WIRELESS POWER
CONSORTIUM

WPC Root CA CP/CPS

WPC Root CA Certificate Policy and Certificate Practice Statement
Redacted Public Version 1.0 | 2021-04-13

NORDICTRUST
SERVICES

Revision History

VERSION	DATE	REVISION DETAILS
0.1	12 Apr 2021	First redacted public draft based on WPC Root CA CPS v.0.7
1.0	13 Apr 2021	Approved public CPS

Content

1. Introduction

This is the combined Certificate Policy and Certificate Practice Statement of the Wireless Power Consortium Root CA service. The current version of the CPS is redacted public version of the WPC Root CA non-public CPS.

1.1 Overview

The WPC Root CA CPS describes the practices and procedures used to address all the requirements identified for the WPC Root CA Certificate Policy. This document combines both the CP and the CPS and it forms the Certificate Policy and the Certificate Practice Statement (CPS) for the Wireless Power Consortium Root CA.

Subscribers and relying parties can consult this redacted version of the CP/CPS to obtain details of the requirements addressed by its CP and how the CP is implemented by the WPC Root CA.

This document follows the framework for CP and CPS described in ETSI EN 319 411-1 and RFC 3647.

This CP/CPS contains the following Annexes:

- Annex 1: WPC Root CA and MCSP certificate profiles

1.2 Document Name and Identification

See Section 2.3.

1.3 Purpose of the CPS

The purpose of the combined WPC Root CA Certificate Policy and Certificate Practice Statement is to address necessary security requirements on the WPC Root CA, i.e., for the signing of Manufacturer certificates and Certificate Revocation Lists.

The purpose of the CP, referenced by a policy identifier in a certificate, states "what is to be adhered to", while the CPS states "how it is adhered to", i.e., the processes it will use in creating and maintaining the certificate.

The Root CA certificate contains data and security components that need to be protected. The system is designed so that a security incident in the Root CA system, such as compromise of certain cryptographic keys, can make serious damage to the entire Wireless Power ecosystem. Therefore, signing of Manufacturer certificates and CRLs must be performed in such a way that necessary security is upheld.

1.4 Document Validity

The CPS is governed by the WPC Root CA Certificate Policy (CP) for the provision on Root Certificate Singing. It is valid from the moment when the WPC Root CA Certificate Policy (CP) is approved by the Wireless Power Consortium PKI Policy Authority. It shall be valid until further notice. Since the document combines the CP and CPS, the CPS validity is simultaneous to the CP.

The validity of the WPC Root CA Certificate Policy ends when the WPC Root CA stops operating or when the Wireless Power Consortium PKI Policy Authority announces the WPC Root CA Certificate Policy is no longer valid, e.g., because a new version of the WPC Root CA Certificate Policy becomes effective.

2. General provisions on Certification Practice Statement and Certificate Policies

2.1 General requirements

The WPC Root CA trust service is dedicated to the issuance of public key certificates to Manufacturer CA Service Providers (MCSP) and signing of CRLs.

The requirements are indicated in terms of the security objectives followed by more specific requirements for controls to meet those objectives when considered necessary to provide the necessary confidence that those objectives will be met. Practices and methods specified in ISO/IEC 27002:2013 are applied in the implementation of these controls.

The WPC Root CA uses the certificate and CRL profiles specified in Annex 1 of this CP/CPS.

2.2 Certification Practice Statement requirements

The WPC Root CA CPS establishes practices concerning the PKI certificate lifecycle services such as certificate issuance, certificate management (including publication and archiving) or revocation.

This is a detailed CPS which contains sensitive details of the Root CA system and this document shall not to published in its entirety. A summary of the CPS shall be edited and published, containing only the provisions from the CPS that are relevant to the participants in the PKI, such as the responsibilities of the parties or the stages of the certificate lifecycle. The summarised CPS shall not contain sensitive provisions of the full CPS that might provide a malicious attacker with useful information about the Root CA's operations.

This CPS does not constitute a contract and it does not automatically bind PKI participants as a contract would. The summarised CPS may be incorporated into any applicable subscriber or relying party agreement.

2.3 Certificate Policy name and identification

The present document is the combined WPC Root CA Certificate Policy (CP) and Certificate Practice Statement (CPS). This CPS is compliant with requirements specified the Wireless Power Consortium.

