Geely Automobile Group Co., Ltd

Version 1.0

Certificate Practice Statement

For Polestar V2G PKI

Geely Automobile Group Co., Ltd
No 1760, Jiangling Road,
Binjiang distr, Hangzhou City
Zhejiang Province
China

Document information and revision history

Document version	1.0
Classification	Public
Author(s)	Wang Jinxuan
Reviewer(s)	Anders Runesson, Wei Guo
Approver(s)	Anders Runesson

Date	Version	Author	Description
2024-01-20	1.0	Wang Jinxuan e-wangjinxuan@geely.com	First version

Structure

This document conforms to the structure of Certificate Policies and Certification Practice Statements specified in RFC 3647[1]. Sections have been added in a way that retains the document structure in RFC 3647.

Intended audience

This document is intended for, but not limited to, all subscribers, stakeholders, and participants in the PKI.

Keywords

Within this document, the key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL”, if written in capitals, are to be interpreted as described in RFC 2119[2]

Terms and abbreviations

Authentication	The process of establishing the truth of an entity’s claim of identity
CA	Certification Authority
CCP	Contract Certificate Pool
CN	Common Name
CPO	Charge Point Operator
CPS	Certification Practice statement
CPS	Certificate Provisioning Service
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DN	Distinguished Name

[1] https://www.ietf.org/rfc/rfc3647.txt
[2] https://datatracker.ietf.org/doc/html/rfc2119

EE	End Entity
eMAID	e-Mobility Account Identifier
EVCC	Electric Vehicle Communication Controller
EVSE	Electric Vehicle Supply Equipment
HSM	Hardware Security Module
Identification	The process whereby an entity makes a claim regarding their identity. Precedes authentication.
IETF	Internet Engineering Task Force
MO	Mobility Operator
OCSP	Online Certificate Status Protocol
OEM	Original Equipment Manufacturer
OID	Object Identifier, global standardized numeric identifiers. See https://en.wikipedia.org/wiki/Object_identifier
PCID	Provisioning Certificate Identifier
PKI	Public Key Infrastructure
PnC, P&C	Plug and Charge based on [ISO15118-2] or [ISO15118-20]
RCP	Root Certificate Pool
RFC	Request For Comment
SECC	Supply Equipment Communication Controller
V2G	Vehicle to grid

References

[ASN.1]	ITU-T Recommendation X.680-X.693 (02/21): Information Technology - Abstract Syntax Notation One (ASN.1) & ASN.1 encoding rules
[FIPS 140-2]	https://csrc.nist.gov/pubs/fips/140-2/upd2/final NIST standard - Security Requirements for Cryptographic Modules
[FIPS 140-3]	https://csrc.nist.gov/pubs/fips/140-3/final NIST standard - Security Requirements for Cryptographic Modules
[FIPS 140]	The text may refer to the FIPS 140 standards without version number in cases where the standards are aligned.
[RFC2986]	https://datatracker.ietf.org/doc/html/rfc2986 PKCS #10: Certification Request Syntax Specification
[RFC3647]	https://www.ietf.org/rfc/rfc3647.txt Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework

[RFC5280]	https://datatracker.ietf.org/doc/html/rfc5280 Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile
[ISO/IEC 15408]	ISO/IEC 15408 2022: Information security, cybersecurity and privacy protection — Evaluation criteria for IT security *Defines Evaluation Assurance Levels (EAL), also known as Common Criteria*
[ISO/IEC 19790]	ISO/IEC 19790:2012: Information technology - Security techniques - Security requirements for cryptographic modules
[ISO15118-2]	Standard ISO 15118-2:2014: Road vehicles -- Vehicle-to-grid Communication Interface – Part 2: Network and application protocol requirements
[ISO15118-20]	Standard ISO 15118-2:2022: Road vehicles – Vehicle to grid communication Interface – Part 20: 2nd generation network layer and application layer requirements
[ISO15118]	The text may refer to ISO15118 without version number in cases where the standards are aligned.
[ISO3166-1]	Standard ISO 3166-1:2020: Codes for the representation of names of countries and their subdivisions - Part 1: Country code
[X.500]	ITU-T Recommendation X.500 (2005) I ISO/IEC 9594-1:2005 Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services

In some cases the standards [ISO15118] may be referenced along with an identifier in the form [V2Gnn-nnnn], for example [ISO15118-2] [V2G2-932]. This is a specific requirement or motivation that can be found by searching for the text in the standard. In this case searching for “[V2G2-932]” results in a requirement that reads: “CertID shall be an alphanumeric String with at maximum length of 18 characters (i.e. A..Z, a..z, 0..9).”

1 INTRODUCTION

1.1 Overview

Geely Automobile Group Co., Ltd (henceforth referred to as 'Geely') designs and manufactures automobiles both in their own name and for other brands in the Geely Group. Sharing core services enables high efficiency and utilization of resources, and PKI is one such service that benefits greatly when managed by one central team instead of many distributed small ones.

PKI is a core security function and is ubiquitous on the internet, as well as in private communications. It is a mature and well understood security technology, and is part of the international standards for Plug and Charge (PnC) [ISO15118]. Geely has established this PKI to support V2G and PnC for any brand in the Geely group.

This CPS regulates how Geely's central PKI issues certificates to Polestar cars and how Geely complies with the requirements from Polestar's PKI team established in their Certificate Policy for Polestar V2G PKI.

1.2 Document name and identification

This document is Geely's Certification Practice Statement for the Polestar V2G PKI and is identified by the following:

- Name: Certification Practice Statement for Polestar V2G PKI
- Version: 1.0
- OID: 1.3.6.1.4.1.59600.2.509.0.1.1.2

The OID arc 1.3.6.1.4.1.59600 is Polestar's IANA assigned Private Enterprise Number[3].

The CPS's full identifier is: 1.3.6.1.4.1.59600.2.509.0.1.1.2

1.3 PKI participants

1.3.1 PKI structure

Polestar's V2G PKI will comprise multiple CA chains, each with three CA tiers. The root CA certifies policy CAs, and policy CAs certify issuing CAs. An issuing CA SHALL only sign end-entity certificates. Geely will deliver issuing CA's chaining up to Polestar's policy CA's, and OCSP responders for those issuing CAs.

CAs in this PKI MUST strictly abide by the certificate types they are allowed to sign in the following table.

