National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme
Validation Report

CA SiteMinder®
Federation Security Services r12 SP1 CR3

Report Number: CCEVS-VR-VID10365-2010
Version 1.1
June 28, 2010

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6757
Fort George G. Meade, MD 20755-6757

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) is R12 SP1 CR3 of the CA SiteMinder Federation Security Services product (CA FSS). The TOE was evaluated by the Booz Allen Hamilton Common Criteria Test Laboratory (CCTL) in the United States and was completed in May 2010. The evaluation was conducted in accordance with the requirements of the Common Criteria, Version 3.1 Revision 3 and the Common Methodology for IT Security Evaluation (CEM), Version 3.1 Revision 3. The evaluation was for Evaluation Assurance Level 3 (EAL3) augmented with ALC_FLR.1 (Basic Flaw Remediation) and ASE_TSS.2 (TOE Summary Specification). In addition, the evaluation was performed against CAP-B (Composition assurance level B - Methodically composed) for integration with validated product CA SiteMinder Web Access Manager r12 SP1 CR3 (CA SM WAM). The evaluation was consistent with National Information Assurance Partnership (NIAP) Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap.ccevs.org).

CA SiteMinder Federation Security Services is an identification and access management application consisting of CA SiteMinder Federation Security Services built on top of CA SiteMinder Web Access Manager r12 SP1 CR3. The TOE allows partnerships to be established between two organizations in order to share user identification information and facilitate single sign-on (SSO) and single logout (SLO) across multiple domains, where each domain has its own Policy Server/Web Agent. CA SiteMinder provides users the ability to easily and securely access the data and applications of these federated entities once they have been authenticated based on the identify information supplied in the federation assertion

The CA SiteMinder Federation Security Services product, when configured as specified in the installation guides and user guides, satisfies all of the security functional requirements stated in the TOE's Security Target.

The cryptography used in this product has not been FIPS-certified, nor has it been analyzed or tested to conform to cryptographic standards during this evaluation. All cryptography has only been asserted as tested by the vendor.

The technical information included in this report was largely derived from the Evaluation Technical Report and associated test reports produced by the evaluation team. The *CA SiteMinder® Federation Security Services r12 SP1 CR3 Security Target version 1.0, dated 5 April 2010* identifies the specific version and build of the evaluated TOE. This Validation Report applies only to that ST and is not an endorsement of the CA SiteMinder Federation Security Services product by any agency of the US Government and no warranty of the product is either expressed or implied.

2 Evaluation Details

Table 2-1. Evaluation details

Evaluated Product	CA SiteMinder® Federation Security Services r12 SP1 CR3
Sponsor & Developer	CA, Inc., Framingham, MA
CCTL	Booz Allen Hamilton, Linthicum, Maryland
Completion Date	May 2010
CC	*Common Criteria for Information Technology Security Evaluation*, Version 3.1 Revision 3, July 2009
Interpretations	None.
CEM	*Common Methodology for Information Technology Security Evaluation*, Version 3.1 Revision 3, July 2009
Evaluation Class	EAL3 Augmented ALC_FLR.1 and ASE_TSS.2 with CAP-B for integration with validated product CA SiteMinder Web Access Manager r12 SP1 CR3
Description	The TOE is the SiteMinder® Federation Security Services r12 SP1 CR3 software, which is a security software product developed by CA, Inc.
Disclaimer	The information contained in this Validation Report is not an endorsement of the SiteMinder® Federation Security Services product by any agency of the U.S. Government, and no warranty of the Access Control product is either expressed or implied.
PP	None
Evaluation Personnel	Chris Gugel Kevin Micciche John Schroeder Amit Sharma
Validation Body	NIAP CCEVS

2.1 Threats to Security

Table 2-2 summarizes the threats that the evaluated product addresses.

Table 2-2. Threats

An administrator may incorrectly install or configure the TOE, or install a corrupted TOE resulting in ineffective security mechanisms
A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data
Users whether they be malicious or non-malicious, could gain unauthorized access to resources protected by the TOE by bypassing identification and authentication countermeasures
Users or administrators could gain unauthorized access to the web resources by bypassing identification and authentication requirements

3 Identification

The product being evaluated is CA SiteMinder® Federation Security Services r12 SP1 CR3.

4 Security Policy

4.1 Identification and Authentication

Users and Administrators must be identified and authenticated to the TOE prior to being able to perform any action on the TOE. Users must re-authenticate when certain conditions are met. Administrators must choose a user authentication scheme supported by the TOE and configure the scheme to be used by the TOE. During configuration, Administrators need to define a method for the authentication scheme to look up a user in a user store, where security attributes are maintained for users. These attributes are associated with subjects acting on behalf of the user.

The TOE relies on the Asserting Party's SM User Store to identify and authenticate a user based on a pre-configured component of their DN, which is then passed along to all federated Relying Parties. Locating the user in the user store is the process of disambiguation. This is the user for which the system generates a session during the authentication process.

The TOE uses the rules enforced by SiteMinder for the realm containing the protected targeted resource. However, it uses its own authentication schemes based on SAML. The rule is triggered during the authorization process by SiteMinder to receive SAML attributes from the session store. The attributes are supplied as HTTP header variables and used by a client application. The headers are then returned to the customer's application.

4.2 Security Management

The TOE provides for two distinct roles – Users and Administrators. Users are those who attempt to access federated resources. Once Federation successfully authenticates the user, SiteMinder enforces authorization to the protected federated resources via the user's web browser. Administrators are those who have full privileges to manage and maintain data as well as create, edit, and delete objects from the Federation Security Services (FSS) Applet UI. Administrators are the only users allowed to modify the following functions:

- SAML affiliations for SAML 2.0
- SAML authentication schemes
- Affiliate domains, which contain:
    - Affiliates (SAML 1.1)
    - Service Providers (SAML 2.0)
- CA SiteMinder objects and policies

4.3 Security Audit

The TOE generates data for log files that contain auditing information about the events that occur within the system, including the startup and shutdown of audit functions and all user and Administrator actions on the TOE. Based on the content of these logs, the TOE is able to associate the event with the user or administrator that caused the event. The audit data generated by the TOE is stored in SiteMinder log files, so audit storage and review is not the responsibility of the TOE.

The TOE employs trace logging in order to monitor the performance of the Web Agent and Policy Server. These logging mechanisms provide comprehensive information about the operation of CA SiteMinder processes so performance and troubleshooting issues can be analyzed.

The component that controls the trace messages for Federation services at the Policy Server is the Fed_Server component. This component monitors activity for the assertion generator and the SAML authentication schemes. FWS logging can be configured by modifying the parameters of the LoggerConfig.properties file.

4.4 Encrypted Communications

The TOE uses symmetric encryption keys generated by SiteMinder to encrypt and decrypt sensitive data passed between TOE components, between TOE and SiteMinder components, and between TOE and users/Administrators. The TOE uses imported public keys and digital signatures in order to protect and validate SAML assertions passed to Relying Parties. 128-bit AES is provided for symmetric key cryptography, and RSA and X509 are used for public keys and digital signing. Once keys are used by the TOE, they are destroyed by the key zeroization capabilities of SiteMinder.

Symmetric keys used by the TOE are stored in the SiteMinder Key Store. Public key and signature information used by the TOE is stored in a separate database called the smkeydatabase, which is installed during the initial setup of the TOE. Operations on this database such as importing certificates are performed using a tool called smkeytool.

Because the FSS Applet UI is accessed from an environmental web browser, encrypting communications between the administrator's browser and the TOE is the responsibility of the environment. However, once the applet has been launched, it uses 128-bit AES cryptography to communicate back to the Policy Server.

4.5 TOE Access

The TOE enacts the process of single logout (SLO) (also known as cross-domain single signout) which results in the simultaneous end of all sessions for a particular user, thereby ensuring security. These sessions must be associated with the browser that initiated the logout. Single logout does not necessarily end all sessions for a user. For example, if the user has two browsers open, that user can establish two independent sessions. Only the session for the browser that initiates the single logout is terminated at all federated entities for that session. The session in the other browser will still be active. Single logout is triggered by a user-initiated logout.

