

Referencia: 2019-15-INF-3071-v1
Difusión: Público
Fecha: 22.06.2020

Creado por: CERT11
Revisado por: CALIDAD
Aprobado por: TECNICO

INFORME DE CERTIFICACIÓN

Expediente # **2019-15**
TOE **NGSIEM LogICA5 versión 7.1**
Solicitante **B-28893139 - I.C.A. Informática y Comunicaciones Avanzadas, S.L.**

Referencias

[EXT-4791] Solicitud de Certificación
[EXT-5766] Informe Técnico de Evaluación

Informe de Certificación del producto NGSiem LogICA5 versión 7.1, según la solicitud de referencia [EXT-4791], de fecha 21/03/2019, evaluado por el laboratorio LAYAKK SEGURIDAD INFORMATICA S.L., conforme se detalla en el correspondiente Informe Técnico de Evaluación, indicado en [EXT-5766], recibido el pasado 07/02/2020.

CONTENIDOS

RESUMEN	3
RESUMEN DEL TOE.....	3
REQUISITOS DE GARANTÍA DE SEGURIDAD	4
REQUISITOS FUNCIONALES DE SEGURIDAD	5
IDENTIFICACIÓN	6
POLÍTICA DE SEGURIDAD	6
HIPÓTESIS Y ENTORNO DE USO	6
ACLARACIONES SOBRE AMENAZAS NO CUBIERTAS	6
FUNCIONALIDAD DEL ENTORNO	7
ARQUITECTURA.....	7
ARQUITECTURA LÓGICA.....	7
ARQUITECTURA FÍSICA.....	8
DOCUMENTOS	9
PRUEBAS DEL PRODUCTO	9
PRUEBAS DE PENETRACIÓN	10
CONFIGURACIÓN EVALUADA.....	10
RESULTADOS DE LA EVALUACIÓN	11
RECOMENDACIONES Y COMENTARIOS DE LOS EVALUADORES	11
RECOMENDACIONES DEL CERTIFICADOR	11
GLOSARIO DE TÉRMINOS	12
BIBLIOGRAFÍA.....	12
DECLARACIÓN DE SEGURIDAD.....	12
RECOGNITION AGREEMENTS.....	13
European Recognition of ITSEC/CC – Certificates (SOGIS-MRA)	13
International Recognition of CC – Certificates (CCRA)	13

RESUMEN

Este documento constituye el Informe de Certificación para el expediente de certificación del producto NGSIEM LogICA5 versión 7.1.

NGSIEM LogICA5 versión 7.1 es una solución NGSIEM (gestión de eventos de seguridad e información de seguridad de nueva generación).

Fabricante: I.C.A. Informática y Comunicaciones Avanzadas, S.L..

Patrocinador: I.C.A. Informática y Comunicaciones Avanzadas, S.L..

Organismo de Certificación: Centro Criptológico Nacional (CCN).

Laboratorio de Evaluación: LAYAKK SEGURIDAD INFORMATICA S.L.

Perfil de Protección: No.

Nivel de Evaluación: Common Criteria for Information Technology Security Evaluation v3.1 R5 - EAL2.

Fecha de término de la evaluación: 20/02/2020.

Fecha de expiración¹: 20/06/2025

Todos los componentes de garantía requeridos por el nivel de evaluación EAL2 presentan el veredicto de "PASA". Por consiguiente, el laboratorio LAYAKK SEGURIDAD INFORMATICA S.L. asigna el VEREDICTO de "PASA" a toda la evaluación por satisfacer todas las acciones del evaluador a nivel EAL2, definidas por Common Criteria for Information Technology Security Evaluation v3.1 R5 y la Common Methodology for Information Technology Security Evaluation v3.1 R5.

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto NGSIEM LogICA5 versión 7.1, se propone la resolución estimatoria de la misma.

