Reference: 2024-53-INF-4723- v1
Target: Limitada al expediente
Date: 06.02.2026

Created by: I008
Revised by: CALIDAD
Approved by: TECNICO

CERTIFICATION REPORT

Dossier #	**2024-53**
TOE	**WSO2 Identity Server v7.0.0, update level 126**
Applicant	**87-0750575 - WSO2 LLC**
References	

[EXT-9363] 2024-11-22_2024-AM_solicitud_certificacion

[EXT-9946] 2025-12-18_2024-53_ETR_vM1

Certification report of the product WSO2 Identity Server v7.0.0, update level 126, as requested in [EXT-9363] dated 29/11/2024, and evaluated by Applus Laboratories, as detailed in the Evaluation Technical Report [EXT-9946] received on 18/12/2025.

CONTENTS

EXECUTIVE SUMMARY

This document constitutes the Certification Report for the certification file of the product WSO2 Identity Server v7.0.0, update level 126.

The TOE is a software application used in enterprise environments to manage identities, access, and authorization through different apps.

Developer/manufacturer: WSO2 LLC

Sponsor: WSO2 LLC.

Certification Body: Centro Criptológico Nacional (CCN) del Centro Nacional de Inteligencia (CNI).

ITSEF: Applus Laboratories.

Protection Profile: Protection profile Enterprise Security Management Identity and Credential Management v2.1 with strict conformance [PP-ESM-I-CM].

Evaluation Level: EAL1 + ASE_SPD.1 + ASE_OBJ.2

Evaluation end date: 22/12/2025

Expiration Date[1]: 18/01/2026

All the assurance components required by the evaluation level EAL1 (augmented with ASE_SPD.1 + ASE_OBJ.2) have been assigned a “PASS” verdict. Consequently, the laboratory Applus Laboratories assigns the “PASS” VERDICT to the whole evaluation due all the evaluator actions are satisfied for the EAL1 level (augmented with ASE_SPD.1 + ASE_OBJ.2), as defined by the CC:2022 r1 and the CEM:2022.

Considering the obtained evidences during the instruction of the certification request of the product WSO2 Identity Server v7.0.0, update level 126, a positive resolution is proposed.

TOE SUMMARY

The Target of Evaluation (TOE) is WSO2 Identity Server (WSO2 IS), version 7.0.0, update level 126. Referred to as TOE from this point forward. The TOE is a powerful, modern identity and access management solution for on-premises or cloud environments. It enables organizations to deliver exceptional, trusted digital experiences to all types of users.

[1] This date refers to the expiration date of the certificate recognition within the scope of the mutual recognition arrangements signed by this Certification Body.

The TOE can handle authentication requests from integrated service providers and redirect them to the appropriate authentication services remotely or locally. The WSO2 Identity Server ensures easy integration with various applications to facilitate single sign-on (SSO), social login, identity federation, API security, strong authentication, account management, and privacy compliance.

SECURITY ASSURANCE REQUIREMENTS

The product was evaluated with all the evidence required to fulfil the evaluation level EAL1 (augmented with ASE_SPD.1 + ASE_OBJ.2), according to Common Criteria 2022 R1.

ASSURANCE CLASS	ASSURANCE COMPONENT
ADV	ADV_FSP.1
AGD	AGD_OPE.1
	AGD_PRE.1
ALC	ALC_CMC.1
	ALC_CMS.1
ASE	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.1
	ASE_TSS.1
	ASE_SPD.1
ATE	ATE_IND.1
AVA	AVA_VAN.1

SECURITY FUNCTIONAL REQUIREMENTS

The product security functionality satisfies the following functional requirements, according to the Common Criteria 2022 Release 1:

SECURITY FUNCTIONAL REQUIREMENT
ESM_EAU.2
ESM_EID.2
ESM_ICD.1
ESM_ICT.1

FAU_GEN.1
FAU_STG.1
FAU_STG.2
FIA_USB.1
FMT_MOF.1
FMT_SMF.1
FMT_SMR.1
FPT_APW_EXT.1
FPT_SKP_EXT.1
FTA_TAB.1
FTP_ITC.1
FTP_TRP.1

IDENTIFICATION

Product: WSO2 Identity Server v7.0.0, update level 126, update level 126

Security Target: WSO2 Identity Server ST v1.7

Protection Profile: Protection profile Enterprise Security Management Identity and Credential Management v2.1 with strict conformance [PP-ESM-I-CM].

