Referencia: 2023-36-INF-4551- v1
Difusión: Limitada al expediente
Fecha: 23.05.2025

Creado por: I008
Revisado por: CALIDAD
Aprobado por: TECNICO

INFORME DE CERTIFICACIÓN

Expediente #	**2023-36**
TOE	**Soffid IAM. IAM-console version 3.5, Sync-server versión 3.5, PAM-launcher version 1.4, y PAM-store version 1.4**
Solicitante	**B57788674 - SOFFID IAM, S.L.**
Referencias	[EXT-8796] Solicitud de certificación del producto SOFFID [EXT-9499] Informe Técnico de Evaluación

Informe de Certificación del producto Soffid IAM. IAM-console version 3.5, Sync-server versión 3.5, PAM-launcher version 1.4, y PAM-store version 1.4, según la solicitud de referencia [EXT-8796], de fecha 10/10/2023, evaluado por el laboratorio Clover Technologies, conforme se detalla en el correspondiente Informe Técnico de Evaluación, indicado en [EXT-9499], recibido el pasado 10/03/2025.

CONTENIDOS

RESUMEN

Este documento constituye el Informe de Certificación para el expediente de certificación del producto Soffid IAM. IAM-console version 3.5, Sync-server versión 3.5, PAM-launcher version 1.4, y PAM-store version 1.4.

Soffid IAM es una aplicación web de gestión de identidades y accesos con capacidad de gestión de acceso privilegiado (PAM)

Fabricante: SOFFID IAM, S.L..

Patrocinador: SOFFID IAM, S.L..

Organismo de Certificación: Centro Criptológico Nacional (CCN).

Laboratorio de Evaluación: Clover Technologies.

Perfil de Protección: No aplicable.

Nivel de Evaluación: Common Criteria v3.1. Release 5 – EAL2.

Fecha de término de la evaluación: TBD

Fecha de expiración[1]: 20/05/2030

Todos los componentes de garantía requeridos por el nivel de evaluación EAL2 presentan el veredicto de "PASA". Por consiguiente, el laboratorio Clover Technologies asigna el VEREDICTO de "PASA" a toda la evaluación por satisfacer todas las acciones del evaluador a nivel EAL2, definidas por Common Criteria v3.1 R5 y CEM v3.1 R5.

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto Soffid IAM. IAM-console version 3.5, Sync-server versión 3.5, PAM-launcher version 1.4, y PAM-store version 1.4, se propone la resolución estimatoria de la misma.

RESUMEN DEL TOE

SOFFID IAM constituye un producto destinado al Gobierno y Administración de Identidad (IGA) y la Gestión de Acceso Privilegiado (PAM) que ofrece a las organizaciones centralizar la gestión de identidad y acceso de sus usuarios. Esto les permite alcanzar una mayor eficiencia en la gestión de acceso a sistemas y aplicaciones, mejorar la seguridad de la información y el cumplimiento de los requerimientos impuestos por la normativa.

[1] Este campo se refiere a la fecha de expiración del reconocimiento del certificado en el ámbito de los acuerdos de reconocimiento mutuo firmados por este Organismo de Certificación.

El principal beneficio de uso de **SOFFID IAM** para las organizaciones recae en su capacidad de protección de datos sensibles frente a amenazas internas y externas, proporcionando una gestión de acceso a los recursos de la organización más segura y efectiva. Adicionalmente, **SOFFID IAM** ofrece una mejora de la eficiencia y productividad del negocio, reduciendo los tiempos y recursos que es necesario invertir en la gestión de identidades y accesos lo que, en última instancia, permite una reducción de costes de gestión.

Dentro de las características y funcionalidades aportadas por **SOFFID IAM**, se distinguen las siguientes:

- **Gestión centralizada de identidad y acceso**. Permite a las organizaciones gestionar de manera centralizada, la identidad y acceso de sus usuarios, proporcionando a los administradores la capacidad de otorgar, revocar y modificar los permisos de accesos en tiempo real.
- **Gestión de autenticación y contraseñas**. **SOFFID IAM** ofrece un producto seguro de gestión de contraseñas que permite a los usuarios configurar contraseñas robustas y proteger las mismas con medidas de seguridad adicionales.
- **Reporte y auditoría**. **SOFFID IAM** proporciona reportes detallados sobre la actividad del usuario y los permisos de acceso, permitiendo a las organizaciones mantener un control completo y detallado de la actividad de sus usuarios.
- **Registro y auditoría de cuentas privilegiadas**. **SOFFID IAM** ofrece la capacidad de inventariar, catalogar y registrar el uso de cuentas privilegiadas.
- **Integración con otros productos**. **SOFFID IAM** permite su integración con productos de otras compañías como, por ejemplo, Active Directory.
- Respecto a los conceptos y herramientas que aparecen en **SOFFID IAM**, se destacan los siguientes:
- **Consola**. El acceso a **SOFFID IAM** siempre se realiza desde la consola de gestión, una herramienta web diseñada acorde a la guía de buenas prácticas de OWASP. Además, esta web cuenta con mecanismos reforzados para responder ante ataques de fuerza bruta. Esto permite el uso de la consola de forma remota desde cualquier ordenador usando Internet Explorer, Firefox o Chrome. **SOFFID IAM** también cuenta con un portal propio usable desde cualquier dispositivo, Android e iOS incluidos, en formato vertical u horizontal totalmente configurable. Los lenguajes disponibles para la consola son: catalán, español o inglés.
- **Seguridad en SOFFID**. Los usuarios de SOFFID pueden tener asignados tres roles distintos entre sí. Dichos roles son creados con el objetivo de garantizar una distribución de responsabilidades segura. La creación de estos roles se realiza durante la instalación del TOE y son los siguientes:

- Usuario Administrador: Este rol permite al usuario gestionar y modificar todas las funcionalidades y atributos de seguridad del sistema.
- Usuario Básico: Rol asignado a los usuarios que no cuentan con ningún permiso con privilegios, únicamente otorgando acceso a su propia información y a cuentas de otros sistemas vinculadas con su usuario de SOFFID.
- Acceso PAM: Este rol es otorgado a usuarios básicos, capacitándoles para acceder a un sistema remoto a través del proceso PAM.

- **Gestión de roles**. La gestión de roles es una característica importante de **SOFFID IAM**, ayudando a las organizaciones a simplificar y mejorar su gestión de identidad y acceso, asegurando que los usuarios cuenten con los permisos correctos para llevar a cabo sus tareas y limitando el acceso a recursos innecesarios.
- **Motor de flujo de trabajo**. Esta característica es clave en **SOFFID IAM** dado que permite a las organizaciones automatizar sus procesos de negocio y de gestión de identidad y acceso. Esta automatización cumple con los requisitos de auditoría y conformidad y permite asegurar la transparencia y colaboración en todo el proceso.
- **Suministro de usuarios**. Se trata de una pieza esencial en **SOFFID IAM**, ayudando a las organizaciones a automatizar la creación, modificación y borrado de cuentas de usuario, accesos a recursos de varios sistemas y aplicaciones, mejorar la eficiencia y precisión, reducir errores y costes asociados a la gestión de cuentas de usuarios de forma manual, y mejorar la eficiencia de la seguridad y operaciones.

Cuentas privilegiadas. Las cuentas privilegiadas constituyen un aspecto crítico de la seguridad de la información en las organizaciones. **SOFFID IAM** ofrece un producto que incluye una gestión segura y robusta de este tipo de cuentas. Concretamente, permite la centralización de la gestión de cuentas privilegiadas de varios sistemas y aplicaciones y la monitorización del uso de dichas cuentas.

REQUISITOS DE GARANTÍA DE SEGURIDAD

El producto se evaluó con todas las evidencias necesarias para la satisfacción del nivel de evaluación EAL2, según Common Criteria v3.1. Release 5.

EAL 2

ASSURANCE CLASS	ASSURANCE COMPONENT
ADV	ADV_ARC.1
	ADV_FSP.2
	ADV_TDS.1
AGD	AGD_OPE.1

	AGD_PRE.1
ALC	ALC_CMC.2
	ALC_CMS.2
	ALC_DEL.1
ASE	ASE_CCL.1
	ASE_ECD.1
	ASE_INT.1
	ASE_OBJ.2
	ASE_REQ.2
	ASE_SPD.1
	ASE_TSS.1
ATE	ATE_COV.1
	ATE_FUN.1
	ATE_IND.2
AVA	AVA_VAN.2

REQUISITOS FUNCIONALES DE SEGURIDAD

La funcionalidad de seguridad del producto satisface los siguientes requisitos funcionales, Common Criteria v3.1 R5.

