Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

2012/78

2 May 2012

Version 1.0

Amendment Record

Version	Date	Description
1.0	02/05/2012	Public release.

Executive Summary

1 The Target of Evaluation (TOE) is Active Directory Federation Services(ADFS) 2.0. The TOE is a product that is designed to provide an identity access solution providing a suite of software components that manage and process authentication and authorisation claims across trusted organisational network boundaries and also across heterogeneous environments. The TOE provides the necessary infrastructure for implementing a web-based single sign on (SSO) capability for claims-aware applications for both local users and external users from trusted partner organisations.

2 This report describes the findings of the IT security evaluation of Microsoft's Active Directory Federation Services 2.0, to the Common Criteria (CC) evaluation assurance level EAL4 + ALC_FLR.3 . The report concludes that the product has met the target assurance level of EAL4 + ALC_FLR.3 and that the evaluation was conducted in accordance with the Common Criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by stratsec lab and was completed on 27 March 2012.

3 With regard to the secure operation of the TOE, the Australasian Certification Authority (ACA) recommends that users and administrators:

a) Ensure that the TOE is operated in the evaluated configuration and that assumptions concerning the TOE security environment are fulfilled;
b) Operate the TOE according to the administrator guidance (Ref [3]); and
c) Maintain the underlying environment in a secure manner so that the integrity of the TOE Security Functions is preserved.

4 This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

5 It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target at Ref [1] and read this Certification Report prior to deciding whether to purchase the product.

Table of Contents

Chapter 1 - Introduction

1.1 Overview

6 This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

1.2 Purpose

7 The purpose of this Certification Report is to:

a) report the certification of results of the IT security evaluation of the TOE, Active Directory Federation Services 2.0, against the requirements of the Common Criteria (CC) evaluation assurance level EAL4 + ALC_FLR.3, and

b) provide a source of detailed security information about the TOE for any interested parties.

8 This report should be read in conjunction with the TOE's Security Target (Ref [1]) which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

1.3 Identification

9 Table 1 provides identification details for the evaluation. For details of all components included in the evaluated configuration refer to section 2.6.1 Evaluated Configuration.

Table 1: Identification Information

Item	Identifier
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	Active Directory Federation Services 2.0
Software Version	KB974408
Security Target	Active Directory Federation Services 2.0 Security Target v1.0, 23 March 2012.
Evaluation Level	EAL4 + ALC_FLR.3
Evaluation Technical Report	Evaluation Technical Report Microsoft Active Directory Federation Services 2.0, Version 1.0, 20 April 2012
Criteria	Common Criteria for Information Technology Security Evaluation Parts 1,2 & 3 July 2009, Version 3.1 Revision 3 Final.
Methodology	Common Methodology for Information Technology Security

	Evaluation, Evaluation Methodology, July 2009, Version 3.1, Revision 3, CCMB-2009-07-004
Conformance	Common Criteria Part 2 conformant, Part 3 Augmented (EAL4 + ALC_FLR.3)
Sponsor	Microsoft One Microsoft Way Redmond, WA 98052 USA
Developer	Microsoft One Microsoft Way Redmond, WA 98052 USA
Evaluation Facility	stratsec lab 1 / 50 Geils Crt Deakin ACT 2600 Australia

Chapter 2 - Target of Evaluation

2.1 Overview

10 This chapter contains information about the Target of Evaluation (TOE), including: a description of functionality provided; its architecture components; the scope of evaluation; security policies; and its secure usage.

2.2 Description of the TOE

11 The TOE is Active Directory Federation Services (ADFS) 2.0 developed by Microsoft.

12 The TOE is a component of Microsoft Windows Server 2008, and provides an identity access solution providing a suite of software components that manage and process authentication and authorisation claims across trusted organisational network boundaries and also across heterogeneous environments. The TOE provides the necessary infrastructure for implementing a web-based single sign on (SSO) capability for claims-aware applications for both local users and external users from trusted partner organisations.

2.3 Security Policy

13 The TOE Security Policy (TSP) is defined in the Security Target (Ref [1]). A summary of the TSP is provided below:

a) CLAIMS-SFP – This Security Functional Policy (SFP) is the only explicitly defined security policy in the ST. This policy defines the rules for issuing and relying on claims between two instances of the TOE.

The Security Target (Ref [1]) additionally contains the following implied TSPs:

a) Authentication policy – when and how is a user authenticated;

b) Secure management policy – rules governing the use of the management functions; and

c) Secure communication policy – policy ensuring secure communication between two instances of the TOE.