CA type	Issued by	Allowed to sign certificate types	Other
Root	Self	Policy CA, OCSP signer	CRL files, OCSP responses
Policy (Sub 1/Tier 1)	Root	Issuing CA, OCSP signer	CRL files, OCSP responses
Issuing (Sub 2/Tier 2)	Policy	End entity, OCSP signer	CRL files, OCSP responses
End entity	Issuing	MUST NOT sign certificates	

[3] See https://www.iana.org/assignments/enterprise-numbers/enterprise-numbers

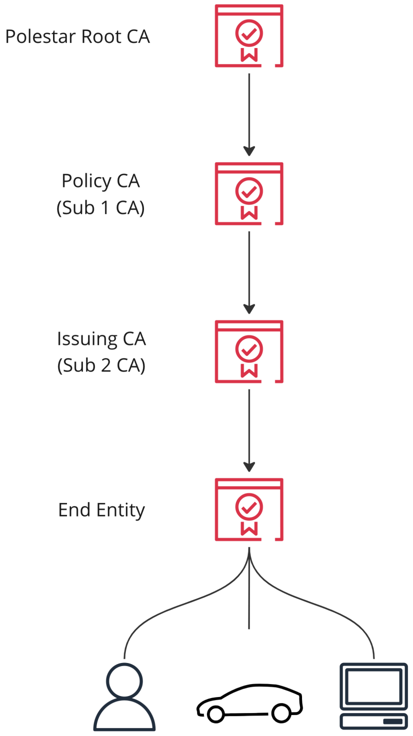


Figure 1 Schematic view of Polestar PKI CA chains

1.3.2 Certification authorities

This CPS will cover Geely's issuing CA's as noted in the following table:

CA name	Signed by	Signs for entity type
CN=Polestar ECC-256 V2G OEM Issuing CA v1, O=Polestar Performance AB, C=SE	CN=Polestar ECC-256 V2G OEM Policy CA v1, O=Polestar Performance AB, C=SE	End entity

1.3.3 Registration authorities

Geely will employ an automated registration authority as part of the CA service.

1.3.4 Subscribers

Polestar vehicles are the only subscribers to the services in this CPS.

1.3.5 Relying parties

Geely's PKI will publish certificates and revocation data to, and retrieve certificates from, PnC ecosystem operators as required and directed by Polestar. This is regulated in separate agreements.

No further stipulations.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

This CA SHALL only sign certificates to Polestar cars for use in PnC.

1.4.2 Prohibited certificate uses

1.4.1 documents the only allowed use cases. Any other use case is prohibited.

1.5 Policy administration

1.5.1 Organization administering the document

This document is owned by Geely's PKI team and published within Polestar's PKI. Geely's PKI team may be contacted as noted in section 1.5.2.

1.5.2 Contact person

Name	Role	Email address
Wang Jinxuan	PKI Business owner	e-wangjinxuan@geely.com
Yin Yang	PKI Business owner	yin.y@geely.com
Wang Jiao	IT system owner	jiao.wang1@geely.com

1.5.3 Person determining CPS suitability for the policy

Polestar's InfoSec team is responsible, and solely authorized to, approve or reject a participating CA's CPS.

1.5.4 CPS approval procedures

Polestar's InfoSec team is responsible, and solely authorized to, approve or reject a participating CA's CPS.

1.6 Definitions and acronyms

See the section Terms and abbreviations at the start of the document.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

Polestar maintains and operates one repository on the public internet accessible at: https://pki.polestar.com. The repository will be open and accessible without restriction or fees.

Geely will additionally interact with the PnC ecosystems and will maintain data within them, including certificates and revocation data. The specifics are beyond this CPS and is regulated in agreements between Geely, Polestar, and the respective ecosystem.

2.2 Publication of certification information

This PKI will only publish information in the PnC ecosystems as directed by Polestar. No additional publication will be done by Geely.

Polestar will publish CA certificate documentation as per their V2G PKI Certificate Policy.

Geely will provide revocation data via standard CRL and OCSP services. See the 7.1 for details per certificate profile.

2.3 Time or frequency of publication

Geely will interact with Polestar's PKI team when changes to documentation is done to ensure timely publication.

Updates regarding certificates or certificate status will be as near-realtime as possible, and shall happen within 24 hours.

2.4 Access controls on repositories

Access to Geely's systems is restricted to Geely's PKI team. Revocation services publish data without read restrictions.

Geely provides no other online repository than revocation services.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

No stipulation beyond Polestar's V2G PKI Certificate Policy. This CPS will strictly adhere to the regulations in the certificate policy.

3.1.1 Types of names

All end entity certificates signed by this CA will use standard X.509 Distinguished Names, using the following format:

DC=OEM,CN=<PCID>,O=Polestar Performance AB

<PCID> shall be generated as a unique identifier for each vehicle, as per section 3.1.2.

3.1.2 Need for names to be meaningful

End entities served by this CA SHALL use PCID format for names, 18 characters using the following generation mechanism:

Length	3 chars (alphanumeric)	14 chars (alphanumeric)	1 char (alphanumeric)
Field content	WMI	OEM vehicle ID	Check digit
Example	LPS	p417prod000011	6
Description	Polestar's WMI code, per ISO3780:2009	Polestar's own ID for the vehicle	Checksum according to DIN 91286:2011-11

3.1.3 Anonymity or pseudonymity of subscribers

Anonymity and pseudonymity SHALL NOT be permitted.

3.1.4 Rules for interpreting various name forms

Distinguished Names SHALL be interpreted according to [RFC5280] and [X.500].

3.1.5 Uniqueness of names

All entities in this PKI must have unique names. Upon receipt of a certification request an issuing CA shall verify that the requested Subject name, in addition to other requirements, is unique within the PKI.

3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

A certificate applicant SHALL prove possession of the private key corresponding to the public key in the certification request. The mechanism used to prove possession SHALL be submission of a Certificate Signing Request (CSR) in PKCS#10 form, described in [RFC2986], which SHALL contain the public key of the applicant, and be signed by the corresponding private key. This enables the RA to verify the applicants possession of the private key.

3.2.2 Authentication of organization identity

This CA will serve only end entities managed by Geely. No organizations can submit certificate requests.

3.2.3 Authentication of individual identity

This CA will issue certificates to machine entities only, and the processes for requesting certificates will be done via automated tooling that may be directly initiated by a person (in a car workshop), or without any human interaction (on the factory line).

For end-entities, in addition to the stipulations section 3.2.1, human initiated exchanges with the RA will happen by using individual password protected accounts identifying the operator initiating the exchange. The communications necessary for transmission of CSR to the RA will be protected by encrypted transport using TLS.

On the factory line only the car ECU will be authenticated by the PKCS#10 signature mechanism.

3.2.4 Non-verified subscriber information

All information included in certificates SHALL be validated by the RA.

3.2.5 Validation of authority

No stipulation, see also section 3.2.2

3.2.6 Criteria for interoperation

No stipulation

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

The requirements for renewal of certificates are identical to the initial request (see 3.2). Renewal without re-keying is not allowed.

3.3.2 Identification and authentication for re-key after revocation

The requirements for renewal of certificates are identical to the initial request (see 3.2). Renewal without re-keying is not allowed.