WPC has registered Object Identifier Component Value: 148 (OID arc). The Certificates used with the authentication protocol require the use of Object Identifiers (OID) with attributes and extensions.

This Certificate Policy has the following ASN.1 object identifier (OID): 2.23.148.1.0

```
joint-iso-itu-t (2) international-organizations (23)
WPC (148) policy-identifiers (1) root-ca(0)
```

The certificate policy ASN.1 object identifier for Manufacturer CA certificates is: 2.23.148.1.1

```
joint-iso-itu-t (2) international-organizations (23)
WPC (148) policy-identifiers (1) wpc-qi-policy (1)
```

The certificate policy ASN.1 object identifier for Product Unit certificates is: 2.23.148.1.2

```
joint-iso-itu-t (2) international-organizations (23)
WPC (148) policy-identifiers (1) wpc-qi-rsid (2)
```

The WPC Root CA CP/CPS follows the requirements specified in the ETSI EN 319 411-1 Lightweight Certificate Policy (LCP). The policy requirements for this CP/CPS are built on the policy requirements for the issuance and management of ETSI LCP certificates, partly enhanced with WPC specific requirements. It includes, except where explicitly indicated, all the Lightweight Certificate Policy (LCP) requirements.

The current version of this CP/CPS is 1.0. This CP/CPS is approved by the Wireless Power Consortium PKI Policy Authority, represented by the board of directors of the Wireless Power Consortium, on [DATE] 2021.

2.4 PKI Participants

This CP/CPS is designed to satisfy the requirements of the Wireless Power Consortium Root CA service.

2.4.1 Certification Authority

The WPC Root CA is operated under the authority and responsibility of the Wireless Power Consortium. The WPC Root CA is responsible for the generation and management of root public-private key pairs with the respective Root CA certificates. The WPC Root CA issues certificates to Manufacturer Certification Authority Service Providers, and signs Certificate Revocation Lists.

The WPC Root CA is a self-signed CA with a self-issued CA certificate, in which the issuer and subject are the same entity. Self-issued certificates are generated to support changes in policy or operations and to provide a root of trust for the certificate validation path. The WPC Root CA self-signed certificate is a self-issued certificate where the digital signature may be verified by the public key bound into the certificate and it is used to convey a public key for use to begin the certification path.

The contact address of the Wireless Power Consortium PKI Policy Authority is:

Wireless Power Consortium

445 Hoes Lane

Piscataway, NJ 08854

USA

2.4.2 Subscriber and Subject

A Subscriber is an End Entity (EE) organisation that has been issued a Certificate and is authorized to use the Private Key that corresponds to the Public Key in the Certificate. The subscriber asserts it uses the key and certificate in accordance with this CP/CPS. The Subscriber is a Manufacturer CA Service Provider, which issues leaf-certificates to devices.

For this policy, subscribers are limited to Manufacturer CA Service Providers. In this CP/CPS the Subscriber is a legal person that can be an Organisation or a unit or a department identified in association with an Organisation that has signed a Manufacturer CA Service Provider Agreement with the Wireless Power Consortium.

When a subscriber is the subject, it will be held directly responsible if its obligations are not correctly fulfilled.

The link between a subscriber and the subject is a Manufacturer agreement stating which Subscriber may request a CA certificate with the Manufacturer's Power Transmitter Manufacturer Code (PTMC) as subject.

2.4.3 Relying Parties (RP)

A Relying Party is the entity that relies on the validity of the binding of the subscriber’s name to a public key. The relying party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information.

For this CP/CPS, the relying party may be any entity that wishes to validate the binding of a public key to the name of a Manufacturer certificate holder. A Relying party may or may not also be a Subscriber within the Root CA service. With the WPC ecosystem, the Relying Party is a device, application or service provider, participating in the manufacturing of wireless power related devices.

2.4.4 Registration Authority (RA)

Any Legal Entity that is responsible for identification and authentication of Subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA MAY assist in the Certificate Application process or revocation process or both. When “RA” is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.

2.4.5 Others

The WPC Root CA hosting, maintenance and operational functions are provided by CardPlus AB Nordic Trust Services, as a managed service, under a contractual agreement with the Wireless Power Consortium.

