions indicated with strike-through ~~bold text and italics~~
Iteration made in ST:	indicated with typical CC requirement naming followed by a colon and number for each iteration (e.g., FMT_MSA.1:1)

6.2 IT Environment Security Functional Requirements

All IT environment security functional requirements included in this ST are listed in the following table. Extended SFRs are identified as “Part 2 extended” and their name ends with "_(EXT)" or a NIAP interpretation tag, such as “-NIAP-0407”.

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

SFR	Ttile	Part 2 or Extended
FAU_GEN.1-NIAP-0407:1	Audit data generation	Part 2 Extended
FAU_GEN.2-NIAP-0410:1	User identity association	Part 2 Extended
FAU_SAR.1	Audit review	Part 2
FAU_SAR.2	Restricted audit review	Part 2
FAU_SAR.3	Selectable audit review	Part 2
FAU_SEL.1-NIAP-0407	Selective audit	Part 2 Extended
FAU_STG.1-NIAP-0429	Protected audit trail storage	Part 2 Extended
FAU_STG.NIAP-0429-1	Protected audit trail storage	Part 2 Extended
FCS_CRM_FPS_(EXT).1	FIPS compliant cryptographic module	Part 2 Extended
FDP_ACC.1:1	Subset access control – PKI Credential Management	Part 2
FDP_ACF.1-NIAP-0407	Security attribute based access control – PKI Credential Management	Part 2 Extended
FDP_RIP.2	Full residual information protection	Part 2
FIA_AFL.1	Authentication failure handling	Part 2
FIA_ATD.1	User attribute definition	Part 2
FIA_UAU.2	User authentication before any action	Part 2
FIA_UAU.7	Protected authentication feedback	Part 2
FIA_UID.2	User identification before any action	Part 2
FIA_USB.1	User-subject binding	Part 2
FMT_MOF.1:1	Management of security function behavior – IT Environment	Part 2
FMT_MSA.1:1	Management of security attributes – IT Environment	Part 2
FMT_MSA.3-NIAP-0429	Static attribute initialization	Part 2 Extended
FMT_MTD.1:1	Management of TSF data – I&A Data	Part 2
FMT_MTD.1:2	Management of TSF data – Authentication Data	Part 2
FMT_MTD.1:3	Management of TSF data – I&A Attempts	Part 2
FMT_MTD.1:4	Management of TSF data – Trust Anchors	Part 2
FMT_MTD.1:5	Management of TSF data – Time	Part 2
FMT_SMF.1:1	Specification of management functions – IT Environment	Part 2
FMT_SMR.1	Security roles	Part 2
FPT_STM.1	Reliable time stamps	Part 2
FPT_TST_SOF_(EXT).1	TSF testing for Software only TOEs	Part 2 Extended
FTA_SSL.1	TSF-initiated session locking	Part 2
FTA_SSL.2	User-initiated locking	Part 2
FTA_TAB.1	Default TOE access banners	Part 2

Table 23: IT Environment Security Functional Requirements

6.2.1 Security Audit (FAU)

6.2.1.1 FAU_GEN.1-NIAP-0407:1 Audit Data Generation

FAU_GEN.1.1-NIAP-0407:;1 The [***IT Environment***] shall able to generate an audit record of the following auditable events**:**

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

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

b) All auditable events listed in Table 24; and

c) no additional events**.**

FAU_GEN.1.2-NIAP-0407:;1 The [***IT Environment***] shall record within each audit record at least the following information:

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, information specified in column three of **Table 24** below.

Requirement	Auditable Events	Additional Audit Record Contents
FAU_GEN.1-NIAP-0407:1	None	
FAU_GEN.2-NIAP-0410:1	None	
FAU_SAR.1	Opening the audit trail	The identity of the Audit Administrator performing the function
FAU_SAR.2	Unsuccessful attempts to read information from the audit records	The identity of the administrator performing the function
FAU_SAR.3	None	
FAU_SEL.1-NIAP-0407	All modifications to the audit configuration that occur while the audit collection functions are operating	The identity of the Security Administrator performing the function
FAU_STG.1-NIAP-0429	None	
FAU_STG.NIAP-0429	None	
FCS_CRM_FPS_(EXT).1	None	
FDP_ACC.1:1	None	
FDP_ACF.1-NIAP-0407	All requests to perform an operation on an object covered by the SFP	Object identity
FDP_RIP.2	None	
FIA_AFL.1	Reaching of the threshold for the unsuccessful authentication attempts	
FIA_ATD.1	None	
FIA_UAU.2	All use of authentication mechanism	
FIA_UAU.7	None	
FIA_UID.2	All use of identification mechanism	User identity

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

Requirement	Auditable Events	Additional Audit Record Contents
FIA_USB.1	Success and failure of binding of user security attributes to a subject (e.g. success and failure to create a subject).	
FMT_SMF.1:1	Use of management function	Management function
FMT_SMR.1	Modifications to the group of users that are part of a role	
FPT_STM.1	Change to the time	
FTA_TAB.1	None	

Table 24: IT Environment Auditable Events

6.2.1.2 FAU_GEN.2-NIAP-0410:1 User identity association

FAU_GEN.2.1-NIAP-0410;1 For audit events resulting from actions of identified users, the [***IT Environment***] shall able to associate each auditable event with the identity of the user that caused the event.

6.2.1.3 FAU_SAR.1 Audit Review

FAU_SAR.1.1 The [***IT Environment***] shall provide [**the administrator**] with the capability to read [**all audit information**] from the audit records.

FAU_SAR.1.2 The [***IT Environment***] shall provide the audit records in a manner suitable for the user to interpret the information.

6.2.1.4 FAU_SAR.2 Restricted Audit Review

FAU_SAR.2.1 The [***IT Environment***] shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.2.1.5 FAU_SAR.3 Selectable Audit Review

FAU_SAR.3.1 The [***IT Environment***] shall provide the ability to perform [**searches and sorting**] ***and*** no other operation of audit data based on [**date, time, user identity and**] **category, event identifier, computer, success of auditable security events, and failure of security events**.

6.2.1.6 FAU_SEL.1-NIAP-0407 Selective Audit

FAU_SEL.1.1-NIAP-0407 The [***IT Environment***] shall [***allow only the administrator***] to include or exclude auditable events from the set of all auditable events based on the following attributes:

a) User identity;

b) Event type;

c) Object identity, host identity

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

d) Success of auditable security events;

e) Failure of auditable security events; and

f) No additional criteria

6.2.1.7 FAU_STG.1-NIAP-0429 Protected Audit Trail Storage

FAU_STG.1.1-NIAP-0429 The [***IT Environment***] shall [***restrict the deletion of***] stored audit records in the audit trail [***to the administrator***].

FAU_STG.1.2-NIAP-0429 The [***IT Environment***] shall be able to [prevent] modifications to the audit records in the audit trail.

6.2.1.8 FAU_STG.NIAP-0429-1 Site-configurable Prevention of audit data loss

FAU_STG.NIAP-0429-1.1 The [***IT Environment***] shall provide an authorized administrator with the capability to select one or more of the following actions [prevent auditable events except those taken by the authorized user with special rights, overwrite the oldest stored audit records] and no additional options to be taken if the audit trail is full.

FAU_STG.NIAP-0429-1.2 The [***IT Environment***] shall prevent auditable events except those taken by the authorized user with special rights and **no other action** if the audit trail is full and no other action has been selected.

6.2.2 Cryptographic Operations (FCS)

6.2.2.1 FCS_CRM_FPS_(EXT).1 FIPS compliant cryptographic module

FCS_CRM_FPS_(EXT).1.1 The IT environment shall provide all cryptographic modules necessary for the TSF.

FCS_CRM_FPS_(EXT).1.2 Each cryptographic module shall be FIPS 140 series Level 1 validated.

6.2.3 User Data Protection (FDP)

6.2.3.1 FDP_ACC.1:1 Subset access control – PKI Credential Management

FDP_ACC.1.1;1 The [***IT Environment***] shall enforce the [**PKI credential management SFP**] on

Subjects: **User**

Objects: [**cryptographic key, public key certificate**], **no additional objects**

Operations: Import, export, and delete public key certificate**, no additional operations.**

6.2.3.2 FDP_ACF.1-NIAP-0407 Security attribute based access control – PKI Credential Management

FDP_ACF.1.1-NIAP-0407 The [***IT Environment***] shall enforce the [**PKI credential management SFP**] to objects based on the following: list of subjects: [**all subjects**]; list of

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

objects:[**cryptographic keys and public key certificate**]; list of subject and object attributes: [**identity of subject and the set of roles that the subject is authorized to assume**] **key access rights.**

FDP_ACF.1.2-NIAP-0407 The [***IT Environment***] shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed public key certificates may be imported, exported, deleted by **owner.**

FDP_ACF.1.3-NIAP-0407 The [***IT Environment***] shall explicitly authorize access of subjects to objects based on the following additional rules: no other rules**.**

FDP_ACF.1.4-NIAP-0407 The [***IT Environment***] shall explicitly deny access of subjects to objects based on the following additional rules: no other rules**.**

6.2.3.3 FDP_RIP.2 Full residual information protection

FDP_RIP.2 The [***IT Environment***] shall ensure that any previous information content of a resource is made unavailable upon the allocation of the resource to all objects.

6.2.4 Identification and Authentication (FIA)

6.2.4.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The [***IT Environment***] shall detect when [an administrator configurable positive integer within] **the range of 3 to 10** unsuccessful authentication attempts occur related to **user authentication**.

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [met ***or*** surpassed], the [***IT Environment***] shall [**prevent all entities requesting authentication other than the administrator from performing activities that require authentication until an action is taken by the administrator**].

6.2.4.2 FIA_ATD.1 User Attribute Definition

FIA_ATD.1.1 The [***IT Environment***] shall maintain the following list of security attributes belonging to individual users: [**user ID, role**].

6.2.4.3 FIA_UAU.2 User authentication before any action

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

6.2.4.4 FIA_UAU.7 Protected authentication feedback

FIA_UAU.7.1 The [***IT Environment***] shall provide only **obscured feedback** to the user while the authentication is in progress.

6.2.4.5 FIA_UID.2 User identification before any action

FIA_UID.2.1 The [***IT Environment***] shall require each user to be successfully identified before allowing any other [***IT Environment***]-mediated actions on behalf of that user.

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

6.2.4.6 FIA_USB.1 User-subject binding

FIA_USB.1.1 The [***IT Environment***] shall associate the following user security attributes with subjects acting on behalf of that user: [**all user security attributes**].

FIA_USB.1.2 The [***IT Environment***] shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: [**none**].

FIA_USB.1.3 The [***IT Environment***] shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: [**none**].

6.2.5 FMT Security Management

6.2.5.1 FMT_MOF.1:1 Management of security functions behaviour – IT Environment

FMT_MOF.1.1;1 The [***IT Environment***] shall restrict the ability to disable, enable the functions [**audit,**] **and no other functions** to [**the administrator**].