Session establishment can also be denied by the TOE. When an assertion (SAML 2.0) is successfully validated, the SAML 2.0 authentication scheme writes assertion data in the expiry data table with a key of the assertion ID and an expiration time. If the scheme cannot write to the table in the session store, the SAML 2.0 authentication scheme denies the authentication in the same manner as an invalid assertion.

4.6 Protection of the TSF and Trusted Path/Channel

All communication between users/Administrators and the TOE are secured via an environmental trusted path using SSL v3.0. All communication between TOE components and, as well as communication between Federation Web Services and the Policy Server, utilize a proprietary algorithm from SiteMinder known as the TLI handshake. This is used by the Asserting Party to establish communications with its Relying Parties for single sign-on. For more information on encryption used by SiteMinder, see the CA SiteMinder Web Access Manager r12 SP1 CR3 Security Target v0.8.

Protecting the Federation Web Services application at the Asserting Party ensures that the services that make up the application are secure. The policies for the Federation Web Services application are created automatically. However, to enforce protection and to specify who can access Federation Web Services, Administrators must authenticate to the FSS Applet UI where they manage the TOE.

There is a pre-configured policy that uses the Basic over SSL authentication scheme to protect the Assertion Retrieval Service. When configuring the policy for the client certificate authentication scheme, this policy is created for a different realm than the realm that uses the Basic over SSL scheme. For protection of data transmitted between separate parts of the TOE, SSL v3.0 is used.

In order to establish single sign-on between the Asserting Party and Relying Party, the SSO bindings supported by the Relying Party need to be specified. In the FSS Applet UI, the SSO tab allows single sign-on to be configured using the artifact or POST binding. This enforces the single use assertion policy for POST binding to prevent the replaying of a valid assertion. When replay is detected, the TOE denies the request and returns an error to the user.

5 Assumptions

5.1 Personnel Assumptions

Table 5-1 – Personnel Assumptions

One or more authorized administrators will be assigned to install, configure and manage the TOE
Administrators exercise due diligence to update the TOE with the latest patches and patch the Operational Environment (e.g., OS and database) so they are not susceptible to network attacks
Administrators of the TOE are not careless, willfully negligent, or hostile and will follow and abide by the instructions provided by the organization's guidance documentation
It is assumed that users will select strong passwords to be enforced by SiteMinder and will protect their authentication data

5.2 Physical Assumptions

Table 5-2 – Physical Assumptions

The TOE will be located within controlled access facilities that will prevent unauthorized physical access

5.3 Connectivity Assumptions

Table 5-3 – Connectivity Assumptions

The administrator will secure the underlying Operating System and data stores in order to protect the files used by the TOE

6 Clarification of Scope

The TOE includes all the code that enforces the policies identified (see section 4).

The evaluated configuration of the TOE includes the CA SiteMinder®
Federation Security Services r12 SP1 CR3 product that is comprised of the following:

- Federation Web Services (FWS) application is installed on a server that has a connection to a SiteMinder Policy Server. Federation Web Services consists of the following:
    - Single Sign On (SSO)
    - Single Log Out (SLO)

  - Artifact Resolution
  - Assertion Consumer
  - Inter-site Transfer
  - SAML Credential Collector
  - Assertion Retriever
  - Agent API
  - Attribute Service
  - Auth URL JSP

- PS Option Pack (aka Federation) enables user store connectivity, authentication functions, and session store abilities. In order to manage the settings of Federation, the Federation Security Services Applet UI must be used. Consists of the following:
  - SAML Assertion Generator
  - Configuration Services
  - SAML Auth Schemes
  - Tunnel Services
  - smkeydatabase
- CA FSS Applet UI is a web application that uses the HTTP protocol to administer and manage the configuration of entities and partnerships and various server settings. Many of the SiteMinder functions can also be accomplished using the WAM Admin UI, but the FSS Applet UI serves as the primary interface for administrators in the evaluated configuration. During configuration of the TOE, the terminal(s) used by the administrator to run the FSS Applet UI must be registered by using the WAM Admin UI.
- CA SiteMinder Web Agent is a software component that controls user access to a protected resource (any URL protected by the TOE). The Web Agent grants or denies access by enforcing policies defined through the Policy Server. Web Agents work with the Policy Server to authorize users for access to web server resources. The Web Agent enables Web applications to personalize content. The network path between the Web Agent and the Policy Server is secured by AES encryption over a standard TCP/IP connection. The Web Agent is integrated with a Web server. The Web Agent intercepts requests for a resource and determines whether or not the resource is protected by the TOE. Web Agents perform the following tasks:

  - Intercept access requests for protected resources and work with the Policy Server to determine whether or not a user should have access.
  - Provide information to a Web application that dictates how content is presented to the user (policy-based personalization) and how to deliver access privileges.
  - Ensure a user's ability to securely access information. Web Agents store contextual information about user access privileges in a session cache. Performance is optimized by modifying the cache settings.
  - Enable single sign-on across web servers in a single cookie domain or across multiple cookie domains without requiring users to re-authenticate.

- CA SiteMinder Policy Server provides functions such as the authentication schemes (SAML 1.1 artifact, SAML 1.1 Post, SAML 2.0 Template) and the Assertion Generator. When a user attempts to access a protected network resource, the Policy Server uses the authentication scheme associated with the resource's realm and protection level to determine how to identify the user. The Policy Server installed at the Asserting Party, includes the assertion generator component. The assertion generator creates SAML assertions, which are XML documents that contain authentication information about a user. For the SAML artifact profile, after an assertion is generated, it is stored by the session store until it is requested by the Relying Party. The AMAssertionGenerator.properties file is required for operation of the Assertion Generator. It contains parameters that the Assertion Generator uses to generate SAML assertions. If any changes are made to the AmAssertionGenerator.properties file, the changes will not be picked up by the Policy Server until it is restarted.
- CA SiteMinder WAM Administrative UI is a web-based administration console for CA SiteMinder that is installed independent of the Policy Server. An administrator uses the CA SiteMinder WAM Administrative UI to view, modify, and delete all Policy Server objects except those related to Federation Security Services. While the CA SiteMinder tasks that CA SiteMinder Federation Security Services builds upon can be configured via the CA SiteMinder WAM Administrative UI or the CA FSS Applet UI, those which apply specifically to CA SiteMinder Federation Security Services (such as configuring affiliates and SAML authentication schemes) must be handled using the FSS Applet UI.

  The SiteMinder WAM Admin UI is used to set up the Policy Server and to get the base component up and running. However, the CA SiteMinder WAM Admin UI is not used in the evaluated configuration.

The scope and requirements for the evaluated configuration are summarized as follows:

1. The CA SiteMinder® Federation Security Services r12 SP1 CR3software (i.e., the TOE) will be installed with the aforementioned components.

