IT Security Evaluation and Certification Scheme Document

October 2020

CCS-01

Information-technology Promotion Agency, Japan (IPA)

Table of Contents

IT Security Evaluation and Certification Scheme Document

Establishment: May 7, 2007 (Jo-So No. 12 of 2007)
Final revision: September 28, 2020 (Jo-So No. 1093 of 2020) Partial revision

Chapter 1 General Provisions

1.1 Purpose of this Scheme Document

This Scheme Document prescribes the Japan IT Security Evaluation and Certification Scheme (hereinafter referred to as "**this Scheme**") operated by the Information-technology Promotion Agency, Japan (hereinafter referred to as "**IPA**") and basic matters related to this Scheme that need to be complied with by suppliers and users of IT products and systems (hereinafter referred to as "**IT products, etc.**") and personnel engaged in the operation of this Scheme pursuant to the Act on Facilitation of Information Processing (Act No. 90 of 1970), and in accordance with the provisions of Item 5, Paragraph 1 of Article 43 of the said Act, which prescribes "the conduct of evaluation for information processing systems (which means aggregates of computers and programs, which are composed for the purpose of performing information processing in an integrated manner) with the aim of ensuring the security and reliability of information processing from a technical perspective."

1.2 Purpose of this Scheme

The purpose of **this Scheme** is to enable users of **IT products, etc.**, or **PPs** to understand correctly and in detail that **IT products, etc.**, and **PPs**, consisting of hardware, software or firmware, in which security functions including identification and authentication functions, cryptographic functions and access control functions are implemented, appropriately protect information assets and system resources that need to be protected by means of evaluation and certification by a third party.

1.3 Principles of this Scheme

To make **this Scheme** gain the trust of users of **IT products, etc.**, and **PPs**, Evaluation Facilities and the Certification Body shall be fair and non-discriminatory without being influenced by commercial interests, and conduct proper **Evaluation and Certification**, or perform confirmation of a Security Target (hereinafter referred to as "**ST confirmation**") based on high technical capabilities in accordance with the ***Common Criteria for Information Technology Security Evaluation (CC)***, ***Common Methodology for Information Technology Security Evaluation (CEM)***, *and* ***their Interpretations*** (hereinafter referred to as the "**CC/CEM**") listed in ***Annex A*** of this Scheme Document.

1.4 Requirements for Evaluation and Certification or ST Confirmation

The requirements for **Evaluation** and **Certification** or **ST confirmation** conducted under **this Scheme** shall be the **CC/CEM**.

1.5 Definition of Terms

(1) Abbreviations

CC: Common Criteria

The general term for the ***Common Criteria for Information Technology Security Evaluation (CC)*** and ***its Interpretations*** listed in ***Annex A*** of this Scheme Document (hereinafter referred to as the "**CC**").

CEM: Common Evaluation Methodology

The general term for the ***Common Methodology for Information Technology Security Evaluation (CEM)*** and ***its Interpretations*** listed in ***Annex A*** of this Scheme Document **(**hereinafter referred to as the "**CEM**").

PP: Protection Profile

A document describing a set of commonly available **security requirements** in a certain **TOE** area (described later) (hereinafter referred to as a "**PP**").

ST: Security Target

A document describing **security requirements** and specifications related to security that are the basis of evaluation of a specific **TOE** (described later) (hereinafter referred to as an "**ST**").

TOE: Target of Evaluation

IT products, etc., and their instruction manuals that are targets of **Evaluation**, **Certification** and **ST confirmation** under this Scheme (hereinafter referred to as a "**TOE**"). For **ST confirmation**, however, instruction manuals are not included.

(2) Terms

Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security:

The international arrangement on the mutual recognition of security evaluation and certification (hereinafter referred to as the "**CCRA**").

ST confirmation:

Verification that **Evaluation** of a **TOE** is conducted in accordance with Scheme Documentation, and that the evaluation result conforms to the **assurance package** covering the **ST** and functional specifications.