2.4 TOE Architecture

14 The TOE consists of the following major architectural components:

a) **Federation Service;**

b) **Federation Service Proxy; and**

c) **AD FS management snap-in.**

15 The Developer's Architectural Design identifies the following components of the TOE:

a) **Federation Service.** This component manages federation trust relationships between organisations and associated policies. The FS also issues security tokens for users successfully authenticated by the external attribute store that includes the claims data. The Federation Service can be deployed on one or more Federation Servers that share a common trust policy. The Federation Service routes and manages authentication requests and generates security tokens for local, remote business partner users from trusted organisations. The Federation Service is the core component of the capability housing the metadata and policy and also the security token service for the TOE.

b) **Federation Service Proxy.** The Federation Service Proxy component is proxy to the Federation Service in the perimeter network (also commonly known as a demilitarised zone or a screened subnet). The Federation Service Proxy uses WS-Federation Passive Requestor Profile (WS-F PRP) protocols to collect user credential information from browser clients, and it sends the user credential information to the Federation Service on the requesting user's behalf. This component processes client token requests and provides a user interface for browser-based clients.

c) **AD FS management snap-in.** The AD FS snap-in is a single Microsoft Management Console (MMC) snap-in. It provides a graphical user interface (GUI) for configuring service and policy settings that are used most commonly with AD FS solution.

16 The following components are considered outside the physical scope of the TOE, but are necessary software elements that support the TOE in delivering the security objectives:

a) **Attribute Stores.** AD FS uses the term ***attribute stores*** to refer to directories or databases that an organisation uses to store its user accounts and their associated attribute values. After it is configured as an identity provider organisation, AD FS retrieves these attribute values from the store and creates claims based on that information so that a web application or service that is hosted in a relying party organisation can make the appropriate authorisation decisions whenever a federated user (a user whose account is stored in the identity provider organisation) attempts to access the application or service. The attribute store also provides the capability to authenticate the user's claims so that appropriate claims can be included in the returned token.

b) **Configuration database.** The AD FS configuration database stores all the configuration data that represents a single instance of AD FS (the Federation Service). The AD FS configuration database defines the set of parameters and rules that a Federation Service requires to identify partners, certificates, attribute stores, claims, and various data about these associated entities. This data store can be in either a Microsoft SQL Server database or the Windows Internal Database feature that is included with Windows Server 2008 and Windows Server 2008 R2.

c) **Claims-aware applications.** Developers will typically use the Windows Identity Foundation (WIF) to build a claims-aware application. However, while some elements of WIF have been used to develop the TOE, the use of this framework and development of the client-side applications is outside the scope of the evaluation.

2.5 Clarification of Scope

17 The scope of the evaluation was limited to those claims made in the Security Target (Ref [1]).

2.5.1 Evaluated Functionality

18 The TOE provides the following evaluated security functionality:

a) **Claims policy management.** AD FS provides a claims rules engine that is used to manage claims policy for the implementation of the capability. In the context of digital identities, claims are statements that one subject makes about itself or another subject. These claims can be made by a person directly or provided to others by a third party. Other parties can rely on the values of the claims to perform a process of digital identification.

b) **Trust management.** AD FS implements the capability to manage cross-organisational (federation-based) collaboration. The determination of the trust relationship depends on whether the organisation will host a web resource to be accessed by other organisations across the Internet—or the reverse.

c) **Token issuance.** AD FS implements a security token service (STS) that processes all claims and requests for tokens.

2.5.2 Non-evaluated Functionality and Services.

19 Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration; Australian Government users should refer to 2012 Australian Government Information Security Manual (ISM) (Ref [2]) for policy relating to using an evaluated product in

an un-evaluated configuration. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

20 It should be noted that this evaluation did not cover the entire functionality of Microsoft Windows. The evaluation was only concerned with the issuing and processing of claims by AD FS.

2.6 Usage

2.6.1 Evaluated Configuration

21 This section describes the configurations of the TOE that were included within scope of the evaluation. The assurance gained via evaluation applies specifically to the TOE in these defined evaluated configuration. Australian Government users should refer to the ISM (Ref [2]) to ensure that configuration meet the minimum Australian Government policy requirements. New Zealand Government users should consult the GCSB.

22 The TOE is comprised of the following software components:

a) Active Directory Federated Services 2.0 (KB974408)

23 The TOE relies on the following hardware:

a) General server grade hardware.