Note that the TOE, in its evaluated configuration, was tested on Linux Red Hat Advanced Server 4.0, Microsoft Windows 2003 SP2, and Solaris 10

2. In addition to the platforms listed in the table above, SSL implementation is also required to run the TOE.

6.1 System Requirements

This section identifies the hardware and software requirements for the platforms described in the evaluated configuration. The TOE was evaluated using Microsoft Windows 2003 SP2, Linux Red Hat Advanced Server 4.0, and Solaris 10. The minimum system requirements to install FWS on each OS are illustrated below:

Table 6-1– FWS minimum system requirements

Component	Windows or Linux	Solaris Unix
CPU	Single or Dual-processor, Intel Pentium III (or compatible), 700-900 MHZ	Sparc Workstation 440 MHz
Memory (RAM)	512 MB system RAM. 1 GB is recommended	512 MB system RAM. 1 GB is recommended
Available Disk Space	540 MB	540 MB
Temp Disk Space	450 MB	450 MB
Web Server	IIS 6.0 or ASF Apache 2.2 on Microsoft Windows 2003 SP2 SunOne Web Server 7.0 or ASF Apache 2.2 on Red Hat Advanced Server 4.0	SunOne Web Server 7.0 or ASF Apache 2.2 on Solaris 10
Servlet Container	Servlet Exec 6.0 on Microsoft Windows 2003 SP2 Servlet Exec 6.0 on Red Hat Advanced Server 4.0	Servlet Exec 6.0 on Solaris 10 Sparc

The minimum system requirements to install Policy Server on each OS are illustrated below:

Table 6-2 – Policy Server minimum system requirements

Component	Windows or Linux	Solaris Unix
CPU	Intel Pentium III or better	Sparc Workstation 440 MHz
Memory	512 MB system RAM	512 MB RAM
Available Disk Space	270 MB	300 MB
Temp Directory	180 MB	200 MB (10 MB is

Component	Windows or Linux	Solaris Unix
Space		required for daily operation)
JRE	The required JRE version is installed on the same system as the Policy Server	The required JRE version is installed on the same system as the Policy Server
LDAP Directory Server	Ensure that LDAP directory server being used as a policy store is supported	Ensure that LDAP directory server being used as a policy store is supported
Web Server	IIS 6.0 or ASF Apache 2.2 on Microsoft Windows 2003 SP2 SunOne Web Server 7.0 or ASF Apache 2.2 on Red Hat Advanced Server 4.0	SunOne Web Server 7.0 or ASF Apache 2.2 on Solaris 10

The supported TOE and Operational Environment components have been illustrated below:

Table 6-3 – Supported TOE and Operational Environment Components

Component	TOE Version	Platforms
Policy Server FSS Applet UI Web Agent PS Option Pack Federation Web Services (FWS)	r12 SP1 CR3	Linux Red Hat Advanced Server 4.0
		Microsoft Windows 2003 SP2
		Solaris 10
Policy Store User Store	r12 SP1 CR3	SunOne LDAP 5.2 on Red Had Advanced Server 4.0
		Windows 2003 Active Directory on Microsoft Windows 2003 SP2
		SunOne LDAP 5.2 on Solaris 10
Key Store Session Store	r12 SP1 CR3	Oracle 10g R2 on Red Hat Advanced Server 4.0
		Oracle 10g R2 on Microsoft Windows 2003 SP2
		Oracle 10g R2 on Solaris 10
Web Servers	r12 SP1 CR3	SunOne Web Server 7.0 on Red Hat Advanced Server 4.0
		ASF Apache 2.2 on Red Hat Advanced Server 4.0
		IIS 6.0 and ASF Apache 2.2 on Microsoft Windows 2003 SP2
		SunOne Web Server 7.0 and ASF Apache 2.2 on Solaris 10
Servlet Container	r12 SP1 CR3	ServletExec 6.0

In addition to the platforms listed in Table 6-3, the following non-TOE software is required to run the TOE:

- SSL v3.0 implementation
- Transport standards HTTP
- Web browser software

7 Architectural Information

The TOE's boundary has been defined in Figure 1. Additionally, Figure 2 illustrates a potential implementation used for a complex federation.

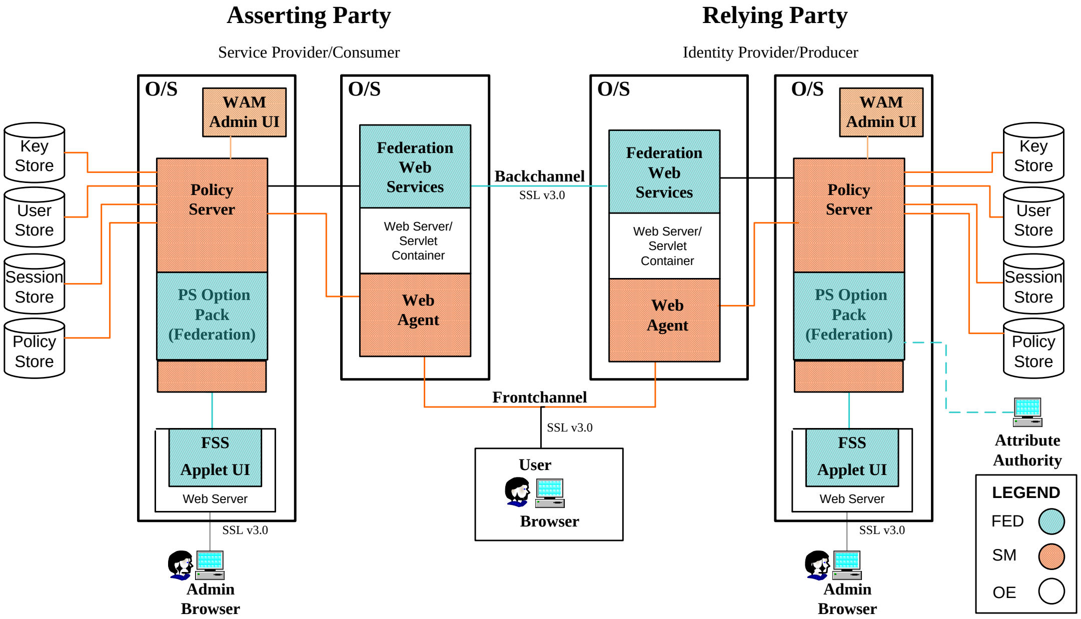

Figure 1 – CA SiteMinder® Federation Security Services r12 SP1 CR3TOE Boundary

7.1.1 Complex Federation Implementation

A federation is not limited to a single Asserting Party (Identity Provider/Producer) and Relying Party (Service Provider/Consumer). As shown in Figure 2, multiple Relying Parties can be configured so that single sign-on can be established between more than two devices. In addition, one or more Attribute Authorities may be used to provide elements of the user DN which are not stored on the Asserting Party itself.

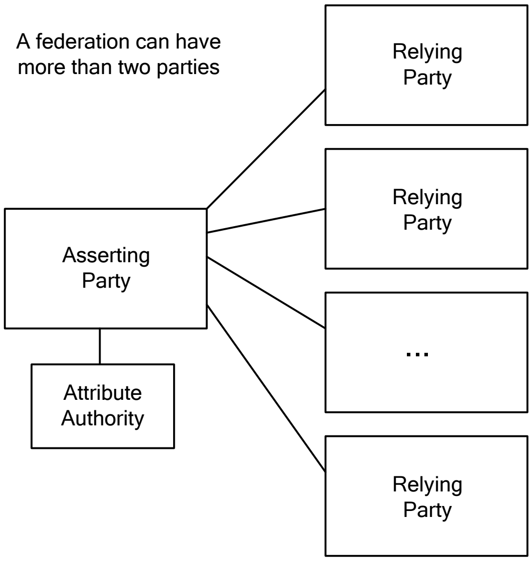

Figure 2: Possible Configuration of SiteMinder Federation Security Services

7.2 TOE Components

7.2.1 Federation Web Services (FWS)

Federation Web Services (FWS) application is installed on a server that has a connection to a CA SiteMinder Policy Server. Federation Web Services consists of the following:

- Single Sign On (SSO)
- Single Log Out (SLO)
- Artifact Resolution
- Assertion Consumer
- Inter-site Transfer
- SAML Credential Collector
- Assertion Retriever
- Agent API
- Attribute Service
- Auth URL JSP

7.2.2 Policy Server Option Pack (PSOP)

The PSOP enables user store connectivity, authentication functions, and session store abilities. In order to manage the settings of Federation, the Federation Security Services Applet UI must be used. Consists of the following:

- SAML Assertion Generator
- Configuration Services

- SAML Auth Schemes
- Tunnel Services
- smkeydatabase

7.2.3 CA FSS Applet UI

The CA FSS Applet UI is a web application that uses the HTTP protocol to administer and manage the configuration of entities and partnerships and various server settings. Many of the CA SiteMinder functions can also be accomplished using the WAM Admin UI, but the CA FSS Applet UI serves as the primary interface for administrators in the evaluated configuration. During configuration of the TOE, the terminal(s) used by the administrator to run the CA FSS Applet UI must be registered by using the WAM Admin UI.