6.2.5.2 FMT_MSA.1:1 Management of security attributes – IT Environment

FMT_MSA.1.1;1 The [***IT Environment***] shall enforce the [**PKI credential management SFP**] to restrict the ability to query, modify, delete the security attributes **user role, key identifier, association between private key and public key certificate** to **user**.

6.2.5.3 FMT_MSA.3-NIAP-0429 Static attributes initialization

FMT_MSA.3.1-NIAP-0429 The [***IT Environment***] shall enforce the [**PKI credential management SFP**] to provide [**specific**] default values for security attributes for security attributes that are used to enforce the SFP.

FMT_MSA.3.2-NIAP-0429 The [***IT Environment***] shall allow the administrator to specify alternative initial values to override the default values when an object or information is created.

6.2.5.4 FMT_MTD.1:1 Management of TSF data – I&A Data

FMT_MTD.1.1;1 The [***IT Environment***] shall restrict the ability to [**initialize and** modify] the [**identification data and authentication data**] to **administrator.**

6.2.5.5 FMT_MTD.1:2 Management of TSF data – Authentication Data

FMT_MTD.1.1;2 The [***IT Environment***] shall restrict the ability to [modify] the [**authentication data**] to **administrator and the user owning the account.**

6.2.5.6 FMT_MTD.1:3 Management of TSF data – I&A Attempts

FMT_MTD.1.1;3 The [***IT Environment***] shall restrict the ability to [**initialize and** modify] the [**number of unsuccessful authentication *attempts***] to **administrator.**

6.2.5.7 FMT_MTD.1:4 Management of TSF data – Trust Anchors

FMT_MTD.1.1;4 The [***IT Environment***] shall restrict the ability to [**add and** delete] the [**trust**

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

anchors] to **administrator.**

6.2.5.8 FMT_MTD.1:5 Management of TSF data – Time

FMT_MTD.1.1;5 The [***IT Environment***] shall restrict the ability to [**initialize and** modify] the [**system time**] to **administrator.**

6.2.5.9 FMT_SMF.1:1 Specification of management functions – IT Environment

FMT_SMF.1.1;1 The [***IT Environment***] shall be capable of performing the following management functions: [**audit management, user identity management, trust anchor management, system time management**], **no additional security management functions**.

6.2.5.10 FMT_SMR.1 Security roles

FMT_SMR.1.1 The [***IT Environment***] shall maintain the roles [**user, administrator**], **DBsign administrator**.

FMT_SMR.1.2 The [***IT Environment***] shall be able to associate users with roles.

6.2.6 Protection of TSF (FPT)

6.2.6.1 FPT_STM.1 Security roles

FPT_STM.1.1 The [***IT Environment***] shall be able to provide reliable time stamps ***for its own and TSF use***.

6.2.6.2 FPT_TST_SOF_(EXT).1 Security roles

FPT_TST_SOF_(EXT).1.1 The [***IT Environment***] shall provide administrator with the capability to verify the integrity of the following TSF data: ***none***.

FPT_TST_SOF_(EXT).1.2 The [***IT Environment***] shall provide administrator with the capability to verify the integrity of stored TSF executable code.

6.2.7 TOE Access (FTA)

6.2.7.1 FTA_SSL.1 TSF-initiated session locking

FTA_SSL.1.1 The [***IT Environment***] shall lock an interactive session after **an administrator configurable specified time interval of user inactivity** by:

a) clearing or overwriting display devices, making the current contents unreadable;

b) disabling any activity of the user's data access/display devices other than unlocking the session.

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

FTA_SSL.1.2 The [***IT Environment***] shall require the following events to occur prior to unlocking the session: [**authentication by the user**].

6.2.7.2 FTA_SSL.2 User-initiated locking

FTA_SSL.2.1 The [***IT Environment***] shall allow user-initiated locking of the user's own interactive session, by:

c) clearing or overwriting display devices, making the current contents unreadable;

d) disabling any activity of the user's data access/display devices other than unlocking the session.

FTA_SSL.2.2 The [***IT Environment***] shall require the following events to occur prior to unlocking the session: [**authentication by the user**].

6.2.7.3 FTA_TAB.1 Default TOE access banners

FTA_TAB.1.1 Before establishing a user session, the [***IT Environment***] shall display an advisory warning message regarding unauthorized use of the [***System***].

6.3 TOE Security Functional Requirements

All TOE security functional requirements included in this ST are listed in the following table. Extended SFRs are identified as "Part 2 extended" and their name ends with "_(EXT)" or a NIAP interpretation tag, such as "-NIAP-0407".

PP Package Name	SFR	Title	Part 2 or Extended
CPV – Basic	FDP_CPD_(EXT).1	Certification path development	Part 2 Extended
	FDP_DAU_CPI_(EXT).1	Certification path initialization – basic	Part 2 Extended
	FDP_DAU_CPV_(EXT).1	Certificate processing – basic	Part 2 Extended
	FDP_DAU_CPV_(EXT).2	Intermediate certificate processing – basic	Part 2 Extended
	FDP_DAU_CPO_(EXT).1	Certification path output – basic	Part 2 Extended
CPV – Basic Policy	FDP_DAU_CPI_(EXT).2	Certification path initialization – basic policy	Part 2 Extended
	FDP_DAU_CPO_(EXT).2	Certification path output – basic policy	Part 2 Extended
CPV – Policy Mapping	FDP_DAU_CPI_(EXT).3	Certification path initialization – policy mapping	Part 2 Extended
	FDP_DAU_CPV_(EXT).3	Intermediate certificate processing – policy mapping	Part 2 Extended
	FDP_DAU_CPO_(EXT).3	Certification path output – policy mapping	Part 2 Extended

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

PP Package Name	SFR	Title	Part 2 or Extended
CPV – Name Constraints	FDP_DAU_CPI_(EXT).4	Certification path initialization – names	Part 2 Extended
	FDP_DAU_CPV_(EXT).4	Certificate processing – name constraints	Part 2 Extended
	FDP_DAU_CPV_(EXT).5	Intermediate certificate processing – name constraints	Part 2 Extended
PKI Signature Generation	FDP_ETC_SIG_(EXT).1	Export of PKI Signature	Part 2 Extended
PKI Signature Verification	FDP_ITC_SIG_(EXT).1	Import of PKI Signature	Part 2 Extended
	FDP_DAU_SIG_(EXT).1	Signature Blob Verification	Part 2 Extended
OCSP Client	FDP_DAU_OCS_(EXT).1	Basic OCSP Client	Part 2 Extended
CRL Validation	FDP_DAU_CRL_(EXT).1	Basic CRL Checking	Part 2 Extended
Audit	FAU_GEN.1-NIAP-0407:2	Audit data generation - TOE	Part 2 Extended
	FAU_GEN.2-NIAP-0410:2	User identity association - TOE	Part 2 Extended
DBsign Features	FDP_ACC.1:2	Subset access control	Part 2
	FDP_ACF.1	Security attribute based access control	Part 2
	FIA_UAU_ENV_(EXT).1	Timing of authentication with a third party	Part 2 Extended
	FIA_UID_ENV_(EXT).1	Timing of identification with a third party	Part 2 Extended
	FMT_MOF.1:2	Management of security function behavior - TOE	Part 2
	FMT_MSA.1:2	Management of security attributes – User Policy	Part 2
	FMT_MSA.3	Static attribute initialization	Part 2
	FMT_SMF.1:2	Specification of management functions – IT Environment	Part 2

Table 25: Security Functional Requirements

6.3.1 Certification Path Validation – Basic Package

6.3.1.1 FDP_CPD_(EXT).1 Certification path development

FDP_CPD_(EXT).1.1 The TSF shall develop a certification path ***from the subscriber to*** ~~***from***~~ a trust anchor provided by [administrator] ~~***to the subscriber***~~ using matching rules for the following ***subscriber*** certificate fields or extensions:

a) distinguished name.

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

FDP_CPD_(EXT).1.2 The TSF shall develop the certification path using the following additional matching rule:

a) none..

FDP_CPD_(EXT).1.3 The TSF shall develop the certification path using the following additional matching rule:

a) none.

FDP_CPD_(EXT).1.4 The TSF shall bypass any matching rules except none if additional certification paths are required.

6.3.1.2 FDP_DAU_CPI_(EXT).1 Certification path initialization - basic

FDP_DAU_CPI_(EXT).1.1 The TSF shall use the trust anchor provided by administrator.

FDP_DAU_CPI_(EXT).1.2 The TSF shall obtain the time of interest called "TOI" from a reliable source local environment.

FDP_DAU_CPI_(EXT).1.3 The TSF shall perform the following checks on the trust anchor

a) none.

FDP_DAU_CPI_(EXT).1.4 The TSF shall derive from the trust anchor:

a) subject distinguished name,

b) subject public key,

c) subject public key algorithm object identifier,

d) subject public key parameters.

6.3.1.3 FDP_CPV_(EXT).1 Certificate processing - basic

FDP_DAU_CPV_(EXT).1.1 The TSF shall reject a certificate if any of the following checks fails:

a) Use parent-public-key, parent-public-key-algorithm-identifier, and parent-public-key-parameters to verify the signature on the certificate;

b) notBefore field in the trust anchor <= TOI;

c) notAfter field in the trust anchor => TOI;

d) issuer field in the certificate = parent-DN; or

e) TSF is able to process all extensions marked critical.

FDP_DAU_CPV_(EXT).1.2 The TSF shall bypass the revocation status check if the certificate contains no-check extension.

FDP_DAU_CPV_(EXT).1.3 The TSF shall bypass the revocation status check if the revocation information is not available and administrator overrides revocation checking.

ST Application Note: DBsign provides the ability for the administrator to enable or disable revocation checking. If revocation checking is disabled, DBsign does not check for revocation

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

information. If revocation checking is enabled and no revocation information is available, DBsign returns an error indicating that the revocation status is unknown.

FDP_DAU_CPV_(EXT).1.4 The TSF shall reject a certificate if the revocation status using CRL ***or*** OCSP demonstrates that the certificate is revoked.

ST Application Note: DBsign supports both CRL and OCSP revocation checking. If one succeeds, the other is not performed.

FDP_DAU_CPV_(EXT).1.5 The TSF shall update the public key parameters state machine using the following rules:

a) Obtain the parameters from the subjectPublickeyInfo filed of certificate if the parameters are presnt in the field; else

b) Retain the old parameters state if the subject public key algorithm of current certificate and parent public key algorithm of current certificate below to the same family of algorithms; else

c) Set parameters = "null".

6.3.1.4 FDP_DAU_CPV_(EXT).2 Intermediate certificate processing - basic

FDP_DAU_CPV_(EXT).2.1 The TSF shall reject an intermediate certificate if any of the following additional checks fails:

a) basicConstraints field is present with cA=TRUE;

b) pathLenConstraint is not violated; or

c) if a critical keyUsage extension is present, ,keyCertSign bit is set.