ST Confirmation Report:

A document issued by the **Certification Body** to provide an overview of the **Evaluation Technical Report (ETR)** on functional specifications of an **ST** and a **TOE**, and matters confirmed in the verification process of the **Evaluation Technical Report (ETR)** to users of **IT products**, **etc.**

Confirmation note:

A document issued by the **Certification Body** to verify the results of **ST confirmation**.

Functional package:

A package compiling requirements related to security functions. It compiles security functional requirements demanded by a procurement entity for a **PP**, for the purpose of reference for an **ST**.

Common Evaluation Methodology:

The general term for the ***Common Methodology for Information Technology Security Evaluation (CEM)*** and ***its Interpretations*** listed in ***Annex A*** of this Scheme Document.

Common Criteria:

The general term for the ***Common Criteria for Information Technology Security Evaluation (CC)*** and ***its Interpretations*** listed in ***Annex A*** of this Scheme Document.

Surveillance:

An examination for confirming the validity of a corresponding **Evaluation** for **IT products, etc.**, of which **Evaluation** and **Certification** or **ST confirmation** was conducted, is referred to as "**surveillance**."

Supporting Document:

A technical document that summarizes information that should be assumed by evaluators, including evaluation methods based on the **CC/CEM** in specific technical fields, relevant vulnerabilities and attack methods. For a Supporting Document approved by the **CCRA**, either "Mandatory" or

"Guidance" is clearly stated in an **Evaluation** based on the **CC/CEM**; it is used as the interpretations of the **CC/CEM** under this Scheme.

Observation Report:

A document created by an **Evaluation Facility**, describing not only any problems the **Evaluation Facility** finds in a **PP**, **ST** or **evaluation deliverables** during an **Evaluation**, but also any inquiries the **Evaluation Facility** makes to the **Certification Body** regarding the **CC/CEM**.

Security Target:

A document describing **security requirements** and specifications related to security that are the basis of evaluation of a specific **TOE**.

Security requirements:

Requirements related to security functions prescribed in the **CC** and matters to be **evaluated** (assurance components).

Certification:

Verification that an **Evaluation** of a **TOE** or **PP** has been conducted in accordance with Scheme Documentation and that the evaluation result conforms to the **assurance package** selected by the applicant (See Section 2.2.1.).

Certification Body:

An organization that conducts **Certification** and **ST confirmation** in accordance with **this Scheme**.

Certificate:

A document issued by the **Certification Body** to verify the results of **Certification**.

Certification Report:

A document issued by the **Certification Body** to provide an overview of the **Evaluation Technical Report (ETR)** for a **TOE** or **PP** and matters confirmed in the verification process of the **Evaluation Technical Report (ETR)** to users of **IT products, etc.**

Certification oversight review:

A document issued by the **Certification Body** to an **Evaluation Facility**, which is used to describe problems when they are found by the **Certification Body** in a **PP**, **ST** or **evaluation**

deliverables during the process of **Evaluation**, as well as defects in evaluation contents.

Evaluation:
Conformance to the **CC** of a **TOE**, **PP** or **ST** shall be assessed in accordance with the **CEM**.

Evaluation Facility:
An organization that conducts **Evaluation** of a **TOE**, **PP** and **ST** in accordance with **this Scheme**.

Target of Evaluation:
IT products, etc., and their instruction manuals that are targets of **Evaluation**, **Certification** and **ST confirmation** under this Scheme. For **ST confirmation**, however, instruction manuals are not included.

Evaluation Technical Report (ETR):
A document issued by an **Evaluation Facility** to report the results of an **Evaluation** for an applicant and the **Certification Body**.

Evaluation Assurance Level:
An assurance package that is defined in 7 levels in advance by the **CC** in order to support the difference in importance of data to handle as well as different usage environments, and to provide cost-effective solutions (hereinafter referred to as an "**EAL**"). Each **EAL** is defined in a manner that adds more advanced items to be evaluated with respect to items that are required by a lower level **EAL**. Refer to the **CC** for details of each level.

Evaluation deliverables:
Deliverables including development documents and instruction manuals, which an applicant or developer is requested to provide in order for an **Evaluation Facility** or the **Certification Body** to conduct **Evaluation** and **Certification** of a **TOE** or **PP**, or perform **ST confirmation**. In case of **Evaluation** and **Certification** of a **TOE**, the **TOE** should be included in the **evaluation deliverables**.

