

Secom Passport for Member 2.0 PUB
Certificate Policy
Version 6.10

May 26, 2025

SECOM Trust Systems Co., Ltd.

Version History		
Version Number	Date	Description
1.00	2008/04/28	Publication of the first version
1.10	2009/03/19	Revision of Certificate Profile (extendedKeyUsage).
2.00	2009/10/13	Addition of the Policy OID Overall revision of the styles
3.00	2013/11/27	Addition of the revised Policy OID associated with the addition of Sha256 Addition of the RootCA repository information
4.00	2014/05/29	Revision associated with the additional use of server authentication Addition of the Policy OID
5.00	2017/01/20	Addition of the Policy OID Revision associated with the start of OCSP server operation Overall revision of the styles
5.01	2020/02/19	Removal of the Certificate policy for server certificate Addition/revision of contents in BR for Code Signing Overall revision of the descriptions and styles
5.02	2020/03/30	Review of "No stipulation"
5.03	2020/06/15	Addition of Extended Key Usage to CA certificate (sha256) profile Addition of Extended Key Usage to Subscriber certificate (sha256) profile
5.04	2020/07/30	From Extended Key Usage of CA certificate (sha256), remove OCSP Signing, change OU, change CP URL From Subscriber certificate (sha256), change OU, change URL of CP, change OCSP URL of AIA, etc.
5.05	2020/09/29	Revision of Reason code for CRL profile
5.06	2021/06/15	Addition of Email Account Authentication
6.00	2021/08/03	Addition of CA Private Key Security Communication Root CA3 Modified Public Key information in Certificate Policy for Code Signing
6.01	2022/06/10	Overall revision of the descriptions and styles

6.02	2022/12/08	<p>Added requirement for Code Signing Certificate to "6.1.5 Key Sizes"</p> <p>Added requirement for Code Signing Certificate to "6.2.7 Private Key Storage on Cryptographic Module"</p> <p>"7.1 Certificate Profile"</p> <p>Modified:</p> <p>"Table 7.1-1 CA certificate (sha1) profile"</p> <p>"Table 7.1-2 CA Certificate (sha256) Profile"</p> <p>"Table 7.1-3 CA certificate (sha384) profile"</p> <p>"Table 7.1-5 Subscriber Certificate (sha256) Profile"</p>
6.03	2023/02/17	<p>Modified the description for "1.1 Overview"</p> <p>Added CP/OID, modified the description for "1.2 Document Name and Identification"</p> <p>Modified the description for "1.4.1 Appropriate Certificate Uses"</p> <p>Added the definition for "1.6 Definitions and Acronyms"</p> <p>Added the description for "3.2.3 Authentication of Applicant and Individual Identity"</p> <p>Added Root CA for "3.2.6 Criteria for Interoperation"</p> <p>Modified the description for "4.3.1 CA Actions during Certificate Issuance"</p> <p>Modified the description for "6.1.1 Key Pair Generation"</p> <p>Modified the description for "6.1.2 Private Key Delivery to Subscriber"</p> <p>Added the description for "6.2.1 Cryptographic Module Standards and Controls"</p> <p>Added the description for "6.2.7 Private Key Storage on Cryptographic Module"</p> <p>Modified the description, added profiles for "7.1 Certificate Profile"</p> <p>Added Root CAs for "7.1.3 Algorithm Object Identifier"</p> <p>Modified the description, added profiles for "7.2 CRL Profile"</p> <p>Modified the description, added profiles for "7.3 OCSP Profile"</p>
6.04	2023/05/17	<p>Update "1.1 Overview"</p> <p>Update "1.2 Document Name and Identification"</p>

		<p>Update “1.6 Definitions and Acronyms”</p> <p>Update “2.3 Time or Frequency of Publication”</p> <p>Update “3.2.2 Authentication of Organization Identity”</p> <p>Update “3.2.6 Criteria for Interoperation”</p> <p>Update “3.2.7 Reliability of verification sources ”</p> <p>Update “4.1.2 Enrollment Process and Responsibilities”</p> <p>Update “4.2.1 Performing Identification and Authentication Functions”</p> <p>Update “4.9.1 Circumstances for Certificate Revocation”</p> <p>Update “4.9.2 Who Can Request Revocation”</p> <p>Update “4.9.3 Procedure for Revocation Request”</p> <p>Update “4.9.5 Time within Which CA Shall Process the Revocation Request”</p> <p>Update “4.9.7 CRL Issuance Frequency”</p> <p>Update “4.9.9 On-Line Revocation/Status Checking Availability”</p> <p>Update “4.9.10 On-Line Revocation/Status Checking Requirements”</p> <p>Update “4.9.11 Other Forms of Revocation Advertisements Available”</p> <p>Update “4.10.2 Service Availability”</p> <p>Update “5.5.1 Types of Records Archived”</p> <p>Update “5.5.2 Retention Period for Archive”</p> <p>Update “5.5.3 Protection of Archive”</p> <p>Update “5.5.4 Archive Backup Procedures”</p> <p>Update “5.5.5 Requirements for Time-Stamping of Records”</p> <p>Update “5.5.6 Archive Collection System”</p> <p>Update “5.5.7 Procedures to Obtain and Verify Archive Information”</p> <p>Update “5.7.1 Incident and Compromise Handling Procedures”</p> <p>Update “5.7.2 Computing Resources, Software, and/or Data are Corrupted”</p> <p>Update “5.7.3 Entity Private Key Compromise Procedures”</p> <p>Update “5.7.4 Business Continuity Capabilities after a Disaster”</p>
--	--	---