6.3.1.5 FDP_DAU_CPO_(EXT).1 Certification path output- basic

FDP_DAU_CPO_(EXT).1.1 The TSF shall ***~~output~~ provide for use internally*** certification path validation failure if any certificate in the certification path is rejected.

FDP_DAU_CPO_(EXT).1.2 The TSF shall ***~~output~~ provide for use internally*** the following variables from the end certificate: subject DN, subject public key algorithm identifier, subject public key, critical keyUsage extension

FDP_DAU_CPO_(EXT).1.3 The TSF shall ***~~output~~ provide for use internally*** the following additional variables from the end certificate certificate.

FDP_DAU_CPO_(EXT).1.4 The TSF shall ***~~output~~ provide for use internally*** the subject public key parameters from the certification path parameter state machine.

6.3.2 Certification Path Validation – Basic Policy Package

6.3.2.1 FDP_DAU_CPI_(EXT).2 Certification path initialization – basic policy

FDP_DAU_CPI_(EXT).2.1 The TSF shall use the initial-certificate-policies provided by **application developer**.

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

6.3.2.2 FDP_DAU_CPO_(EXT).2 Certification path output – basic policy

FDP_DAU_CPO_(EXT).2.1 The TSF shall ***~~output~~ provide for use internally*** the certificate policies using the following rule: intersection of certificatePolicies extensions in all the certificates in certification path and initial-certificate-policies.

6.3.3 Certification Path Validation –Policy Mapping Package

6.3.3.1 FDP_DAU_CPI_(EXT).3 Certification path initialization –policy mapping

FDP_DAU_CPI_(EXT).3.1 The TSF shall use the explicit-policy-indicator, policy-mapping-inhibit-indicator, inhibit-any-policy-indicator provided by **application developer**.

6.3.3.2 FDP_DAU_CPV_(EXT).3 Intermediate certificate processing - policy mapping

FDP_DAU_CPV_(EXT).3.1 The TSF shall use the intermediate certificate to update the following state variables in accordance with X.509 Standard::

a) explicit-policy-indicator;

b) policy-mapping-inhibit-indicator

c) inhibit-any-policy-indicator.

6.3.3.3 FDP_DAU_CPO_(EXT).3 Certification path output – policy mapping

FDP_DAU_CPO_(EXT).3.1 The TSF shall perform policy processing in accordance with X.509 standard.

FDP_DAU_CPO_(EXT).3.2 The TSF shall map policies in the calculation of the policies intersection if and only if policy-mapping-inhibit-indicator is not set.

FDP_DAU_CPO_(EXT).3.3 During the calculation of the policy intersection, the TSF shall match any-policy to all policies if and only if inhibit-any-policy-indicator is not set.

FDP_DAU_CPO_(EXT)3.4 The TSF shall ***~~output~~ provide for use internally*** certification path failure if the intersection of certificatePolicies (as modified by policy mapping and inhibit-any-policy) is null and explicit-policy-indicator is set.

FDP_DAU_CPO_(EXT).3.5 The TSF shall ***~~output~~ provide for use internally*** certification path failure if the intersection of certificatePolicies (as modified by policy mapping and inhibit-any-policy) and initial-certificate-policies is null and explicit-policy-indicator is set.

FDP_DAU_CPO_(EXT).3.6 The TSF shall ***~~output~~ provide for use internally*** policy mapping history.

FDP_DAU_CPO_(EXT).3.7 The TSF shall ***~~output~~ provide for use internally*** policy qualifiers applicable to output policies.

6.3.4 Certification Path Validation –Name Constraints Package

6.3.4.1 FDP_DAU_CPI_(EXT).4 Certification path initialization –names

FDP_DAU_CPI_(EXT).4.1 The TSF shall initialize the following: permitted-subtrees = ∞, excluded-

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

subtrees = Ø.

6.3.4.2 FDP_DAU_CPV_(EXT).4 Certificate processing – name constraints

FDP_DAU_CPV_(EXT).4.1 The TSF shall reject a certificate if any one of the following is not satisfied:

a) subject DN is in at least one of the permitted-subtrees for DN;

b) subject DN is in none of the excluded-subtrees for DN;

c) each hierarchical name form of type DN, RFC-822, URL in the subjectAlternateName field is in at least one of the permitted-subtrees for that name form; or

d) each hierarchical name from of type DN, RFC-822, URL in the subjectAlternateName field is in none of the excluded-subtrees for that name form.

6.3.4.3 FDP_DAU_CPV_(EXT).5 Intermediate Certificate processing – name constraints

FDP_DAU_CPV_(EXT).5.1 The TSF shall use the intermediate certificate to update the following states:

a) permitted-subtrees

b) excluded-subtrees.

6.3.5 PKI Signature Generation Package

6.3.5.1 FDP_ETC_SIG_(EXT).1 Export of PKI Signature

FDP_ETC_SIG_(EXT).1.1 The TSF shall invoke the cryptographic module with the user selected private key to generate digital signature.

FDP_ETC_SIG_(EXT).1.2 The TSF shall include the following information with the digital signature hashing algorithm, signature algorithm, ***signing time, and if configured by the administrator*** signer public key certificate, ***certificate chain, signed data***.

6.3.6 PKI Signature Verfication Package

6.3.6.1 FDP_ITC_SIG_(EXT).1 Import of PKI Signature

FDP_ITC_SIG_(EXT).1.1 The TSF shall use the following information from the signed data hashing algorithm, signature algorithm, ***signing time, and if so configured by the administrator*** signer public key certificate, ***certificate chain, signed data*** during signature verification.

6.3.6.2 FDP_DAU_SIG_(EXT).1 Export of PKI Signature

FDP_DAU_SIG_(EXT).1.1 The TSF shall invoke the cryptographic module with the following information from Certification Path Validation to verify digital signature on signed

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

data: subject public key algorithm, subject public key, subject public key parameters.

FDP_DAU_SIG_(EXT).1.2 The TSF shall verify that the KeyUsage extension output from the Certification Path Validation has the nonRepudiation or digital signature.

FDP_DAU_SIG_(EXT).1.3 The TSF shall apply the following additional checks **revocation checking**.

6.3.7 Online Certificate Status Protocol Client Package

6.3.7.1 FDP_DAU_OCS_(EXT).1 Basic OCSP Client

FDP_DAU_OCS_(EXT).1.1 The TSF shall formulate the OCSP requests in accordance with PKIX RFC 2560.

FDP_DAU_OCS_(EXT).1.2 The OCSP request shall contain the following extensions: none ***unless nonces are enabled by the administrator, then*** nonce.

FDP_DAU_OCS_(EXT).1.3 The TSF shall obtain the public key, algorithm, and public key parameters of the OCSP Responder from OCSP responder certificate..

FDP_DAU_OCS_(EXT).1.4 The TSF shall perform the following additional function establish trust in OCSP responder certificate using certification path validation – basic policy, certification path validation – policy mapping, certification path validation – name constraint.

FDP_DAU_OCS_(EXT).1.5 The TSF shall invoke the cryptographic module to verify signature on the OCSP response using trusted public key, algorithm, and public key parameters of the OCSP responder.

FDP_DAU_OCS_(EXT).1.6 The TSF shall verify that if the OCSP responder certificate contains extendedKeyUsage extension, the extension contains the PKIX OID for ocsp-signing or the anyExtendedKeyUsage OID.

FDP_DAU_OCS_(EXT).1.7 The TSF shall match the responderID in the OCSP response with the corresponding information in the responder certificate

FDP_DAU_OCS_(EXT).1.8 The TSF shall match the certID in a request with certID in singleResponse.

FDP_DAU_OCS_(EXT).1.9 The TSF shall reject the OCSP response for an entry if all of the following are true:

a) time checks are not overridden;

b) TOI > producedAt + x where x is provided by administrator;

c) TOI > thisUpdate for entry + x where x is provided by administrator; and

d) TOI > nextUpdate for entry + x if nextUpdate is present and where x is provided by administrator.

FDP_DAU_OCS_(EXT).1.10 The TSF shall permit none to override time checks.

FDP_DAU_OCS_(EXT).1.11 The TSF shall reject OCSP response if the response contains “critical”

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

extension(s) that TSF does not process.

FDP_DAU_OCS_(EXT).1.12 The TSF shall perform the following additional checks **none unless nonces are enabled by the administrator, then request nonce = response nonce**.

6.3.8 Certificate Revocation List (CRL) Validation Package

6.3.8.1 FDP_DAU_CRL_(EXT).1 Basic CRL Checking

FDP_DAU_CRL_(EXT).1.1 The TSF shall obtain the CRL from local cache, location pointed to by the CRL DP in public key certificate of interest.

FDP_DAU_CRL_(EXT).1.2 The TSF shall obtain the trusted public key, algorithm, and public key parameters of the CRL issuer.

FDP_DAU_CRL_(EXT).1.3 The TSF shall invoke the cryptographic module to verify signature on the CRL using trusted public key, algorithm, and public key parameters of the CRL issuer.

FDP_DAU_CRL_(EXT).1.4 The TSF shall verify that if a critical keyUsage extension is present in CRL issuer certificate, cRLSign bit in the extension is set in the certificate.

FDP_DAU_CRL_(EXT).1.5 The TSF shall match the issuer field in the CRL with what it assumes to be the CRL issuer.

FDP_DAU_CRL_(EXT).1.6 The TSF shall reject the CRL if all of the following are true:

a) Time check are not overridden;

b) TOI > thisUpdate + x where x is provided by, administrator; and

c) TOI > nextUpdate + x if nextUpdate is present and where x is provided by administrator.

FDP_DAU_CRL_(EXT).1.7 The TSF shall permit none to override time checks.

FDP_DAU_CRL_(EXT).1.8 The TSF shall reject CRL if the CRL contains “critical” extension(s) that TSF does not process.

FDP_DAU_CRL_(EXT).1.9 The TSF shall perform the following additional checks none.

6.3.9 Audit Package

6.3.9.1 FAU_GEN.1-NIAP-0407:2 Audit data generation - TOE

FAU_GEN.1.1-NIAP-0407;2 The TSF shall be able to generate an audit record of the following auditable events:

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

b) All auditable events listed in Table 26; and

c) **No additional events**.

FAU_GEN.1.2-NIAP-0407;2 The TSF shall record within each audit record at least the following

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

information:

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

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, information specified in column three of Table 26 below.

