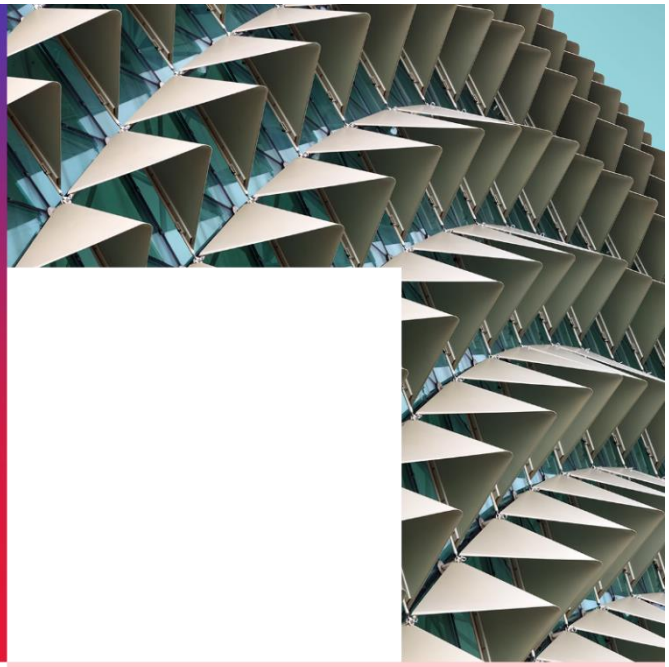


Certificate Practice Statement for Polestar

CGI Certificate Service

Version: 1.1

2024-03-13

Client classified

Table of Contents

1 INTRODUCTION

1.1 Overview

CGI Certificate Service provides Polestar a service for managing certificates within their environment through their own Certificate Authorities. The certificates may be used for authentication, encryption and signing. This document ONLY covers CGI Certificate Service Responsibility from a total picture of the Certificate issuing Process.

The trust that one can have in a digital certificate depends on the rules that are followed to generate and to manage this certificate. Those rules are formalized in policy documents: The Certificate Policy (owned by Polestar) and the Certification Practice Statement (this document).

The ITU-T X.509 standard defines a Certificate Policy (CP) as “a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements”. The term Certification Practice Statement (CPS) is defined by the American Bar Association Guidelines as: "A statement of the practices which a certification authority employs in issuing certificates."

A certificate policy states the generation, management, applicability and user community of particular types of certificates for specific applications while a Certification Practice Statement states the generation and management of certificates by a particular Certification Authority (that can deliver certificates compliant with different certificate policies). The Certificate Policy is a less specific document than the certification practice statement. This certification practice statement gives a more detailed description of the practices of a certification authority when issuing and managing Certificates. This certification practice statement defines how a specific certification authority meets the technical, organizational and procedural requirements identified in a Certificate Policy. In case of a conflict between the information in the Certificate Policy, CPS and other PKI documentation, the Certificate Policy shall always take precedence.

Certificates can be used for one (or several) of the following purposes:

- Authentication – the process of determining whether someone or something is, in fact, who or what it declares itself to be.
- Encryption – the conversion of data into a format that cannot be easily understood by unauthorized people or systems.
- Digital signature – the binding between a collection of information and the signer that guarantees that the information has not been tampered with and that the signer is not able to repudiate the act.

1.2 Document name and identification

This document is CGI’s Certificate Practice Statement for Polestar root.

- Name: Certificate Practice Statement for Polestar V2G PKI
- Version: 1.0
- OID: 1.3.6.1.4.1.59600.2.509.0.1.1.1

The OID arc 1.3.6.1.4.1.59600 is Polestar’s IANA assigned Private Enterprise Number[1].

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

1.3 PKI participants

1.3.1 PKI structure

The root CA certifies policy CAs, and policy CAs certify issuing CAs. An issuing CA SHALL only sign end-entity certificates.

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	

The scope of responsibility for this CPS is Root and Policy. Not Issuing CA. Issuing CAs are responsibility of other Polestar appointed parties and we sign their issuing CA with our Policy CA.

1.3.2 Certification authorities

To support plug and charge ISO15118-2 the CAs below exist. This CPS cover all CAs listed.

Type	Validity Period	Key usage period	Responsible for
Polestar ECC-256 Root CA v1	40 years	20	Sign policy CAs
Polestar ECC-256 V2G OEM Policy CA v1	30 years	5	Sign OEM issuing CA

1.3.3 Registration authorities

Submission of CSRs are done manually after agreement in meeting between CGI and subscriber.

1.3.4 Subscribers

Polestar is the only subscriber.

1.3.5 Relying parties

No stipulation.

1.3.6 Other participants

No stipulation.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

These CAs SHALL only be used in the plug and charge ecosystem and what is specified in ISO15118.

1.4.2 Prohibited certificate uses

These CAs SHALL NOT be used outside of plug and charge ecosystem and what is specified in ISO15118.

1.5 Policy administration

1.5.1 Organization administering the document

This CPS and any related documents is maintained by the CGI Certificate Service.

1.5.2 Contact person

Service Delivery Manager CGI certificate service.

Gunnar Klintberg

CGI Sverige AB

Englundavägen 7

171 41 Stockholm

se.certificateservice-managers@cgi.com

1.5.3 Person determining CPS suitability for the policy

Polestar InfoSec team determine the suitability of this CPS according to the procedure specified in 1.5.4 in the CP.

1.5.4 CPS approval procedures

Polestar CISO team determine the suitability of this CPS according to the procedure specified in 1.5.4 in the CP.

1.6 Definitions and acronyms

No stipulation.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

CGI certificate service provide a CA repository for certificate status (OCSP). It is located as follows:

Name	OCSP URL
Polestar ECC-256 Root CA v1	http://pki-ocsp1.polestar.com
Polestar ECC-256 V2G OEM Policy CA v1	http://pki-ocsp1.polestar.com

2.2 Publication of certification information

For the Root CA and Policy CA the following information is published:

- Certificate Revocation List for all revoked CA certificates are sent to Polestar to be stored at their repository.