The contact address for WPC Root CA managed service provider is:

Nordic Trust Services
CardPlus Sverige AB

Platensgatan 20
SE-591 35 Motala, Sweden

email: support@cardplus.se

2.5 Certificate Usage

The LCP policy places no constraints on the user community and applicability of the certificate. In this CP/CPS, the applicability of other certificates is as described below.

The WPC Root CA certificate usage is restricted to signing in the following use cases:

1. Manufacturer Certification Authority Service Provider certificate signing
2. Signing of Certificate Revocation Lists

2.6 Policy Administration

The Wireless Power Consortium PKI Policy Authority administers the WPC Root CA PKI. The WPC Executive Director is responsible for registration, maintenance, and interpretation of this CPS.

The contact information is:

WIRELESS POWER CONSORTIUM, INC.

c/o IEEE-ISTO, WPC Administration
445 Hoes Lane
Piscataway, NJ 08854
USA

TEL: +1-732-465-5843

EMAIL: please use contact form:

2.7 Definitions and Acronyms

See Section 12.

3. Publication and Repository Responsibilities

The WPC Root CA operates and maintains repositories to support the WPC Root CA PKI operations. The location of any publication is available to Subscribers and Relying Parties as specified in this CPS. Information in the WPC Root CA repositories is protected in accordance with the European General Data Protection Regulation, national privacy laws and WPC's Privacy Policy and Procedures documents.

Certificates shall be available for retrieval only to WPC member organisations, which have adhered to the terms and conditions stated in this CP/CPS.

The WPC Root CA Repository is responsible for:

- Maintaining a secure system for storing and retrieving certificates
- Maintaining a current copy of this CPS and hosting of deprecated versions of the CPS
- Maintaining other information relevant to certificates
- Providing information regarding the status of certificates as valid or invalid that can be determined by a Relying Party

The WPC Root CA posts the Root Certificate at the following location, accessible using

HTTPS:

- https://www.wirelesspowerconsortium.com/qi-authentication/WPCRoot.p7c

The WPC Root CA posts CRLs at the following location, accessible using HTTPS:

- https://www.wirelesspowerconsortium.com/qi-authentication/WPCRootCA.crl

The HTTP access is defined in the CRL Distribution Point field of end entity certificates.

3.1 Naming

Requirements for naming in certificates are as specified in IETF RFC 5280.

For the purpose of this CP/CPS, the certificate Name fields describe a hierarchical name composed of attributes and corresponding values. The name field values in the WPC Root CA certificate are the following:

- distinguished name qualifier (DN);
- common name (CN);
- serial number (SN)

The issuer distinguished name and subject distinguished name fields are used to perform name chaining for certification path validation. Name chaining is performed by matching the issuer distinguished name in one certificate with the subject name in a CA certificate. The WPC Root CA is a self-issued certificate and the names in the issuer and subject fields must match.

3.2 Initial Identity Validation

Identity validation is part of at least the following processes:

- Certificate application
- Certificate issuance

The initial identity validation process is used to establish the identity of the subject. The subject is always a legal entity.