24 The TOE is a component of the Windows Server 2008 operating system. As such, there is not a security configuration beyond a standard installation and topology development. The evaluated configuration is based on default installation of the TOE. Microsoft provides the following guidance to assist their customers understand the deployment and usage of the TOE, as referenced in the installation guidance.

2.6.2 Delivery procedures

25 The TOE is downloaded from the Microsoft website.

2.6.3 Determining the Evaluated Configuration

26 To verify the ADFS 2.0 Package is downloaded from the trusted source, perform the following steps:

a) Download the package from Microsoft website. The download link is http://www.microsoft.com/downloads/en/details.aspx?familyid=118c3588-9070-426a-b655-6cec0a92c10b&displaylang=en

b) Locate the AdfsSetup.exe file, right-click and select Properties. This will bring up the Properties dialog box;

c) At the top, click the Digital Signatures tab;

d) Click on Details. Look for Signer Information and note the value. It should be Microsoft Corporation;

e) Click the View Certificate;

f) At the top, click the Details tab;

g) Look for Issuer and note the value. It should be Microsoft Code Signing PCA; and

h) Close the Properties window.

27 To verify the build numbers of the ADFS 2.0 Services perform the following steps:

a) Click on Start | Control Panel | Programs and Features;

b) At the left pane, click on View installed updates;

c) Look for Active Directory Federation Services 2.0 (KB974408);

d) KB974408 is the update code from Microsoft Corporation; and

e) Close the Installed Updates dialog box.

2.6.4 Documentation

28 It is important that the TOE is used in accordance with guidance documentation in order to ensure secure usage. The following documentation is available upon request from the developer:

a) Guidance Documentation and associated references (Ref [3]).

2.6.5 Secure Usage

29 The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met.

30 The following assumptions were made:

Identifier	Assumption statement
A.COMMS	It is assumed that any connection between an untrusted network and the underlying servers for the federation service is appropriately secured by a firewall.
A.INSTALL	It is assumed that the TOE will be delivered, installed, configured and set up in accordance with documented delivery and installation/setup procedures.

Identifier	Assumption statement
A.ACCESS	It is assumed that the underlying server operating systems will provide access control mechanisms to restrict modification to TOE executables, the platform itself, configuration files and databases only to the administrators authorised to perform these functions.
A.I&A	It is assumed that underlying server operating systems will provide the capability to enforce identification and authentication of local administrators.
A.ATTRIBUTE	It is assumed that the IT environment will provide secure methods for storing managing and supplying identity related attributes for populating submitted claims as requested by the TOE.
A.CONFIG	It is assumed that the IT environment will provide secure methods for storing and managing TSF data for the TOE.
A.UNTRUSTED	It is assumed that no untrusted software is installed on machines with the TOE.
A.COMPETENT	It is assumed that there will be one or more competent administrators assigned to manage the TOE, its platform and the security of the information both of them contain.
A.NO_EVIL	It is assumed that the administrator(s) are not careless, willfully negligent, nor hostile, and will follow and abide by the instructions provided by the administration documentation.
A.PARTNERS	It is assumed that organisations that enter into a trust relationship are capable of providing the necessary IT environment and operational support to effectively manage their attribute store, federation service and underlying platforms.
A.CERTIFICATES	It is assumed that the IT environment and underlying server operating systems are capable of producing and securely managing the necessary cryptographic certificates required.
A.PROTECT	It is assumed that the TOE and its platform will be located within facilities providing controlled access to prevent unauthorised physical access.

Chapter 3 - Evaluation

3.1 Overview

31 This chapter contains information about the procedures used in conducting the evaluation and the testing conducted as part of the evaluation.

3.2 Evaluation Procedures

32 The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 3 (Refs [4], [5], and [6]). The methodology used is described in the Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 3 (CEM) (Ref [7]). The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs [8], [9] and [10]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [11]) were also upheld.

3.3 Functional Testing

33 To gain confidence that the developer's testing was sufficient to ensure the correct operation of the TOE, the evaluators analysed the evidence of the developer's testing effort. This analysis included examining: test coverage; test plans and procedures; and expected and actual results. The evaluators drew upon this evidence to perform a sample of the developer tests in order to verify that the test results were consistent with those recorded by the developers.

3.4 Penetration Testing

34 The developer performed a vulnerability analysis of the TOE in order to identify any obvious vulnerability in the product and to show that the vulnerabilities were not exploitable in the intended environment of the TOE. This analysis included a search for possible vulnerability sources in publicly available information .