2.3 Time or frequency of publication

This CPS and any subsequent changes are made publicly available within one week of approval according to 1.5.4.

The Root CA and Policy CAs CRLs and OCSP are updated every six months.

2.4 Access controls on repositories

Only Certificate Service administrators have modify access and they use two factor authentication.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

Naming of the CA's are according to CP chapter 3 and 7.

3.1.2 Need for names to be meaningful

Certificate names must follow the X.509 conventions for specifying a meaningful name.

3.1.3 Anonymity or pseudonymity of subscribers

Anonymity and pseudonymity SHALL NOT be permitted.

3.1.4 Rules for interpreting various name forms

No stipulation.

3.1.5 Uniqueness of names

All entities in this PKI must have unique names.

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

The method to prove possession of a private key shall be PKCS#10 as described in RFC2986.

3.2.2 Authentication of organization identity

When issuing certificates used for identifying an organization the CA have a list of authorized persons from the subscriber organization that can request an organization certificate.

3.2.3 Authentication of individual identity

No stipulation. With this CPS we do not issue certificates for end-entities

3.2.4 Non-verified subscriber information

No stipulation.

3.2.5 Validation of authority

No stipulation.

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

No stipulation.

3.3.2 Identification and authentication for re-key after revocation

No stipulation.

3.4 Identification and authentication for revocation request

The CA will have a list of authorized persons from the subscriber organization that can request a revocation.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

In this CPS the term “certificate application” refers to the process of registration of a Sub CA.

Only authorized persons from the subscriber organization are authorized to submit a request for a Sub CA.

4.1.2 Enrollment process and responsibilities

A manual request is sent to the CA with all needed information. The CA will also verify back with a list of authorized personnel at the customer organisation.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Polestar shall ensure that the request is valid and that the CSR is accurate. CGI shall validate that the request is from a trusted source as per the agreement between Polestar and CGI.

4.2.2 Approval or rejection of certificate applications

CGI is responsible to validate the application and approve if it's aligned to the rules of this CPS and it comes from a trusted source at Polestar. CGI will reject all applications that not followed by the rules of this CPS. CGI will also reject the application if it comes from a non-trusted source.

4.2.3 Time to process certificate applications

GGI will process the application in reasonable time.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Certificate services verifies the PKCS#10 Certificate Signing Request package.

Certificate services publishes the issued certificate to the repositories using a manual process.

4.3.2 Notification to subscriber by the CA of issuance of certificate

Certificate services notifies subscribers that they have created such certificates, and provide subscribers via e-mail with the certificate and an out of band message of the certificates fingerprint.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

No stipulation.

4.4.2 Publication of the certificate by the CA

OCSP responder will respond with a "good" status to all certificate queries as long as the certificate is valid and not revoked.

4.4.3 Notification of certificate issuance by the CA to other entities

Other entities will not be notified.

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

4.5.2 Relying party public key and certificate usage

No stipulation.

4.6 Certificate renewal

Certificate renewal is not used, 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.

4.8 Certificate modification

Not applicable since Certificate modification is not allowed.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

See same chapter in Certificate Policy.

4.9.2 Who can request revocation

See same chapter in Certificate Policy.

4.9.3 Procedure for revocation request

CGI Certificate Service personnel performs a call back to another authorized requester to verify the legitimacy of the request.

4.9.4 Revocation request grace period

The process to revoke a certificate SHALL be started as soon as possible after the decision to revoke the certificate has been made.

4.9.5 Time within which CA must process the revocation request

CGI Certificate Service SHALL have started the processing of all revocation requests within two hours within the operational hours agreed for CGI Certificate Service.

4.9.6 Revocation checking requirement for relying parties

No stipulation.

4.9.7 CRL issuance frequency (if applicable)

A CA in this PKI SHALL regularly issue a new CRL, even if no changes have happened.

- CRL of root CA: Issued no later than every 7 months
- CRL of policy CA: Issued no later than every 7 months

4.9.8 Maximum latency for CRLs (if applicable)

A new CRL SHOULD be posted to the repository promptly after creation.

4.9.9 On-line revocation/status checking availability

Specified in SLA agreement with subscriber.

4.9.10 On-line revocation checking requirements

No stipulation.

4.9.11 Other forms of revocation advertisements available

There are no other forms of revocation available.

4.9.12 Special requirements re key compromise

No stipulation.

4.9.13 Circumstances for suspension

Certificate suspension is not supported.

4.10 Certificate status services

CGI Certificate Service makes certificate status information available via CRL and OCSP

4.11 End of subscription

Subscription is synonymous with the Certificate's validity period. The subscription ends when the Certificate is revoked or expires.

4.12 Key escrow and recovery

Key escrow is not supported.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

CGI Certificate Service has documented detailed physical control and security policies which the CAs adhere to. Compliance with these policies is included in the CGI Certificate Service independent audit requirements described in Section 8. These documents contain sensitive security information and are only available upon agreement with CGI. An overview of the requirements is described in the following sub-sections.

5.1.1 Site location and construction

CGI Certificate Service performs its CA operations in secure site. The secured site is operated under a security plan to ensure that no unauthorized logical or physical access is allowed. The safe in the secure site are physically separated from the organization's other systems so that only authorized employees of the CA can access them. The safes are alarmed and will alert an external alarm company in case of an intrusion attempt.

5.1.2 Physical access

CGI protects the offline root CA with physical security mechanisms to:

- Permit only authorized access to the hardware

- Store hardware in secure containers
- Monitor, either manually or electronically, for unauthorized intrusion at all times
- Require two person physical access controls to all sensitive computer systems and cryptographic equipment as Hardware Security Modules (HSMs).