- ESM_EAU.2
- ESM_EID.2
- ESM_ICD.1
- ESM_ICT.1
- ESM_MPA_EXT.1
- FAU_GEN.1
- FAU_STG_EXT.1
- FIA_AFL.1
- FIA_SOS.1
- FIA_USB.1
- FMT_MOF.1
- FMT_MTD.1
- FMT_SMF.1
- FMT_SMR.1

- FPT_APW_EXT.1
- FPT_SKP_EXT.1
- FTA_SSL_EXT.1
- FTA_SSL.3
- FTA_SSL.4
- FTA_TAB.1
- FTP_ITC.1
- FTP_TRP.1

IDENTIFICACIÓN

Producto: Soffid IAM. IAM-console version 3.5, Sync-server versión 3.5, PAM-launcher version 1.4, y PAM-store version 1.4.

Declaración de Seguridad: Soffid IAM Security Target Version 10, 05/03/2025.

Perfil de Protección: No aplicable

Nivel de Evaluación: Common Criteria v3.1 R5 EAL2

POLÍTICA DE SEGURIDAD

El uso del producto Soffid IAM. IAM-console version 3.5, Sync-server versión 3.5, PAM-launcher version 1.4, y PAM-store version 1.4, debe implementar una serie de políticas organizativas, que aseguran el cumplimiento de diferentes estándares y exigencias de seguridad.

El detalle de estas políticas se encuentra en la Declaración de Seguridad en el apartado 3.2 (“Organizational Security Policies”).

HIPÓTESIS Y ENTORNO DE USO

Las siguientes hipótesis restringen las condiciones sobre las cuales se garantizan las propiedades y funcionalidades de seguridad indicadas en la Declaración de Seguridad. Estas mismas hipótesis se han aplicado durante la evaluación en la determinación de la condición de explotables de las vulnerabilidades identificadas. Por tanto, para garantizar el uso seguro del TOE, se parte de las siguientes hipótesis para su entorno de operación.

En caso de que alguna de ellas no pudiera asumirse, no sería posible garantizar el funcionamiento seguro del TOE. Se pueden encontrar en el apartado 3.3 (“Assumptions”) de la declaración de seguridad.

ACLARACIONES SOBRE AMENAZAS NO CUBIERTAS

Las siguientes amenazas no suponen un riesgo explotable para el producto Soffid IAM. IAM-console version 3.5, Sync-server versión 3.5, PAM-launcher version 1.4, y PAM-store version 1.4, aunque los agentes que realicen ataques tengan potencial de ataque correspondiente a Básico de EAL2, y siempre bajo el cumplimiento de las hipótesis de uso y la correcta satisfacción de las políticas de seguridad.

Para cualquier otra amenaza no incluida en esta lista, el resultado de la evaluación de las propiedades del producto, y el correspondiente certificado, no garantizan resistencia alguna.

Las amenazas cubiertas por las propiedades de seguridad del TOE se encuentran en el apartado apartado 3.1 (“Threats”) de la declaración de seguridad.

FUNCIONALIDAD DEL ENTORNO

El producto requiere de la colaboración del entorno para la cobertura de algunos objetivos del problema de seguridad definido.

Los objetivos que se deben cubrir por el entorno de uso del TOE se encuentran en el apartado 4.2 ("Security Objectives for the operational Environment") de la declaración de seguridad.

Los detalles de la definición del entorno del producto (hipótesis, amenazas y políticas de seguridad) o de los requisitos de seguridad del TOE se encuentran en la correspondiente Declaración de Seguridad.

ARQUITECTURA

ARQUITECTURA LÓGICA

The logical TOE boundary is composed by the following TOE Security Functions:

- **Enterprise Security Management**

The TOE provides the ability to authenticate and identify users using their own internal authentication mechanism. The TOE also has the ability to securely import already existing user´s authentication information, together with their attributes and configuration, from an Active Directory into the Soffid Repository. The TOE has the ability to securely manage user's attributes and functions within the system.

The TOE provides the functionality of defining a password policy that complies with the security requirements of the TSF.

- **Security Audit**

The TOE generates logs of every action performed by the users within the application. These logs record every configuration or changes that are made. The TOE also generates logs of all the remote connections sessions. These logs are stored according to the action that is being documented. On the one hand, configurations and events related to the docker containers and sessions from PAM Access record screen capture and keystrokes are stored inside the corresponding docker volume. On the other hand, rest of actions are stored inside the local database, which in the TOE architecture is represented by the Soffid Repository component.

- **Cryptographic Support**

The TOE ensures secure communications in support of TLS and HTTPS communications. The TOE ensures the communication between the components is secure and complies with the minimum

standards established in [CCN-STIC-807]. Trust needed to enforce secure and private communications stems from Certification Authority (CA) acting as a trusted third party.