RESUMEN DEL TOE

NGSIEM LogICA5 es una solución NGSIEM (gestión de eventos de seguridad e información de seguridad de nueva generación). Los subsistemas pertenecientes al TOE son proporcionados por los siguientes componentes o *plugins base core*:

- Servidores de front end 1.1.12
- Bus de streaming y procesado en tiempo real 1.1.12

y su extensión en funcionalidad proporcionada por los componentes o *plugins de extensión core*:

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.

- Gestión de usuarios y roles 1.1.12
- Gestión de auditoría 1.1.12
- Inventario de activos 1.1.12
- Gestión de incidentes 1.1.12
- Análisis forense 1.1.12
- Análisis en tiempo real y correlación de eventos de seguridad 1.1.12
- Planificación de tareas 1.1.12

Todos los componentes anteriormente indicados se empaquetan en un único paquete de instalación:

- LogICA5-core-1.1.12.-Release.x86_64.rpm

SHA-256: 057b01f8384b7a219ba2df6ceee659d463622f345aea72776b50bb462aa87e99

Cualquier otro componente no especificado no forma parte del TOE y por lo tanto no ha sido evaluado en el marco de esta certificación.

Las funciones evaluadas son las siguientes:

- Auditoría de seguridad
- Operaciones con claves criptográficas
- Autenticación e identificación
- Gestión de los datos y funciones de seguridad
 - Gestión de usuarios de front end
 - Asignación de roles a usuarios de front end
 - Políticas de seguridad
 - Gestión de mecanismos de acceso a datos de los sistemas cedentes.
 - Gestión de la configuración de entradas de líneas de log
 - Gestión de la activación de reglas de correlación
 - Gestión de la respuesta – alarmas - debido a funciones de correlación
 - Notificación a destinatarios de correo electrónico ante la respuesta – alarmas -.
- Acceso y Protección
- Rutas confiables

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 for Information Technology Security Evaluation v3.1 R5.

CLASE	NOMBRE	COMPONENTE	NOMBRE
ADV	Development	ADV_ARC.1	Security architecture description
		ADV_FSP.2	Security-enforcing functional specification
		ADV_TDS.1	Basic design
AGD	Guidance documents	AGD_OPE.1	Operational user guidance
		AGD_PRE.1	Preparative procedures
ALC	Life-Cycle support	ALC_CMC.2	Use of a CM system
		ALC_CMS.2	Parts of the TOE CM coverage
		ALC_DEL.1	Delivery procedures
ASE	Security Target Evaluation	ASE_CCL.1	Conformance claims
		ASE_ECD.1	Extended components definition
		ASE_INT.1	ST introduction
		ASE_OBJ.2	Security objectives
		ASE_REQ.2	Derived security requirements
		ASE_SPD.1	Security definition
		ASE_TSS.1	TOE summary specification
ATE	Test	ATE_COV.1	Evidence of coverage
		ATE_FUN.1	Functional testing
		ATE_IND.2	Independent testing – sample
AVA	Vulnerability Assessment	AVA_VAN.2	Vulnerability analysis

REQUISITOS FUNCIONALES DE SEGURIDAD

La funcionalidad de seguridad del producto satisface los siguientes requisitos funcionales, según los Common Criteria for Information Technology Security Evaluation v3.1 R5. La especificación de los requisitos funcionales se encuentra en la sección 5.1 *Security functional requirements* de la declaración de seguridad [ST].

IDENTIFICACIÓN

Producto: NGSiem LogICA5 versión 7.1.

Declaración de Seguridad: NGSiem LogICA5 Security Target, versión 4.8, 20/01/2020.

Perfil de Protección: No.

Nivel de Evaluación: Common Criteria v3.1 R5 - EAL2.

POLÍTICA DE SEGURIDAD

El uso del producto NGSiem LogICA5 versión 7.1, 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 sección 3.2 *Organisational security policies* de la Declaración de Seguridad [ST].

HIPÓTESIS Y ENTORNO DE USO

Las 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.

El detalle de las hipótesis definidas se encuentra en la sección 3.3 *Assumptions* de la Declaración de Seguridad [ST].