5.1.3 Power and air conditioning

The secure site have industry standard power equipment and air conditioning equipment to ensure continuous operation and staff access.

5.1.4 Water exposures

CGI has taken commercially reasonable efforts to ensure that the secure site where the offline root CA´s is located is secure and protected from flood and water damage.

5.1.5 Fire prevention and protection

CGI has taken commercially reasonable efforts to ensure that the secure site where the offline root CA´s is located is secure and protected from fires and exposure to flames or smoke.

5.1.6 Media storage

CA media is stored in safes to protect it from accidental damage (such as water, fire, electromagnetic, etc.) and unauthorized access.

5.1.7 Waste disposal

Sensitive documents are shredded prior to disposal. Electronic Media is wiped clean by a trusted source upon the expiration of the data. All media is rendered unreadable prior to its disposal and, where possible, is physically destroyed.

5.1.8 Off-site backup

Backups is made in line with any change of the offline root CA to an off-site location.

5.2 Procedural controls

Employees, contractors, and consultants that manage the CGI infrastructure are classified as a "Trusted Person" after they been approved by the Service manager of CGI Certificate Service.

The Service manager verifies:

- that Human Resources and the persons staff manager have performed the background verification,
- that the person has the correct education for the trusted role.

All signed authorizations by the Service manager should be archived.

5.2.1 Trusted roles

Employees, contractors, and consultants that are designated to handle the CA shall be considered to be “Trusted Persons”. Persons seeking to become Trusted Persons by obtaining a Trusted Position shall meet the screening requirements of this CPS.

Trusted Persons include all employees, contractors, and consultants that have access to or control authentication or cryptographic operations that may materially affect:

- the validation of information in Certificate Applications;

- the acceptance, rejection, or other processing of certificate applications, revocation requests, or renewal requests;
- the issuance, or revocation of certificates, including personnel having access to restricted portions of its repository or the handling of subscriber information or requests.
- Backups and restores

The Hardware Security Modules are administrated by the following roles:

- HSM Admin (Blue PED Key)
    - Owned by Service Delivery manager, Security Officer or Service Manager
- Domain Admin (RED PED Key)
    - Owned by Service Delivery manager, Security Officer or Service Manager
- User (Black PED Key)
    - Owned by Service operator
- Remote PED Key
    - Used by Service operator.

The Service has defined the following roles and responsibilities:

a) Access Administrator: The Access Administrator is responsible for adding and removing access rights.
b) Service Auditor: The Auditor is responsible for the day to day review of the service.
c) Business Developer: The Business developer is responsible for managing sale leads from new customers with complex needs and provide input to the Service Road Map from potential customers.
d) Developer: The Developer is responsible for the development of new features and correcting bugs. Documentation of software, install and configuration instructions. Maintenance of the software and documentation. Creating releases.
e) Security Officer: The Security Officer is responsible for verifying that the service complies with the security polices which the service shall follow. Initiating and making sure there is a completed annual audit of CGI Certificate Services. Initiating and making sure there is an annual review of access for all personnel, including background check of personnel. Grant or deny personnel to act as different roles in the service.
f) Service Delivery Manager: The Delivery Manager is responsible for the day to day running of the service. To coordinate the operators and make sure the service is delivered according to agreed SLAs. Schedule changes and coordinate incidents. Continuous improvement of the delivery of the service. Life-cycle management of hardware and software.
g) Service Manager: The Service manager is responsible for the long term management of the service. Presenting reports according to agreements. Receiving and clarifying customer requests. Making sure CGI Certificate Service personnel have tools and knowledge of how to time report. Plan and coordinate projects for customers and internal to the service. Maintain and create sales material such as service description and product sheets. That proper service documentation exists. Supplier agreements and approving purchases. Identify and manage risks related to the service. Making sure the service complies to decided standards. Budget and results. Service road map.
h) Service Operator: The Operator is responsible for the day to day management of the service. When not directly monitoring the service the Operator also work with customers or internal projects. The Operator is involved in changes to improve the service. The Operator is involved in continuous improvements with focus on defining requirements and verifying new releases. Service Operators are responsible for applying security patches and general keeping the system up to date.
i) Service Owner: The Service owner is responsible for the funding of the service. Ordering the service from the Service Manager

5.2.2 Number of persons required per task

CGI Certificate Service has established rigorous control procedures to ensure the separation of duties based on job responsibility and to ensure that multiple Trusted Persons are required to perform sensitive tasks. The procedures for separation of duties must be compliant to ETSI TS 102 042.

Policy and control procedures are in place to ensure separation of duties based on job responsibilities. The most sensitive tasks, such as access to and management of CA cryptographic hardware module (HSM) and associated key material must require multiple Trusted Persons.

These internal control procedures are designed to ensure that at a minimum of two trusted personnel are required to have either physical or logical access to the device. Access to all forms of CA cryptographic hardware (HSM's and HSM Backup units) is strictly enforced by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction.

Other manual operations such as:

- Activating the CA's,
- Signing a new Sub CA
- Performing changes in the infrastructure such as updating of operating systems and other software,

Preforming configuration changes must require the participation of at least 2 (two) Trusted Persons

5.2.3 Identification and authentication for each role

All logical access to the CA service by trusted personal is done via encrypted communication and authentication via two factor authentication.

5.2.4 Roles requiring separation of duties

Roles that requiring separation of duties is audit roles and root/administrative system management roles.

The following roles are separated:

- HSM operation requires separation of user roles and the other administrative roles to ensure that there are a minimum of two trusted persons working on the HSM.
- Access control requires a process where the approval of access is separated from the operation team.
- Auditing cannot be performed by someone from the operation team

5.3 Personnel controls

Every two years CGI staff acting in a Trusted Role need to, together with HR and management, renew the background control. The Service management shall also verify that the person in Trusted Roles shall constantly educate themselves in the PKI area and the service delivery processes.