7.2.4 CA SiteMinder Web Agent

SiteMinder Web Agent is a software component that controls user access to a protected resource (any URL protected by the TOE). The Web Agent grants or denies access by enforcing policies defined through the Policy Server. Web Agents work with the Policy Server to authorize users for access to web server resources. The Web Agent enables Web applications to personalize content. The network path between the Web Agent and the Policy Server is secured by AES encryption over a standard TCP/IP connection. The Web Agent is integrated with a Web server. The Web Agent intercepts requests for a resource and determines whether or not the resource is protected by the TOE. Web Agents perform the following tasks:

- Intercept access requests for protected resources and work with the Policy Server to determine whether or not a user should have access.
- Provide information to a Web application that dictates how content is presented to the user (policy-based personalization) and how to deliver access privileges.
- Ensure a user's ability to securely access information. Web Agents store contextual information about user access privileges in a session cache. Performance is optimized by modifying the cache settings.
- Enable single sign-on across web servers in a single cookie domain or across multiple cookie domains without requiring users to re-authenticate.

7.2.5 CA SiteMinder Policy Server

CA SiteMinder Policy Server provides functions such as the authentication schemes (SAML 1.1 artifact, SAML 1.1 Post, SAML 2.0 Template) and the Assertion Generator. When a user attempts to access a protected network resource, the Policy Server uses the authentication scheme associated with the resource's realm and protection level to determine how to identify the user. The Policy Server installed at the Asserting Party, includes the assertion generator component. The assertion generator creates SAML assertions, which are XML documents that contain authentication information about a user. For the SAML artifact profile, after an assertion is generated, it is stored by the session store until it is requested by the Relying Party. The AMAssertionGenerator.properties file is required for operation of the Assertion Generator. It contains parameters that the Assertion Generator uses to generate SAML assertions. If any changes are made to the AmAssertionGenerator.properties file, the changes will not be picked up by the Policy Server until it is restarted.

7.2.6 CA SiteMinder WAM Administrative UI

CA SiteMinder WAM Administrative UI is a web-based administration console for SiteMinder that is installed independent of the Policy Server. An administrator uses the SiteMinder WAM Administrative UI to view, modify, and delete all Policy Server objects except those related to Federation Security Services. While the SiteMinder tasks that Federation Security Services builds upon can be configured via the SiteMinder WAM Administrative UI or the CA FSS Applet UI, those which apply specifically to Federation Security Services (such as configuring affiliates and SAML authentication schemes) must be handled using the FSS Applet UI.

The SiteMinder WAM Admin UI is used to set up the Policy Server and to get the base component up and running. However, the SiteMinder WAM Admin UI is not used in the evaluated configuration.

8 Documentation

The documents were evaluated to satisfy assurance requirements:

Table 8-1 – Assurance Documents Evidence

Component	Document(s)	Rationale
ADV_ARC.1 Security Architecture Design	TOE Design Specification Document for CA Federation Security Services R12 SP1 CR3 V1.0 (dated November 12, 2009)	This document describes the security architecture of the TOE.
ADV_FSP.3 Functional Specification with complete summary	CA SiteMinder Federation Security Services r12 SP1 CR3 Functional Specification v1.0 (dated November 12, 2009)	This document describes the functional specification of the TOE with complete summary.
ADV_TDS.2 Architectural Design	[1] CA SiteMinder Federation Security Services r12 SP1 CR3 TOE Design Specification v1.0 (dated November 12, 2009) [2] CA SiteMinder Federation Security Services r12 SP1 CR3 Functional Specification v1.0 (dated November 12, 2009)	This document describes the architectural design of the TOE.

AGD_OPE.1 Operational User Guidance	[1] CA SiteMinder® Federation Security Services - Federation Security Services Guide r12 SP1 Second Edition [2] Evaluated Configuration for CA SiteMinder® Federation Security Services r12 SP1 CR3 (dated February 8, 2010)	This document describes the operational user guidance for CA SiteMinder Federation Security Services r12 SP1 CR3.
AGD_PRE.1 Preparative Procedures	Evaluated Configuration for CA SiteMinder® Federation Security Services r12 SP1 CR3 (dated February 8, 2010)	This document describes the preparative procedures that need to be done prior to installing CA SiteMinder Federation Security Services r12 SP1 CR3.
ALC_CMC.3 Authorizations Controls	[1] CA Clearcase Configuration Management Plan Version 1 [2] CA SiteMinder Federation Security Services - Configuration Management for Common Criteria r12sp1 [3] submission-approved_RE Mainline submission request to proj-hemlock-sp1 .txt [4] submission-request_Mainline submission request to proj-hemlock-sp1 for C65917 .txt [5] project-configuration-management.doc [6] FSS-12-SP1-Configuration-Item_List.zip [7] FSS-r12-SP1-CR3-Configuration-Item_List.zip	This document describes the authorization controls for the TOE.
ALC_CMS.3 CM Scope	[1] CA Clearcase Configuration Management Plan Version 1 [2] FSS-r12-SP1-CR3-Configuration-Item_List.zip	These documents describe the CM scope of the TOE.
ALC_DEL.1 Delivery Procedures	CA SiteMinder® Federation Security Services r12 SP1--- NIAP Download/Installation instruction	This document describes product delivery for CA SiteMinder Federation Security Services r12 SP1 CR3 and a description of all procedures used to ensure objectives are not compromised in the delivery process.

ALC_DVS.1 Identification of Security Measures	[1] 11-Backup_Procedure-GIS-2008Jun09.doc (dated May 5, 2008) [2]1619-GRC-Global_Security-Pre-employment_Screening-2008Apr05.doc (dated April 5, 2007 / 1.4) [3] 1621 - GSAP.doc (dated July 23, 2007 / 1.2) [4] 3649-Access_Procedure-2007Jun29.pdf (June 29, 2007 / 3.0) [5]5153-Project_360_Reference_Guide-2008Jul25.doc Revision 5.0 [6]5725-GRC-BP-C-RIM-Records_Security_and_Confidentiality_Policy-2008May23.doc (dated May 23, 2008) [7]5727-GRC-BP-C-RIM-Records_Disposal_Procedure-2008May15.doc (dated May 15, 2008) [8] 5804-Privileged_Access-2008Jun24.doc (dated June 30, 2008) [9]7417-Enterprise_Procedure-Privacy_and_Data_Protection-2007Mar06.doc (dated March 6, 2007 / 1.0) [10]7705-Inactive_User_Account_Procedure-2007Jun29.pdf (dated June 29, 2007 / 1.0) [11]7726-Server_Security_Procedure-2008Jun24.doc (dated June 29, 2008 / 3.0) [12] 7978-US_Employee_Handbook-NorthAmerica-USA-2008Jul14.pdf (dated July 14, 2008)	This document provides an identification of security measures for the TOE.
ALC_LCD.1 Life-Cycle Definition	Project 360 Reference Guide revision 5.0	This document provides the life-cycle definition of the TOE.
ASE_CCL.1 Conformance Claims	CA SiteMinder Federation Security Services r12 SP1 CR3 Security Target v1.0 (April 5, 2010)	This document describes the CC conformance claims made by the TOE.
ASE_ECD.1 Extended Components Definition	CA SiteMinder Federation Security Services r12 SP1 CR3 Security Target v1.0 (April 5, 2010)	This document provides a definition for all extended components in the TOE.
ASE_INT.1 Security Target Introduction	CA SiteMinder Federation Security Services r12 SP1 CR3 Security Target v1.0 (April 5, 2010)	This document describes the Introduction of the Security Target.
ASE_OBJ.2 Security Objectives	CA SiteMinder Federation Security Services r12 SP1 CR3 Security Target v1.0 (April 5, 2010)	This document describes all of the security objectives for the TOE.
ASE_REQ.2 Security Requirements	CA SiteMinder Federation Security Services r12 SP1 CR3 Security Target v1.0 (April 5, 2010)	This document describes all of the security requirements for the TOE.
ASE_SPD.1 Security Problem Definition	CA SiteMinder Federation Security Services r12 SP1 CR3 Security Target v1.0 (April 5, 2010)	This document describes the security problem definition of the Security Target.