ACLARACIONES SOBRE AMENAZAS NO CUBIERTAS

Las siguientes amenazas no suponen un riesgo explotable para el producto NGSiem LogICA5 versión 7.1, aunque los agentes que realicen ataques tengan potencial de ataque **básico** correspondiente al nivel de evaluación 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 la declaración de seguridad, el resultado de la evaluación de las propiedades del producto, y el correspondiente certificado, no garantizan resistencia alguna.

El detalle de las amenazas cubiertas se encuentra en la sección 3.1 *Threats* de la Declaración de Seguridad [ST].

FUNCIONALIDAD DEL ENTORNO

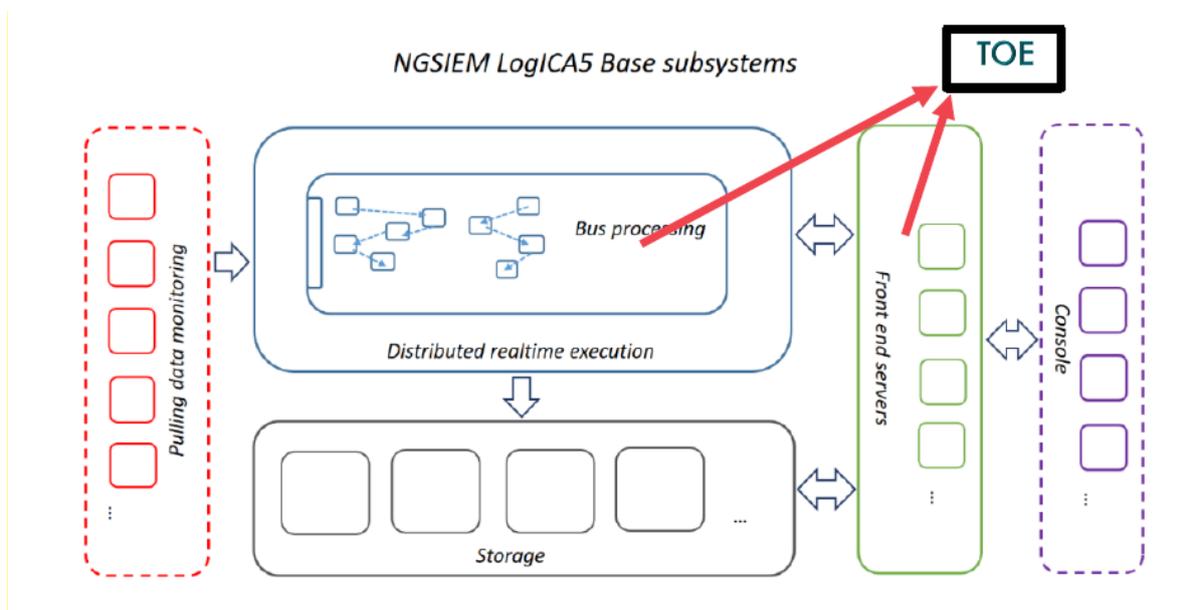
El producto requiere de la colaboración del entorno para la cobertura de algunos objetivos del problema de seguridad definido.

El detalle de los objetivos de seguridad definidos se encuentra en la sección 4.2 *Security objectives for the operational environment* de la Declaración de Seguridad [ST].

ARQUITECTURA

ARQUITECTURA LÓGICA

El siguiente diagrama muestra los límites del TOE frente al resto de subsistemas de la plataforma NGSiem LogICA5 que no son parte constituyente del TOE:



El TOE se encuentra constituido por los subsistemas base pertenecientes al entorno de aplicación de NGSiem LogICA5 7.1 proporcionados por los componentes o plugins base core, más la extensión en funcionalidad proporcionada por los componentes o plugins de extensión core. Los subsistemas base pertenecientes al TOE son:

- Bus de streaming y procesado en tiempo real
- Servidores de front end

Los componentes o plugins de extensión addon, extienden en funcionalidad los subsistemas base del entorno de aplicación de NGSiem LogICA5, pero estos componentes o plugins addon, y por tanto su extensión proporcionada, no forman parte del TOE. Los siguientes subsistemas no forman parte del TOE:

- Sistema de almacenamiento
- Sistema distribuido de ejecución en tiempo real
- Monitores de extracción de datos
- Consola

Las funciones evaluadas son las siguientes:

- Auditoría de seguridad
- Operaciones con claves criptográficas
- Autenticación e identificación
- Gestión de los datos y funciones de seguridad
 - Gestión de usuarios de front end
 - Asignación de roles a usuarios de front end
 - Políticas de seguridad
 - Gestión de mecanismos de acceso a datos de los sistemas cedentes.
 - Gestión de la configuración de entradas de líneas de log
 - Gestión de la activación de reglas de correlación
 - Gestión de la respuesta – alarmas - debido a funciones de correlación
 - Notificación a destinatarios de correo electrónico ante la respuesta – alarmas -.
- Acceso y Protección
- Rutas confiables

ARQUITECTURA FÍSICA

El TOE se distribuye como un archivo rpm con la siguiente identificación:

- LogICA5-core-1.1.12.-Release.x86_64.rpm
SHA-256: 057b01f8384b7a219ba2df6ceee659d463622f345aea72776b50bb462aa87e99

Además, la siguiente documentación es parte del TOE:

- LogICA5-GuiaInstalacion_1.10.pdf
- LogICA5-GuiaOperacion_1.11.pdf
- LogICA5-Distribución_2.5.pdf

El entorno operacional del TOE es:

- Sistema operativo CentOS7. CentOS Linux 7.x 64-bit
- Base de datos MongoDB 3.6.8
- Plataforma de ejecución de nodejs 8.12.0

- Plataforma de ejecución java 1.8.0_161
- Manejador de cluster Apache Zookeeper 3.4.12
- Broker Kafka 2.12-1.0.0
- Base de datos Redis 0:3.2.12-2.el7
- Plataforma distribuida Apache Storm 1.0.6
- Sistema de auditoria Nmap
- Librerías adicionales

Los mínimos requerimientos hardware del appliance son:

- Arquitectura: x86_64
- CPU:1 x 8C o equivalente (2 x 8C recomendado)
- Memoria: 128 GB (512 GB recomendado)
- Espacio Disco: 2T (mínimo)
- Partición Root: 50 GB (mínimo)
- Dos interfaces de red de 1G.

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.

- NGSiem LogICA5 7.1. Guía de Instalación, versión 1.10. 10/01/2020.
 - LogICA5-GuiaInstalacion_1.10.pdf
 - SHA-256: 93bb4bbbc5c27efdbcdc95fb43149c39bd4f028e8610588186081d349e84d1aa
- NGSiem LogICA5 7.1. Guía de Operación, versión 1.11. 20/01/2020.
 - LogICA5-GuiaOperacion_1.11.pdf
 - SHA-256: cb515a27014f0e75174dbf5effb1564ec89f5f995f27b14c31afd2cecf16be9c
- Proceso de distribución NGSiem LogICA5 7.1 – TOE, versión 2.5. 20/01/2020.
 - LogICA5-Distribución_2.5.pdf
 - SHA-256: 0f73384401c236d5f5079a73e15f73428eb79b13f8bbaae02347364a2ba89de8

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 satisfactorio.

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 todas 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.

PRUEBAS DE PENETRACIÓN

El laboratorio ha realizado un análisis de vulnerabilidades teniendo en cuenta el estado del arte en el momento de la evaluación y teniendo en cuenta la arquitectura, diseño y especificación funcional de seguridad del TOE en el entorno operacional. Teniendo en cuenta este análisis el laboratorio ha definido una serie de pruebas de penetración que ha ejecutado.