5.3.1 Qualifications, experience, and clearance requirements

The CGI Certificate Service Manager verifies that personnel seeking to become Trusted Persons have:

- Passed the CGI HR background verification
- Is qualified for the role the person seeks.
- Has correct knowledge and education.

5.3.2 Background check procedures

CGI Certificate Service Manager conduct, with help of HR and Staff Managers, a background check for personnel seeking to become Trusted Persons in CGI Certificate Service.

Background checks are repeated for personnel holding Trusted Positions at least every two (2) years. The process is described in the background check policy document.

CGI Certificate Service manager let HR or Staff Managers verify the following:

- Misrepresentations made by the candidate or Trusted Person,
- Unfavourable or unreliable professional references,
- Certain criminal convictions, and
- Indications of a lack of financial responsibility.

Background investigation of persons seeking to become a Trusted Person includes:

- a confirmation of previous employment or assignments,
- a check of professional references,
- a confirmation of the highest or most relevant educational degree obtained,
- a search of criminal records.

5.3.3 Training requirements

CGI Certificate Service has an education program for CGI Staff applying for a Trusted Role in the service. The program makes sure that the personal before they are granted to act as a trusted person have knowledge in:

- Security principles and mechanisms of the CGI Certificate Service,
- Hardware and software versions in use,
- All duties the person is expected to perform,
- Incident and Compromise reporting and handling, and
- Disaster recovery and business continuity procedures.

5.3.4 Retraining frequency and requirements

The persons assigned to Trusted Roles are to continuously refresh their knowledge gained in the training using a training environment. The Service Manager annually makes sure that the trusted person has passed the CGI internal training including Incident handling and reporting.

5.3.5 Job rotation frequency and sequence

No stipulation

5.3.6 Sanctions for unauthorized actions

The Service manager should together with CGI staff manager and CGI HR discuss what sanction is needed for each case.
If sever unauthorised actions has been performed the privileges for the trusted person shall be withdrawn.

5.3.7 Independent contractor requirements

An Independent Contractor will be treated the same and answer to the same policys and regulation as a CGI trusted person.

5.3.8 Documentation supplied to personnel

CGI Certificate Service provide their personnel with the required training and access to other documentation needed to perform their job responsibilities competently and satisfactorily.

5.4 Audit logging procedures

CGI Certificate Service keeps audit logs and system log files.

All relevant events related to the security of the CA, certificate status systems, and RA are logged with date and time. Where possible, the security audit logs are automatically collected. Where this is not possible, a logbook, a paper form, or other physical mechanism is used. All security audit logs, both electronic and non-electronic, are retained and maintained in accordance with section 5.5.2, Retention period for archive.

5.4.1 Types of events recorded

All logs, whether electronic or manual, shall contain date and time of the event, and the identity of the entity that caused the event.

Every CA shall keep auditable logs including, but not limited to:

- Operational events
- Certificate lifecycle events
- Trusted employee events
- Discrepancy and compromise reports

The details of the auditor routines are stored in the auditor-service document located at CGI and can be viewed during audit of certificate services..

5.4.2 Frequency of processing log

The logs shall be inspected manually on each activation of the CA. Log processing and review SHALL entail verifying that the logs have not been tampered with and that the recorded events are expected and can be traced back to the normal CA activities.

5.4.3 Retention period for audit log

Audit logs are retained onsite for at least two (2) months after processing and thereafter archived in accordance with Section 5.5.2.

5.4.4 Protection of audit log

Logs are protected against improper alteration through the logical protection mechanism of the operating system and through the system itself not being physically or logically accessible other than by authorized personnel. The audit logs are signed with a specific log signing key. All log posts are individually time-stamped.

5.4.5 Audit log backup procedures

Backups of audit logs is stored in safes and also scanned and digitally signed copies at CGI approved document site

5.4.6 Audit collection system (internal vs. external)

No stipulation

5.4.7 Notification to event-causing subject

No stipulation

5.4.8 Vulnerability assessments

The CGI Certificate Service makes an in-depth vulnerability scanning once a year, and before major changes are set in production. CGI Certificate Service shall monitor vulnerability in the components used and have a documented patching process.

5.5 Records archival

5.5.1 Types of records archived

- HSM-backup
- Database backups
- Configuration set and all change/modification of them
- Log set (see that chapter 5.4.1)
- Audit reports
- Access decisions (add/remove/renew)
- Key ceremony protocols
- Signatures on archives and application to both create and verify archives.
- Policy Document

Types of Archiving records specified in the CP	Covered by CGI Certificate Service via Archived Records
Certificate Policies, CPSs	Policy Document
Compliance Audit Reports	Audit reports
System equipment configuration.	Configuration set and all change/modification of them
Modifications or updates to any of the above data items.	Configuration set and all change/modification of them
Certificate issuance, revocation, suspension, restoration, and key recovery requests.	Database backups, Log set (see that chapter 5.4.1)
Subscriber identity Authentication documentation, in accordance with section 3.2.3.	Database backups, Log set (see that chapter 5.4.1), Access decisions (add/remove/renew)
Documentation of receipt and acceptance of Certificates, in accordance with section 4.4	N/A
Documentation of receipt of Tokens, in accordance with section 3.2.1	Key ceremony protocols

All Certificates and CRLs (or other revocation information) as issued or published.	Database backups
Security audit data (in accordance with section 5.4)	Access decisions (add/remove/renew), Log set (see that chapter 5.4.1)
Other data or applications sufficient to verify archive contents	Signatures on archives and application to both create and verify archives.

5.5.2 Retention period for archive

- CGI Certificate Service are to the extend allowed by applicable laws and regulations, maintained the archive without any data loss according to the for a period of:
- At least ten years and six months.
- At least until the time of decommission of the CA plus one year.

CGI Certificate service will make sure that the archived can be accessible and readable during required retention period.