- **Identification and Authentication**

The TOE guarantees the association of each user with the role associated to the corresponding account. When a user authenticates to the TOE, this user is given the corresponding abilities depending on the account's role. The three roles defined in the TOE are: administrative users, basic users and access PAM. Administrative users have all applications permissions and can operate as highest privilege users. Basic users, on the other hand, will only be able to access their Console component and check its own information. Other permissions can only be provided by an administrative account. If the basic user is also given the access PAM role, the user will also be able to control a specific machine through PAM.

The TOE provides mechanisms to prevent the possibility of unauthorized access to an account. The credentials associated with an account are stored locally and properly hashed. The TOE also provides the ability to configure the maximum number of authentication attempts and secure policies for the establishment of the password quality.

- **Security Management**

The TOE is managed by authorized administrator through a web GUI, which in the TOE architecture is represented by Console component. The TOE uses a role-based access control policy, where the actions a user can do are defined after the user is authenticated in the system and the role for this user is determined. Administrative users have the ability to make all the security management decisions within the TOE, while the actions that basic users can do are defined by the configurations of each individual user.

- **Protection of the TSF**

The TOE hashes all passwords and user's credentials before they are stored inside the Soffid Repository. The TOE does not offer any mechanism to disclose the plain text stored credential. The Soffid Repository is created in an individual container.

- **TOE Access**

The user can terminate their own session at any moment by login out of the user account.

The TOE can be configured to display an informative banner, this banner will be displayed before allowing any user to authenticate into the TOE.

- **Trusted Path/Channels**

The TOE provides a secure communication among the containers where each of the components are hosted using HTTPS and TLS.

When a communication is established between the TOE and an external agent located out of the TOE´s evaluation scope, that connection needs to be secured, following the necessary procedures to protect it. There are four different types of remote access connections with external agents: 1)

Connection with a Windows system is done through the RDP windows protocol, 2) connection with a Linux system is done using SSH, 3) connection with a database is done using JDBC and 4) communication with Active Directory is done using LDAPS. External agents need to be configured according to their respective security requirements, so when the TOE connect with them, that communication is properly protected.

ARQUITECTURA FÍSICA

The physical boundary of the TOE does not include the application server software Apache TomEE, the Operating System (OS), or any other third-party software which is required for the TOE to run. Even though these components are not under the scope of the TOE, the TOE requires the following components, and their corresponding versions, to be installed:

Component	Solution
Server OS	CentOS Stream 9
Container software	Docker Engine: V:23.0.1
Application Server	Apache Tomcat V:8.5.41
Soffid Repository	MariaDB V:11.1.2
Firefox Browser	Firefox V:131.0.2

- Linux server: Ubuntu 23.04
- Active Directory: Windows server 2019 standard
- Windows server: Windows 10 PRO 10.0.19045
- Database administrador client: DBeaver 22.3.0
- MySQL server: MariabDB 10.11.2
- Linux SSH connection: Remmina 1.4.25
- Windows remote desktop: Xfreerdp 2.6.1
- Browser: Firefox V:131.0.2

The hardware layer (outside of the TOE) that has been used for the evaluation of the TOE has the following specifications:

Hardware Component	Specification
CPU	2 CPUs
RAM	16 GB
Data storage	250 Gb

DOCUMENTOS

El producto incluye los documentos indicados a continuación, y que deberán distribuirse y facilitarse de manera conjunta a los usuarios de la versión evaluada.

Referencia	Organismo de emisión	Título	Fecha	Versión	Nombre del archivo
[ST_10]	Soffid IAM S.L.	Soffid IAM Security Target	05/03/2025	10	SOFFID_Security_Target_v10F
[PES_7]	Clover Technologies S.L.	Procedimiento de empleo seguro Soffid IAM	05/03/2025	7	*CLOVER-LEV23-Soffid_PES_Soffid_IAM_v7*
[AUX_1.3]	Soffid IAM S.L.	Información adicional para ADV, ALC y ATE	24/04/2024	1.3	*SOFFID-ALC-ADV-ATE-v1.3*
[TST_1.3]	Soffid IAM S.L.	Información adicional para ADV, ALC y ATE	24/04/2024	1.3	*SOFFID-Pruebas Funcionales-v1.3*
[DOC_8]	Soffid IAM S.L.	Documentación entregada para la evaluación	05/03/2025	8	*SOFFID-Documentacion entregada para evaluacion_v8*

PRUEBAS DEL PRODUCTO

El fabricante ha realizado pruebas para todas las funciones de seguridad. Todas las pruebas han sido realizadas por el fabricante, en sus instalaciones, con resultado satisfactorios.

