

Organization Validation Certificate Policy Version 1.25

May 26, 2025

SECOM Trust Systems Co., Ltd.

| Version History | | |
|-----------------|------------|--|
| Version Number | Date | Description |
| 1.00 | 2018/07/24 | Publication of the first version |
| 1.10 | 2018/10/12 | Modified the contents of the profile |
| 1.11 | 2019/05/24 | Revision of overall descriptions and style Deleted IP address for domain authentication |
| 1.12 | 2020/03/30 | Revision of chapters, and added some "No stipulation" contents |
| 1.13 | 2020/09/01 | Changed Certificate validity period from 825 days to 398 days |
| 1.14 | 2020/09/29 | Modified Reason code in CRL profile |
| 1.15 | 2020/12/18 | Added OID assigned to CP Added Security Communication ECC Root CA1 issued CA profile |
| 1.16 | 2021/05/31 | Modified the description for domain authentication Modified certificate revocation reasons Added special requirements for key compromise |
| 1.17 | 2021/06/15 | Revision of descriptions and style Modified certificate revocation reasons |
| 1.18 | 2021/11/30 | Modified the description for domain authentication Revision of overall descriptions and style |
| 1.19 | 2022/06/10 | Revision of overall descriptions and style |
| 1.20 | 2023/05/17 | Update "1.2 Document Name and Identification" Update "2.3 Time or Frequency of Publication" Update "4.9.1 Circumstances for Certificate Revocation" Update "5.5.1 Types of Records Archived" Update "5.5.2 Retention Period for Archive" Update "5.5.3 Protection of Archive" Update "5.5.4 Archive Backup Procedures" Update "5.5.5 Requirements for Time-Stamping of Records" Update "5.5.6 Archive Collection System" Update "5.5.7 Procedures to Obtain and Verify Archive Information" |

| | | |
|------|------------|---|
| | | <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 “7.1 Certificate Profile”</p> <p>Update “7.2 CRL Profile”</p> <p>Update “7.2.2 CRL Entry Extensions”</p> |
| 1.21 | 2023/08/28 | <p>Update “1.6 Definitions and Acronyms”</p> <p>Update “7.1 Certificate Profile”</p> |
| 1.22 | 2024/04/01 | <p>Update “1.1 Overview ”</p> <p>Update “1.6 Definitions and Acronyms”</p> <p>Update “2.2 Publication of Certificate Information”</p> <p>Update “3.2.2.4 “Domain Authentication”</p> <p>Update “3.2.3 Authentication of Applicant and Individual Identity ”</p> <p>Update “3.2.5 Validation of Authority”</p> <p>Update “3.2.6 Criteria for Interoperation”</p> <p>Update “4.5.1 Subscriber Private Key and Certificate Usage”</p> <p>Update “4.9.8 Maximum Latency for CRLs”</p> <p>Update “6.1.7 Key Usage Purposes</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 “8 Compliance Audit and Other Assessments”</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> |

| | | |
|------|------------|--|
| 1.23 | 2024/08/21 | <p>Update the below:</p> <p>1.3.1 CA</p> <p>1.3.2 RA</p> <p>1.3.3 Subscribers</p> <p>1.3.4 Relying Party</p> <p>1.6 Definitions and Acronyms</p> <p>2.1 Repository</p> <p>2.2 Publication of Certificate Information</p> <p>4.1.2 Enrollment Process and Responsibilities</p> <p>4.2.1 Performing Identification and Authentication Functions</p> <p>4.9.1 Circumstances for Certificate Revocation</p> <p>4.9.7 CRL Issuance Frequency</p> <p>6.1.1 Key Pair Generation</p> <p>7.1 Certificate Profile</p> <p>7.2 CRL Profile</p> <p>7.2.2 CRL Entry Extensions</p> <p>Delete the below:</p> <p>4.2.4 CAA Records Processing</p> |
| 1.24 | 2024/10/23 | <p>Update the below:</p> <p>1.5.2 Contact Information</p> <p>1.6 Definitions and Acronyms</p> <p>2.2 Publication of Certificate Information</p> <p>3.2.2.4 Domain Authentication</p> <p>3.2.2.9 Multi-Perspective Issuance Corroboration</p> <p>4.3.1.1 Manual authorization of certificate issuance for Root CAs</p> <p>4.3.1.2 Linting of to-be-signed Certificate content</p> <p>4.3.1.3 Linting of issued Certificates</p> <p>4.9.11 Other Forms of Revocation Advertisements Available</p> <p>6.2.1 Cryptographic Module Standards and Controls</p> <p>6.2.7 Private Key Storage on Cryptographic Module</p> <p>7.1.1 Version Number(s)</p> <p>7.1.2 Certificate Extension</p> <p>7.1.8 Policy Qualifier Syntax and Semantics</p> |

| | | 7.2.1 Version Number(s) |
|------|------------|---|
| 1.25 | 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.