35 The evaluators' penetration tests are based on an independent vulnerability analysis of the TOE using the guidance documentation, functional specification, TOE design, security architecture description, implementation representation as well as available public information. The evaluators used these tests to determine that the TOE is resistant to attacks performed by an attacker possessing Enhanced-Basic attack potential. The following factors have been taken into consideration during the penetration tests:

a) Time taken to identify and exploit (elapsed time);

b) Specialist technical expertise required (specialist expertise);

c) Knowledge of the TOE design and operation (knowledge of the TOE);

d) Window of opportunity; and

e) IT hardware/software or other equipment required for exploitation.

Chapter 4 - Certification

4.1 Overview

36 This chapter contains information about the result of the certification, an overview of the assurance provided by the level chosen, and recommendations made by the certifiers.

4.2 Certification Result

37 After due consideration of the conduct of the evaluation as witnessed by the certifiers and of the Evaluation Technical Report (Ref [12]), the Australasian Certification Authority certifies the evaluation of Active Directory Federation Services 2.0 - Product performed by the Australasian Information Security Evaluation Facility, stratsec lab.

38 stratsec lab has found that Active Directory Federation Services 2.0 upholds the claims made in the Security Target (Ref [1]) and has met the requirements of the Common Criteria (CC) evaluation assurance level EAL4 + ALC_FLR.3.

39 Certification is not a guarantee of freedom from security vulnerabilities.

4.3 Assurance Level Information

40 EAL4 provides assurance by a full security target and an analysis of the SFRs in that ST, using a functional and complete interface specification, guidance documentation, a description of the basic modular design of the TOE, and a subset of the implementation, to understand the security behaviour.

41 The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification and TOE design, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, implementation representation, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with an Enhanced-Basic attack potential.

42 EAL4 also provides assurance through the use of development environment controls and additional TOE configuration management including automation, and evidence of secure delivery procedures.

43 This EAL represents a meaningful increase in assurance from EAL3 by requiring more design description, the implementation representation for the entire TSF, and improved mechanisms and procedures that provide confidence that the TOE will not be tampered with during development.

4.4 Recommendations

44 Not all of the evaluated functionality present in the TOE may be suitable for Australian and New Zealand Government users. For further guidance, Australian Government users should refer to ISM (Ref [2]) and New Zealand Government users should consult the GCSB.

45 In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance document is followed (Ref [3], the ACA also recommends that users and administrators:

a) Ensure that the TOE is operated in the evaluated configuration; and
b) Maintain the underlying environment in a secure manner so that the integrity of the TOE Security Functions is preserved.

Annex A - References and Abbreviations

A.1 References

[1] Active Directory Federation Services 2.0 Security Target v1.0, 23 March 2012.

[2] 2012 Australian Government Information Security Manual (ISM), Defence Signals Directorate, (available at www.dsd.gov.au).

[3] Active Directory Federation Services (AD FS) 2.0, Guidance documentation, Version 0.2, 08-JUL-2011.

[4] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model July 2009 Version 3.1 Revision 3 Final CCMB-2009-07-001.

[5] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components July 2009 Version 3.1 Revision 3 Final CCMB-2009-07-002.

[6] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components July 2009 Version 3.1 Revision 3 Final CCMB-2009-07-003.

[7] Common Methodology for Information Technology Security Evaluation, Evaluation methodology, July 2009, Version 3.1, Revision 3, CCMB-2009-07-004.

[8] AISEP Publication No. 1 – Program Policy, AP 1, Version 3.1, 29 September 2006, Defence Signals Directorate.

[9] AISEP Publication No. 2 – Certifier Guidance, AP 2. Version 3.3, September 2007, Defence Signals Directorate.

[10] AISEP Publication No. 3 – Evaluator Guidance, AP 3. Version 3.1, 29 September 2006, Defence Signals Directorate.

[11] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000.

[12] Evaluation Technical Report, Microsoft Active Directory Federation Services 2.0, Version 1.0, 20 April 2012.

A.2 Abbreviations

AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
CC	Common Criteria
CEM	Common Evaluation Methodology
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GCSB	Government Communications Security Bureau
PP	Protection Profile
SFP	Security Function Policy
SFR	Security Functional Requirements
ST	Security Target
STS	Security Token Service
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
WIF	Windows Identity Foundation
WS-F PRP	Web Service-Federation Passive Requestor Profile (protocol).