Como resultado de estas pruebas no se han detectado desviaciones con respecto a los resultados esperados para estas pruebas, por lo que ningún escenario de ataque teniendo en cuenta el entorno operacional definido en [ST] ha tenido éxito teniendo en cuenta un potencial de ataque básico.

CONFIGURACIÓN EVALUADA

El TOE NGSIEM LogICA5 versión 7.1 evaluado es identificado por el siguiente paquete de software:

- LogICA5-core-1.1.12.-Release.x86_64.rpm

SHA-256: 057b01f8384b7a219ba2df6ceee659d463622f345aea72776b50bb462aa87e99

El TOE ha sido instalado y configurado siguiendo las guías identificadas en la sección DOCUMENTOS.

Para más información sobre la configuración evaluada ver la sección *1.7.3 Evaluated configuration* de la declaración de seguridad [ST].

RESULTADOS DE LA EVALUACIÓN

El producto NGSiem LogICA5 versión 7.1 ha sido evaluado en base a la Declaración de Seguridad NGSiem LogICA5 Security Target, versión 4.8, 20/01/2020.

Todos los componentes de garantía requeridos por el nivel de evaluación EAL2 presentan el veredicto de “PASA”. Por consiguiente, el laboratorio LAYAKK SEGURIDAD INFORMATICA S.L. asigna el **VEREDICTO de “PASA”** a toda la evaluación por satisfacer todas las acciones del evaluador a nivel EAL2, definidas por los Common Criteria for Information Technology Security Evaluation v3.1 R5 y la Common Methodology for Information Technology Security Evaluation v3.1 R5.

RECOMENDACIONES Y COMENTARIOS DE LOS EVALUADORES

El equipo evaluador no ha proporcionado ningún comentario o recomendación adicional.

RECOMENDACIONES DEL CERTIFICADOR

A la vista de las pruebas obtenidas durante la instrucción de la solicitud de certificación del producto NGSiem LogICA5 versión 7.1, se propone la resolución estimatoria de la misma.

El certificador informa que los potenciales consumidores deben seguir estrictamente todas las indicaciones para la instalación y configuración segura del TOE que se proporcionan en las guías identificadas en la sección DOCUMENTOS de este informe de certificación. Por otro lado, se deben observar las hipótesis definidas en la sección 3.3 *Assumptions* de la Declaración de Seguridad [ST], y en caso de que alguna de ellas no pudiera asumirse por los potenciales consumidores, no sería posible garantizar el funcionamiento seguro del TOE.

Adicionalmente se debe tener en cuenta lo siguiente:

- Para utilizar el TOE conforme a la configuración evaluada, el usuario debe interactuar con el TOE única y exclusivamente a través del API REST del TOE. La Consola de administración que suministra el Fabricante, al igual que el resto de componentes adicionales opcionales del Fabricante, no han sido evaluados. Específicamente, el uso de la Consola modificaría la instalación respecto de la configuración evaluada puesto que se instala mediante un paquete software en el propio sistema donde se ejecuta el TOE. Además, ese paquete instala también componentes software adicionales.
- La configuración evaluada es en modo *standalone*, es decir, el TOE se ejecuta en un único nodo dedicado en exclusiva a la ejecución tanto del TOE como de los componentes del entorno operacional. La instalación en varios nodos supondría la exposición de interfaces que no han sido evaluados por no quedar expuestos en la configuración de un único nodo.

GLOSARIO DE TÉRMINOS

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

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.

DECLARACIÓN DE SEGURIDAD

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

- NGSiem LogICA5 Security Target, versión 4.8, 20/01/2020.

La versión pública de este documento constituye la “Declaración de Seguridad LITE” que ha sido revisada siguiendo el documento con código [CCDB-2006-04-004], y se publica con el informe de certificación en las webs del CCRA y del OC. El identificador de la “Declaración de Seguridad LITE” es:

- NGSiem LogICA5 Security Target Lite, versión 1.0, 03/02/2020.

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.org>.

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 assurance components up to EAL4.

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 up to EAL2 and ALC_FLR.