3.4 Identification and authentication for revocation request

The CA may receive revocation requests from workshop tooling when replacing ECU hardware, or resetting ECU software. This request shall authenticate the operator sending the request.

Polestar’s InfoSec team SHALL have the right to request revocation of a certificate from this CA.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

Certificate requests can be submitted to this CA from Geely’s factory systems, or workshop tooling. The end entity is always a car manufactured by Geely for Polestar.

4.1.2 Enrollment process and responsibilities

The enrolment process is the same as the certificate request process. An entity is considered enrolled when the CA has validated the certificate request and signed the certificate.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Every request to the CA SHALL be authenticated by the RA before the application is accepted. The authentication SHALL verify that the request comes from a known source (factory line or workshop station) and in the case of a workshop, an authenticated operator station.

4.2.2 Approval or rejection of certificate applications

The RA MUST reject any certificate request that does not comply with the requirements in this CP (in particular chapters 3, 4, and 7), or the applicable CPS.

4.2.3 Time to process certificate applications

The PKI regulated by this CPS is online and is expected to issue certificates promptly when a request is made. No delays shall be longer than 1 hour.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

After successful validation by the RA the CA SHALL issue the certificate and store logging information according to sections 5.4 and 5.5.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The CA SHALL respond with a rejection or signed certificate in the same communications channel used by the requester to send the request.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

No stipulation

4.4.2 Publication of the certificate by the CA

The CA will publish certificates for end-entities and CA’s in this PKI as described in chapter 2.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulations.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Certificates and their corresponding private keys SHALL only be used in the following ways and circumstances (ALL the following apply at all times):

- by the subscriber or end entity they certify
- in accordance with the usage attributes and validity times encoded in the certificate
- in accordance with the use cases defined in [ISO15118]

See also section 1.4 for further specifications of acceptable use, and section 6.1 regarding private key security.

4.5.2 Relying party public key and certificate usage

A relying party SHALL use a certificate and its public key to perform authentication of and end-entity in this PKI, validate integrity of signed data, or perform encryption of data intended for the end entity. These activities may include a number of substeps, including but not limited to:

- the relying party SHALL validate that the certificate chains to the expected root CA
- the relying party SHOULD validate that the certificate chains to a V2G policy CA
- the relying party SHOULD validate that the certificate has not been revoked

The specific steps taken SHALL follow the requirements from [ISO15118].

4.6 Certificate renewal

Renewal is not supported, see re-key.

4.7 Certificate re-key

Certificate re-key is the process for issuing a certificate to the same entity, using the same subject DN and other certificate data, and using a new key pair for the subscriber. The requirements for this process is the same as for requesting a new certificate for a new subscriber. This CA SHALL handle all certificate applications in the same manner, regardless of whether the request is for a re-key or a new certificate application. See chapter 3 and section 4.3.

4.8 Certificate modification

Certificate modification is not allowed in this PKI.

4.9 Certificate revocation and suspension

A sub CA or an end entity in this PKI may have its certificate revoked under certain circumstances (see section 4.9.1). A root CA certificate cannot be revoked, as it is self signed and acts as the trust anchor. It does therefore not have a superordinate authority that can revoke it.

4.9.1 Circumstances for revocation

See CP

4.9.2 Who can request revocation

The following SHALL always be able to request revocation of a certificate:

- A workshop station when the vehicle needs ECU replacement or reconfiguration.
- Polestar’s InfoSec team

4.9.3 Procedure for revocation request

When requested via automated tooling the request shall be performed promptly following authentication. Manual requests MUST be validated via call back to the person initiating the request.

After revocation the information SHALL be published as soon as possible.

4.9.4 Revocation request grace period

This CA will not honor any grace period.

4.9.5 Time within which CA must process the revocation request

Following validation the revocation MUST happen within 1 hour.

4.9.6 Revocation checking requirement for relying parties

No stipulation

4.9.7 CRL issuance frequency (if applicable)

This CA publishes revocation data via OCSP only. The OCSP will be updated immediately after publishing.

4.9.8 Maximum latency for CRLs (if applicable)

See 4.9.7

4.9.9 On-line revocation/status checking availability

See 4.9.7. The OCSP service is available globally 24/7 with 99% uptime.

4.9.10 On-line revocation checking requirements

No stipulations beyond section 4.9.6.

4.9.11 Other forms of revocation advertisements available

No stipulations.

4.9.12 Special requirements re key compromise

No stipulations.

4.9.13 Circumstances for suspension

Certificate suspension is not supported by this CA.

4.10 Certificate status services

No stipulations beyond section 4.9.

4.11 End of subscription

A subscription ends when a subscriber does not request a new certificate to replace an existing certificate when it expires, or is revoked.

4.12 Key escrow and recovery

Key escrow is not supported by this CA.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

Geely’s PKI services are housed in secure data centers with strong physical security controls and policies, and are certified with ISO27000 to demonstrate the compliance.

5.1.1 Site location and construction

All facilities used by the CA services are inside a secure part of Geely’s campus to prevent access to unauthorized individuals.

5.1.2 Physical access

To access the CA services the premises are protected by:

1. External access gates
2. Access cards to internal doors
3. Camera monitoring

5.1.3 Power and air conditioning

The power systems and HVAC systems are industry grade and provide continuous electricity and air supply, with backup systems in place.

5.1.4 Water exposures

The facilities have been designed to handle water exposure by accidents or flooding from natural causes and disasters to a high but reasonable degree.

5.1.5 Fire prevention and protection

The facilities are equipped with state of the art fire detection and protection systems that are frequently tested to ensure correct operation.

5.1.6 Media storage

All data is protected by redundant storage media and backed up to an off site location.

5.1.7 Waste disposal

Equipment taken out of service will be erased on site and then physically destroyed.

5.1.8 Off-site backup

The CA is continually backed up (1/hour) using online backup features. Every night full backups are made to a secondary facility.

5.2 Procedural controls

5.2.1 Trusted roles

The CA staff are appointed the following roles with the given responsibilities as per this table:

Role	Responsibilities
System operator	Manage operating system and software not directly related to the CA service itself. Perform system maintenance, updates, patch management, OS backups.
Certificate manager	Validate certificate requests and certificate revocation requests. Approves and denies the requests. Signs CRLs.
HSM operator	Manage HSM hardware and software on both HSM devices and systems integrated with the HSM. Manages backups for HSMs.
Security Officer	Activate HSMs, generates and destroys keys in HSMs
Auditor	Reviews documentation and logs

5.2.2 Number of persons required per task

HSM operator tasks and Security Officer tasks require two persons to perform the work.

5.2.3 Identification and authentication for each role

The access to CA software and hardware always require authentication with at least two factors before access is granted.