5.5.3 Protection of archive

CGI Certificate Service maintain an archive of records and protect the archive so that only the entity's authorized Trusted Persons are able to obtain access to the archive.
The archive is protected against unauthorized viewing, modification, deletion, or other tampering by storage within a trustworthy system. The media holding the archive data and the applications required to process the archive data are maintained to ensure that the archive data can be accessed for the time period set forth in this CPS.

5.5.4 Archive backup procedures

Entities compiling electronic information are backed up on an hourly basis. Backups are also stored at an off-site secure facility.

5.5.5 Requirements for time-stamping of records

All records in the CA database and log files are time-stamped.
All Server systems in the CGI Certificate service is synchronized with trusted time sources in the CGI Data centres.

Manual Access log files shall have at least date and time on all records.

5.5.6 Archive collection system (internal or external)

The archive collection systems are internal.

5.5.7 Procedures to obtain and verify archive information

Only authorized Trusted Personnel are able to obtain access to the archive. The integrity of the information is verified when it is restored.

5.6 Key changeover

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

CGI Certificate Service has a Business Continue Plan and a disaster recovery plan that covers the situation of corruption of system, software, data or suspicion of private key compromise.

If a CA Key is suspected to be compromised the procedures outlined in section 5.7.3 is followed.

If the OCSP responders key is suspected to be compromised, the CA should issue a new Certificate and the old certificate shall be revoked.

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

If a disaster occurs that prevents proper operation of a CA, the CA operations are suspended. An investigation starts to verify whether the private key has been compromised.

After ensuring the integrity of the CA systems, CGI Certificate Service re-initiate its operations and defected hardware are replaced. Software, data and keys are restored using Back-up copies.
The CA shall give priority to re-establishing the generation of certificate status information.

If the Private Keys are destroyed, the CA shall re-establish operations as quickly as possible, giving priority to generating certificates.

If compromise cannot be ruled out, the procedures of section 5.7.3 are applied.

5.7.3 Entity private key compromise procedures

If compromise of a private CA key is discovered, the CA involved stops its operation immediately. In particular, the interface for receiving automatically processed requests is disabled.
The CA certificate should be revoked and the revocation information should immediately be published in the repository specified in section 2.1. Information to subscriber and relaying parties should also be sent out.

5.7.4 Business continuity capabilities after a disaster

CGI Certificate Service has a Business Continue Plan and a Disaster Recovery Plan that has specified the Recovery Time Objectives in case of a natural, technical or man-made disaster. The BCP Is tested at least once every year.

5.8 CA or RA termination

If CGI Certificate Service is about to terminate its operation, CGI should inform the contact person stated in 1.5.2 about this as early as possible.

When the date of termination is known, the CA will not issue certificates that are valid after the termination date. A CA is not terminating operation during the lifetime of its certificate if not the contract between CGI and Polestar has ended.

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

CGI Trusted Services operational sites operate under a security plan designed to, within reason, detect, deter and prevent unauthorized logical or physical access to CA related facilities. This section outlines the technical security control mechanisms, service levels and personnel policy in use to provide trustworthy and reliable CA operations.

6.1.1 Key pair generation

All CA keys are generated during the key ceremony in FIPS 140-2 Level 3 validated cryptographic modules using multiple individuals acting in Trusted Roles.

When generating key material, the CA shall create auditable evidence to show that the CA enforced role separation and followed its key generation process.

All CA keys used for issuing certificates are generated on a hardware security module (HSM) evaluated as FIPS 140-2 Level 3-compliant HSMs. The HSM is also physically protected from unauthorized access.

Activation of the private CA keys is configured so authorization needs to be done by at least two persons with the appropriate role enforcing the 4-eyes-principle.
CGI has deployed significant environmental and physical protections of the CGI Trusted Services delivery locations, thus the CGI Trusted Services has not deployed FIPS 140-2 Level 4 HSM that mainly is for deployments that is unprotected from environmental effects and has low or none physical protections.

6.1.2 Private key delivery to subscriber

No stipulation from this CPS, see CP for overall stipulations.

6.1.3 Public key delivery to certificate issuer

When a public key is transferred to the issuing CA to be certified, it is delivered through a mechanism ensuring that the public key has not been altered during transit and that the Certificate Applicant possesses the private key corresponding to the transferred public key.

The acceptable mechanism within the CGI Trusted Services for public key delivery is a PKCS#10 Certificate signing request package.

All certificate requests provide the public key to the CA using a PKCS#10 certificate signing request (CSR).

6.1.4 CA public key delivery to relying parties

CGI Trusted Services publish Policy and issuing CA’s via its repository according to chapter 2.1 that is publicly available.

6.1.5 Key sizes

Key size for the CGI Trusted Services is specified in the appendix Certificate profiles and the requirement came from the Polestar CP.

6.1.6 Public key parameters generation and quality checking

No Stipulation.

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

Key usage purposes are defined in the certificate profiles, see Chapter 7.1

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

The CA uses hardware cryptographic modules rated to at least FIPS 140-2 Level 3 for private key generation.

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

CGI Trusted Services uses the HSM's built in dual control to split the activation function of the CA's private keys. At least two persons with HSM user PED key role acting as Service operator must be available at the same time to be able to activate the CA's Keys. List of keyholders is specified in the HSM key ceremony document keyholder matrix.

6.2.2.1 Root and policy CA

For root CAs and policy CAs the HSMs storing the CA private keys MUST enforce multi-person access control to prevent any single individual to access and activate key material. Activation data and access keys or cards MUST also be protected in a tamper-evident manner so any attempt to bypass the controls will be detected.

6.2.2.2 Issuing CAs

No Stipulation.

6.2.3 Private key escrow

Key Escrow is not supported

6.2.4 Private key backup

CGI Trusted Services CA keys are generated and stored inside FIPS 140-2 level 3 certified hardware. The keys are backed up and always kept encrypted. The Backup units are stored in Safes at physical separated location from the CA infrastructure.