ASE_TSS.2 TOE Summary Specification	CA SiteMinder Federation Security Services r12 SP1 CR3 Security Target v1.0 (April 5, 2010)	This document describes the TSS section of the Security Target.
ATE_COV.2 Analysis of Coverage	Common-Criteria-Federation-MappingList_V5.0.xls	This document provides an analysis of coverage for the TOE.
ATE_DPT.1 Basic Design	Common-Criteria-Federation-MappingList_V5.0.xls	This document describes the basic design of the TOE.
ATE_FUN.1 Functional Tests	Common-Criteria-Federation-MappingList_V5.0.xls	This document describes the functional tests for the TOE.
ATE_IND.2 Independent Testing	Common-Criteria-Federation-MappingList_V5.0.xls	This document describes the independent testing for the TOE.
AVA_VAN.2 Vulnerability Analysis	Vulnerability Analysis, CA Siteminder® Federation Security Services R12 SP1 CR3 Version 0.5, October 15, 2009	This document describes the vulnerability analysis of the TOE.
ACO_COR.1 Composition Rationale	[1] CA SiteMinder Federation Security Services r12 SP1 CR3 TOE Design Specification v1.0 (dated November 12, 2009) [2] CA SiteMinder Federation Security Services r12 SP1 CR3 Functional Specification v1.0 (dated November 12, 2009) [3] TOE Design Specification Document for CA SiteMinder R12 SP1 v1.7 (January 22, 2009) [4] Functional Specification Document for CA SiteMinder R12 SP1 v2.2 (January 22, 2009)	This document describes the composition rationale for the Composed TOE.
ACO_CTT.2 Rigorous Interface Testing	Common-Criteria-Federation-MappingList_V5.0.xls	This document describes the interface testing for the Composed TOE.
ACO_DEV.2 Basic Evidence of Design	[1] CA SiteMinder Federation Security Services r12 SP1 CR3 TOE Design Specification v1.0 (dated November 12, 2009) [2] CA SiteMinder Federation Security Services r12 SP1 CR3 Functional Specification v1.0 (dated November 12, 2009) [3] TOE Design Specification Document for CA SiteMinder R12 SP1 v1.7 (January 22, 2009) [4] Functional Specification Document for CA SiteMinder R12 SP1 v2.2 (January 22, 2009)	This document describes the basic evidence of design for the Composed TOE.
ACO_REL.1 Basic Reliance Information	[1] CA SiteMinder Federation Security Services r12 SP1 CR3 TOE Design Specification v1.0 (dated November 12, 2009) [2] CA SiteMinder Federation Security Services r12 SP1 CR3 Functional Specification v1.0 (dated November 12, 2009) [3] TOE Design Specification Document for CA SiteMinder R12 SP1 v1.7 (January 22, 2009) [4] Functional Specification Document for CA SiteMinder R12 SP1 v2.2 (January 22, 2009)	This document describes the basic reliance information for the Composed TOE.

ACO_VUL.2 Composition Vulnerability Analysis	Vulnerability Analysis, CA Siteminder® Federation Security Services R12 SP1 CR3 Version 0.5, October 15, 2009	This document describes the vulnerability analysis for the Composed TOE.

These documents were provided as evaluation evidence, only the documents under the ASE and AGD Classes (bolded and underlined) are provided to customers who have purchased the TOE.

9 TOE Acquisition

The NIAP-certified CA SiteMinder® Federation Security Services product is acquired via normal sales channels, and digital delivery of the TOE is coordinated with the end customer by CA Technologies.

10 IT Product Testing

The test team's test approach is to test the security mechanisms of the CA SiteMinder® Federation Security Services by exercising the external interfaces to the TOE and viewing the TOE behavior either remotely, or on the platform. Each TOE external interface is described in the appropriate design documentation (e.g., FSP) in terms of the relevant claims on the TOE that can be tested through the external interface. The ST, TOE Design Specification (TDS), Functional Specification (FSP), and the vendor's test plans were used to demonstrate test coverage of all *appropriate* EAL3 requirements for all *security relevant* TOE external interfaces. TOE external interfaces that were determined to be *security relevant* are interfaces that

- Change the security state of the product,
- Permit an object access or information flow that is regulated by the security policy,
- Are restricted to subjects with privilege or behave differently when executed by subjects with privilege, or
- Invoke or configure a security mechanism.

Security functional requirements were determined to be *appropriate* to a particular interface if the behavior of the TOE that supported the requirement could be invoked or observed through that interface.

The evaluation team created a test plan that contained the vendor functional test suite, and supplemental functional testing of the vendors’ tests. Booz Allen also performed vulnerability assessment and penetration testing.

10.1 TEST METHODOLOGY

10.1.1 Vulnerability Testing

The evaluation team executed the following vulnerability tests against CA SiteMinder® Federation Security Services r12 SP1 CR3:

- Eavesdropping on Communications
  In this test, the evaluators manually inspected network traffic to and from the TOE in order to ensure that no useful or confidential information could be obtained by a malicious user on the network. This test was specialized for the following interfaces:
    - FSS Front Channel
    - FSS Back Channel
    - Policy Server – Federation Web Services
    - FSS Applet UI

- Port Scanning
  Remote access to the TOE should be limited to the standard TOE interfaces and procedures. This test attempted to find ways to bypass these standard interfaces of the TOE and open any other vectors of attack.

- Buffer Overflow / Format String / Unexpected Input Attack
  In this attack, the evaluators attempted to discover and exploit any software errors that do not appropriately handle various non standard inputs. The evaluators attempted to inject known malicious inputs into the various TOE interfaces. These malicious inputs form 3 categories.
    - Buffer Overflows: In this case, larger and larger inputs are injected to try to overflow a buffer and corrupt the program stack.
    - Format Strings: In this case, format strings are injected to attempt to see if they are not handled correctly by the program.
    - Special Characters: In this case, unexpected special characters are injected in an attempt to induce non standard behavior.

- Vulnerability Scanner (Nessus)
  This test used the Nessus Vulnerability scanner to test any and all open interfaces on any applicable systems of the TOE. The scanner probes a wide range of vulnerabilities that includes but is not limited to the following:

Backdoors CGI abuses Denial of Service Finger abuses Firewalls FTP Gain a shell remotely	Gain root remotely General Miscellaneous Netware NIS Port scanners Remote file access	RPC Settings SMTP Problems SNMP Untested Useless services

- TCP Malformed Packet Flooding
  This test attempted to shutdown TOE resources by flooding the network with large amounts of malformed tcp packets.

- Unauthenticated Access / Directory Traversal Attack
  This test used "URL hacking" to attempt to access protected TOE resources by injecting unexpected input into requests that were sent to the TOE. This was done using two different approaches to URL exploitation.
  - The first part attempted to access protected TOE resources as an unauthenticated outsider.
  - The second part attempted to access local TOE resources that should be protected from any remote access (unauthenticated and authenticated).

- SQL Injection / Cross Site Scripting Attack / Xpath Injection
  This test executed automated SQL Injection and Cross Site Scripting attacks against the TOE. The evaluators determined any fields or variables that could be prone to attack. They then used a scanner, which contained a large database of standard strings that are used for testing SQL Injection and Cross Site Scripting issues. These strings were input into the various fields and variables and the output was analyzed for inconsistencies.

- Documented Server Vulnerabilities
  This test attempted to exploit publicly known vulnerabilities that potentially exist in the web servers of the product.

- Web Server Vulnerability Scanner (Nikto)
  This test used the Nikto web server vulnerability scanner to test for any known vulnerabilities that could be present in the TOE's web interfaces. This scanner probed a wide range of vulnerabilities that included the following:

File Upload. Interesting File / Seen in logs. Misconfiguration / Default File. Information Disclosure. Injection (XSS/Script/HTML). Remote File Retrieval.	Denial of Service. Command Execution / Remote Shell. SQL Injection. Authentication Bypass. Software Identification. Remote source inclusion.