5.2.4 Roles requiring separation of duties

No person can simultaneously hold the roles HSM operator and Security Officer.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

Geely's PKI team require qualified staff and hiring procedures ensure the PKI teams requirements are met before appointing new staff. All new hires are subject to background checks and examination of qualifications to ensure staff is of suitable competence and trustworthiniess.

5.3.2 Background check procedures

Background checks are performed by HR to ensure the candidate is giving an accurate representation of themselves regarding job experience, education, and other circumstances that are relevant for employment. Other factors can be criminal records or other questionable behaviours.

5.3.3 Training requirements

Geely requires adequate training for appointment to any role. There is no formal education that maps directly to the PKI team's skills, so there is no specific training or education required. The candidate shall however be able to demonstrate that they posess adequate skills.

5.3.4 Retraining frequency and requirements

Retraining is done as required, generally every year.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

Unauthorized activities is strictly forbidden and will at least lead to a written warning. In serious offences the person can be removed from their duties immediately.

5.3.7 Independent contractor requirements

Geely's PKI team may employ contractors to fulfil certain duties. The responsibility to manage the contractor staff is on Geely and from the PKI service's perspective there is no difference between staff employed directly by Geely, or a contractor.

5.3.8 Documentation supplied to personnel

Geely's PKI team create rigorous documentation to ensure all staff can perform all duties as expected.

5.4 Audit logging procedures

All activities in the PKI will be subject to logging, both audit logging (for traceability and accountability) and technical logs (for troubleshooting/maintenance).

5.4.1 Types of events recorded

System level events:

- Account management: This type of event is captured in the IAM system.
- Authentication settings: Captured in both OS logs and CA system logs
- Network connections established between CA systems: Captured in both OS logs and CA system logs
- Log in and, where possible, log out events of CA systems: Captured in both OS logs and CA system logs
  Security settings: Captured in both OS logs and CA system logs
- Operational settings: Captured in both OS logs and CA system logs
- Software lifecycle: Captured in both OS logs and CA system logs
- Database: Database level changes are captured in database system logs. Individual record updates are not logged in the database itself.

RA events:

- Receipt of certificate application: logged in CA system
- Receipt of a revocation request: logged in CA system
- Submission of a certificate request to the CA: logged in CA system
- Receipt of a signed certificate from the CA: logged in CA system
- Distribution of a signed certificate to a subscriber: logged in CA system

CA events:

- Receipt of a certificate request from RA: logged in CA system
- Receipt of a revocation request: logged in CA system
- Signing of a certificate: logged in CA system
- Sending a signed certificate to RA: logged in CA system
- CRUD events for key pairs: logged in CA system
- Data exports from CA database or cryptographic material: logged in CA system
- Usage of cryptographic material belonging to the CA: logged in CA system

Administrative events:

- Access management: This type of event is captured in the IAM system, as well as CA system

5.4.2 Frequency of processing log

Geely's CA service is an online service and logging is performed in real-time. From the CA system the logs are captured into a log management system that is kept and maintained separately. Logs in this system are protected for both availability, confidentiality, and integrity to prevent unauthorized or unintentional changes.

Logs are scanned by online systems to detect operational anomalies that could lead to downtime or indicate a risk of leaks or breaches.

5.4.3 Retention period for audit log

System level events defined in 5.4.1 SHALL be logged and retained until both the following are fulfilled:

- the next full audit has been performed
- at least 1 years has passed

RA, CA, and administrative events defined in 5.4.1 SHALL be logged and retained until until the CA ceases its operation, at which point it SHALL be archived by Polestar.

Log data is stored in the respective systems for at least 1 month, and then stored in archives in accordance with the time requirements in 5.5.2 in the CP.

5.4.4 Protection of audit log

The audit log is protected, both in operational systems and backups, by industry grade encryption and integrity protection mechanisms. All transport is protected by TLS 1.2 or later, and all data is stored at-rest on encrypted hard drives.

5.4.5 Audit log backup procedures

Audit logs are backed up with the rest of the CA systems.

5.4.6 Audit collection system (internal vs. external)

The audit log system is Geely’s internal system.

5.4.7 Notification to event-causing subject

No stipulation

5.4.8 Vulnerability assessments

The environment is continually scanned to detect known vulnerabilities and flaws, and the output of this process is fed into the patch management and development processes.

5.5 Records archival

5.5.1 Types of records archived

The following types of records are archived in this PKI:

- All logs generated in section 5.4 in accordance with requirements in that section
- Certificate application information and any supporting documentation
- CA certificates
- Signed certificates
- Certificate revocation information and the latest CRL
- Key ceremony reports
- Audit log review logs
- Audit reports according to chapter 8
- Configuration sets and changes to configuration, using some form of version control
- Policy documents including historical versions

5.5.2 Retention period for archive

The records archive will be retained until the CA ceases operation, at which point the archive will be handed over to Polestar’s InfoSec team.

5.5.3 Protection of archive

See 5.4.4. The protection level is the same for the archive as the audit log.

5.5.4 Archive backup procedures

Backups of OS are taken daily. Backups of CA software is taken daily. Databases are mirrored in real time, and backed up hourly (incremental) and daily (full)

5.5.5 Requirements for time-stamping of records

Geely’s services use reliable national NTP sources for time synchronization.

5.5.6 Archive collection system (internal or external)

All Geely systems are internal.

5.5.7 Procedures to obtain and verify archive information

The archive is only accessible to Geely's PKI team, and can be shown to Polestar's Information Security team on request.

5.6 Key changeover

Re-key requirements are specified in section 4.7. When a CA certificate is approaching its renewal period it will prepare by generating a new key pair in advance and request a new CA certificate from its superordinate CA.

A CA certificate will be renewed when it is approaching the end of its operational period as defined in 6.3.2. This ensures there will be no gaps in certificate issuance.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

Geely has an established process for incident management and security incident management. These processes are described in detail in separate documents, which are available on request to Polestar's Information Security team.

Geely will adhere to the notification requirements in the corresponding section of the CP and notify Polestar's Information Security team if there is any serious confirmed security incident or operational incident that threaten the deliveries to Polestar.

5.7.2 Computing resources, software, and/or data are corrupted

This is covered by Geely's incident response plan, and the PKI teams operational plan for disaster recovery.

5.7.3 Entity private key compromise procedures

In case of a confirmed breach of a CA private key Geely's PKI team will immediately notify Polestar's Information Security team to perform revocation of the affected CA's certificate.