Protection Profile:
A document describing a set of commonly available security requirements in a certain **TOE** area.

Assurance Continuity:

Maintaining the previous certification even if the **Target of Evaluation (TOE)** of IT products, on which **Evaluation** and **Certification** were conducted, is changed. If an Impact Analysis Report (IAR), created by an applicant or developer, or the development environment is changed, the Certification Body examines the Evaluation Technical Report (ETR) submitted by an Evaluation Facility. The assurance is maintained if the Certification Body confirms that the change is minor and that the impact of the **Target of Evaluation** on security functions is minor.

Assurance Continuity Maintenance Report:
A document issued by the **Certification Body** to report results of **Assurance Continuity** to an applicant.

Assurance package:
A set of items to be **evaluated** (assurance components). Applicants can create an **assurance package** in combination with items to be **evaluated** (assurance components).

Chapter 2 Structure of Scheme

2.1 Documentation Related to this Scheme

The documentation related to **this Scheme** is shown as follows:

A document that prescribes basic details related to **this Scheme** that applicants, users and personnel engaged in the operation of **this Scheme** need to comply with.

<Scheme Document for IT Security Evaluation and Certification Scheme>	
IT Security Evaluation and Certification Scheme Document (CCS-01)	"***Scheme Document***"

A document that prescribes details that members of the **Certification Body** need to comply with.

<Document related to the operation of certification services>	
Organization and Operational Manual for IT Security Certification Body (CCM-01)	"***Operational Manual***"

A document that prescribes details that applicants that apply for certification need to comply with.

<Document related to certification, etc.>	
Requirements for IT Security Certification (CCM-02)	"***Requirements for Certification***"

A document that prescribes details that personnel that apply for approval of **Evaluation Facility** need to comply with.

<Document related to approval of Evaluation Facility, etc.>	
Requirements for Approval of IT Security Evaluation Facility (CCM-03)	"***Requirements for Evaluation Facility***"

A document that prescribes details that applicants that apply for ST confirmation need to comply with.

<Document related to ST confirmation, etc.>	
Requirements for ST Confirmation (STM-01)	"***Requirements for Confirmation***"

Note 1: Terms in double quotation indicate abbreviations.

Note 2: Symbols consisting of three letters in the above parenthesis are derived from the following:

CCS… Common Criteria certification Scheme

CCM... Common Criteria certification body Management system

STM ...Security Target evaluation and Confirmation Manual for sponsors

2.2 Participants in the Scheme

Participants in **this Scheme** are prescribed as follows.

2.2.1 Applicant

An applicant in this Scheme is an entity that applies for **Certification** or **ST confirmation** in accordance with the "***Requirements for IT Security Certification***" (hereinafter referred to as the "***Requirements for Certification***") and the "***Requirements for ST Confirmation***" (hereinafter referred to as the "***Requirements for Confirmation***"). In principle, an applicant indicates a procurement entity that conducts procurement by using **PPs**, a supplier of a **TOE** or **PP**, a vendor, or other corporation and agency in CCRA signatory nations.

2.2.2 Evaluation Facility

An **Evaluation Facility** in **this Scheme** is an organization that conducts **Evaluation** of a **TOE**, **PP** and **ST** in accordance with the **CC/CEM**. An **Evaluation Facility** shall be accredited as an **IT Security Evaluation Facility** of **this Scheme** by the **Accreditation Body**, and it shall obtain approval regarding a corresponding product field from the **Certification Body** in accordance with the procedure prescribed in the "***Requirements for Approval of IT Security Evaluation Facility***" (hereinafter referred to as the "***Requirements for Evaluation Facility***").

2.2.3 Certification Body

The **Certification Body** in **this Scheme** is the organization that is established within IPA and conducts **Certification** and **ST confirmation** based on results of evaluation conducted by **Evaluation Facilities**. The **Certification Body** shall construct the structure and operate the Scheme to satisfy the requirements prescribed in JIS Q 17065 or the **CCRA**.