SFR	Auditable Events	Additional Audit Record Contents
FDP_CPD_(EXT).1	Success or failure to build path	For success, matching rules bypassed
FDP_DAU_CPI_(EXT).1	None	
FDP_DAU_CPV_(EXT).1	Success or failure of certificate processing Bypass of revocation status checking	For failure, reason(s) for failure
FDP_DAU_CPV_(EXT).2	Success or failure of certificate processing	For failure, reasons for failure
FDP_DAU_CPO_(EXT).1	None	
FDP_DAU_CPI_(EXT).2	None	
FDP_DAU_CPO_(EXT).2	None	
FDP_DAU_CPI_(EXT).3	None	
FDP_DAU_CPV_(EXT).3	None	
FDP_DAU_CPO_(EXT).3	Success or failure	
FDP_DAU_CPI_(EXT).4	None	
FDP_DAU_CPV_(EXT).4	Success or failure	
FDP_DAU_CPV_(EXT).5	None	
FDP_ETC_SIG_(EXT).1	Invocation of the function	
FDP_ITC_SIG_(EXT).1	***Invocation of the function***	
FDP_DAU_SIG_(EXT).1	Success or failure	In case of failure, reason for failure
FDP_DAU_OCS_(EXT).1	Rejection of OCSP response Override time checks	Reason for rejection
FDP_DAU_CRL_(EXT).1	Rejection of CRL Override time checks	Reason for rejection
FAU_GEN.1-NIAP-0407:2	None	
FAU_GEN.2-NIAP-0410:2	None	
FDP_ACF.1	All requests to perform an operation using a certificate or digital signature template that fail due to the User Policy	
FIA_UAU_ENV_(EXT).1	All use of the authentication	

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

SFR	Auditable Events	Additional Audit Record Contents
	mechanism in the IT environment	
FIA_UID_ENV_(EXT).1	All use of the identification mechanism in the IT environment	
FMT_MOF.1:2	All modifications in behaviour of the functions of the TSF.	
FMT_MSA.1:2	Modifications of the values of security attributes.	
FMT_MSA.3	Modifications of the default setting.	

Table 26: TOE Auditable Events

6.3.9.2 FAU_GEN.2-NIAP-0410:2 User identity association - TOE

FAU_GEN.2.1-NIAP-0410;2 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the user that caused that event.

6.3.10 DBsign Additional SFRs

6.3.10.1 FDP_ACC.1:2 Subset access control

FDP_ACC.1.1:2 The TSF shall enforce the **User Policy** on.

- **Subjects: client users**
- **Objects: certificates, digital signature templates**
- **Operations: sign**

6.3.10.2 FDP_ACF.1 Security attribute based access control

FDP_ACF.1.1 The TSF shall enforce the **User Policy** to objects based on the following.

- **Client user subjects: user name, active flag, list of allowed certificate/security level pairs**
- **Certificate object: security level**
- **Digital Signature Template object: security level**

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

a) If the User Policy feature is not enabled, permit access

b) If the User Policy feature is enabled, the client user subject's active flag is not set to "N" and the security level of the template is higher than the security level of the user's certificate, allow the user to sign access

c) If the User Access Control feature is enabled, the client user subject's

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

active flag is not set to "N", and the subject user identity is included in the list of authorized user identities associated with the object, permit access

d) **Else deny access**.

FDP_ACF.1.3 The TSF shall explicitly authorize access of subjects to objects based on the following additional rules: **the User Access Control feature is not enabled**:

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following additional rules: **the client user subject's active flag is set to "N"**:

6.3.10.3 FIA_UAU_ENV_(EXT).1 Timing of Authentication with a third party

FIA_UAU_ENV_(EXT).1.1 The TSF shall allow **all actions, except use of the Administration Tools identified in Section 7.3** on behalf of the user to be performed before the user is authenticated by the IT environment.

FIA_UAU_ENV_(EXT).1.2 The TSF shall require each user to be successfully authenticated by the IT environment before allowing any other TSF-mediated actions on behalf of that user.

6.3.10.4 FIA_UID_ENV_(EXT).1 Timing of Identification with a third party

FIA_UID_ENV_(EXT).1.1 The TSF shall allow **all actions, except use of the Administration Tools identified in Section 7.3** on behalf of the user to be performed before the user is identified by the IT environment.

FIA_UID_ENV_(EXT).1.2 The TSF shall require each user to be successfully identified by the IT environment before allowing any other TSF-mediated actions on behalf of that user.

6.3.10.5 FMT_MOF.1:2 Management of security functions behaviour – TOE

FMT_MOF.1.1;2 The TSF shall restrict the ability to determine the behaviour of, disable, enable, modify the behaviour of the functions

a) Manage the DBsign signature templates which are used to define how DBsign operates on data in the RDBMS

b) Modify the descriptions of the DBsign security levels

c) Configure the DBsign User Policy feature

d) Configure the list of certificate authorities DBsign trusts to issue certificates to end users

e) Configure the audit log settings

f) Manage the certificates and CRLs that DBsign stores in the RDBMS

g) Configure the list of OCSP responders DBsign trusts to provide certificate revocation status information

h) Create and populate the DBsign System Tables with initial data

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

to **the DBsign administrator**.

6.3.10.6 FMT_MSA.1;2 Management of security attributes – User Policy

FMT_MSA.1.1;2 The TSF shall enforce the **User Policy** to restrict the ability to modify, delete, **create** the security attributes **User Policy security attributes** to **DBsign administrator**.

6.3.10.7 FMT_MSA.3 Static Attributes Initialization

FMT_MSA.3.1 The TSF shall enforce the **User Policy** to provide restrictive default values for security attributes that are used to enforce the SFP.

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

6.3.10.8 FMT_SMF.1:2 Specification of management functions – IT Environment

FMT_SMF.1.1;2 The TSF shall be capable of performing the following management functions:

a) Manage the DBsign signature templates which are used to define how DBsign operates on data in the RDBMS

b) Modify the descriptions of the DBsign security levels

c) Configure the DBsign User Policy feature (enable, disable, define/query/edit DBsign user definition, specify user's certificates)

d) Configure the list of certificate authorities DBsign trusts to issue certificates to end users

e) Configure the audit log settings

f) Manage the certificates and CRLs that DBsign stores in the RDBMS

g) Configure the list of OCSP responders DBsign trusts to provide certificate revocation status information

h) Create and populate the DBsign System Tables with initial data

6.4 TOE Security Assurance Requirements

The Security assurance requirements (SARs) provide grounds for confidence that the TOE meets its security objectives (for example, configuration management, testing, and vulnerability assessment).

This TOE claims Basic Robustness assurance as defined in the PP. A Basic Robustness TOE is considered sufficient for low threat environments or where compromise of protected information will not have a significant impact on mission objectives. This implies that the motivation of the threat agents will be low in environments that are suitable for TOEs of this robustness. In general, basic robustness results in "good commercial practices" that counter threats based in casual and accidental disclosure or compromise of data protected by the TOE. The basic

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

robustness assurance requirements are based on this principle and consist of EAL 2 augmented with the following addition:

- ALC_FLR.2 Flaw Reporting Procedures

The following table provides a list of the assurance requirements needed for Basic Robustness. These Security Assurance Requirements are drawn from the CC, Part 3, Version 3.1, Revision 3, July 2009.

Assurance Class	Assurance Component ID	Assurance Component Name
ADV: Development	ADV_ARC.1	Security architecture description
	ADV_FSP.2	Security-enforcing functional specification
	ADV_TDS.1	Basic design
AGD: Guidance documents	AGD_OPE.1	Operational user guidance
	AGD_PRE.1	Preparative procedures
ALC: Life-cycle support	ALC_CMC.2	Use of a CM System
	ALC_CMS.2	Parts of the TOE CM coverage
	ALC_DEL.1	Delivery procedures
	ALC_FLR.2	Flaw reporting procedures
ASE: Security Target evaluation	ASE_CCL.1	Conformance claims
	ASE_ECD.1	Extended components definition
	ASE_INT.1	ST introduction
	ASE_OBJ.2	Security objectives
	ASE_REQ.2	Derived security requirements
	ASE_SPD.1	Security problem definition
	ASE_TSS.1	TOE summary specification
ATE: Tests	ATE_COV.1	Evidence of coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent testing – sample
AVA: Vulnerability assessment	AVA_VAN.2	Vulnerability analysis

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

Table 27: Security Assurance Requirements

6.5 Security Requirements Rationale

6.5.1 IT Environment Dependency Rationale

This section includes a table of all IT environment SFRs and their associated dependencies. All dependencies are satisfied.

Requirement	Dependencies
FAU_GEN.1-NIAP-0407:1	FPT_STM.1
FAU_GEN.2-NIAP-0410:1	FAU_GEN.1 (met by FAU_GEN.1-NIAP-0407:1) FIA_UID.1 (met by FIA_UID.2)
FAU_SAR.1	FAU_GEN.1 (met by FAU_GEN.1-NIAP-0407:1)
FAU_SAR.2	FAU_SAR.1
FAU_SAR.3	FAU_SAR.1
FAU_SEL.1-NIAP-0407	FAU_GEN.1 (met by FAU_GEN.1-NIAP-0407:1) FMT_MTD.1
FAU_STG.1-NIAP-0429	FAU_GEN.1 (met by FAU_GEN.1-NIAP-0407:1)
FAU_STG.NIAP-0429-1	FAU_STG.1 (met by FAU_STG.1-NIAP-0429) FMT_MTD.1
FCS_CRM_FPS_(EXT).1	None
FDP_ACC.1:1	FDP_ACF.1 (met by FDP_ACF.1-NIAP-0407)
FDP_ACF.1-NIAP-0407	FDP_ACC.1 FMT_MSA.3 (met by FMT_MSA.3-NIAP-0429)
FDP_RIP.2	None
FIA_AFL.1	FIA_UAU.1 (met by FIA_UAU.2)
FIA_ATD.1	None
FIA_UAU.2	FIA_UID.1 (met by FIA_UID.2)
FIA_UAU.7	FIA_UAU.1 (met by FIA_UAU.2)
FIA_UID.2	None
FIA_USB.1	FIA_ATD.1
FMT_MOF.1:1	FMT_SMF.1 (satisfied by FMT_SMF.1:1) FMT_SMR.1
FMT_MSA.1:1	FMT_SMF.1 (satisfied by FMT_SMF.1:1) FMT_SMR.1 FDP_ACC.1 or FDP_IFC (satisfied by FDP_ACC.1:1)

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

Requirement	Dependencies
FMT_MSA.3-NIAP-0429	FMT_MSA.1 FMT_SMR.1
FMT_MTD.1:1 through 5	FMT_SMF.1 (satisfied by FMT_SMF.1:1) FMT_SMR.1
FMT_SMF.1:1	None
FMT_SMR.1	FIA_UID.1 (met by FIA_UID.2)
FPT_STM.1	None
FPT_TST_SOF_(EXT).1	None
FTA_SSL.1	FIA_UAU.1 (met by FIA_UAU.2)
FTA_SSL.2	FIA_UAU.1 (met by FIA_UAU.2)
FTA_TAB.1	None

6.5.2 TOE Dependency Rationale

This section includes a table of all the TOE security functional requirements and their associated dependencies. All dependencies are satisfied by TOE or IT environment SFRs.

