# Certification Application for an ICT Product

under the EUCC Scheme

# Manufacturer/Developer applying for Certification (Applicant)

|  |  |  |
| --- | --- | --- |
| Organization name | | |
| Legal Status (e.g., public, private limited, government) | | |
| Full mailing address (also used as invoice address unless otherwise stated under 6; Other Information) | | |
| Corporate Identity Number | VAT-number (for companies outside of Sweden) | |
| Applicant’s certification point of contact: Name | Title | |
| Email address | Telephone | Mobile telephone |

# Information about TOE Certification

## Type of Certification

|  |
| --- |
| Initial certification |
| Composite product certification |
| Certificate Maintenance |
| Re-certification |
| Extension of the certification scope |

## CCRA Recognition

|  |
| --- |
| The applicant requires a CCRA certificate |

## Target of Evaluation Specification

Full and unique name, version, type of product, platform(s), used PPs (Name and certification-ID), Technical Domain competency claimed, if any

|  |
| --- |
|  |

## Intended use of the ICT product and the analysis of the levels of risks associated with such usage

|  |
| --- |
|  |

### Information related to any outsourced process used for producing the target of evaluation

|  |
| --- |
|  |

### Locations where the target of evaluation is produced

|  |
| --- |
|  |

## Assurance Levels

### EUCC Assurance Level as per the CSA

|  |  |
| --- | --- |
| Substantial | High |
|  |  |

### Assurance Level as per the CC

**Evaluation Assurance Levels**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| EAL1 | EAL2 | EAL3 | EAL4 | EAL5 | Other |
|  |  |  |  |  |  |

## Evaluation Assurance Augmentations (optional)

|  |
| --- |
| List any augmentations to the selected EAL (e.g., ALC\_PAM, ALC\_FLR) |

# Ongoing Certifications List

|  |
| --- |
| The applicant wants to have the Certification registered on the “Ongoing Certifications List” on the atsec CB website |

# ITSEF Contracted by the Developer

|  |
| --- |
| Name of Associated ITSEF with atsec CB |
| ITSEF point of contact: Name and Email address |
| Date of contract signing |

# List of the Certification Application Attachments

|  |  |  |  |
| --- | --- | --- | --- |
| Included | Document | Mandatory/optional | Document title and version |
|  | Security Target | Mandatory |  |
|  | Protection Profile | Optional for registered PPs, mandatory otherwise |  |
|  | Evaluation work plan | Mandatory |  |
|  | Impact analysis report (in case of a re-certification) | Mandatory for re-certifications |  |
|  | Maintenance report (in case of Certificate maintenance) | Mandatory |  |
|  | Old Certification ID (in case of a re-certification and Certificate Maintenance) | Mandatory |  |
|  | Security target used in the previous certification (in case of a re-certification and Certificate Maintenance) | Mandatory if the ST is not available on a CB’s website |  |
|  | Certification report of the previous certification (in case of a re-certification and Certificate Maintenance) | Mandatory if the Certification report is not available on a CB’s website |  |
|  | ETR of dependent certificates in case of Composite Evaluations | Mandatory if Composite Evaluation |  |
|  | Other attachments: | | |

# Other Information (including invoice address, if different than mailing address mentioned above)

|  |
| --- |
|  |

# Terms and Conditions

Once the application is accepted by the CB, a tender will be sent to the Developer. The signed application form with the documents listed above and the accepted tender constitute the full application package.

## Based on the regulations defined by ISO/IEC 17065:2012

The applicant shall commit to the following terms and conditions:

1. The applicant shall provide to the certification body and the ITSEF with all the necessary complete and correct information, and to provide additional necessary information if requested.
2. The applicant shall always fulfil the certification requirements, including implementing appropriate changes when they are communicated by atsec CB.
3. If the certification applies to ongoing production, the certified product continues to fulfil the product requirements.
4. The applicant shall provide information that is deemed reliable for the certification and will not risk falsifying the judgement of the certification.
5. The applicant shall not declare or promote the product as certified while the certification is still ongoing.
6. The applicant makes all necessary arrangements:

* to conduct the evaluation, surveillance when requested by atsec CB including provision for examining documentation and records, access to the relevant equipment, location(s), area(s), personnel, and Developer’s subcontractors (if applicable)
* to investigate complaints
* for the participation of observers, if applicable

1. When the certification body deems it necessary, the applicant shall make the necessary arrangements for a Certifier, assessment team from national accreditation body (SWEDAC) to participate in the site-visits and testing oversight activities along with the ITSEF.
2. The applicant makes the claims for marketing/advertising regarding certification that are consistent with the scope of certification.
3. The applicant does not use its product certification in such a manner that the certification body gets disrepute.
4. The applicant does not make any statement regarding its product certification that atsec CB may consider misleading or unauthorized.
5. Upon suspension, withdrawal, or termination of certification, the applicant stops the advertisement mentioning the certification immediately.
6. The applicant makes sure that products manufactured in the series and sold, in connection with the issued certificate are strictly identical to the product that was certified.
7. If the applicant provides copies of the certification documents to other parties, the documents shall be reproduced in their entirety or as specified in the certification scheme.
8. The applicant shall comply with the requirements of the certification body and/or the requirements specified by the certification scheme when referring to the product certification in communication media, e.g., in documents, brochures or advertising.
9. The applicant shall store the following securely for a period of at least 5 years after the expiration or withdrawal of the relevant EUCC certificate:

* records of the information provided to the certification body and to the ITSEF during the certification process;
* specimen of the certified ICT product
* Upon request by the certification body the applicant shall make available the records and copies of the above

1. The applicant shall promote the ICT product as being certified only with respect to the scope set out in the EUCC certificate;
2. The applicant shall cease immediately the promotion of the ICT product as being certified in the event of the suspension, withdrawal or expiry of the EUCC certificate.
3. When the certification body issued a new EUCC certificate after withdrawal of the previous certificate, the holder shall retain the documentation of the withdrawn EUCC certificate together with and as long as for the new EUCC certificate.
4. The applicant complies with any requirements that may be prescribed in the certification scheme relating to the use of marks of conformity, and on information related to the product. See also ISO/IEC 17030, ISO/IEC Guide 23 and ISO Guide 27.
5. The applicant keeps a record of all complaints made known to it relating to compliance with certification requirements and makes these records available to atsec CB when requested. The applicant shall:

* Take appropriate action with respect to such complaints and any deficiencies found in products that affect compliance with the requirements for certification
* Document the actions taken
* Verification of the above actions by the certification body is to be followed as per the certification scheme

1. The applicant shall inform atsec CB, without undue delay, of changes that may affect its ability to conform with the certification requirements.

NOTE: Examples of changes can include the following:

* the legal, commercial, organizational status or ownership
* organization and management (e.g., key managerial, decision-making or technical staff)
* modifications to the product or the production method or the modification to the development cycle and environment
* contact address and production sites
* major changes to the quality management system

1. The applicant shall upon confirmed deviations or irregularities associated to a non-compliance of the requirements related to a certificate shall provide amendments within the time period set by atsec CB (max. 30 days) in order to restore compliance.
2. The Developer shall have a vulnerability management process as described by the Commission Implementing Regulation (EU) of 31.1.2024 laying down rules for the application of Regulation (EU) 2019/881 of the European Parliament and of the Council as regards the adoption of the European Common Criteria based cybersecurity scheme (EUCC) in the chapter VI:

* The holder of an EUCC certificate shall establish and maintain all necessary vulnerability management procedures in accordance with the rules laid down by the EUCC and, where necessary, supplemented by the procedures set out in ISO/IEC 30111.
* The holder of an EUCC certificate shall maintain and publish appropriate methods for receiving information on vulnerabilities related to their products from external sources, including users, certification bodies and security researchers.
* Where a holder of an EUCC certificate detects or receives information about a potential vulnerability affecting a certified ICT product, it shall record it and carry out a vulnerability impact analysis.
* When a potential vulnerability impacts a composite product, the holder of the EUCC certificate shall inform the holder of dependent EUCC certificates about potential vulnerability.
* In response to a reasonable request by the certification body that issued the certificate, the holder of an EUCC certificate shall transmit all relevant information about potential vulnerabilities to that certification body.

1. Vulnerability impact analysis shall be carried out in a timeframe appropriate for the exploitability and criticality of the potential vulnerability of the certified ICT product and produce a vulnerability impact analysis report. The report shall show if the vulnerability has a likely impact on the conformity of the ICT product with its certificate.
2. Where applicable, an attack potential calculation shall be performed in accordance with the CC and the CEM and the relevant state-of-the-art documents if applicable as per the EUCC, in order to determine the exploitability of the vulnerability. The AVA\_VAN level of the EUCC certificate shall be taken into account.
3. The contents of the vulnerability impact analysis report shall be as per Article 35 of the EUCC regulation.
4. The holder of the EUCC certificate shall monitor any residual vulnerabilities to ensure that they cannot be exploited in case of the changes in the operational environment.
5. If the patch management procedure was also evaluated and certified during the initial certification and if the certificate is valid, and when there is a need to apply a patch on the certified ICT product to resolve vulnerabilities, the information regarding the application of the patch must be provided to atsec CB within five working days by the applicant.
6. The holder of the EUCC certificate shall work in cooperation with atsec CB to support their monitoring activities.

# Applicant’s Signature

|  |  |
| --- | --- |
| Date | Place |
| Signature (authorized representative) | |
| Name | Title |

atsec CB shall process the personal data for handling the application process for certification and shall follow the rules specified by the General Data Protection Regulation.

If you have questions regarding atsec’s processing of personal data or if you would like to exercise any of your rights as data subject, please contact [cb@atsec.com](mailto:cb@atsec.com).

In addition, please send the signed copy to:

atsec information security AB

Svärdvägen 23

182 33 Danderyd, Sweden

Phone: +46 (0)8-55 110 400