2.2.4 Accreditation Body

The Accreditation Body is the organization that accredits **Evaluation Facilities** in accordance with JIS Q 17025 or ISO/IEC 17025.

Chapter 3 Evaluation and Certification

3.1 Application for Certification

Applicants shall perform the procedures of application for certification to the **Certification Body** in accordance with the ***Requirements for Certification***. The **Certification Body** receives applications for **Certification** from applicants in accordance with the ***Organization and Operational Manual for IT Security Certification Body*** (hereinafter referred to as the "***Operational Manual***").

3.2 Evaluation

Evaluation Facilities evaluate the **ST** and **evaluation deliverables**, or **PP**, in accordance with the **CC/CEM** selected by applicants. **Evaluation Facilities** can request cooperation from applicants or external organizations if equipment or facilities are required for evaluation. **Evaluation Facilities** shall prepare the **Evaluation Technical Report (ETR)** and submit the report to the **Certification Body**.

3.3 Certification

The **Certification Body** shall perform **Certification** on the **Evaluation Technical Report (ETR)** submitted by **Evaluation Facilities**, issue and grant a **Certificate** and **Certification Report** to applicants in accordance with the ***Operational Manual***.

3.4 Assurance Continuity

An applicant of **IT products, etc.**, to which **Certification** is granted (hereinafter referred to as a "**registrant**"), can perform the procedure for maintaining assurance in accordance with the ***Requirements for Certification*** when maintaining the original effects of **Certification** for a

subsequent version of a certified TOE (hereinafter referred to as a "**changed TOE**"). The **Certification Body** applies Assurance Continuity according to the Assurance Continuity procedure prescribed in the ***Operational Manual***. However, if changes to the **changed TOE** are major, **Assurance Continuity** cannot be applied. In this case, the applicant shall obtain **certification** by applying the original procedure of **Evaluation** and **Certification**.

3.5 Expenses that Applicant Must Pay

Applicants shall bear expenses required for **Evaluation** and **Certification**. Expenses that applicants must pay to an **Evaluation Facility** shall be determined with the agreement concluded between both parties. Expenses that need to be paid to the **Certification Body** are separately published via the website of **IPA**, etc.

3.6 Expenses that Evaluation Facility Must Pay

Evaluation Facilities shall bear expenses required for the approval of the **Evaluation Facility**. Expenses that need to be paid to the **Certification Body** are separately published via the website of **IPA**, etc.

Chapter 4 Evaluation and ST Confirmation

4.1. Application for ST Confirmation

Applicants shall perform the procedures of application for ST confirmation to the **Certification Body** in accordance with the ***Requirements for Certification***. The **Certification Body** receives applications for **ST confirmation** from applicants in accordance with the ***Operational Manual***.

4.2 Evaluation

Evaluation Facilities evaluate the **ST** and **evaluation deliverables** in accordance with the **CC/CEM** selected by applicants. The **Evaluation Facilities** shall prepare the **Evaluation Technical Report (ETR)** and submit the report to the **Certification Body**.

4.3. ST Confirmation

The **Certification Body** shall perform **ST confirmation** for the **Evaluation Technical Report (ETR)** submitted by **Evaluation Facilities**, prepare and grant a **Confirmation note** and **ST Confirmation Report** to applicants in accordance with the ***Operational Manual***.

4.4 Expenses that Applicant Must Pay

Applicants shall bear expenses required for **Evaluation** and **ST confirmation**. Expenses that applicants must pay to an **Evaluation Facility** shall be determined with the agreement concluded between both parties. Expenses that need to be paid to the **Certification Body** are separately published via the website of **IPA**, etc.

4.5 Expenses that Evaluation Facility Must Pay

Evaluation Facilities shall bear expenses required for approval of the **Evaluation Facility**. Expenses that need to be paid to the **Certification Body** are separately published via the website of **IPA**, etc.