3.3 Identification and Authentication for Re-key Requests

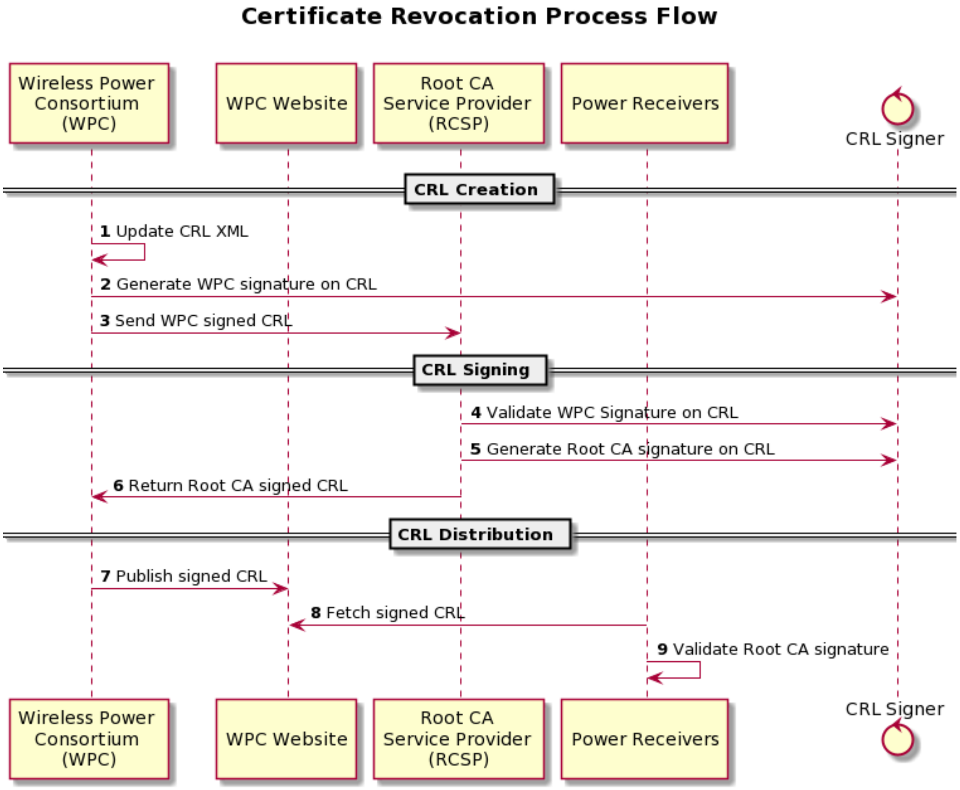
No re-keying of certificates is allowed.

3.4 Identification and Authentication for Revocation Requests

The publication of the CRL is not time-critical and a 24-hour distribution delay is not guaranteed. The WPC issues the CRL at the disposal of phone manufactures, which decide themselves when the CRL is distributed to subsequent devices.

The revocation decision process is detailed in Annex B of the Manufacturer and Manufacturer CA Service Provider Agreements.

Certificate Revocation Requests can only be submitted by the WPC. Certificate Revocation Requests are submitted using the following process:


Certificate Revocation Process Flow
Wireless Power Consortium (WPC)
WPC Website
Root CA Service Provider (RCSP)
Power Receivers
CRL Signer
CRL Creation
1 Update CRL XML
2 Generate WPC signature on CRL
3 Send WPC signed CRL
CRL Signing
4 Validate WPC Signature on CRL
5 Generate Root CA signature on CRL
6 Return Root CA signed CRL
CRL Distribution
7 Publish signed CRL
8 Fetch signed CRL
9 Validate Root CA signature
Wireless Power Consortium (WPC)
WPC Website
Root CA Service Provider (RCSP)
Power Receivers
CRL Signer

The WPC Root CA system provides confirmation that the request for revocation has been processed.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

The subject's key pair is generated by the subject. The requirements for key pair generation are defined in Section 6.1 of the CP/CPS.

4.2 Certificate Application Processing

The application for certificates by Manufacturer CA Service Providers (MCSP) is processed by the WPC trusted registration service. The Root CA has a trust relationship with the WPC registration service, and it accepts certificate applications from Manufacturer CA Service Providers which are listed in the WPC website. The WPC Administration compiles a spreadsheet (WPC-ALA) with the request validation data, which is used as reference for verifying requests.

The Root CA operator maintains a list of “Authorized Persons” and their registration agent certificate identifiers. The Registration Agent certificate is specific to:

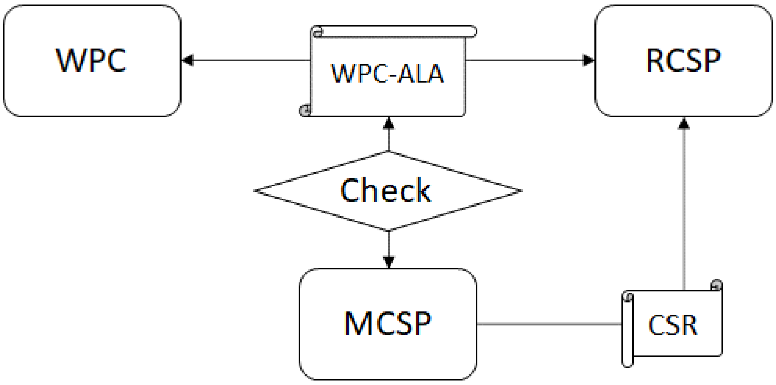
- the Root CA operational management and;
- the WPC Root CA service provider.

The WPC-ALA validation document is maintained and provided by WPC Administration.