Requirement	Dependencies
CPV – Basic Package	
FDP_CPD_(EXT).1	None
FDP_DAU_CPI_(EXT).1	FCS_COP.1 (met by FCS_CRM_FPS_(EXT).1) FPT_STM.1
FDP_DAU_CPV_(EXT).1	FCS_COP.1 (met by FCS_CRM_FPS_(EXT).1) FPT_STM.1 FDP_DAU_OCS_(EXT).1 or FDP_DAU_CRL_(EXT).1
FDP_DAU_CPV_(EXT).2	FDP_DAU_CPV_(EXT).1
FDP_DAU_CPO_(EXT).1	FDP_DAU_CPV_(EXT).1
CPV – Basic Policy Package	
FDP_DAU_CPI_(EXT).2	FDP_DAU_CPI_(EXT).1 (See Note 1)
FDP_DAU_CPO_(EXT).2	FDP_DAU_CPO_(EXT).1 (See Note 1)
CPV – Policy Mapping Package	
FDP_DAU_CPI_(EXT).3	FDP_DAU_CPI_(EXT).2 (See Note 2)
FDP_DAU_CPV_(EXT).3	FDP_DAU_CPV_(EXT).2 (See Note 3)
FDP_DAU_CPO_(EXT).3	FDP_DAU_CPO_(EXT).2 (See Note 2)

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

Requirement	Dependencies
CPV – Name Constraints Package	
FDP_DAU_CPI_(EXT).4	FDP_DAU_CPI_(EXT).1 (See Note 1)
FDP_DAU_CPV_(EXT).4	FDP_DAU_CPV_(EXT).1 (See Note 1)
FDP_DAU_CPV_(EXT).5	FDP_DAU_CPV_(EXT).2 (See Note 1)
PKI Signature Generation Package	
FDP_ETC_SIG_(EXT).1	FCS_CRM_FPS_(EXT).1
PKI Signature Verification Package	
FDP_ITC_SIG_(EXT).1	None
FDP_DAU_SIG_(EXT).1	FCS_CRM_FPS_(EXT).1 FDP_DAU_CPO_(EXT).1 (See Note 1)
Online Certificate Status Protocol Client Package	
FDP_DAU_OCS_(EXT).1	FCS_CRM_FPS_(EXT).1 FPT_STM.1
Certificate Revocation List (CRL) Validation Package	
FDP_DAU_CRL_(EXT).1	FCS_CRM_FPS_(EXT).1 FPT_STM.1
Audit Package	
FAU_GEN.1-NIAP-0407:2	FPT_STM.1
FAU_GEN.2-NIAP-0410:2	FAU_GEN.1 (met by FAU_GEN.1-NIAP-0407:2) FIA_UID.1 (met by FIA_UID.2 in the IT Environment)
DBsign Additional SFRs	
FDP_ACC.1:2	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3
FIA_UAU_ENV_(EXT).1	FIA_UID.1 or FIA_UID_ENV_(EXT).1
FIA_UID_ENV_(EXT).1	None
FMT_MOF.1:2	FMT_SMF.1 (satisfied by FMT_SMF.1:2) FMT_SMR.1 (met by FMT_SMR.1 in the IT Environment)
FMT_MSA.1:2	FMT_SMF.1 (satisfied by FMT_SMF.1:2) FMT_SMR.1 FDP_ACC.1 or FDP_IFC (satisfied by FDP_ACC.1:2)
FMT_MSA.3	FMT_MSA.1 (met by FMT_MSA.1:2 in the IT Environment) FMT_SMR.1 (met by FMT_SMR.1 in the IT Environment)
FMT_SMF.1:2	None

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

Note 1: The dependency is satisfied by including the CPV – Basic Package

Note 2: The dependency is satisfied by including the CPV – Basic Policy Package

Note 3: The dependency is satisfied by including the CPV – Basic Package and the CPV – Basic Policy Package.

6.5.3 IT Environment SFR Tracings and Rationale

Objective	SFRs
OE.AUDIT_GENERATION	FAU_GEN.1-NIAP-0407:1 FAU_GEN.2-NIAP-0410:1 FIA_USB.1 FAU_SEL.1-NIAP-0407
OE.AUDIT_PROTECTION	FAU_SAR.2 FAU_STG.1-NIAP-0429 FAU_STG.NIAP-0429-1 FMT_MOF.1:1
OE.AUDIT_REVIEW	FAU_SAR.1 FAU_SAR.3
OE.Configuration	AGD_PRE.1
OE.CORRECT_TSF_OPERATION	FPT_TST_SOF_(EXT).1 ATE_COV.1 ATE_IND.1 ATE_FUN.1;
OE.CRYPTOGRAPHY	FCS_CRM_FPS_(EXT).1
OE.DISPLAY_BANNER	FTA_TAB.1
OE.Basic	AVA_VAN.2
OE.MANAGE	FMT_MOF.1:1 FMT_MSA.1:1 FMT_MSA.3-NIAP-0429 FMT_MTD.1:1 FMT_MTD.1:2 FMT_MTD.1:3 FMT_MTD.1:4 FMT_MTD.1:5 FMT_SMF.1:1 FMT_SMR.1
OE.MEDIATE	FDP_ACC.1 FDP_ACF.1-NIAP-0407
OE.NO_EVIL	AGD_OPE.1

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

Objective	SFRs
OE.PHYSICAL	AGD_PRE.1
OE.RESIDUAL_INFORMATION	FDP_RIP.2
OE.SELF_PROTECTION	ADV_ARC.1
OE.TIME_STAMPS	FPT_STM.1 FMT_SMF.1:1 FMT_MTD.1:5
OE.TIME_TOE	FPT_STM.1
OE.TOE_ACCESS	FIA_AFL.1 FIA_ATD.1 FIA_UID.2 FIA_UAU.2 FIA_UAU.7 FTA_SSL.1 FTA_SSL.2
OE.TOE_PROTECTION	ADV_ARC.1

OE.AUDIT_GENERATION state that the IT Environment will provide the capability to detect and create records of security-relevant events associated with users. This objective is satisfied by the following requirements:

- **FAU_GEN.1-NIAP-0407:1**defines the set of events that the IT Environment must be capable of recording. This requirement ensures that the Administrator has the ability to audit any security relevant event that takes place in the TOE. This requirement also defines the information that must be contained in the audit record for each auditable event. This requirement also places a requirement on the level of detail that is recorded on any additional security functional requirements an ST author adds to this PP.
- **FAU_GEN.2-NIAP-0410:1** ensures that the audit records associate a user identity with the auditable event.
- **FIA_USB.1** plays a role is satisfying this objective by requiring a binding of security attributes associated with users that are authenticated with the subjects that represent them in the IT Environment. This only applies to authorized users, since the identity of unauthenticated users cannot be confirmed. Therefore, the audit trail may not always have the proper identity of the subject that causes an audit record to be generated.
- **FAU_SEL.1-NIAP-0407** allows the Administrator to configure which auditable events will be recorded in the audit trail. This provides the administrator with the flexibility in recording only those events that are deemed necessary by site policy, thus reducing the amount of resources consumed by the audit mechanism

OE.AUDIT_PROTECTION states that the IT Environment will provide the capability to protect audit information. This objective is satisfied by the following requirements:

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

- **FAU_SAR.2** restricts the ability to read the audit trail to the Administrator, thus preventing the disclosure of the audit data to any other user. However, the IT Environment is not expected to prevent the disclosure of audit data if it has been archived or saved in another form (e.g., moved or copied to an ordinary file).

- **FAU_STG.1-NIAP-0429; FAU_STG.NIAP-0429-1:** The **FAU_STG** family dictates how the audit trail is protected. **FAU_STG.1-NIAP-0429** restricts the ability to delete audit records to the administrator. **FAU_STG.NIAP-0429-1** defines the actions that must be available to the administrator, as well as the action to be taken if there is no response. This helps to ensure that audit records are kept until the administrator deems they are no longer necessary. This requirement also ensures that no one has the ability to modify audit records (e.g., edit any of the information contained in an audit record). This ensures the integrity of the audit trail is maintained.

- **FMT_MOF.1:!** restricts the capability to modify the behavior of the audit function to the administrator. This requirement ensures that only administrator can turn audit on or off, this ensuring users actions are audited according to a site defined policy.

OE.AUDIT_REVIEW states that the IT Environment will provide the capability to selectively view audit information. This objective is satisfied by the following requirements:

- **FAU_SAR.1** provides the administrator with the capability to read all the audit data contained in the audit trail. This requirement also mandates the audit information be presented in a manner that is suitable for the administrator to interpret the audit trail, which is subject to interpretation. It is expected that the audit information be presented in such a way that the administrator can examine an audit record and have the appropriate information (that required by FAU_GEN.2) presented together to facilitate the analysis of the audit review

- **FAU_SAR.3** complements FAU_SAR.1 by providing the administrator the flexibility to specify criteria that can be used to search or sort the audit records residing in the audit trail. FAU_SAR.3 requires the administrator be able to establish the audit review criteria based on a user ID and source subject identity, so that the actions of a user can be readily identified and analyzed.

OE.Configuration states that the TOE shall be installed and configured properly for starting up the TOE in a secure state. This objective covers A.Configuration, an assumption that states that the TOE will be properly installed and configured. This objective is supported by:

- The startup and installation guides required by the **AGD_PRE.1** assurance requirement, which states that accurate installation and configuration documentation must be provided that allows the TOE to be properly (i.e., in a secure state) installed and configured.

OE.CORRECT_TSF_OPERATION states that the IT Environment will provide the capability to test the TSF to ensure the correct operation of the TSF at a customer's site.

- **FPT_TST_SOF_(EXT).1** is necessary to ensure the correctness of the TSF configuration files and TSF data and executable. If TSF software is corrupted it is possible that the TSF would no longer be able to enforce the security policies. This also holds true for TSF data, if TSF data is corrupted, the TOE may not correctly enforce its

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

security policies.

- **ATE** security assurance requirements will provide assurance that the TOE has been tested to ensure the correct operation of the TSF. Work units for **ATE_COV.1**, **ATE_FUN.1**, and **ATE_IND.1** will demonstrate that the TOE testing contained enough coverage to test TOE TSF functionality.

OE.CRYPTOGRAPHY states that the TOE shall use NIST FIPS 140-2 validated cryptographic services provided by the IT Environment. This objective is satisfied by the following requirements:

- **FCS_CRM_FPS_(EXT).1**, FIPS compliant cryptographic module, which requires that the IT Environment shall provide all cryptographic modules necessary for the TSF and that each cryptographic module shall be FIPS 140 series Level 1 validated.

OE.DISPLAY_BANNER states that the IT Environment will display an advisory warning regarding use of the TOE. This objective is satisfied by the following requirements:

- **FTA_TAB.1** meets this objective by requiring the IT Environment to display an administrator defined banner before a user can establish an authenticated session. This banner is under complete control of the administrator in which they specify any warnings regarding unauthorized use of the TOE and remove any product or version information if they desire.