- Vulnerability Scanner (Retina)
  This test uses the Retina Vulnerability scanner to test any and all open interfaces on any applicable systems of the TOE.
  The scanner probes a wide range of vulnerabilities that includes but is not limited to the following:

Accounts Anti-Virus Backdoors CGI Scripts Database Issues	DoS IP Services Registry Remote Access RPC Services	Service Control Spyware Web Services CVE Issues SecurityFocus BID Issues

10.1.2 Vulnerability Results

The following lists any issues that were discovered as a result of the vulnerability testing process. These issues along with the related guidance for mitigation have been included in the "Evaluated Configuration for CA SiteMinder® Federation Security Services r12 SP1 CR3" (08 February 2010) addendum to the product Administrator Guidance.

- HTTP Over SSL/TLS Configuration
  All web servers that are being used to in conjunction with Federation must be configured to use only HTTPS and should be configured using valid certificates signed by a trusted Certificate Authority. Any use of standard HTTP should be disabled.
  Without this secure channel, user credentials will be sent in clear-text and can be intercepted even on a switched network using sniffing and arp poisoning.
  Attackers can also employ man-in-the middle attacks to steal SAML assertions when they pass across the network.
  It was seen that even if the original request is over HTTPS, subsequent requests can be sent over standard HTTP if configured as such in the Policy Server objects.
  An insecure Policy Server configuration could allow for an assertion or artifact to be posted in the clear.
  The HTTPS requirement should also be levied on information that travels across the backchannel to the artifact resolution service in order to prevent sniffing and man-in-the-middle attacks.

- SSL Cipher Suite Downgrade
  The evaluators discovered that the default configuration for the SSL modules in Federation web servers allowed a client to use cryptographic ciphers that were below the strength level described in the ST (Security Target). All web and application servers should be configured to only allow clients that support high strength cipher suites. They should also only support SSLv3/TLS because there are known issues in previous versions of the protocol. All certificates used for SSL communications should be signed by trusted Certificate Authority using only strong hashing algorithms.

- Dangerous HTTP Methods
  Several of the Federation web-servers allowed unnecessary HTTP methods that are potentially dangerous. These methods should be disabled globally on all web and application servers in Federation.
  TRACE
  DELETE
  PUT
  MOVE

- Default Servlets Deployed on ServletExec
  There evaluators discovered that there were several default servlets that were deployed on ServletExec. These were the following:
  /servlet/DateServlet
  /servlet/SessionServlet
  All default code should be removed from production servers.

- All Assertions Must be Signed

It was discovered that there is an option in Federation to leave assertions over the backchannel unsigned. In the Common Criteria configuration, all assertions should be signed to verify their validity.

- Applet UI Agent Name Information Disclosure
  In the proprietary CA encrypted wire protocol used for Applet UI communications, the Agent name is visible in clear-text over the network. The username, password, and agent passphrase are all appropriately secured and login is not possible without all of these fields. However, a user should not rely on the secrecy of the Agent name field to preserve the security of a system.

- Applet UI Agent Sessions
  It was discovered that using the correct agent name and passphrase in the Applet UI establishes a session that is used for subsequent username and password attempts. The case describing this behavior is as follows:
  - A user enters incorrect username/password but correct agentname/passphrase.
    - The user is denied access.
  - The user then enters the correct username/password but incorrect agentname/passphrase
    - The session from the previous attempt is preserved and the user is allowed access.

  Successful login does require all four fields of the prompt, but an agent session is persisted until log-out or exit from the Applet even though it is not indicated by the UI. This behavior should be noted and understood by an administrator of the product.

- Blind Redirects
  Federation comes with a jsp file “redirect.jsp” that can be used to redirect a user from the login page directly to the assertion generation service used to begin a Federated session. However, the location of this service is given as a parameter in the URL of the redirect page and is not checked to ensure that it is valid. The presence of this page could allow for a phishing style attack in which a user is redirected to a malicious site from a Federation login page. The malicious could then steal the user’s credentials by requesting that they re-login. The user would likely not realize that they have left a valid site. Depending on the browser, the Federation page could still be shown in location bar.
  A similar attack arises if the web site allows for both HTTP and HTTPS logins. In this case, the attacker could redirect the user to a valid Federation page, but in standard HTTP instead of secure HTTPS. If redirected to a page that requests additional login, the user’s credentials could be sent in clear-text over the network. However, if HTTP is disabled per the guidance, this style of attack does not apply.
  In order to prevent these attacks, the user will be instructed to remove the redirect.jsp page completely and to hardcode all links in html. After login, the user will have to click on the link in order to begin the Federated session.

- Sample Files and Web Directory Listing

The evaluators discovered that accessing the URL “/siteminderagent/” on a Federation Web Agent allows an unauthenticated user to view directory contents on the server. This directory contains sample files that are included with Siteminder/Federation that should be removed before placing the server in production. The ability to list the content of the directory should be disabled on the hosting web server.

11 Results of the Evaluation

The evaluation was carried out in accordance with the Common Criteria Evaluation and Validation Scheme (CCEVS) process and scheme. The evaluation demonstrated that the CA SiteMinder® Federation Security Services r12 SP1 CR3 TOE meets the security requirements contained in the Security Target.

The criteria against which the CA SiteMinder® Federation Security Services r12 SP1 CR3 TOE was judged are described in the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009. The evaluation methodology used by the evaluation team to conduct the evaluation is the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3, July 2009. The Booz Allen Hamilton Common Criteria Test Laboratory determined that the evaluation assurance level (EAL) for the CA SiteMinder® Federation Security Services r12 SP1 CR3 TOE is EAL 3. The TOE, configured as specified in the installation guide, satisfies all of the security functional requirements stated in the Security Target.

The evaluation was completed in May 2010. Results of the evaluation and associated validation can be found in the Common Criteria Evaluation and Validation Scheme Validation Report.

12 Validator Comments/Recommendations

12.1 Secure Installation and Configuration Documentation

The “Evaluated Configuration for CA SiteMinder® Federation Security Services r12 SP1 CR3” (08 February 2010) define the recommendations and secure usage directions for the TOE as derived from testing.

12.2 Installation and Configuration

Through the course of the evaluation of the CA SiteMinder® Federation Security Services it was determined that the installation and configuration of the product requires a level of familiarity with the product and the SAML protocol to successfully and securely install and configure CA SiteMinder® Federation Security Services in a real world application. It is recommended that if assistance is needed that the vendor be contacted to support the installation and configuration efforts.

12.3 Apache

The TOE requires a web server to perform its functionality. One web server tested in the evaluated configuration was Apache. During testing it was determined that Apache version 2.2 or later should be utilized and that the RewriteEngine flag should not be enabled.

12.4 Blind Redirects

CA SiteMinder® Federation Security Services comes with a jsp file "redirect.jsp" that can be used to redirect a user from the login page directly to the assertion generation service used to begin a Federated session. This configuration could allow a phishing attack unless the CA recommended secureredirect procedure is followed. Customers should use secureredirect instead of redirect to encrypt the SMPORTALURL query parameter. Encrypting the portal URL protects it from being modified by a malicious user.

Details:

CA SiteMinder® Federation Security Services comes with a jsp file "redirect.jsp" and secureredirect.jsp to encrypt the URL that can be used to redirect a user from the login page directly to the assertion generation service used to begin a Federated session.

However in the case of the redirect.jsp, the location of this service is given as a parameter in the URL of the redirect page and is not checked to ensure that it is valid. To prevent disclosure or modification of the URL parameter, CA recommends that a new jsp page secureredirect.jsp be deployed. Administrators should use the Secure URL feature to ensure the SSO Service encrypts the SMPORTALURL query parameter and that it appends to the Authentication URL prior to redirecting the user to establish a SiteMinder session. A similar attack may be possible if the Web site allows for both HTTP and HTTPS logins. However, if HTTP is disabled per the product documentation, this style of attack does not apply. For instructions on performing this configuration refer to "Evaluated Configuration for CA SiteMinder® Federation Security Services r12 SP1 CR3" (08 February 2010).