6.2.5 Private key archival

The CA shall not archive any private keys, just take a backup of the CA's keys that are stored in the HSM see 6.2.4.

6.2.6 Private key transfer into or from a cryptographic module

Where private keys are backed up to another cryptographic hardware security module, such keys are transferred between devices in encrypted format only.

All communication between the HSM's are encrypted, the communication between the administrators and the HSM is also encrypted.

6.2.7 Private key storage on cryptographic module

CGI Trusted Services private CA keys are generated and stored in HSMs that are certified according to FIPS 140-2 level 3 and EAL 4+.

6.2.8 Method of activating private key

Activating CA private keys requires authentication via the HSM's Activation station. The Activation can only be done with dual control, where two of the HSM key activator administrators must do this together to be able to activate the private keys. The HSM key administrators have special tokens that are also PIN protected which must be known to operate the token.

6.2.9 Method of deactivating private key

Done during key ceremony procedure. It is done under dual control according to the HSM manufacture´s guidelines.

6.2.10 Method of destroying private key

The destruction of any private CA key must be authorized by the CGI Trusted Services Owner. It is done under dual control according to the HSM manufacture´s guidelines.

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

All CA public keys are archived as part of the certificate archive process and are stored in the CAs internal database together with its certificate.

6.3.2 Certificate operational periods and key pair usage periods

Type	Validity Period	Key usage period
Polestar ECC-256 Root CA v1	40 years	20
Polestar ECC-256 V2G OEM Policy CA v1	30 years	5
Polestar ECC-256 V2G OEM Issuing CA v1	25 years	1
Polestar ECC-256 V2G OEM Policy CA v1 OCSP Signer	13 months	No longer than the validity period
OEM provisioning	20 years	No longer than the validity period
Contract	1 day – 2 years	No longer than the validity period

Relying Parties may still validate signatures generated with these keys after expiration of the certificate.

The CA may retire its CA Private Keys before the periods listed above to accommodate key changeover processes.

6.4 Activation data

6.4.1 Activation data generation and installation

Activation data of CA keys are configured during key-ceremony of the HSM with multi-person control as described in section 6.2.2 for the HSM activation PED key.

For activation of CA there must be two administrators from the correct trusted HSM roles specified in this document available to be able to perform activation of the CA HSM.

6.4.2 Activation data protection

Every administrator that has an HSM activation key (PED) is responsible for keeping and protecting his secrets against loss, theft, modification, unauthorized disclosure, or unauthorized use. Administrators of CGI Trusted Services have safes with individual locked storage box where they store their secrets.

6.4.3 Other aspects of activation data

CGI Trusted Services changes the activation data for the HSM:s at every re-key and after returning from maintenance which we do internally. CGI Trusted Services never sends away Production HSM:s for service, we buy new hardware and destruct HSM:s that cannot be fixed in our secure locations.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The Certificate Authorities employ strict access control where only authorized administrators can connect to the servers. The access to the servers is protected by several layers of firewalls to protect the service. The Operating System is hardened and only run services that are required for operating the service.

The client that administrators use to connect to the Servers is a dedicated workstation located on a separate administrative network separated from Internet and other Polestar or CGI local LAN.

Production networks are logically separated from other components.

Direct access to a Polestar PKI CAs server is limited to Trusted Persons having a valid business reason for such access from the separated Administrative LAN.

All Access to CA productions systems is restricted to Smart Card two factor solutions.

All system use trusted time source to make sure that the time is always correct on the servers.

CGI is certified according to ISO 27001 and can be audited.

6.5.2 Computer security rating

No stipulation

6.6 Life cycle technical controls

6.6.1 System development controls

The CGI Trusted Services CA system development process meets the following requirements:

- The CA use software that has been designed and developed under a formal, documented development methodology.

- All hardware and software are purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase or the vendor uses tamper-evident packaging).
- CA platform (server hardware, operating system software, and CA application software) are dedicated to performing CA functions. There shall be no non-CA applications installed on the CA platform.
- Certificate validation system platform (server hardware, operating system software, and certificate validation application software) are dedicated to performing certificate validation functions. Applications which are not related to certificate validation are not installed on the certificate validation system platform.
- All Applications used by the system are signed in a release process.

6.6.2 Security management controls

CGI Trusted Services has developed a security plan for the service that covers the demands for management controls. That document is named “Trusted Services - Security Plan” and can be showed on demand.

6.6.3 Life cycle security controls

Cryptographic hardware may be transported between locations in tamper evident packaging only. Upon receipt of cryptographic hardware, the service trusted personnel inspect the tamper evident packaging to determine whether seals are intact. This is followed by acceptance testing.

After acceptance testing the cryptographic hardware is added to an inventory list. To prevent tampering, cryptographic hardware is stored in a secure site, with access limited to authorized personnel. Each piece of cryptographic hardware is tracked during its life cycle; any change in its state (removal from storage, integration into the production environment, removal from service etc.) is reflected in an event journal.

The handling, installation and removal of cryptographic hardware are performed in the presence of no less than two by the service trusted personal. The same controls apply to recovery routines.

CGI Trusted Services cryptographic hardware is never serviced or repaired off-site and subsequently put back into production. CA software is permanently under supervision after installation. CA and certificate status validation system software development takes place in a secure and controlled environment dedicated for CGI Trusted Services development staff. The entire development process is well defined and documented.

Software used by the service is as stated in 6.6.2 signed in the release process to guarantee that it originated from the expected supplier. The release process verifies that only signed software is deployed to the system and has had proper testing in a rigorously process before reaching production systems.

Destruction of retired hardware is done by two personnel working together and by following the destruction protocol, one of the persons is always the service delivery manger.