		<p>Update “6.1.2 Private Key Delivery to Subscriber”</p> <p>Update “6.1.6 Public Key Parameters Generation and Quality Checking”</p> <p>Update “7.1 Certificate Profile”</p> <p>Update “7.1.4 Name Format”</p> <p>Update “7.1.6 Certificate Policy Object Identifier</p> <p>Update “7.2 CRL Profile”</p> <p>Update “7.3 OCSP Profile”</p>
6.05	2023/08/28	<p>Update “4.9.1 Circumstances for Certificate Revocation”</p> <p>Update “7.1 Certificate Profile”</p> <p>Update “7.3 OCSP Profile”</p> <p>Update “9.6.1 CA Representation and Warranties”</p> <p>Update “9.6.3 Applicant and Subscriber Representations and Warranties”</p>
6.06	2024/04/01	<p>Update “1.1 Overview “</p> <p>Update “1.6 Definitions and Acronyms”</p> <p>Update “3.2.3 Authentication of Applicant and Individual Identity ”</p> <p>Update “3.2.6 Criteria for Interoperation”</p> <p>Update “4.9.8 Maximum Latency for CRLs”</p> <p>Update “6.1.1 Key Pair Generation</p> <p>Update “6.1.5 Key Sizes”</p> <p>Update “6.2.1 Cryptographic Module Standards and Controls”</p> <p>Update “7.1 Certificate Profile”</p> <p>Update “7.1.3 “Algorithm Object Identifier”</p> <p>Update “7.2 “CRL Profile”</p> <p>Update “7.2.2 “Certificate Revocation Lists and CRL Entry Extensions”</p> <p>Update “7.3 OCSP Profile”</p> <p>Update “8.1 Frequency and Circumstances of Assessment”</p> <p>Update “8.2 Identity/Qualifications of Assessor”</p> <p>Update “8.3 Assessor’s Relationship to Assessed Entity”</p> <p>Update “8.4 Topics Covered by Assessment”</p> <p>Update “8.5 Actions Taken as a Result of Deficiency”</p> <p>Update “8.6 Communication of Results”</p>

6.07	2024/05/17	Update the below: “3.2.3 Authentication of Applicant and Individual Identity” “4.2.1 Performing Identification and Authentication Functions” “7.1 Certificate Profile” “7.2 CRL Profile” “7.3 OCSP Profile”
6.08	2024/08/21	Update the below: “3.2.3 Authentication of Applicant and Individual Identity” “3.2.5 Validation of Authority” “6.1.1 Key Pair Generation” “6.2.6 Private Key Transfer into or from a Cryptographic Module” “9.6.1 CA Representation and Warranties”
6.09	2024/10/23	Update the below: 1.3.3 Subscribers 1.5.2 Contact Information 1.6 Definitions and Acronyms 4.2.1 Performing Identification and Authentication Functions 4.2.2.1 Certification authority authorization (CAA) 6.1.1 Key Pair Generation 6.2.1 Cryptographic Module Standards and Controls 6.2.7 Private Key Storage on Cryptographic Module 7.1.1 Version Number(s) 7.1.2 Certificate Extension 7.1.8 Policy Qualifier Syntax and Semantics 7.2.1 Version Number(s) 8.7 Self-Audits
6.10	2025/05/26	The contents of this document have been incorporated into the "SECOM Publicly Trusted Certificate Policy / Certification Practice Statement".

Notice Regarding the Integration of CP/CPS (Certificate Policy / Certification Practice Statement)

This document has transitioned to the newly integrated CP/CPS as of 2025-05-26.

The new CP/CPS is available at the following URL:

SECOM Publicly Trusted Certificate Policy / Certification Practice Statement

<https://repo1.secomtrust.net/spcpp/publicly-trusted-cpcps/>

This document is no longer subject to updates, and all certification operations are conducted in accordance with the new CP/CPS.

For further details regarding certification operations, please refer to the new CP/CPS.