Evaluation Level: EAL1 + ASE_SPD.1 + ASE_OBJ.2

SECURITY POLICIES

The use of the product WSO2 Identity Server v7.0.0, update level 126 shall implement a set of security policies assuring the fulfilment of different standards and security demands.

The detail of these policies is documented in the Security Target, section 4.3.2 (“Organizational Security Policies”).

ASSUMPTIONS AND OPERATIONAL ENVIRONMENT

The following assumptions are constraints to the conditions used to assure the security properties and functionalities compiled by the security target. These assumptions have been applied during the evaluation in order to determine if the identified vulnerabilities can be exploited.

In order to assure the secure use of the TOE, it is necessary to start from these assumptions for its operational environment. If this is not possible and any of them could not be assumed, it would not be possible to assure the secure operation of the TOE.

The detail of these assumptions is documented in the Security Target, section 4.3.3 ("Assumptions").

CLARIFICATIONS ON NON-COVERED THREATS

The following threats do not suppose a risk for the product WSO2 Identity Server v7.0.0, update level 126, although the agents implementing attacks have the attack potential according to the Basic of EAL1 + ASE_SPD.1 + ASE_OBJ.2 and always fulfilling the usage assumptions and the proper security policies satisfaction.

For any other threat not included in this list, the evaluation results of the product security properties and the associated certificate, do not guarantee any resistance.

The threats covered by the security properties of the TOE are those defined in the Security Target, section 4.3.1 ("Threats").

OPERATIONAL ENVIRONMENT FUNCTIONALITY

The product requires the cooperation from its operational environment to fulfil some of the objectives of the defined security problem.

The security objectives declared for the TOE operational environment are those defined in the Protection Profile and they are documented in the Security Target, section 4.2 ("Security Objectives for the operational Environment").

ARCHITECTURE

LOGICAL ARCHITECTURE

The TOE is the main point of cohesion in an enterprise environment. It manages user accounts, credentials, and attributes used within the enterprise environment. The TOE also logs and controls users' actions through different applications.

Figure 1, "TOE Environment," presents the components that are in the TOE's scope. That is, TOE includes Identity and Credential management with control of repositories that keep identity and credential data, as well as relevant attributes.

The TOE can manage user accounts and their attributes and transmit these data by provisioning them to external entities.

Furthermore, the TOE permits the recording of different events as audit logs in a local and external database, thus registering all users' actions related to enterprise identification and authentication.

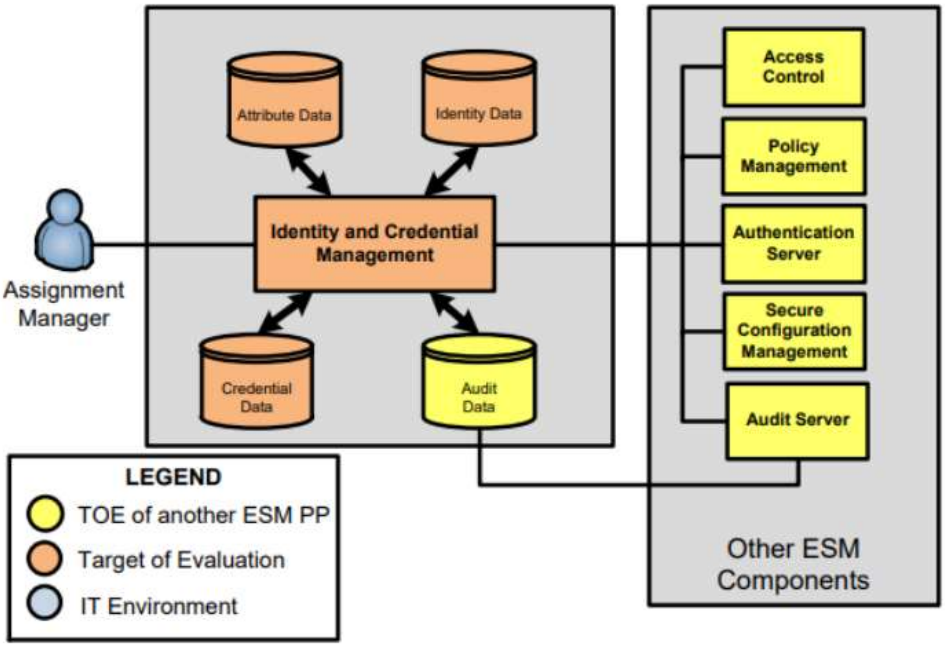

Figure 1 TOE Environment

PHYSICAL ARCHITECTURE

WSO2 Identity Server is a software-only TOE, and therefore, its physical boundary is its software. The TOE does not include the hardware or operating system of the system on which it is installed. It also does not include the third-party software that is required for the TOE to run (indicated in NonTOE software/hardware). The software bundle is available at the developer's GitHub delivered as a zip file.