6.7 Network security controls

CGI Trusted Services has configured network zones and firewall layering in such a way it will be as hard as possible to attack the system (firewalls, intrusion detection mechanisms, etc.).

Access to all servers is subject to authentication. Users are provided direct access only to the services that they have been specifically authorized to use.

All communication from the operational network and server infrastructure in point-to-point encrypted.

6.8 Time-stamping

System time for CGI Trusted Services computers is updated from The Swedish national time scale, UTC (by SP Technical Research Institute of Sweden) is a national realisation of the Coordinated Universal Time, using the Network Time Protocol (NTP) to synchronize time.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profiles

All Polestar Certificates conform generally to the ITU-T Recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997 and RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, May 2008.

See the certificate profile appendix.

7.1.1 Version number(s)

All Polestar Certificates are X.509 version 3 certificates and contains data as specified by Polestar CP.

7.1.2 Certificate extensions

The algorithm object identifiers conform to the standards, see the Certificate profile appendix.

7.1.3 Algorithm object identifiers

7.1.4 Name forms

The subject and issuer fields of each X.509 certificate are populated with a unique Distinguished Name (DN) in accordance with one or more of the X.500 series standards, with the attribute type as further constrained by RFC5280.

7.1.5 Name constraints

Name Constraint extension is not used.

7.1.6 Certificate policy object identifier

See the certificate profile appendix.

7.1.7 Usage of Policy Constraints extension

See the certificate profile appendix.

7.1.8 Policy qualifiers syntax and semantics

Policy Constraint extension is not used.

7.1.9 Processing semantics for the critical Certificate Policies

No Stipulation

7.2 7.2 CRL profile

All Polestar Certificates conform generally to the ITU-T Recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997 and RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, May 2008.

7.2.1 Version number(s)

CRL version 2.

7.2.2 CRL and CRL entry extensions

No extensions is used for CRL:s

7.3 OCSP profile

Polestar uses OCSP to provide information about all of its certificates.

OCSP responders conforms to RFC 6960.

7.3.1 Version number(s)

7.3.2 OCSP extensions

OCSP nonce is supported in the OCSP Responders and is recommend for all OCSP requests.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

Every participating CA in this PKI SHALL undergo regular compliance audits to ensure adherence to this CPS and the corresponding CP.

- Each root or policy CA SHALL perform a full audit before any end entity certificates are issued from the certificate chain. A full audit SHALL happen at least every 3 years.
- Each issuing CA SHALL perform a full audit before it starts issuing certificates to end entities. A full audit SHALL happen at least every 3 years.

If any nonconformance is discovered, the next full audit SHALL happen within 12 months of the failed audit.

CAs in this PKI SHALL participate in the audit as directed by Polestar. The audited part SHALL bear their own costs for the efforts of the audit.

It´s the responsibility of Polestar to initialise the audits.

8.2 Identity/qualifications of assessor

The assessor must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with the requirements which a CA service had to adhered to.
The assessor should perform such compliance audits as a primary responsibility.

8.3 Assessor's relationship to assessed entity

The assessor should not have any organizational relationship with the audited party. A person cannot be assessor if he/she:

1. Is an employee of CGI.
2. Is in a relationship that compromise the ability to do a fair and balanced assessment.

8.4 Topics covered by assessment

The purpose of the assessment is to verify that CGI Certificate Service and any engaged Sub-contractors are complying with the requirements of this policy and CP section 8.4.

8.5 Actions taken as a result of deficiency

The PKI operator shall inform Polestar of any planned actions to mitigate or solve any flaws, weaknesses or risks found during the assessment without undue delay. The result of the mitigations and corrections shall be documented and submitted to Polestar.

8.6 Communication of results

The assessor will provided a copy of the audit report to Polestar and CGI Certificate Service management The results will not be made public unless required by law

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

No stipulation.

9.1.2 Certificate access fees

No stipulation.

9.1.3 Revocation or status information access fees

No stipulation.

9.1.4 Fees for other services

No stipulation.

9.1.5 Refund policy

No stipulation.

9.2 Financial responsibility

9.2.1 Insurance coverage

This part is regulated between an agreement between Polestar and CGI.

9.2.2 Other assets

This part is regulated between an agreement between Polestar and CGI.

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

Information which is not excluded in section 9.3.2, or otherwise defined as public in this policy or in applicable policy, shall be treated as confidential.

9.3.2 Information not within the scope of confidential information

The following information shall not be deemed to be confidential:

- Issued certificates including public keys
- Revocation lists and OCSP responses
- Key holder terms and conditions
- This Certificate Practice Statement

9.3.3 Responsibility to protect confidential information

All confidential information shall be physically and/or logically protected from unauthorized viewing, modification or deletion.

Storage media used by the CA system are protected from environmental threats such as temperature, humidity and magnetism and that also applies to backup and archive media.

Confidentiality keys are backed up by CGI Certificate Service, and in those cases the keys will be protected in accordance with Section 6, and will not be disclosed without prior consent of the Subscriber or a duly authorized representative of the issuing CA.

CGI shall disclose confidential information if a court or other legal authority subject to Swedish law so decides. Private keys linked to issued certificates cannot be supplied where these are not stored by CGI or any of CGIs subcontractors.

9.4 Privacy of personal information

9.4.1 Privacy plan

We follow applicable Swedish laws and regulations in regard to Privacy and we follow EU GDPR.

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.

9.6.1 CA representations and warranties

No stipulation.

9.6.2 RA representations and warranties

No stipulation.

9.6.3 Subscriber representations and warranties

No stipulation.

9.6.4 Relying party representations and warranties

No stipulation.

9.6.5 Representations and warranties of other participants

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 CPS becomes effective on the date it is published and remains effective until a new version if published.

9.10.2 Termination

This CPS becomes effective on the date it is published and remains effective until a new version if published or until the agreement between Polestar and CGI is terminated.