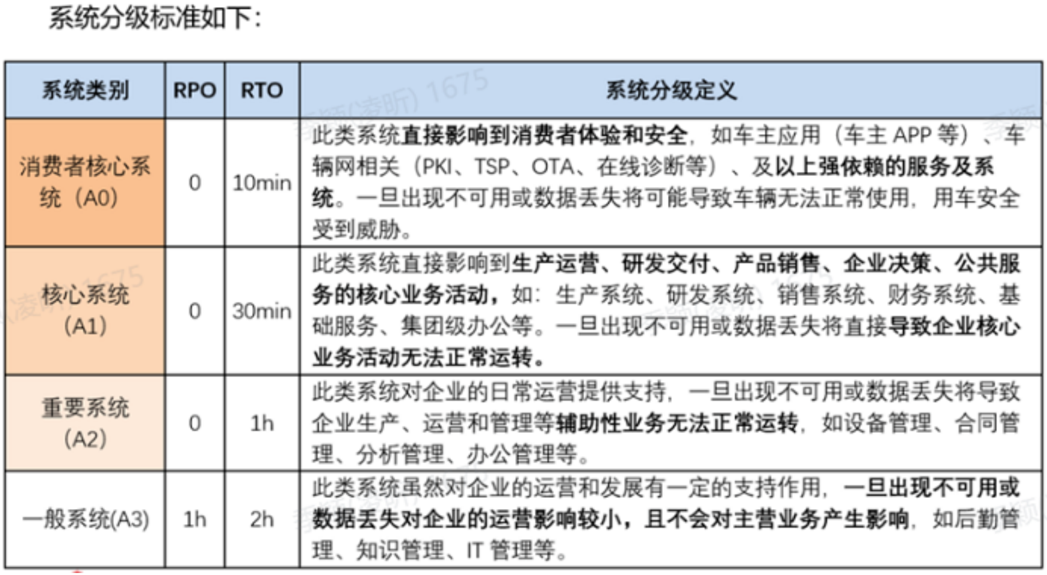
Work will start immediately to determine and fix the cause of the breach to enable Geely's PKI team to re-establish secure operations and create a new CA with a fresh key pair to replace the breached CA.

5.7.4 Business continuity capabilities after a disaster

Geely has a Business Continuity Plan that has been developed over several years. Each critical service is required to do recovery testing regularly to ensure the ability to recover from a large failure.

All critical systems are furthermore deployed in a redundant fashion to minimize the risk of outages.

System Category	RPO	RTO	Description
Cusumer related, key system.	0	10min	As a system which will affect cusumer use experience and safety, such as vehicle related APP, connected car related system(PKI,TSP,OTA,GNDS) and all above service and system. If the system is unavailable or data loss, vehicle related function or safety issue can happen.



系统分级标准如下：

系统类别	RPO	RTO	系统分级定义
消费者核心系统（A0）	0	10min	此类系统**直接影响到消费者体验和安全**，如车主应用（车主 APP 等）、车辆网相关（PKI、TSP、OTA、在线诊断等）、及**以上强依赖的服务及系统**。一旦出现不可用或数据丢失将可能导致车辆无法正常使用，用车安全受到威胁。
核心系统（A1）	0	30min	此类系统直接影响到**生产运营、研发交付、产品销售、企业决策、公共服务的核心业务活动，**如：生产系统、研发系统、销售系统、财务系统、基础服务、集团级办公等。一旦出现不可用或数据丢失将直接**导致企业核心业务活动无法正常运转。**
重要系统（A2）	0	1h	此类系统对企业的日常运营提供支持，一旦出现不可用或数据丢失将导致企业生产、运营和管理等**辅助性业务无法正常运转**，如设备管理、合同管理、分析管理、办公管理等。
一般系统(A3)	1h	2h	此类系统虽然对企业的运营和发展有一定的支持作用，**一旦出现不可用或数据丢失对企业的运营影响较小，且不会对主营业务产生影响**，如后勤管理、知识管理、IT 管理等。

5.8 CA or RA termination

Geely will coordinate with Polestar regarding termination of any CA or RA. Whenever possible, it shall be planned to coincide with the expiry of the CA's certificate. When a decision is made, Geely will communicate to Polestar and inform of the last date of operation and whether the CA will be replaced.

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

Key pair generation is performed by a documented ceremony, with multiple persons present to fulfill the requirements in section 5.2 regarding role separation and number of persons per task. This procedure is designed to be secure and guarantee that no collusion can take place.

6.1.2 Private key delivery to subscriber

Key pairs for subscribers in this PKI SHALL NOT be generated by the CA. There is no need for a CA to distribute private keys, and it is not permitted in this PKI.

6.1.3 Public key delivery to certificate issuer

Public keys are generated by the subscriber and submitted to the CA by using PKCS#10 encoded Certificate Signing Requests. The submission will happen online via Geely's factory systems and workshop tooling systems.

6.1.4 CA public key delivery to relying parties

Any relying party that will depend on the CA's public key must download it from Polestar's online PKI repository defined in the CP, section 2.1. Geely will not provide any other source relying parties to retrieve the CA public keys.

6.1.5 Key sizes

Certificates applications in this CA MUST use public keys compliant with [ISO15118]. Certificate applications with key types or sizes not explicitly allowed by [ISO15118] MUST be rejected.

6.1.6 Public key parameters generation and quality checking

This CA will only accept public keys in certificate applications that conform to requirements in the certificate profiles in section 7.1. If a request uses a different public key type the application will be rejected.

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

Key usage is defined in section 4.5 and this corresponds to the KeyUsage attribute in the certificate profiles in section 7.1. No other key usage is permitted.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

Geely's PKI service is based on HSM devices certified to the following standard (for CA keys):

SecHSM is a multi chip independent hardware encryption module that can provide data encryption , data decryption, signature generation, signature verification, message digest, message authentication code (IaC), random number generation, and key management functions.

SecHSM has passed FIPS 140-2 level 3 certification (certificate number # 3350) and can be found on the NIST official website.

Key storage for end entity devices are based on Secure Hardware Extension in the EVCC controller. The key pairs generated are stored within the secured hardware and cannot be exported.

6.2.2 Private key (n out of m) multi-person control

Geely's CA enforces multi-person control for creating new keys on an HSM, and copying, backing up, or restoring private keys to or from an HSM.

6.2.3 Private key escrow

Key escrow SHALL NOT be used by this CA.

6.2.4 Private key backup

CA private keys will be backed up when key material is changed inside a HSM. The backup will be done to a special purpose hardware device intended by the manufacturer to hold HSM backup data. The device will not contain any data other than HSM backups and is not a general purpose storage or backup solution.

All data will be encrypted when backed up.

6.2.5 Private key archival

Private key archival SHALL NOT be used by this CA.

6.2.6 Private key transfer into or from a cryptographic module

Private keys will only be transferred for the purposes of backing up or restoring the key. These procedures will only be performed between a HSM and the nominated backup device, and only using strong encryption for the transfer.

6.2.7 Private key storage on cryptographic module

No stipulation beyond section 6.2.1.

6.2.8 Method of activating private key

The HSM must be activated before any key material it stores can be used. Activation is based on an activation password (used between the OS and CA software and the HSM) and must be performed by a Security Officer, authenticated with strong authentication.