Chapter 5 Rights and Obligations of Applicants

5.1 Rights and Obligations of Applicant to which Certification is Granted

A **registrant** has the following rights and obligations regarding a **TOE** or **PP**.

a) The **registrant** shall comply with the responsibilities of applicants to which **Certification** is granted in accordance with the ***Requirements for Certification***.

b) The **registrant** can supply certified **TOE** or **PP**.

c) The **registrant** can use the "Certification Mark" and "Common Criteria Certification Mark" in accordance with the ***Requirements for Certification*** when supplying certified **TOE** or **PP**. In this case, the registrant shall comply with the "Use of Certification Mark and Common Criteria Certification Mark, etc." prescribed in the ***Requirements for Certification***.

5.2 Rights and Obligations of Applicant to which ST Confirmation is Granted

An applicant of a **TOE** to which **ST confirmation** is granted (hereinafter referred to as an "**ST registrant**") has the following rights and obligations regarding the supply of the **TOE**.

a) The **ST registrant** shall comply with the responsibilities of applicants to which **ST confirmation** is granted in accordance with the ***Requirements for Confirmation***.

b) The **ST registrant** can supply a **TOE** for which ST confirmation has been performed.

c) The **ST registrant** can use the "Certification Mark" in accordance with the ***Requirements for Confirmation*** when supplying a certified **TOE** for which ST confirmation has been performed. In this case, the ST registrant shall comply with the "Use of Certification Mark, etc." prescribed in the ***Requirements for Confirmation***.

Chapter 6 Suspension or Revocation of Certification and ST Confirmation

6.1 Surveillance

The **Certification Body** may perform **surveillance** for **Certification** or **ST confirmation** in accordance with the ***Operational Manual***.

6.2 Re-evaluation

The **Certification Body** may give instruction to conduct re-evaluation in accordance with the ***Operational Manual*** as needed after issuing a "**Certificate**" and "**Confirmation note**."

6.3 Suspension or Revocation

The **Certification Body** may suspend or revoke **Certification** or **ST confirmation** of a **TOE**, for which certification or ST confirmation has been performed, in accordance with the ***Operational Manual*** based on the results of **surveillance** and re-evaluation.

Chapter 7 Miscellaneous Provisions

7.1 Confidentiality

Evaluation Facilities and the **Certification Body** shall prevent confidential information from being transmitted to unauthorized persons during the processes of **Evaluation**, **Certification** and **ST confirmation** so as not to damage the confidentiality of information. The confidentiality procedures in the **Certification Body** are prescribed in the ***Operational Manual***.

7.2 Prohibited Matters

Evaluation Facilities, the **Certification Body**, and personnel of these organizations shall not perform the following:

a) Making a profit that may affect the results of **Evaluation**, **Certification** and **ST confirmation**, except for compensation for legitimate activities.
b) Developing a **TOE** that is a target of **Evaluation**, **Certification** and **ST confirmation**.
c) Providing consulting services to applicants.
   Note that these consulting services do not include the integration or reorganization of many existing documents created by applicants.

7.3 Services Required for Smooth Operation of this Scheme Conducted by the Certification Body

7.3.1 Preparation and Maintenance of Scheme Documentation

The **Certification Body** shall prescribe **this Scheme**, prepare, issue, distribute, revise, update and abolish Scheme Documentation that prescribe policies and rules for the purpose of operation of **this Scheme**, and interpret policies and rules of **this Scheme** as needed.

7.3.2 Issuance and Publication of Guidance

The **Certification Body** publishes the operation and interpretation of the **CC/CEM** and guidance on the operation of **this Scheme, etc.**, via the website of **IPA**.

7.3.3 Interviews regarding Progress of Evaluation

The **Certification Body** can conduct interviews regarding the progress of **Evaluation** and details of evaluation results with respect to either an applicant or an **Evaluation Facility** or both parties as needed.

In addition, the **Certification Body** can state neutral and fair opinions with respect to either an applicant or an **Evaluation Facility** or both parties as needed from the perspective of the operation of the Scheme.

7.4 Copyright of Certificate, etc.

The **Certification Body** owns the copyrights regarding a **certificate**, **Certification Report** and **Assurance Continuity Maintenance Report**. However, an applicant is authorized to copy and distribute a **certificate**, **Certification Report** and **Assurance Continuity Maintenance Report** unless the applicant copies these documents in full.