OE.Basic states that the TOE shall be designed and implemented for a minimum attack potential of "Basic" as validated by the vulnerability analysis. This objective covers the vulnerability analysis (**AVA_VAN.2**).

OE.MANAGE states that the IT Environment will provide all the functions and facilities necessary to support the administrators in their management of the security of the TOE, and restrict these functions and facilities from unauthorized use. This objective is satisfied by the following requirements:

- **FMT_MOF.1:1** requires that the ability to use particular TOE capabilities be restricted to the Administrator.
- **FMT_MSA.1:1** requires that the ability to perform operations on security attributes be restricted to particular roles.
- **FMT_MSA.3-NIAP-0429** requires that default values used for security attributes are restrictive, and that the Administrator has the ability to override those values.
- **FMT_MTD.1:1, FMT_MTD.1:2, FMT_MTD.1:3, FMT_MTD.1:4, and FMT_MFT.1:5** require that the ability to manipulate IT Environment and TOE data is restricted to Administrators and authorized users.
- **FMT_SMF.1:1** requires that appropriate administrators manage the audit and other functions.
- **FMT_SMR.1** defines the specific security roles to be supported to perform the functions listed in the list above.

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

OE.MEDIATE states that the IT Environment will protect user data in accordance with its security policy. This objective is satisfied by the following requirements:

- **FDP_ACC.1:1** defines that an Access Control policy that will be enforced on a list of subjects acting on the behalf of users attempting to gain access to a list of named objects. All the operations between subject and object covered are defined by the policy. The "subjects" are generally the IT Environment's "Agents." The "named objects" are things that the IT Environment is protecting for itself and for the TOE
- **FDP_ACF.1-NIAP-0407** defines the Security Attribute used to provide Access Control to objects based on the following above Access Control policy and access control rules based on those security attributes.

OE.NO_EVIL states that sites using the TOE will ensure that administrators are non-hostile, appropriately trained and follow all administrator guidance. This objective is supported by:

- The user guidance document as defined under assurance requirements **AGD_OPE.1**.

OE.PHYSICAL states that the non-IT environment will provide an acceptable level of physical security so that the TOE cannot be tampered with or be subject to side channel attacks such as the various forms of power analysis and timing analysis. This objective is supported by:

- The preparative procedures as defined under assurance requirements **AGD_PRE.1**. The user guidance defines the security policy for the installation and operation of the TOE.

OE.RESIDUAL_INFORMATION which states that the IT Environment will ensure that any information contained in a protected resource within its Scope of Control is not released when the resource is reallocated. This objective is satisfied by the following requirements:

- **FDP_RIP.2** is used to ensure the contents of resources are not available to subjects other than those explicitly granted access to the data.

OE.SELF_PROTECTION which states that the IT Environment will maintain a domain for its own execution that protects it and its resources from external interference, tampering, or unauthorized disclosure. This objective is satisfied by the following requirements:

- **ADV_ARC.1** provides an architecture that ensures that the IT Environment makes policy decisions on all interfaces that perform operations on subjects and objects that are scoped by the policies. Without this non-bypassability requirement, the IT Environment could not be relied upon to completely enforce the security policies, since an interface(s) may otherwise exist that would provide a user with access to TOE resources (including TSF data and executable code) regardless of the defined policies. This includes controlling the accessibility to interfaces, as well as what access control is provided within the interfaces. **ADV_ARC.1** will also provides an architecture that ensure the IT Environment provides a domain that protects itself from untrusted users. If the IT Environment cannot protect itself it cannot be relied upon to enforce its security policies.

OE.TIME_STAMPS states that the IT Environment will provide reliable time stamps and the capability for the administrator to set the time used for these time stamps. This objective is satisfied by the following requirements:

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

- **FPT_STM.1** requires that the IT Environment provide time stamps for its own use and for the TOE use.
- **FMT_SMF.1:1** requires that the IT Environment provide an administrator with the capability to modify system time.
- **FMT_MTD.1:5** requires that the IT Environment restrict the capability to modify system time to an administrator.

OE.TIME_TOE states that The IT Environment will provide reliable time for the TOE use. This objective is satisfied by the following requirements:

- **FPT_STM.1** requires that the IT Environment provide time stamps for its own use and for the TOE use.

OE.TOE_ACCESS states that the IT Environment will provide mechanisms that control a user's logical access to the TOE. This objective is satisfied by the following requirements:

- **FIA_AFL.1** provides a detection mechanism for unsuccessful authentication attempts by the users. The requirement enables an administrator settable threshold that prevents unauthorized users from gaining access to authorized user's account by guessing authentication data by locking the targeted account. Thus, limiting an unauthorized user's ability to gain unauthorized access to the TOE.
- **FIA_ATD.1** defines the attributes of users, including a user ID that is used to by the IT Environment to determine a user's identity and enforce what type of access the user has to the IT Environment (e.g., the IT Environment associates a user ID with any role(s) they may assume).
- **FIA_UID.2** requires that a user be identified to the IT Environment in order to do anything.
- **FIA_UAU.2** requires that a user be authenticated by the IT Environment in order to do anything.
- **FIA_UAU.7** provides that the authentication data provided by the user is not echoed back in plaintext, thus serving to protect that data.
- **FTA_SSL.1 and FTA_SSL.2** components deal with automatic session locking and termination, either initiated by the IT Environment or a user. They protect from an unauthorized entity to use the unattended session.

OE.TOE_PROTECTION states that the IT Environment will protect the TOE and TOE resources from external interference, tampering, or unauthorized disclosure and modification. This objective is satisfied by the following requirements:

- **ADV_ARC.1** provides an architecture that ensures that the IT Environment provides a domain that protects TSF from untrusted users. If the TSF cannot be protected, it cannot be relied upon to enforce its security policies.

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

6.5.4 TOE SFR Tracings and Rationale

Objective	SFRs
Mapping for CPV – Basic Package	
O.Availability	FDP_DAU_CPV_(EXT).1
O.Correct_Temporal	FDP_DAU_CPI_(EXT).1
O.Current_Certificate	FDP_DAU_CPV_(EXT).1
O.Get_KeyInfo	FDP_DAU_CPO_(EXT).1
O.Path_Find	FDP_CPD_(EXT).1
O.Trusted_Keys	FDP_DAU_CPI_(EXT).1
O.User	FDP_DAU_CPV_(EXT).2
O.Verified_Certificate	FDP_DAU_CPV_(EXT).1
O.Valid_Certificate	FDP_DAU_CPV_(EXT).1
Mapping for CPV – Basic Policy Package	
O.Provide_Policy_Info	FDP_DAU_CPV_(EXT).2 FDP_DAU_CPO_(EXT).2
Mapping for CPV –Policy Mapping Package	
O.Map_Policies	FDP_DAU_CPI_(EXT).3 FDP_DAU_CPV_(EXT).3 FDP_DAU_CPO_(EXT).3
O.Policy_Enforce	FDP_DAU_CPI_(EXT).3 FDP_DAU_CPV_(EXT).3 FDP_DAU_CPO_(EXT).3
Mapping for CPV – Name Contraints Package	
O.Authorised_Names	FDP_DAU_CPI_(EXT).4 FDP_DAU_CPV_(EXT).4 FDP_DAU_CPV_(EXT).5
Mapping for PKI Signature Generation Package	
O.Give_Sig_Hints	FDP_ETC_SIG_(EXT).1
Mapping for PKI Signature Verification Package	
O.Use_Sig_Hints	FDP_ITC_SIG_(EXT).1
O.Linkage_Sig_Ver	FDP_DAU_SIG_(EXT).1

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

Objective	SFRs
Mapping for Online Certificate Status Protocol (OCSP) Client Package	
O.Accurate_OCSP_Info	FDP_DAU_OCS_(EXT).1
O.Auth_OCSP_Info	FDP_DAU_OCS_(EXT).1
O.Current_OCSP_Info	FDP_DAU_OCS_(EXT).1
O.User_Override_Time_OCSP	FDP_DAU_OCS_(EXT).1
Mapping for Certificate Revocation List (CRL) Validation Package	
O.Accurate_Rev_Info	FDP_DAU_CRL_(EXT).1
O.Auth_Rev_Info	FDP_DAU_CRL_(EXT).1
O.Current_Rev_Info	FDP_DAU_CRL_(EXT).1
O.User_Override_Time_CRL	FDP_DAU_CRL_(EXT).1
Mapping for Audit Package	
O.PKE_Audit	FAU_GEN.1-NIAP-0407:2 FAU_GEN.2-NIAP-0410:2
Mapping for DBsign Additional SFRs	
O.ACCESS	FDP_ACC.1:2 FDP_ACF.1
O.MANAGE	FIA_UAU_ENV_(EXT).1 FIA_UID_ENV_(EXT).1 FMT_MOF.1:2 FMT_MSA.1:2 FMT_MSA.3 FMT_SMF.1:2

Table 28: Mappings between TOE SFRs and Security Objectives

6.5.4.1 Security Objectives Rationale for CPV - Basic Package

O.Availability states that the TSF shall continue to provide security services even if revocation information is not available. This objective is met by:

- **FDP_DAU_CPV_(EXT).1**, Certificate processing – basic, which requires that the TSF bypass the revocation check if the revocation information is not available.

O.Correct_Temporal states that the TSF shall provide accurate temporal validation results. This objective is met by:

- **FDP_DAU_CPI_(EXT).1**, Certification path initialisation – basic, which requires that the TSF obtain the time of interest called “TOI" from a reliable source.

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

O.Current_Certificate states that the TSF shall only accept certificates that are not expired as of TOI. This objective is met by:

- **FDP_DAU_CPV_(EXT).1**, which requires that the TSF accept a certificate only if the specified checks succeed, including that the certificate is not expired as of TOI.

O.Get_KeyInfo states that the TSF shall provide the user public key and related information in order to carry out cryptographic functions. This objective is met by:

- **FDP_DAU_CPO_(EXT).1**, Certification path output – basic, which requires that the TSF output the subject public key from the certification path and other information specified by the ST author.

O.Path_Find states that the TSF shall be able to find a certification path from a trust anchor to the subscriber. This objective is met by:

- **FDP_CPD_(EXT).1**, Certification path development, which requires that the TSF shall develop a certification path from a trust anchor to the subscriber.

O.Trusted_Keys states that the TSF shall use trusted public keys in certification path validation. This objective is met by:

- **FDP_DAU_CPI_(EXT).1**, Certification path initialisation -- basic, which requires that the TSF use trusted public keys in the certification path validation.

O.User states that the TSF shall only accept certificates issued by a CA. This objective is met by:

- **FDP_DAU_CPV_(EXT).2**, Intermediate certificate processing – basic, which requires that the TSF accept an intermediate certificate only when the certificate is issued by a CA.

O.Verified_Certificate states that the TSF shall only accept certificates with verifiable signatures. This objective is met by:

- **FDP_DAU_CPV_(EXT).1**, Certificate processing – basic, which requires that the TSF accept certificates only with verifiable signatures.