6.2.9 Method of deactivating private key

The deactivation of a private key when it will not be needed is done by executing the relevant commands while logged in to the HSM as a HSM operator, or by shutting down the HSM.

6.2.10 Method of destroying private key

When a key is no longer in use it shall be destroyed by deleting it from HSM storage, and any backup HSMs.

6.2.11 Cryptographic Module Rating

See section 6.2.1

6.3 Other aspects of key pair management

6.3.1 Public key archival

Public keys shall be archived according to section 5.5.

6.3.2 Certificate operational periods and key pair usage periods

This CA will strictly adhere to the time periods defined in the CP. This CA will only issue OEM provisioning certs and OCSP responder certs.

Certificate type	Validity period	Key usage period
Issuing CA	25 years	1 years
OEM provisioning	20 years	No longer than the validity period
OCSP responder	13 months	No longer than the validity period

6.4 Activation data

6.4.1 Activation data generation and installation

Activation for HSMs are allocated to partitions and not keys. Each partition has its own partition challenge that must be supplied by the software interacting with it. This password will be created as a 32 character random string.

6.4.2 Activation data protection

Passwords (shared and personal) are stored in a password management solution in Geely's secure environment and protected by strong encryption and access management processes to ensure their confidentiality. Shared passwords are rotated when team members leave.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The requirements from Polestar's CP have been implemented in their entirety, including but not limited to:

- Secure identity lifecycle controls
  - Ensure identities are personal, valid, and current
  - Ensure identities are deleted/deactivated when no longer needed
- Strong authentication controls
  - Strong passwords
  - Rotation of knowledge-based secrets
  - Multifactor authentication where technically possible
- Role-based access controls
  - Segregation of concerns
  - Least privilege
- System hardening
  - Implement a local security baseline based on an established hardening framework (such as STIG or CIS benchmarks) to strengthen security of a running operating system
- Network security controls
  - Reducing attack surface on network connections by closing unnecessary ports/services
- Auditing and logging
  - Changes to security parameters or runtime parameters
  - Access attempts, successful and failed, must be logged
- Backup
  - Systems must use backups to enable recovery of the service including all data after a failure

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls

All Geely's systems are placed under an SDLC process to ensure proper documentation, dependency management, version control, etc.

6.6.2 Security management controls

Geely's security program is based on an ISO27000 risk based methodology to ensure that security risks are identified, prioritized, and fixed or mitigated in a timely manner.

6.6.3 Life cycle security controls

HSM hardware for the service has a planned lifespan of 5 years before being replaced. Hardware taken out of service is physically destroyed by HSM staff before being sent for material recycling. Hardware is never sent off site for repairs. If it can be repaired by HSM staff on site it will be, otherwise it will be destroyed and replaced with a new device.

Software is managed to ensure it is up-to-date and has the latest security fixes installed. A patch release process is used to minimize risk of unintended impact to runtime services.

6.7 Network security controls

Geely's CA systems are run in a logically separated environment with several layers of firewalls and intrusion protection services in between the CA systems and any high-risk environments or endpoints. No traffic is allowed by default to reach the CA systems, and all network ports are closed by default.

All connectivity to and from CA systems use encrypted transport only.

6.8 Time-stamping

Geely's PKI services rely on trustworthy national time sources using NTP for time synchronization.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profiles

Symbols in the tables are interpreted as follows:

x	Required
(x)	Optional
-	MUST NOT be present
nc	Extension MUST be marked as non-critical
c	Extension MUST be marked as critical
<text>	Variable data, as specified in section 3.1 and in the Attribute Processing section (7.1.1) below
String starting with ”id-”	OID name

N.N.N.N	OID value, string of numbers separated by dots.
”text”	Literal value. Certificate SHALL contain exactly this string, excluding quotation marks.

7.1.1 Attribute processing

Variable name	Description
<Signing CA name>	Used for OCSP responders. Replace with the Subject name of the CA for whom this responder signs OCSP responses and signs the responder’s certificate.
<Issuer CRL file>	File name of the signing CAs CRL file. Used in the CRL Distribution Point attribute.

7.1.2 Version number(s)

All certificates shall be based on X509 version 3 (indicated by numeric value “2” in the version attribute encoded in certificates) and contain data as defined throughout section 7.1.

7.1.3 Guidance

1. [ISO15118-2] erroneously states that signatureValue in certificates shall be encoded as OCTET STRING. It SHALL be encoded as BIT STRING.
2. Root certificates SHALL NOT include revocation attributes (CRLDistributionPoints or AIA (OCSP))
3. Non-root CA certificates SHALL contain at least one of CRLDistributionPoints or AIA (OCSP) URLs for revocation checking. Both are marked as optional in the profiles below, but at least one is mandatory.
4. SerialNumber SHALL be non-sequentially generated and include at least 64 bits of random data.

7.1.3.1 OEM provisioning certificate profiles (ISO15118-2)

		Name	OEM Root CA	OEM Policy CA	OEM Issuing CA
		Role	Root	Intermediate	Issuing
Certificate		signatureAlgorithm	id-ecdsa-with-SHA256	id-ecdsa-with-SHA256	id-ecdsa-with-SHA256
		signatureValue	bit string	bit string	bit string
tbsCertificate		Version	2	2	2
		SerialNumber	Integer, 20 octets	Integer, 20 octets	Integer, 20 octets
		Signature	id-ecdsa-with-SHA256	id-ecdsa-with-SHA256	id-ecdsa-with-SHA256
	Issuer	Country	SE	SE	SE
		Organization	Polestar Performance AB	Polestar Performance AB	Polestar Performance AB
		Common Name	Polestar <t> Root CA <g>	Polestar <t> Root CA <g>	Polestar <t> OEM Policy CA <n> <g>
	Validity		40 years	30 years	25 years
	Subject	Country	SE	SE	SE
		Organization	Polestar Performance AB	Polestar Performance AB	Polestar Performance AB
		Common Name	Polestar <t> Root CA <g>	Polestar <t> OEM Policy CA <n> <g>	Polestar <t> OEM Issuing CA <n> <g>
		Domain Component	-	-	-
	SubjectPublic KeyInfo	Public key	x	x	x
		Cryptographic algorithm	id-ecPublicKey	id-ecPublicKey	id-ecPublicKey
		Parameters	ECParameters	ECParameters	ECParameters
		namedCurve	secp256r1	secp256r1	secp256r1
	Extensions	AuthorityKeyIdentifier	x	x	x
		SubjectKeyIdentifier	x	x	x
		KeyUsage	x / c	x / c	x / c
		digitalSignature	0	0	0
		nonRepudiation	0	0	0
		keyEncipherment	0	0	0
		dataEncipherment	0	0	0
		keyAgreement	0	0	0
		keyCertSign	1	1	1
		cRLSign	1	1	1
		encipherOnly	0	0	0
		decipherOnly	0	0	0
		ExtendedKeyUsage	-	-	-
		id-kp-clientAuth	-	-	-
		id-kp-serverAuth	-	-	-
		CertificatePolicies	-	-	-
		BasicConstraints	x / c	x / c	x / c
		isCA	1	1	1
		PathLength	-	1	0
		cRLDistributionPoints	-	(x)/nc http://pki-cdp.polestar.com/<Issuer CRL file>	(x)/nc http://pki-cdp.polestar.com/<Issuer CRL file>
		AIA (OCSP)	-	(x)/nc http://pki-ocsp1.polestar.com/	http://pki-ocsp1.polestar.com/