9.10.3 Effect of termination and survival

Participants in this PKI are bound to the terms of this CPS for as long as certificates are within their validity period or until the agreement between Polestar and CGI is terminated.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

This CPS do not use amendments.

9.12.1 Procedure for amendment

No stipulation.

9.12.2 Notification mechanism and period

No stipulation.

9.12.3 Circumstances under which OID must be changed

No stipulation.

9.13 Dispute resolution provisions

No stipulation.

9.14 Governing law

Swedish law and Swedish regulations. Disputes to be processed according to Swedish legal systems.

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

According to the agreement between Polestar and CGI.

9.17 Other provisions

No stipulation.

10 Appendix A

Root CA

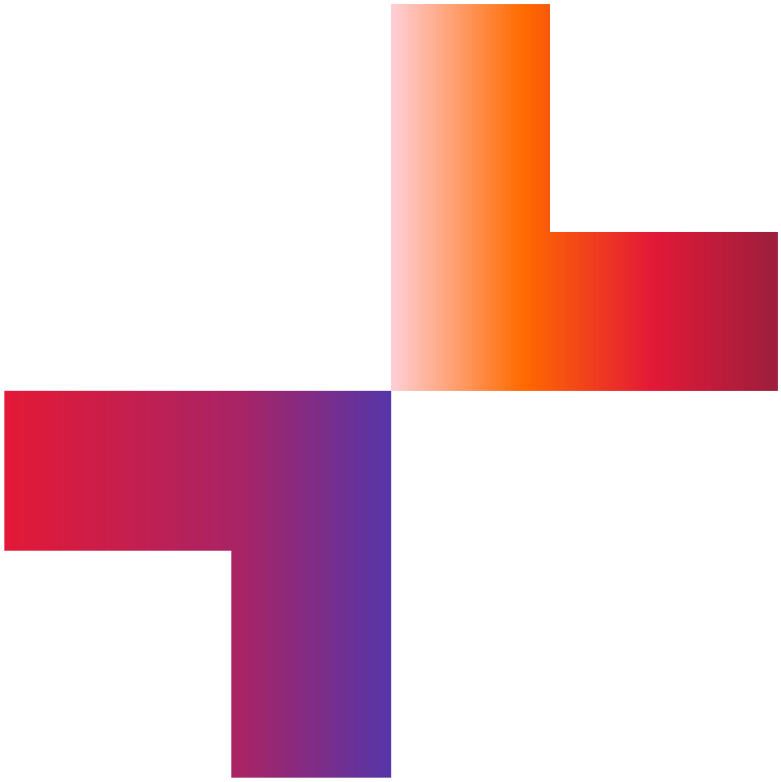
KEY	Value
X509 version	3 (0x2)
Serial number	GENERATED-16-BYTES
Signature Algorithm	ecdsa-with-SHA256
Validity - Not Before	Issue date
Validity - Not After	Issue date + 40 years.
Issuer DN	CN = Polestar ECC-256 Root CA v1, O = Polestar Performance AB, C = SE
Subject DN	CN = Polestar ECC-256 Root CA v1, O = Polestar Performance AB, C = SE
Public Key Algorithm	id-ecPublicKey
Public Key Length	256 bit
AIA OCSP URI	none
AIA CA Cert URI	none
Basic Constraints Critical	yes
Basic Constraints CA	CA:TRUE
Authority Key Identifier	
Subject Key Identifier	
Certificate Policy Id	
Certificate Policies Crit.	no
CRL Distribution Points	none
CDP Critical	no
Key usage	Certificate Sign, CRL Sign
Key Usage critical	yes
Extended Key Usage	none
Ext. Key Usage critical	no

Policy CA

Key	Value
x509 version	3 (0x2)
Serial number	GENERATED-16-BYTES
Signature Algorithm	ecdsa-with-SHA256
Validity - Not Before	Issue date
Validity - Not After	Issue date + 30 years.
Issuer DN	CN = Polestar ECC-256 Root CA v1, O = Polestar Performance AB, C = SE
Subject DN	CN = Polestar ECC-256 V2G OEM Policy CA v1, O = Polestar Performance AB, C = SE
Public Key Algorithm	id-ecPublicKey
Public Key Length	256 bit
AIA OCSP URI	none
AIA CA Cert URI	none
Basic Constraints Critical	yes
Basic Constraints CA	CA:TRUE, pathlen:1
Authority Key Identifier	
Subject Key Identifier	
Certificate Policy Id	
Certificate Policies Crit.	no
CRL Distribution Points	http://pki-cdp.polestar.com/psecc256rootcav1.crl
CDP Critical	no
Key usage	Certificate Sign, CRL Sign
Key Usage critical	yes
Extended Key Usage	none
Ext. Key Usage critical	no

Issuing CA

Key	Value
x509 version	3 (0x2)
Serial number	GENERATED-16-BYTES
Signature Algorithm	ecdsa-with-SHA256
Validity - Not Before	Issue date
Validity - Not After	Issue date + 25 years.
Issuer DN	CN = Polestar ECC-256 V2G OEM Policy CA v1, O = Polestar Performance AB, C = SE
Subject DN	CN = Polestar ECC-256 V2G OEM Issuing CA v1, O = Polestar Performance AB, C = SE
Public Key Algorithm	id-ecPublicKey
Public Key Length	256 bit
AIA OCSP URI	http://pki-ocsp1.polestar.com/
AIA CA Cert URI	none
Basic Constraints Critical	yes
Basic Constraints CA	CA:TRUE, pathlen:0
Authority Key Identifier	
Subject Key Identifier	
Certificate Policy Id	
Certificate Policies Crit.	no
CRL Distribution Points	http://pki-cdp.polestar.com/psecc256v2goempolicycav1.crl
CDP Critical	no
Key usage	Certificate Sign, CRL Sign
Key Usage critical	yes
Extended Key Usage	none
Ext. Key Usage critical	no



cgi.com