The **Certification Body** owns the copyrights regarding a **Confirmation** and **ST Confirmation Report**. However, an applicant is authorized to copy and distribute a **Confirmation** and **ST Confirmation Report** unless the applicant copies these documents in full.

7.5 Handling of Unauthorized Use of Certificate, etc.

The **Certification Body** gives instruction for improvement if the **Certification Body** acknowledges the fact of a breach of a ***Written Oath*** prescribed by the **Certification Body** including when a **registrant** or **ST registrant** misuses the “Certification Mark,” “Common Criteria Certification Mark,” **certificate**, **Certification Report**, **Assurance Continuity Maintenance Report, Confirmation note** or **ST Confirmation Report** or their copies, or uses these materials for advertisement and explanation in such a manner that misunderstanding occurs. If the effect of an instruction for improvement is not acknowledged after an instruction for improvement is provided, the corresponding **Certification** and **ST confirmation** can be revoked. More details required for revocation of the corresponding **Certification** and **ST confirmation** are

prescribed in the ***Operational Manual***.

7.6 Handling of Appeals, Complaints and Disputes

The **Certification Body** shall handle the processes related to appeals, complaints and disputes with respect to certification services according to the procedures prescribed in the ***Operational Manual***. **Evaluation Facilities** shall prepare and maintain procedures of processes related to appeals, complaints and disputes with respect to **Evaluation**.

Supplementary provisions (May 7, 2007 Jo-So No. 12 of 2007, Full revision)

(Date of enforcement)

1 This Scheme Document shall come into effect as of May 15, 2007.

(Abolition of Guidelines for Assurance Continuity concerning IT Security Certification)

2 The Guidelines for Assurance Continuity concerning IT Security Certification (July 29, 2005 Jo-So No. 39 of 2005) has been abolished.

Supplementary provision (January 25, 2011 Jo-So No. 160 of 2010, Partial revision)

This Scheme Document shall come into effect as of February 1, 2011.

Supplementary provision (April 3, 2012 Jo-So No. 160 of 2011, Partial revision)

This Scheme Document shall come into effect as of March 29, 2012.

Supplementary provision (March 28, 2014 Jo-So No. 170 of 2013, Partial revision)

This Scheme Document shall come into effect as of April 1, 2014.

Supplementary provision (May 28, 2015 Jo-So No. 51 of 2015, Partial revision)

This Scheme Document shall come into effect as of June 1, 2015.

Supplementary provision (June 28, 2018 Jo-So No. 176 of 2018, Partial revision)

This Scheme Document shall come into effect as of July 1, 2018.

Supplementary provision (September 28, 2020 Jo-So No. 1093 of 2020, Partial revision)

This Scheme Document shall come into effect as of August 15, 2020.

Annex A: Requirements for this Scheme

The following standards (1) to (4) are defined as the requirements used in this Scheme. Those who use these standards shall select the standard to be used from (1) and (2) respectively. If relevant standards (3) and (4) exist when using these standards (1) and (2), these standards (3) and (4) shall be jointly used. The Certification Body separately publishes information regarding the effective standard version, etc., for these standards via the website of IPA, and so on.

(1) IT Security Evaluation Criteria
  (i) ISO/IEC 15408 Information technology - Security techniques – Evaluation criteria for IT security
  (ii) Common Criteria for Information Technology Security Evaluation (CC)
    Note: This is the standard for IT security evaluation issued by the international mutual recognition arrangement "Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (CCRA)."
  (iii) This standard is established by standardizing the Japanese version of (ii).

(2) IT Security Evaluation Methodology
  (i) ISO/IEC 18045 Information technology - Security techniques – Methodology for IT security evaluation
  (ii) Common Methodology for Information Technology Security Evaluation (CEM)
    Note: This is the standard for IT security evaluation issued by the international mutual recognition arrangement "Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (CCRA)."
  (iii) The standard which is established by standardizing the Japanese version of (ii).

(3) IT Security Evaluation Criteria and its Interpretations
  Supplementary document for Common Criteria for Information Technology Security Evaluation (CC) published by the Certification Body.

(4) IT Security Evaluation Methodology and its Interpretations
  Supplementary document for Common Methodology for Information Technology Security Evaluation (CEM) published by the Certification Body.