		Name	OEM Provisoning cert
		Role	Leaf
Certificate		signatureAlgorithm	id-ecdsa-with-SHA256
		signatureValue	bit string
tbsCertificate		Version	2
		SerialNumber	Integer, 20 octets
		Signature	id-ecdsa-with-SHA256
	Issuer	Country	SE
		Organization	Polestar Performance AB
		Common Name	Polestar <t> OEM Issuing CA <n> <g>
	Validity		20 years
	Subject	Country	-
		Organization	Polestar Performance AB
		Common Name	<PCID>
		Domain Component	”OEM”
	SubjectPublic KeyInfo	Public key	x
		Cryptographic algorithm	id-ecPublicKey
		Parameters	ECParameters
		namedCurve	secp256r1
	Extensions	AuthorityKeyIdentifier	x
		SubjectKeyIdentifier	x
		KeyUsage	x / c
		digitalSignature	1
		nonRepudiation	0
		keyEncipherment	0
		dataEncipherment	0
		keyAgreement	1
		keyCertSign	0
		cRLSign	0
		encipherOnly	0
		decipherOnly	0
		ExtendedKeyUsage	-
		id-kp-clientAuth	-
		id-kp-serverAuth	-
		id-kp-oCSPSigning	-
		Id-pkix-oCSP-nocheck	-
		CertificatePolicies	-
		BasicConstraints	x / c
		isCA	0
		PathLength	-
		cRLDistributionPoints	-
		AIA (OCSP)	http://pki-ocsp4.polestar.com/

7.1.3.2 Mobility Operator certificate profiles (ISO15118-2)

		Name	MO Root CA	Mo Policy CA	Mo Issuing CA
		Role	Root	Intermediate	Issuing
Certificate		signatureAlgorithm	id-ecdsa-with-SHA256	id-ecdsa-with-SHA256	id-ecdsa-with-SHA256
		signatureValue	bit string	bit string	bit string
tbsCertificate		Version	2	2	2
		SerialNumber	Integer, 20 octets	Integer, 20 octets	Integer, 20 octets
		Signature	id-ecdsa-with-SHA256	id-ecdsa-with-SHA256	id-ecdsa-with-SHA256
	Issuer	Country	SE	SE	SE
		Organization	Polestar Performance AB	Polestar Performance AB	Polestar Performance AB
		Common Name	Polestar <t> Root CA <g>	Polestar <t> Root CA <g>	Polestar <t> MO Policy CA <n> <g>
	Validity		40 years	20 years	10 years
	Subject	Country	SE	SE	SE
		Organization	Polestar Performance AB	Polestar Performance AB	Polestar Performance AB
		Common Name	Polestar <t> Root CA <g>	Polestar <t> MO Policy CA <n> <g>	Polestar <t> MO Issuing CA <n> <g>
		Domain Component	-	-	-
	SubjectPublic KeyInfo	Public key	x	x	x
		Cryptographic algorithm	id-ecPublicKey	id-ecPublicKey	id-ecPublicKey
		Parameters	ECParameters	ECParameters	ECParameters
		namedCurve	secp256r1	secp256r1	secp256r1
	Extensions	AuthorityKeyIdentifier	x	x	x
		SubjectKeyIdentifier	x	x	x
		KeyUsage	x / c	x / c	x / c
		digitalSignature	0	0	1
		nonRepudiation	0	0	1
		keyEncipherment	0	0	0
		dataEncipherment	0	0	0
		keyAgreement	0	0	0
		keyCertSign	1	1	1
		cRLSign	1	1	1
		encipherOnly	0	0	0
		decipherOnly	0	0	0
		ExtendedKeyUsage	-	-	-
		id-kp-clientAuth	-	-	-
		id-kp-serverAuth	-	-	-
		CertificatePolicies	-	-	-
		BasicConstraints	x / c	x / c	x / c
		isCA	1	1	1
		PathLength	-	1	0
		cRLDistributionPoints	-	(x)/nc http://pki-cdp.polestar.com/<Issuer CRL file>	(x)/nc http://pki-cdp.polestar.com/<Issuer CRL file>
		AIA (OCSP)	-	(x)/nc http://pki-ocsp1.polestar.com/	http://pki-ocsp1.polestar.com/

		Name	Contract cert
		Role	Leaf
Certificate		signatureAlgorithm	id-ecdsa-with-SHA256
		signatureValue	bit string
		tbsCertificate	
tbsCertificate		Version	2
		SerialNumber	Integer, 20 octets
		Signature	id-ecdsa-with-SHA256
	Issuer	Country	SE
		Organization	Polestar Performance AB
		Common Name	Polestar <t> MO Issuing CA <n> <g>
	Validity		Up to 2 years
	Subject	Country	-
		Organization	Polestar Performance AB
		Common Name	<EMAID>
		Domain Component	-
	SubjectPublic KeyInfo	Public key	x
		Cryptographic algorithm	id-ecPublicKey
		Parameters	ECParameters
		namedCurve	secp256r1
	Extensions	AuthorityKeyIdentifier	x
		SubjectKeyIdentifier	x
		KeyUsage	x / c
		digitalSignature	1
		nonRepudiation	1
		keyEncipherment	1
		dataEncipherment	0
		keyAgreement	1
		keyCertSign	0
		cRLSign	0
		encipherOnly	0
		decipherOnly	0
		ExtendedKeyUsage	-
		id-kp-clientAuth	-
		id-kp-serverAuth	-
		id-kp-oCSPSigning	-
		CertificatePolicies	-
		BasicConstraints	x / c
		isCA	0
		PathLength	-
		cRLDistributionPoints	(x)/nc http://pki-cdp3.polestar.com/<Issuer CRL file>
		AIA (OCSP)	http://pki-ocsp3.polestar.com/

7.1.4 Certificate extensions

All approved extensions, and their values, are specified in the profile tables above. No other extensions are permitted in this PKI.

7.1.5 Algorithm object identifiers

All identifiers for algorithms MUST be used in accordance with [ISO15118]. See the identifiers in the tables above.

7.1.6 Name forms

See section 3.1.

7.1.7 Name constraints

Name contraints are not supported in this PKI.

