AUTOCRYPT

AutoCrypt V2X-PKI

Test Certificate Policy for Autocrypt V2X Public Key Infrastructure

V1.0.1

1. Introduction

1.01 Overview

Autocrypt Co., Ltd. (hereinafter referred to as "AUTOCRYPT") has developed a Vehicle-to-Everything (V2X) Public Key Infrastructure (PKI) for testing purposes, following the IEEE 1609.2 standards. The AutoCrypt V2X-PKI comprises a Root Certification Authority (RCA) and Subordinate Certification Authorities, serving as trust anchors within the infrastructure.

This Certificate Policy (CP) is established to provide a standardized framework for managing certificates within the AutoCrypt V2X-PKI for testing purposes. It outlines the procedures and requirements for issuing, managing, and revoking certificates within the V2X PKI system.

The guidelines outlined in this CP are for testing purposes ONLY.
AUTOCRYPT disclaims any liability arising from the use of this Certificate Policy.

1.02 PKI participants

No stipulation.

1.03 Certificate usage

1.03.1 Permitted certificate use cases

Certificates issued under this policy should be used for testing purposes ONLY.

1.03.2 Prohibited certificate use cases

Certificates issued under this policy should NOT be used for real-world security applications.
This Certificate Policy does not guarantee any level of assurance.

1.04 Policy administration

1.04.1 Organization administering the document

Autocrypt Policy Authority (PA) is responsible for all aspects of this Certificate Policy.

1.04.2 Contract information

Any questions regarding this document shall be directed to the organization administering this document via electronic mail at martin@autocrypt.io

1.04.3 Person determining CPS suitability for the policy

This CP may be used without a CPS.

1.04.4 CPS approval procedures

No stipulation.

2. Publication and repository’s responsibility

No stipulation.

3. Identification and authentication

No stipulation.

4. Certificate life-cycle operational requirements

No stipulation.

5. Facility management and operational controls

No stipulation.

6. Technical security controls

No stipulation.

7. Certificate, CRL and OCSP profiles

No stipulation.

8. Audit methods

No stipulation.

9. Other business and legal matters

9.01 Fees

No stipulation.

9.02 Financial responsibility

No stipulation.

9.03 Confidentiality of business information

No stipulation.

9.04 Privacy of personal information

No stipulation.

9.05 Intellectual property rights

No stipulation.

9.06 Representations and warranties

No stipulation.

9.07 Disclaimers of warranties

No stipulation.

9.08 Limitations of liability

AUTOCRYPT disclaims any liability that may arise from the use of any certificates issued by any CA that asserts this certificate policy.

9.09 Indemnities

No stipulation.

9.10 Term and termination

No stipulation.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

No stipulation.

9.13 Dispute resolution provisions

No stipulation.

9.14 Governing law

No stipulation.

9.15 Compliance with applicable law

No stipulation.

9.16 Miscellaneous provisions

No stipulation.

9.17 Other provisions

No stipulation.

References:

- Washington, D.C.: U.S. Department of Commerce.
  Computer Security Division (CSD), NIST -. 2012. “Test Certificate Policy to Support Pki Pilots and Testing.”
  https://csrc.nist.gov/CSRC/media/Projects/Computer-Security-Objects-Register/documents/test_policy.pdf

Document change history:

Date	Description	Version
2023/12/10	First release	1.0.0
2024/03/22	Content update, visual update	1.0.1