O.Valid_Certificate states that the TSF shall use certificates that are valid, i.e., not revoked. This objective is met by:

- **FDP_DAU_CPV_(EXT).1**, Certificate processing – basic, which requires that that the TSF shall use only those certificates that are valid, i.e., revocation status demonstrates that the certificate is not revoked.

6.5.4.2 Security Objectives Rationale for CPV – Basic Policy Package

O.Provide_Policy_Info states that the TSF shall provide certificate policies for which the certification path is valid. This objective is met by:

- **FDP_DAU_CPI_(EXT).2**, Certification path initialisation – basic policy, which requires that the TSF shall use the initial-certificate-policies provided by user roles specified by

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

the ST author.

- **FDP_DAU_CPO_(EXT).2**, Certification path output – basic policy, which requires that The TSF shall output the certificate policies using the following rule: intersection of certificatePolicies extensions in all the certificates in certification path and initial-certificate-policies.

6.5.4.3 Security Objectives Rationale for CPV –Policy Mapping Package

O.Map_Policies states that the TSF shall map certificate policies in accordance with user and CA constraints. This objective is met by:

- **FDP_DAU_CPI_(EXT).3**, Certification path initialisation – policy mapping, which requires that the TSF use the explicit-policy-indicator, policy-mapping-inhibit-indicator, inhibit-any-policy-indicator provided by a role specified by the ST author.
- **FDP_DAU_CPV_(EXT).3**, Intermediate certificate processing – policy mapping, which requires that the TSF use the intermediate certificate to update specified state variables.
- **FDP_DAU_CPO_(EXT).3**, Certification path output – policy mapping, which requires that the TSF shall map policies in the calculation of the policies intersection according to defined user and CA constraints.

O.Policy_Enforce states that the TSF shall validate a certification path in accordance with certificate policies acceptable to the user. This objective is met by:

- **FDP_DAU_CPI_(EXT).3**, Certification path initialisation – policy mapping, which requires that the TSF use the explicit-policy-indicator, policy-mapping-inhibit-indicator, inhibit-any-policy-indicator provided by a role specified by the ST author.
- **FDP_DAU_CPV_(EXT).3**, Intermediate certificate processing – policy mapping, which requires that the TSF use the intermediate certificate to update specified state variables.
- **FDP_DAU_CPO_(EXT).3**, Certification path output – policy mapping, which requires that the TSF shall map policies in the calculation of the policies intersection according to defined user and CA constraints and that specified policies be enforced.

6.5.4.4 Security Objectives Rationale for CPV –Name Constraints Package

O.Authorised_Names states that the TSF shall validate a certificate only if the CA is authorized to issue a certificate to the subject. This objective is met by:

- **FDP_DAU_CPI_(EXT).4**, Certification path initialisation – names, which requires that the TSF initialize the following: permitted-subtrees = ∞, excluded-subtrees = $\varnothing$.
- **FDP_DAU_CPV_(EXT).4**, Intermediate certificate processing – name constraints, which requires that the TSF accept a certificate only if the conditions specified by the requirement, including verification of authorization, is satisfied.
- **FDP_DAU_CPV_(EXT).5**, Intermediate Certificate processing – name constraints,

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

states that the TSF shall use the intermediate certificate to update the following states: permitted-subtrees and excluded-subtrees.

6.5.4.5 Security Objectives Rationale for PKI Signature Generation Package

O.Give_Sig_Hints states that the TSF shall provide hints for selecting correct certificates for PKI signature verification. This objective is met by:

- **FDP_ETC_SIG_(EXT).1**, Export of PKI Signature, which requires that the TSF use the user selected private to key perform digital signature and that the TSF include additional information specified by the ST author with the digital signature to facilitate signature verification.

6.5.4.6 Security Objectives Rationale for PKI Signature Verification Package

O.Use_Sig_Hints states that the TSF shall use hints for selecting correct certificates for signature verification. This objective is met by:

- **FDP_ITC_SIG_(EXT).1**, Import of PKI Signature, which requires that the TSF use the following information from the signed data: hashing algorithm, signature algorithm, signer public key certificate, signer DN, signer subject alternative name, signer subject key identifier, or other data during signature verification.

O.Linkage_Sig_Ver states that the TSF shall use the correct user public key for signature verification. This objective is met by:

- **FDP_DAU_SIG_(EXT).1**, Signature Blob Verification, which requires that the TSF invoke a cryptographic module with the following information from Certification Path Validation to verify digital signature on signed data: subject public key algorithm, subject public key, subject public key parameters and that the TSF perform other verification checks as specified by the ST author.

6.5.4.7 Security Objectives Rationale for Online Certificate Status Protocol (OCSP) Package

O.Accurate_OCSP_Info states that the TSF shall accept only accurate OCSP responses. This objective is met by:

- **FDP_DAU_OCS_(EXT).1**, Basic OCSP Client, which requires that only accurate revocation information be accepted from the OCSP responder.

O.Auth_OCSP_Info states that the TSF shall accept the OCSP responses from an authorized source. This objective is met by:

- **FDP_DAU_OCS_(EXT).1**, Basic OCSP Client, which requires that the OCSP responder be verified as an authorized source.

O.Current_OCSP_Info states that the TSF may accept only OCSP responses current as of TOI. This objective is met by:

- **FDP_DAU_OCS_(EXT).1**, Basic OCSP Client, which requires that only reasonably

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

current as of TOI revocation information may be accepted through a series of policy and parameter checks.

O.User_Override_Time_OCSP states that the TSF shall permit the user to override the time checks on the OCSP response. This objective is met by:

- **FDP_DAU_OCS_(EXT).1**, Basic OCSP Client, which requires that a role or roles specified by the ST author be able to override the time checks on the OCSP response.

6.5.4.8 Security Objectives Rationale for Certificate Revocation List (CRL) Validation Package

O.Accurate_Rev_Info states that the TSF shall accept only accurate revocation information. This objective is met by:

- **FDP_DAU_CRL_(EXT).1**, Basic CRL checking, which requires that the TSF accept accurate revocation information. Accuracy is determined through a series of verification and policy requirements within this extended stated requirement.

O.Auth_Rev_Info states that the TSF shall accept the revocation information from an authorized source for CRL. This objective is met by:

- **FDP_DAU_CRL_(EXT).1**, Basic CRL checking, which requires that the TSF accept revocation information from an authorized source as selected or assigned by the ST author.

O.Current_Rev_Info states that the TSF shall accept only CRL current as of TOI. This objective is met by:

- **FDP_DAU_CRL_(EXT).1**, Basic CRL checking, which requires that the TSF accept only reasonably current as of TOI revocation information through a series of policy requirements defined in FDP_DAU_CRL_(EXT).1.

O.User_Override_Time_CRL states that the TSF shall permit the user to override the time checks on the CRL. This objective is met by:

- **FDP_DAU_CRL_(EXT).1**, Basic CRL checking, which requires that the TSF accept the CRL as current if a role assigned by the ST author overrides time checks.

6.5.4.9 Security Objectives Rationale for Audit Package

O.PKE_Audit states that the TSF shall audit security relevant PKE events. This objective is met by:

- **FAU_GEN.1-NIAP-0407** defines the set of events that the TOE must be capable of recording. This requirement ensures that the Administrator has the ability to audit events that take place in the TOE. This requirement also defines the information that must be contained in the audit record for each auditable event. This requirement also places a requirement on the level of detail that is recorded on any additional security functional requirements an ST author adds to this PP.

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

- **FAU_GEN.2-NIAP-0410** ensures that the audit records associate a user identity with the auditable event.

6.5.4.10 Security Objectives Rationale for DBsign Additional SFRs

O.ACCESS states that the TSF shall provide the ability to restrict access to the digital signing operations. This objective is met by:

- **FDP_ACC.1:2** defines the User Policy that can be enforced on client users attempting to sign RDBMS data using the certificate and digital signature template objects.
- **FDP_ACF.1-NIAP-0407** defines the Security Attributes used to implement the User Policy and defines the access control rules based on those security attributes.

O.MANAGE states that the TSF will provide all the functions and facilities necessary to manage and configure the security of the TOE and restrict these functions and facilities from unauthorized use.

- **FIA_UAU_ENV_(EXT).1** requires that the TSF require that the IT environment authenticate users prior to allowing them to perform security management functions..
- **FIA_UID_ENV_(EXT).1** requires that the TSF require that the IT environment identify users prior to allowing them to perform security management functions..
- **FMT_MOF.1:2** requires that the ability to use particular TOE capabilities be restricted to the DBsign Administrator.
- **FMT_MSA.1:2** require that the ability to perform operations on User Policy security attributes be restricted to the DBsign administrator.
- **FMT_MSA.3** requires that default values used for security attributes are restrictive, and that the DBsign Administrator has the ability to override those values.
- **FMT_SMF.1:2** requires that DBsign administrators manage the audit, User Policy, Certificates, CRLs, and OCSP functions.

6.5.5 SAR Rationale

The TOE and this ST are EAL2 conformant, augmented with ALC_FLR.2

EAL2 was chosen to provide a low level of independently assured security in the absence of ready availability of the complete development record from the vendor. The chosen assurance level is consistent with the postulated low threat environment or with an environment where compromise of protected information will not have a significant impact on mission objectives. The motivation of the threat agents in which the TOE will operate is considered low. EAL2 was chosen to provide a low level of assurance that is consistent with good commercial practices that counter threats based in casual and accidental disclosure or compromise of data protected by the TOE.

EAL2 is augmented with ALC_FLR.2 to assist in ensuring that discovered security flaws are tracked and corrected by the developer and to provide flaw reporting procedures to the users of

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

the TOE.

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

7 TOE Summary Specification

This section presents a description of how the TOE SFRs are satisfied.

7.1 Auditing

The DBsign Universal Web Signer generates audit records for all audit events associated with digitally signing data and verifying digitally signed data, including requests that fail due to the User Policy.

The DBsign Server generates audit records for the following types of audit events:

- Successful and failed requests to digitally sign data
- Successful and failed requests to verify digitally signed data

The DBsign Administration Tools generates audit records for the following types of audit events:

- All DB connection events (identification and authentication performed by the IT environment at the request of the TOE)
- All modifications in behaviour of the functions of the TSF as defined in FMT_MOF.1:2
- All modifications of the values of User Policy security attributes as described in FMT_MSA.1:2.
- All modifications of the default settings described in FMT_MSA.3.

The audit logging feature may be enabled or disabled by the administrator. The evaluated configuration of the TOE requires, at a minimum, the audit logging feature to be enabled and configured to record the auditable events identified in Table 26. Audit record generation occurs on both the client and server system.

Each audit event recorded includes the date and time of the event, type of event, subject identity (if applicable, the record may include the user name obtained from the underlying OS), and the outcome (success or failure) of the event.

For audit records of successful certification paths developed, the audit event record will include the matching rules bypassed.

For audit records resulting from failed certificate processing or failed digital signature verification, the audit event record will include the reason for the failure.