Durante el proceso de evaluación se han verificado cada una de las pruebas individuales, comprobando que se identifica la función de seguridad que cubre y que la prueba es adecuada a la función de seguridad que se desea cubrir.

Todas las pruebas se han realizado sobre un mismo escenario de pruebas, acorde a la arquitectura identificada en la Declaración de Seguridad.

Se ha comprobado que los resultados obtenidos en las pruebas se ajustan a los resultados esperados.

Para verificar los resultados de las pruebas del fabricante, el laboratorio ha repetido en las instalaciones del fabricante todas estas pruebas funcionales. Igualmente, ha escogido y repetido en torno a un 25 % de las pruebas funcionales definidas por el fabricante, en la plataforma de pruebas montada en el laboratorio de evaluación, seleccionando una prueba por cada una de las clases funcionales más relevantes.

Adicionalmente, el laboratorio ha desarrollado una prueba por cada una de las funciones de seguridad del producto, verificando que los resultados, así obtenidos, son consistentes con los resultados obtenidos por el fabricante.

Se ha comprobado que los resultados obtenidos en las pruebas se ajustan a los resultados esperados, y en aquellos casos en los que se presentó alguna desviación respecto de lo esperado, el evaluador ha constatado que dicha variación no representa un problema para la seguridad, ni supone una merma en la capacidad funcional del producto.

CONFIGURACIÓN EVALUADA

Se ha evaluado el producto con la configuración descrita en [PES_7]

RESULTADOS DE LA EVALUACIÓN

El producto Soffid IAM. IAM-console version 3.5, Sync-server versión 3.5, PAM-launcher version 1.4, y PAM-store version 1.4 ha sido evaluado en base a la Declaración de Seguridad Soffid IAM Security Target Version 10, 05/03/2025.

Todos los componentes de garantía requeridos por el nivel de evaluación EAL2 presentan el veredicto de “PASA”. Por consiguiente, el laboratorio Clover Technologies asigna el **VEREDICTO de “PASA”** a toda la evaluación por satisfacer todas las acciones del evaluador a nivel EAL2, definidas por Common Criteria v3.1 R5 y CEM v3.1 R5.

RECOMENDACIONES Y COMENTARIOS DE LOS EVALUADORES

A continuación, se proporcionan las recomendaciones acerca del uso seguro del producto. Estas recomendaciones han sido recopiladas a lo largo de todo el proceso de evaluación y se detallan para que sean consideradas en la utilización del producto.

Se ha encontrado una vulnerabilidad residual para cuya explotación se necesita un usuario administrador, los cuales son confiables. Por lo tanto, es fundamental cumplir con esta hipótesis sobre el entorno de ejecución. Se recomienda, además, solucionar esta vulnerabilidad en el futuro.

RECOMENDACIONES DEL CERTIFICADOR.

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto Soffid IAM. IAM-console version 3.5, Sync-server versión 3.5, PAM-launcher version 1.4, y PAM-store version 1.4, se propone la resolución estimatoria de la misma.

GLOSARIO DE TÉRMINOS

Acrónimo	Descripción
CC	*Common Criteria*
EAL	*Evaluation Assurance Level*
ETRP	*Partial evaluation technical report*
IAM	*Identnty Access Management*
IGA	*Identity Governance and Administration*
IT	*Information Technology*
OR	*Observation Report*
OSP	*Organizational Security Policy*
PAM	*Privileged Access Management*
PP	*Protection Profile*
SAR	*Security Assurance Requirements*
SFR	*Security Functional Requirement*
ST	*Security Target*
TOE	*Target of Evaluation*
TSF	*TOE Security Functionality*
TSS	*TOE summary specification*

BIBLIOGRAFÍA

Se han utilizado las siguientes normas y documentos en la evaluación del producto:

[CC_P1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, R5 Final, April 2017.

[CC_P2] Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, R5 Final, April 2017.

[CC_P3] Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, R5 Final, April 2017.

[CEM] Common Methodology for Information Technology Security Evaluation: Version 3.1, R5 Final, April 2017.

[PP] Standard Protection Profile for Enterprise Security Management Identity and Credential Management, version 2.1, NIAP, 24/10/2013.

DECLARACIÓN DE SEGURIDAD O DECLARACIÓN DE SEGURIDAD LITE (SI APLICA)

Junto con este Informe de Certificación, se dispone en el Organismo de Certificación de la Declaración de Seguridad completa de la evaluación:

Seguridad Soffid IAM Security Target Version 10, 05/03/2025

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 SOGIS-MRA for all assurance components selected.