DOCUMENTS

The product includes the following documents that shall be distributed and made available together to the users of the evaluated version.

- WSO2 Identity Server Preparative Procedures version 1.6
- WSO2 Identity Server Operational User Guidance version 1.5
- WSO2 Identity Server Security Target version 1.7
- WSO2 Identity Server API Calls Description version 1.0
- WSO2 Identity Server Documentation version 1.0

PRODUCT TESTING

All the tests have been executed using the testing scenario appropriate to the established architecture in the security target. It has also been checked that the obtained results during the tests fit or correspond to the previously estimated results.

In addition, the lab has devised a test for each of the security function of the product as required by the Protection Profile. It has been checked that the obtained results conform to the expected results and in the cases where a deviation in respect to the expected results was present, the evaluator has confirmed that this variation neither represents any security problem nor a decrease in the functional capacity of the product. Through the tests performed by the Laboratory it is concluded that all the SFRs are correctly implemented by the TOE.

EVALUATED CONFIGURATION

The TOE is defined by WSO2 Identity Server 7.0.0 with update level 126. The secure acceptance and installation procedures are given in WSO2 Identity Server Preparative Procedures version 1.6 and WSO2 Identity Server Operational User Guidance version 1.5 documents.

TOE Installation prerequisites are:

> Prior to installing the WSO2 Identity Server (TOE), it is necessary to have the appropriate prerequisite software installed on your system.
>
> The following details the supported operating system and hardware requirements:
>
> - **CPU:** 4 vCPUs (x86_64 Architecture)
> - **Memory:** 4 GB RAM
> - **Disk:** 10 GB disk space, excluding space allocated for log files and databases.
> - **OS:** Windows Server 2016 / Windows OS 10
>
> **Note:** Operating System (OS) versions can be later than the version shown above.

Also, the following additional software is needed:

> It is assumed that the system administrator will safely source, verify and install the correct version of these additional applications for the chosen operating system:

Software	Description	Version
Oracle Java JDK	For environment compatibility, the TOE requires that Oracle Java JDK is downloaded and installed on the machine.	17.0.2
MySQL	Used to replace the default database, as the default database used by the TOE must be changed for successful configuration of the TOE.	8.0 or above
Apache Ant	A requirement for the cipher tool, it is necessary to install this software for the cipher tool to perform its function.	1.9.x or above

EVALUATION RESULTS

The product WSO2 Identity Server v7.0.0, update level 126 has been evaluated against the Security Target WSO2 Identity Server ST v1.7.

All the assurance components required by the evaluation level EAL1 (augmented with ASE_SPD.1 + ASE_OBJ.2) have been assigned a "PASS" verdict. Consequently, the laboratory Applus Laboratories assigns the "**PASS**" **VERDICT** to the whole evaluation due all the evaluator actions are satisfied for the evaluation level EAL1 (augmented with ASE_SPD.1 + ASE_OBJ.2), as defined by the CC:2022 r1 and the CEM:2022.

COMMENTS & RECOMMENDATIONS FROM THE EVALUATION TEAM

Next, recommendations regarding the secure usage of the TOE are provided. These have been collected along the evaluation process and are detailed to be considered when using the product.

- To follow the security guidance's of the TOE strictly.

CERTIFIER RECOMMENDATIONS

Considering the obtained evidences during the instruction of the certification request of the product WSO2 Identity Server v7.0.0, update level 126, a positive resolution is proposed.