For audit records resulting from rejected OCSP responses or rejected CRLS, the reason for the rejection is included in the audit event record.

The TSF does not allow for the bypass of revocation status checking, therefore there is no associated audit record generated.

The audit records are stored in flat text files on the underlying operating systems. There is an audit log file created for each administration tool, for the DBsign UWS, and for the DBsign

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

Server.

The TOE depends upon the IT environment to provide a mechanism (via a text viewer/editor) for viewing the events recorded in the audit log. The TOE also relies upon the underlying operating systems to protect the audit records.

This function implements the following SFRs:

FAU_GEN.1-NIAP-0407:2

FAU_GEN.2-NIAP-0410:2

7.2 User Policy

The TOE provides the optional ability to restrict access to the digital signing operations. By default, the User Policy system is disabled. To support the User Policy feature, DBsign maintains a list of authorized users and associated certificates, but does not authenticate these users. DBsign relies on the underlying operating system to identify and authenticate the users.

Each DBsign user account has the following attributes:

User Name	A name that uniquely identifies the user to DBsign
First Name	The user's first name; used for informational purposes only
Last Name	The user's last name; used for informational purposes only
Active Flag	Indicates if the user account is active or disabled.
Certificates	List of certificates with which the user is permitted to sign documents. If there is more than one certificate associated with a user, DBsign will prompt the user for which one to use.

Each certificate has the following attributes:

Security Level	The DBsign security level of this certificate
Description	A short description of this certificate's intended use
Notary Flag	A flag indicating whether the certificate is intended to be used for data integrity or non-repudiation purposes.

Each digital signature template includes a security level. Digital signature templates define how DBsign will operate on data stored in the RDBMS that is unique to the host application. DBsign signature templates have the following qualities:

- Specify which DB data elements to sign or verify
- Specify which data values uniquely identify the data to be signed or verified
- Specify the data format for each data item being retrieved
- Specify how data is related enabling the representation of complex database relationships

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

- Specify where to store digital signature information in the DB

When the DBsign User Policy feature is enabled, DBsign will not allow a user to sign a template if the security level of the template is higher than the security level of the user's certificate.

This function implements the following SFRs:

FDP_ACC.1:2

FDP_ACF.1

7.3 Security Management

The TOE provides a graphical user interface called the DBsign Administration Tools which implement the security management functionality. The DBsign Administration Tools require that administrators identify and authenticate themselves to the DB in order to connect to the DB and use the selected tools. The DBsign Administration Tools access and store the TOE configuration data in the DB.

The DBsign Database Login dialog box requires the administrator to specify a database username, password and a database connection definition (used to select the database) prior to modifying any the DBsign configuration data.

The TOE provides the following DBsign Administration Tools:

Template Designer	Provides the abilty to view, create, edit or delete the digital signature templates.
Security Level Manager	Modify the descriptions of the DBsign security levels. DBsign supports 10 security levels.
User Manager	Configures the DBsign User Policy feature, including defining, editing and deleting DBsign user definitions.
Trusted Certs Manager	Configures the list of certificate authorities (CAs) that DBsign trusts to issue certificates to end users.
Log Settings Manager	Configures the types of audit records that are generated and under what conditions the audit records are generated.
Certificate/CRL Browser	Manages the certificates and CRLs that DBsign stores in the database and provides the ability to view the trusted CA certificates.
OCSP Responder Manager	Configures the list of OCSP responders DBsign trusts to provide certificate revocation status information.
Initial Table Creation Tool	Creates and populates the DBsign System Tables in the DB with initial data.

In addition, the TOE includes the DBsign Configuration File Editor. The DBsign Configuration

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

File Editor creates a new DBsign Server configuration file that can be installed on the DBsign Server. The configuration options are divided into five categories

- Global Settings – configuration items that control the operation of the DBsign Server across all configured DBs.
- Databases– configuration items pertaining to a specific DB, such as connection parameters.
- Crypto – configuration items pertaining to cryptographic operations, such as certificate chains, signer's certificates, etc.
- Caches – configuration items that control how certificates and CRLs cached in memory are managed
- Instances – defines the DBsign Web Servlet instances

This function implements the following SFRs:

FIA_UAU_ENV_(EXT).1

FIA_UID_ENV_(EXT).1

FMT_MOF.1:2

FMT_MSA.1:2

FMT_MSA.3

FMT_SMF.1:2

7.4 Certification Path Processing

DBsign performs X.509 certification path validation checks. Certification path validation consists of validating certificates starting with the one issued to the subscriber of interest and ending with a trust anchor. DBsign supports X.509 version 3 Certificates.

All certification path processing performed by DBsign is X.509 and PKIX RFC3280 compliant.

There are three categories of public key certificates involved in certificate path validation:

- Trust Anchors: The trust anchors can be in the form of self-signed certificates. The trust anchor is used to obtain the Distinguished Name (DN), public key, algorithm identifier, and the public key parameters (if applicable). DBsign permits validation of trust anchor if it is in the form of a self-signed certificate, including validating signature and verifying that the self-signed certificate validity period has not expired.
- Intermediate certificates: These are the certificates issued to the CAs. All certificates in a certification path are intermediate certificates, except the last one.
- End certificate: This is the last certificate in the certification path and is issued to the subscriber of interest. This is typically an end-entity (i.e., not a CA) certificate. However,

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

this package permits this certificate to be a CA certificate also.

DBsign processes the following security-related certificate extensions: no-check, keyUsage, and basicConstraints.

DBsign provides the ability to validate certification paths as of the time of interest (TOI), which can be the current time or earlier. DBsign depends upon the IT environment to provide certificates and either OCSP responses or CRLs for the TOI.

DBsign performs the processing of the following certificate policy-related extensions: certificatePolicies, policyMapping, inhibitAnyPolicy, policyConstraints, and nameConstraints extensions.

This function implements the following SFRs. Refer to these SFR definitions for details on the exact extensions, matching rules, TOI source, and constraints implemented by DBsign.

FDP_CPD_(EXT).1

FDP_DAU_CPI_(EXT).1

FDP_DAU_CPV_(EXT).1

FDP_DAU_CPV_(EXT).2

FDP_DAU_CPO_(EXT).1

FDP_DAU_CPI_(EXT).2

FDP_DAU_CPO_(EXT).2

FDP_DAU_CPI_(EXT).3

FDP_DAU_CPV_(EXT).3

FDP_DAU_CPO_(EXT).3

FDP_DAU_CPI_(EXT).4

FDP_DAU_CPV_(EXT).4

FDP_DAU_CPV_(EXT).5

7.5 Certificate Revocation Processing

DBsign sends Online Certificate Status Protocol (OCSP) requests in accordance with PKIX RFC 2560 and validates OCSP responses to determine the revocation status of public key certificates. The DBsign administrator configures a list of OCSP responder certificates that are trusted to do OCSP. DBsign establishes trust in the OCSP responder by performing Certification Path Validation.

DBsign allows applications to determine the revocation status of a certificate using a Certificate Revocation List (CRL). DBsign may be used to process CRLs obtained from locations indicated by a CRL Distribution Point (CRLDP) extension in a certificate and from the local cache, which

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

is the DBsign certificate and CRL archive. The locations that may be indicated in the CRLDP extension are LDAP or HTTP URLs. DBsign supports X.509 CRLs, version 2.

DBsign permits the use of the same public key for CRL signature verification as the one used for verifying the signature on the certificate. DBsign can also develop a certification path to CRL signers and then verify the signature.

This function implements the following SFRs. Refer to these SFR definitions for details on the exact extensions, OCSP Responder sources, TOI constraints implemented by DBsign.

FDP_DAU_OCS_(EXT).1

FDP_DAU_CRL_(EXT).1

7.6 PKI Signature Generation

The TOE provides a digital signature function which enables a user to generate a digital signature. The TOE digitally signs data using FIPS validated cryptographic modules in the IT environment. Under normal operations, the client side of DBsign performs the digital signing using the subscriber's certification. Using the Notary Signing feature, the application can request that the DBsign server perform the digital signing using a certificate issued to the application.

The Digital Signature security function provides DBsign the capability to digitally sign data stored within a database, memory buffer, or file.

To digitally sign data stored within a database, a user must initiate a DBsign session and then make a call to the DBS_MakeSig() API function. The DB_MakeSig() API function is a part of the DBsign API which provides developers a way to integrate the DBsign digital signature functionality into their product. When DBS_MakeSig() is called upon, DBsign checks the primary key values as defined by the signature template. When the digital signing operation has completed, DBS_MakeSig() logs the action to the DBsign audit log and records whether the event was a success or failure.

To digitally sign application-constructed data stored in a memory buffer or a file, a user must initiate a DBsign session and then make a call to the DBS_AppSign() API function.

The digital signatures always include the following information: hashing algorithm, signature algorithm. In addition, DBsign supports the ability to include signed data, signing time, signer cert, and cert chain.

This function implements the following SFRs:

FDP_ETC_SIG_(EXT).1

7.7 PKI Signature Verification

The TOE provides a digital signature function which verifies a digital signature applied to data. This allows for the author of the signed data to be uniquely identified and for the authenticity and integrity of the signed data to be verified. In addition, the digital signature function enforces personal accountability for approved changes made by an administrator to the security sensitive

© 2009 Gradkell Systems, Inc.. All Rights Reserved.

configuration data contained in the DBsign system tables. The TOE verifies digitally signed data and data integrity using FIPS validated cryptographic modules in the IT environment.

The TOE provides data integrity verification by enabling applications to verify the data integrity of previous transactions from unauthorized modification, based on the originator's digital signature. The data integrity verification function is performed whenever the digital signature function verifies digitally signed data using the DBS_CheckSig() API function of the DBsign UWS or corresponding HTTP request to DBsign Server.

The digital signature verification uses the following information from the CPV: subject public key algorithm, subject public key, subject public key parameters.

DBsign verifies the following keyUsage extension bits during signature verification: nonRepudiation or digitalSignature.

The Digital Signature security function provides DBsign the capability to verify digitally signed data stored within a database, memory buffer, or file.

To verify digitally signed data stored within a database, a user must initiate a DBsign session and then make a call to the DBS_CheckSig() API function. The DBS_CheckSig()API function is a part of the DBsign API which provides developers a way to integrate the DBsign digital signature verification functionality into their product. When DBS_CheckSig() is called upon, DBsign checks the primary key values as defined by the signature template. When the digital signature verification operation has completed, DBS_CheckSig() logs the action to the DBsign audit log and records whether the event was a success or failure.

To verify digitally signed application-constructed data stored within a memory buffer or file, a user must initiate a DBsign session and then make a call to the DBS_AppVerifyBuffer() API function or corresponding HTTP request.

This function implements the following SFRs:

FDP_ITC_SIG_(EXT).1

FDP_DAU_SIG_(EXT).1

© 2009 Gradkell Systems, Inc.. All Rights Reserved.