13 Security Target

The security target for this product's evaluation is *CA SiteMinder® Federation Security Services r12 SP1 CR3 Security Target version 1.0, dated April 5, 2010.*

14 List of Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
CA (not vendor)	Certificate Authority
CAP	Composed Assurance Package
CC	Common Criteria
CRL	Certificate Revocation List
DB	Database
DER	Distinguished Encoding Rules
DNS	Domain Name Service

Acronym	Definition
EAL	Evaluation Assurance Level
ECP	Enhanced Client or Proxy
FIPS	Federal Information Processing Standards
FSS	Federation Security Services
FTP	File Transfer Protocol
FWS	Federation Web Services
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol over SSL
ID	Identification
IDP	Identity Provider
IETF	Internet Engineering Task Force
IT	Information Technology
J2EE	Java 2 Platform, Enterprise Edition
JSP	Java Server Pages
LDAP	Lightweight Directory Access Protocol
MDSSO	Multi-domain Single Sign-On
OASIS	Organization for the Advancement of Structured Information Standards
OCSP	Online Certificate Status Protocol
ODBC	Open Database Connectivity
OS	Operating System
PKCS	Public Key Cryptography Services
PEM	Privacy-Enhanced Electronic Mail
PS	Policy Server
RP	Relying Party
SAML	Security Assertion Markup Language
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SLO	Single Logout
SM	SiteMinder
SMTP	Simple Message Transfer Protocol
SP	Service Provider
SPS	Secure Proxy Server
SQL	Structured Query Language
SSL	Secure Socket Layer
SSO	Single Sign-on
ST	Security Target
TCP/IP	Transmission Control Protocol/Internet Protocol
TOE	Target of Evaluation
TSF	TOE Security Functionality
UI	User Interface
URL	Uniform Resource Locator
WA	Web Agent
WAM	Web Access Management
WS	Web Server

15 Terminology

Term	Definition
Account Linking	The process by which a user’s identification information is used to bridge two distinct accounts.

Term	Definition
Administrator	A trusted user who has privileges to administer the TOE.
Affiliate Domain	A logical grouping of federated entities associated with one or more user stores. The affiliate domain not only contains federated entities but it also defines which user stores are associated with the domain. To authenticate a user, CA SiteMinder must have access to the user store where a user record is defined. The Policy Server locates a user record by querying the user stores specified in the affiliate domain's search order. The search order is defined when adding user store connections to an affiliate domain. The order of directories can be shifted.
Artifact	A reference to a SAML assertion.
Artifact Resolution Service	Provides a mechanism by which SAML protocol messages may be passed by reference using a small, fixed-length value called an artifact. The artifact receiver uses the Artifact Resolution Service to ask the message creator to dereference the artifact and return the actual protocol message. The artifact is passed to a message recipient using one SAML binding (e.g. HTTP Redirect) while the resolution request and response take place over a synchronous binding, such as SOAP.
Asserting Party	A SAML authority that generates an assertion for use by a Relying Party. The Asserting Party creates, maintains, and manages identity information for users and provides user authentication to other relying parties. In SAML 2.0, an Asserting Party is the Identity Provider. In SAML 1.1, an Asserting Party is the producer.
Assertion	An assertion contains several different internal statements about authentication, authorization, and attributes. The valid structure and contents of an assertion are defined by the SAML assertion XML schema. Assertions are created by an Asserting Party based on a request of some sort from a Relying Party, although under certain circumstances, the assertions are delivered to a Relying Party in an unsolicited manner. SAML defines two browser-based protocols that specify how SAML assertions are passed between partners to facilitate single sign-on. The profiles are: • Browser/artifact profile—defines a SAML artifact as a reference to a SAML assertion. • Browser/POST profile—returns a response that contains an assertion. Note: For SAML 2.0, the artifact and POST profiles are referred to as HTTP bindings.
Assertion Query/Request Profile	The SAML Attribute Authority adheres to the SAML 2.0 Assertion Query/Request profile. It relies on the Attribute Service to process a query message and create attribute assertions. The SAML Requester is a SAML entity that uses the SAML 2.0 Assertion Query/Request profile to request attributes for a user
Attribute Authority	The SAML Attribute Authority adheres to the SAML 2.0 Assertion Query/Request profile. It relies on the Attribute Service to process a query message and create attribute assertions. These assertions contain user attributes that a SAML Requester uses for CA SiteMinder to authorize access to protected resources. The Attribute Service is part of the Federation Web Services application.

Term	Definition
Attribute Service	The Attribute Service uses the NameID to disambiguate the user so it knows what values to return for the requested attributes. The Attribute Service returns a response message that includes an attribute assertion wrapped in a SOAP message. This response includes the user attributes. When an attribute is configured, Administrators indicate whether the attribute is used as part of a single sign-on request, or to satisfy an attribute query request. The attributes function is determined by the Retrieval Method field in the SAML Service Provider Attribute dialog.
Attribute Statement	Specific identifying attributes about the subject
Authentication Scheme	An authentication scheme is a Policy Server object that determines the credentials a user will need to access a protected resource. Authentication schemes are assigned to realms. When a user tries to access a resource in a realm, the authentication scheme of the realm determines the credentials that a user must supply in order to access the resource.
AuthnRequest Service (SAML 2.0)	This service enables a Service Provider to generate an AuthnRequest message for cross-domain single sign-on. This message contains information that enables Federation to redirect the user’s browser to the Single Sign-on Service at the Identity Provider. The AuthnRequest service is used for single sign-on using POST and artifact binding. *Note: The format of the AuthnRequest message issued by this service is specified in the Profiles for the OASIS Security Assertion Markup Language (SAML) v2.0.*
Authorization	The process of identifying and authenticating an administrator user by the TOE.
Backchannel	Used for secure communications directly with remote partner (i.e. not through user browser); Federated Web Server(s) in communication with a Web Agent
Binding	SAML Binding refers to how the various SAML protocol messages are carried over underlying transport protocols. Note: For SAML 2.0, the artifact and POST profiles are referred to as HTTP bindings.
Consumer	The Relying Party (SAML 1.1). A consumer is the entity that uses the SAML assertions to authenticate a user and to establish a session for the user.
Disambiguation	The method by which the TOE locates a user in the user store.
Enhanced Client and Proxy (ECP) Profile	Defines a specialized SSO profile where enhanced clients or proxies use the Reverse-SOAP (PAOS) and SOAP bindings.
Entity Role	An Asserting or Relying Party.
Entity Type	A local or remote entity.
Federated Network	In a federated network, there is an entity that generates SAML assertions (Asserting Party). Assertions contain information about a user whose identity is maintained locally at the federated entity that generates them. There is another entity that uses the SAML assertions (Relying Party) to authenticate a user and to establish a session for the user. Depending on the protocol, these two entities are named differently, but the functions they serve are the same. In SAML 1.1, the Asserting Party is known as a producer, while the Relying Party is known as a consumer. In SAML 2.0, the Asserting Party is known as an Identity Provider (IdP), while the Relying Party is known as a Service Provider (SP). A federated entity may be both a producing authority (Identity Provider/IdP) and a consuming authority (Service Provider/SP).