GLOSSARY

CCN Centro Criptológico Nacional

CNI Centro Nacional de Inteligencia

EAL Evaluation Assurance Level

ETR Evaluation Technical Report

OC Organismo de Certificación

TOE Target Of Evaluation

BIBLIOGRAPHY

The following standards and documents have been used for the evaluation of the product:

[CC1] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model CC:2022 Revision 1

[CC2] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements CC:2022 Revision 1

[CC3] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements CC:2022 Revision 1

[CC4] Common Criteria for Information Technology Security Evaluation, Part 4: Framework for the specification of evaluation methods and activities CC:2022 Revision 1

[CC5] Common Criteria for Information Technology Security Evaluation, Part 5: Pre-defined packages of security requirements CC:2022 Revision 1

[CCCEM] Common Methodology for Information Technology Security Evaluation, Evaluation methodology CEM:2022 Revision 1

[CC2022_Errata] Errata and Interpretation for CC:2022 (Release 1) and CEM:2022 (Release 1) Version 1.1, 2024-07-22

[PRE-2740-2007] Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información 19/09/2007

[PP_ESM_ICM_2.1] Protection profile Enterprise Security Management Identity and Credential Management v2.1 Version 2.1, 24/10/2013

[SOGIS_ACM_1.3] SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms Version 1.3, February 2023

[PO-005] Certificación de productos, v39 Version 39, 09/10/2023

[IT-012] Mecanismos Criptográficos en certificaciones Version 4, 12/01/2022

[ST] WSO2 Identity Server Security Target version 1.7 15/12/2025

RECOGNITION AGREEMENTS

In order to avoid multiple certification of the same product in different countries a mutual recognition of IT security certificates - as far as such certificates are based on ITSEC or CC - under certain conditions was agreed.

European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)

The SOGIS-Mutual Recognition Agreement (SOGIS-MRA) Version 3 became effective in April 2010. It defines the recognition of certificates for IT-Products at a basic recognition level and, in addition, at higher recognition levels for IT-Products related to certain SOGIS Technical Domains only.

The basic recognition level includes Common Criteria (CC) Evaluation Assurance Levels EAL 1 to EAL 4 and ITSEC Evaluation Assurance Levels E1 to E3 (basic). For "Smartcards and similar devices" a SOGIS Technical Domain is in place. For "HW Devices with Security Boxes" a SOGIS Technical Domains is in place, too. In addition, certificates issued for Protection Profiles based on Common Criteria are part of the recognition agreement.

The new agreement has been signed by the national bodies of Austria, Finland, France, Germany, Italy, The Netherlands, Norway, Spain, Sweden and the United Kingdom. The current list of signatory nations and approved certification schemes, details on recognition, and the history of the agreement can be seen on the website at https://www.sogis.eu.

The SOGIS-MRA logo printed on the certificate indicates that it is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under SOGIS-MRA for all assurance components selected.

International Recognition of CC – Certificates (CCRA)

The international arrangement on the mutual recognition of certificates based on the CC (Common Criteria Recognition Arrangement, CCRA-2014) has been ratified on 08 September 2014. It covers CC certificates based on collaborative Protection Profiles (cPP) (exact use), CC certificates based on assurance components up to and including EAL 2 or the assurance family Flaw Remediation (ALC_FLR) and CC certificates for Protection Profiles and for collaborative Protection Profiles (cPP).

The CCRA-2014 replaces the old CCRA signed in May 2000 (CCRA-2000). Certificates based on CCRA-2000, issued before 08 September 2014 are still under recognition according to the rules of CCRA-2000. For on 08 September 2014 ongoing certification procedures and for Assurance Continuity (maintenance and re-certification) of old certificates a transition period on the recognition of certificates according to the rules of CCRA-2000 (i.e. assurance components up to and including EAL 4 or the assurance family Flaw Remediation (ALC_FLR)) is defined until 08 September 2017.

As of September 2014 the signatories of the new CCRA-2014 are government representatives from the following nations: Australia, Austria, Canada, Czech Republic, Denmark, Finland, France, Germany, Greece, Hungary, India, Israel, Italy, Japan, Malaysia, The Netherlands, New Zealand, Norway, Pakistan, Republic of Korea, Singapore, Spain, Sweden, Turkey, United Kingdom, and the United States.

The current list of signatory nations and approved certification schemes can be seen on the website: http://www.commoncriteriaportal.org.

The Common Criteria Recognition Arrangement logo printed on the certificate indicates that this certification is recognised under the terms of this agreement by the nations listed above.

The certificate of this TOE is recognized under CCRA for all assurance components selected.