7.1.8 Certificate policy object identifier

CP identifiers will not be encoded into certificates. The relevant extensions are not permitted in this PKI.

7.1.9 Usage of Policy Constraints extension

Policy constraints are not supported in this PKI.

7.1.10 Policy qualifiers syntax and semantics

No stipulations.

7.1.11 Processing semantics for the critical Certificate Policies extension

The Certificate Policies extension is not permitted in this PKI.

7.2 CRL profile

7.2.1 Version number(s)

The CRLs SHALL be based on X.509 version 2 (encoded as numeric value 1 in CRL files) in [RFC5280].

7.2.2 CRL and CRL entry extensions

The following extensions SHALL be encoded into CRL files:

- Authority Key Identifier
- CRL Number

7.3 OCSP profile

7.3.1 OCSP profile (ISO15118-2)

		Name	OCSP Responder
		Role	OCSP signer cert
Certificate		signatureAlgorithm	id-ecdsa-with-SHA256
		signatureValue	bit string
tbsCertificate		Version	2
		SerialNumber	Integer, 20 octets
		Signature	id-ecdsa-with-SHA256
	Issuer	Country	SE
		Organization	Polestar Performance AB
		Common Name	<Signing CA name>
	Validity		Up to 13 months
	Subject	Country	SE
		Organization	Polestar Performance AB
		Common Name	Polestar OCSP responder
		Domain Component	-
	SubjectPublic KeyInfo	Public key	x
		Cryptographic algorithm	id-ecPublicKey
		Parameters	ECParameters
		namedCurve	secp256r1
	Extensions	AuthorityKeyIdentifier	x
		SubjectKeyIdentifier	x
		KeyUsage	x / c
		digitalSignature	1
		nonRepudiation	0
		keyEncipherment	0
		dataEncipherment	0
		keyAgreement	0
		keyCertSign	0
		cRLSign	0
		encipherOnly	0
		decipherOnly	0
		ExtendedKeyUsage	x / nc
		id-kp-clientAuth	-
		id-kp-serverAuth	-
		id-kp-oCSPSigning	x
		Id-pkix-oCSP-nocheck	x
		CertificatePolicies	-
		BasicConstraints	x / c
		isCA	0

		PathLength	-
		cRLDistributionPoints	-
		AIA (OCSP)	-

7.3.2 Version number(s)

The OCSP responder MUST support at least version 1 of the OCSP specification [RFC2560].

7.3.3 OCSP extensions

No stipulations.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

Geely will adhere to the assessment schedule in Polestar's CP.

8.2 Identity/qualifications of assessor

The audit SHALL be performed by Polestar, or an auditor appointed by Polestar. Appointment SHALL be the sole discretion of Polestar.

8.3 Assessor's relationship to assessed entity

No stipulation. Polestar will nominate the assessor.

8.4 Topics covered by assessment

All statements in this CPS shall be covered by the assessment. The assessment SHALL verify:

- That issued certificates and the certificate application processes comply with the requirements in this CPS and the CP. These requirements are described in chapters 3, 4, and 7.
- The CAs procedural, physical, and technical security controls are effective and comply with the documentation in this CPS. These requirements are described in the CP, chapters 4, 5, and 6.

8.4.1 Root and Policy CAs

The assessment SHALL contain a full review of all signature operations and all access to the CA hardware and software.

8.4.2 Issuing CAs

For an issuing CA the volume of certificates will be too large to validate each certificate manually. Similarly, technical logs, access logs and the like will also be too large for manual inspection. The PKI operator is expected to perform monitoring via automated tools that can generate reports regarding policy compliance.

The compliance assessment SHALL be based on small random samples of data (certificates and logs), and the output of automated tools. If a CA issues multiple types of certificates, e.g certificates based on different profiles (see chapter 7), the sampling SHALL include certificates from all issued certificate types.

8.5 Actions taken as a result of deficiency

The assessor SHALL describe any deficiencies found in an audit report shared with Polestar. The PKI operator SHALL inform Polestar and take actions to mitigate or solve any flaws, weaknesses, or risks found during assessments without undue delay. The result of the mitigations and corrections SHALL be documented and submitted to Polestar.

8.6 Communication of results

The assessors report SHALL be communicated to Polestar within 14 days of completion of the assessment.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

Polestar will not collect any fees from any of the participants in this PKI, for the services provided as part of this PKI described in this CP. Polestar MAY collect fees from other services, such as consulting services, that are outside the scope of this CP.

9.2 Financial responsibility

9.2.1 Insurance coverage

CAs in this PKI SHALL have a reasonable level of insurance to cover liabilities caused by their own services and/or operations.

9.2.2 Other assets

CAs SHALL be sufficiently financed to maintain operations and processes to the degree required by this CP.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

The following types of information SHALL be kept confidential. This is the minimum required set of information that shall be kept confidential, and participating CA MAY opt to keep additional information types private (except for information covered by section 9.3.2.

- CA private keys
- Passwords, PINs, access tokens, and similar data
- User names
- Audit logs
- Certificate application records

9.3.2 Information not within the scope of confidential information

The following information SHALL NOT be kept confidential by any participant in this PKI.

- CA certificates
- CRL files
- OCSP signer certificates
- This Certificate Policy

9.3.3 Responsibility to protect confidential information

Each participating CA is responsible for ensuring the confidentiality of the information they produce.

9.4 Privacy of personal information

Each CA in this PKI MUST consider laws, regulations, and contractual obligations in the markets where they operate and where their subscribers reside to ensure that they are in compliance. Privacy by design SHALL be a foundational design principle for all CAs in this PKI.

This PKI SHALL NOT sign certificates for persons, or include personally identifiable information in a signed certificate. This minimizes the risk for exposure of private information.

9.4.1 Privacy plan

No stipulation.

9.4.2 Information treated as private

No stipulation.

9.4.3 Information not deemed private

No stipulation.

9.4.4 Responsibility to protect private information

No stipulation.

9.4.5 Notice and consent to use private information

No stipulation.

9.4.6 Disclosure pursuant to judicial or administrative process

No stipulation.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

No stipulation.

9.6 Representations and warranties

No stipulation.

9.7 Disclaimers of warranties

No stipulation.

9.8 Limitations of liability

No stipulation.

9.9 Indemnities

No stipulation.

9.10 Term and termination

9.10.1 Term

This CP becomes effective on the date it is published, and remains effective until a new version is published.

9.10.2 Termination

This CP becomes effective on the date it is published, and remains effective until a new version is published.

9.10.3 Effect of termination and survival

Participants in this PKI are bound to the terms of this CP for as long as certificates are within their validity period.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

This CP SHALL NOT use amendments. If any update is needed it SHALL be made in the form of a new version of this CP.

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

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

No stipulation.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other provisions

No stipulation.