Term	Definition
Federation	A federation consists of one Asserting Party (Identity Provider/IdP) and one or more relying parties (Service Provider/SP). A federation provides a means for these partner services to agree on and establish a common, shared name identifier to refer to the user in order to share information about the user across the organizational boundaries.
Federated Entity	A partner in a federated network.
Federation Web Services	Also referred to as Web Agent Option Pack. Consists of the following: • Single Sign On (SSO) • Single Log Out (SLO) • Artifact Resolution • Assertion Consumer • Inter-site Transfer • SAML Credential Collector • Assertion Retriever • Agent API • Attribute Service • Auth URL JSP FWS provides the SAML credential collector servlet, which consumes assertions and other services for federated network configurations.
Get/Put/POST	An HTTP operation known as a user's request. It is received by the Web Agent and forwarded to the Policy Server.
Groups	A group (agent group, rule group, response group) contains individual items or groups of its own type. For example, a rule group can contain rules and/or groups of rules.
HTTP Artifact Binding	Defines that an artifact (described above in the Artifact Resolution Protocol) needs to be transported from a message sender to a message receiver using HTTP. Two mechanisms are provided: either an HTML form control or a query string in the URL."
HTTP Redirect Binding	Defines how SAML protocol messages are transported using HTTP redirect messages (302 status code responses)
HTTP POST Binding	Defines how SAML protocol messages are transported within the base64-encoded content of an HTML form control.
Identity Mapping	The method of user identification; the user identification decision determines what information (one or more user attributes) is sent as the user identity in the assertion.
Identity Provider (IdP)	The Asserting Party (SAML 2.0). The IdP generates SAML assertions to be used by the Service Provider.
Key Store	Entity used by the CA SiteMinder Policy Server to store encryption keys used by the Policy Server when communicating with CA SiteMinder Web Agents.
Option Pack	The Policy Server Option Pack is an add-on to the CA SiteMinder Policy Server. It contains the central processing of the TOE, which includes the operations to create and extract data from SAML assertions, and query and modification of CA SiteMinder data stores. This add-on is not a separate installer; instead, it is a selectable option during the installation of the Policy Server.
Policy	A policy is a Policy Server object that binds users, rules, responses, and optionally, time restrictions and IP address restrictions together. Policies establish entitlements for a CA SiteMinder protected entity. When a user attempts to access a resource, the policy is what CA SiteMinder ultimately uses to resolve the request.

Term	Definition
Policy Domains	A policy domain is a logical grouping of one or more user stores, administrators, and realms. This Policy Server object is the basis for entitlement data. By creating policy domains, an administrator creates a container for entitlements that surround a particular group of resources (realm), as well as the users who may access the resources, and the administrator who sets up entitlements.
Policy Server	CA SiteMinder software component that provides a platform for managed key operations, authentication, authorization, and security management. The Policy Server provides the SAML authentication scheme at the Relying Party. It also provides the SAML assertion generator used by a producing federated entity.
Policy Server Option Pack	See Option Pack.
Policy Store	Collection of CA SiteMinder Policy Server objects. Policy stores reside in an ODBC (see page 19)-enabled database or an LDAP (see page 17) directory.
Producer	The Asserting Party (SAML 1.1). A producer is the entity that generates the SAML assertions.
Profile	SAML profiles define how the SAML assertions, protocols, and bindings are combined and constrained to provide greater interoperability in particular usage scenarios. Some of these profiles are examined in detail later in this document.
Protocol Message	SAML protocol messages are used to make the SAML-defined requests and return appropriate responses. The structure and contents of these messages are defined by the SAML-defined protocol XML schema.
Protected Resource	Any set of data or applications that require authorization and authentication in order to gain access.
Protection Level	A number between 0 and 1000 that is given to authentication schemes. A higher number indicates a higher level of protection.
Realm	A realm is a Policy Server object that identifies a group of resources. Realms define a directory or folder and possibly its subdirectories.
Relying Party	A SAML entity that uses information from a SAML authority to provide access to services. The Relying Party uses assertions it receives from an Asserting Party to authenticate a user. In SAML 2.0, the Relying Party is the Service Provider. In SAML 1.1, the Relying Party is the consumer.
Reverse SOAP (PAOS) Binding	Defines a multi-stage SOAP/HTTP message exchange that permits an HTTP client to be a SOAP responder. Used in the Enhanced Client or Proxy Profile and particularly designed to support WAP gateways.
Rule	A Policy Server object that identifies a resource and the actions that will be allowed or denied access to the resource. Rules also include actions associated with specific events, such as what to do if a user fails to authenticate correctly when asked for their credentials.
SAML Attribute	A component of a user's Distinguished Name (DN) required by a Relying Party in a federation to disambiguate the user during Single Sign-On.
Scope	Indicates whether the administrator's privileges extend to all domains and applications or to only specific domains and applications.
Secure Proxy Engine	Forwards traffic to backend servers; employs web server, servlet engine, proxy server and Federation Web Services features. This engine consists of two components – Apache Web Server and Tomcat server.
Security Assertion Markup Language (SAML)	This standard defines an XML-based framework for describing and exchanging security information between on-line business partners. In the evaluated configuration, SAML v1.1 and v2.0 are used.
Security Zone	A security zone is a segment of a single cookie domain, used as a method of partitioning applications to permit different security requirements for resource access.
Service Provider (SP)	The Relying Party (SAML 2.0)

Term	Definition
Single Logout Profile	Defines how the SAML Single Logout Protocol is used with SOAP, HTTP Redirect, HTTP POST, and HTTP Artifact bindings.
Single Logout Protocol	Defines a mechanism to allow near-simultaneous logout of active sessions associated with a principal. The logout is directly initiated by the user, or initiated by an IdP or SP because of a session timeout, administrator command, etc.
Single Sign-on Service (SAML 2.0)	This service enables an Identity Provider to process IdP-or SP-initiated requests for federated resources. The Identity Provider gathers the necessary Service Provider configuration information to generate an assertion that it passes back to the Service Provider. The Service Provider then uses the assertion for authentication purposes.
CA SiteMinder Object	Rules, realms, domains, and other components of CA SiteMinder which can be managed by the TOE. Refer to Table 7-2 for applicable functions.
SLO Service	This service allows a user to log out of all applications in the federation simultaneously, with a single logout event. Single logout is initiated by an Identity Provider or a Service Provider.
Smkeydatabase	The smkeydatabase is a key and certificate database used for signing, verification, encryption, and decryption between a CA SiteMinder consuming authority and a CA SiteMinder producing authority. The database is made up of multiple files. Administrators manage and retrieve keys and certificates in this database using the CA SiteMinder tool called smkeytool.
Tunnel Services	Tunnel Services provides an API which is used to facilitate trusted channels for communications between distributed parts of the TOE
User	An authorized user of the TOE without administrative privileges.
User Store	A user store in CA SiteMinder is an object that contains details for connecting to an existing user store that resides outside of CA SiteMinder. This allows an administrator to configure a simple connection to an existing user store, instead of replicating user information within CA SiteMinder. The username space is an LDAP directory server.
User Session	An instance of a user requesting a federated resource or an Administrator managing the TOE. Once granted access to the federated resource by CA SiteMinder, the session is established across the federation and becomes a global session.
Web Agent	A Web Agent is installed on a Web server to secure access to resources.
Web Agent Configuration Object	An Agent Configuration Object holds configuration parameters for one or more Web Agents.
Web Agent Group	A Web Agent group is a Policy Server object that points to a group of Agents. The Agents in the group can be installed on different servers, but all of the Agents protect the same resources. Agent groups are configured in CA SiteMinder for groups of servers that distribute the workload for access to a popular set of resources.
Web Agent Option Pack	See Federation Web Services.
Xpath Query	Xpath is how an Administrator specifies a path to a specific component of an XML file. Xpath is used to define where to look up user information in the XML file.

16 Bibliography

1. Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and general model, Version 3.1 Revision 3.
2. Common Criteria for Information Technology Security Evaluation – Part 2: Security functional requirements, Version 3.1 Revision 3.
3. Common Criteria for Information Technology Security Evaluation – Part 3: Security assurance requirements, Version 3.1 Revision 3.
4. Common Evaluation Methodology for Information Technology Security Evaluation, Version 3.1 Revision 3.
5. CA SiteMinder® Federation Security Services r12 SP1 CR3 Security Target version 1.0, April 5, 2010
6. Evaluation Technical Report for a Target of Evaluation "CA SiteMinder® Federation Security Services r12 SP1 CR3 Security Target v1.0" Evaluation Technical Report v3.0 dated 5 April 2010.