The WPC Administration maintains the following Validation Data in the WPC-ALA:

- Manufacturer CA Service Provider Agreement (MCSPA) repository (or list of Authorized Persons)
- List of Manufacturers by PTMC and the approved Manufacturer CA Service Providers (MCSPs) for that PTMC
- PTMC list with PTMC-sequence numbers that are in use

The certificate application process overview is the following:



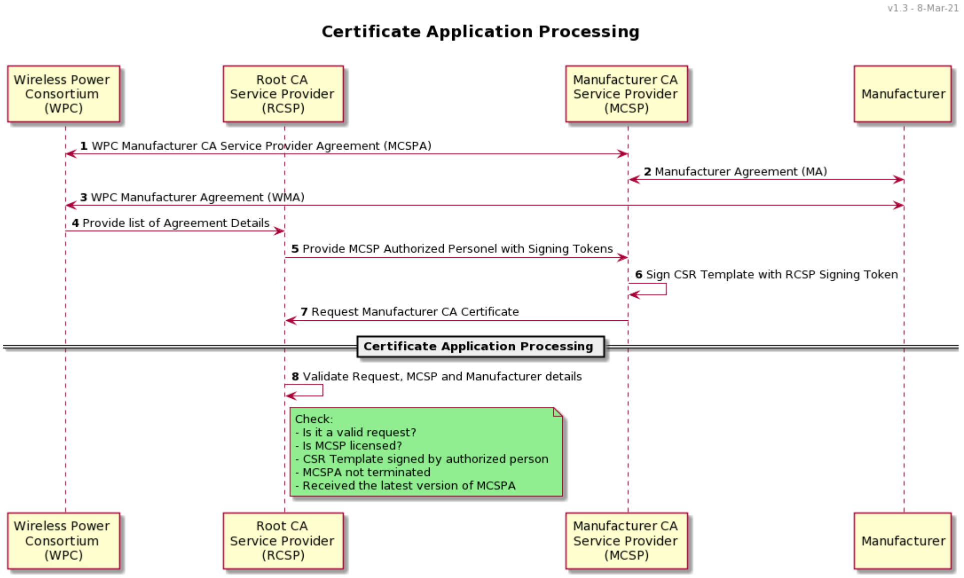
Using this validation data, the Root CA service operator processes certificate applications in the following way:

- A Certificate Signing Request (CSR) is received in an electronically signed PDF document, which contains the administrative details. The Certificate Signing Request is an encoded character string embedded in the PDF document;
- During the administrative request validation, the operator verifies that the application was submitted by a currently licensed Manufacturer CA Service Provider;
- The electronic signature on the application form is verified and checked that it matches the person identified in the Manufacturer CA Service Provider Agreement as ‘authorized person’ for the Manufacturer CA Service Provider;
- The electronic signature is validated for integrity, validity and trust. The validated signature provides a signed confirmation that the requestor is in possession of the private key associated with the CSR;
- The operator verifies that the Manufacturer CA Service Provider Agreement was not terminated;
- The operator also verifies that the Manufacturer CA Service Provider Agreement is the latest version of the agreement, with the latest list of authorized persons.

The WPC-ALA document is used as the primary source and method for request verification.

No registration authorities external to the WPC are accepted.

The certificate application process is the following:


v1.3 - 8-Mar-21
Certificate Application Processing
Wireless Power Consortium (WPC)
Root CA Service Provider (RCSP)
Manufacturer CA Service Provider (MCSP)
Manufacturer
1 WPC Manufacturer CA Service Provider Agreement (MCSPA)
2 Manufacturer Agreement (MA)
3 WPC Manufacturer Agreement (WMA)
4 Provide list of Agreement Details
5 Provide MCSP Authorized Personel with Signing Tokens
6 Sign CSR Template with RCSP Signing Token
7 Request Manufacturer CA Certificate
Certificate Application Processing
8 Validate Request, MCSP and Manufacturer details
Check:
- Is it a valid request?
- Is MCSP licensed?
- CSR Template signed by authorized person
- MCSPA not terminated
- Received the latest version of MCSPA
Wireless Power Consortium (WPC)
Root CA Service Provider (RCSP)
Manufacturer CA Service Provider (MCSP)
Manufacturer

4.3 Certificate Issuance

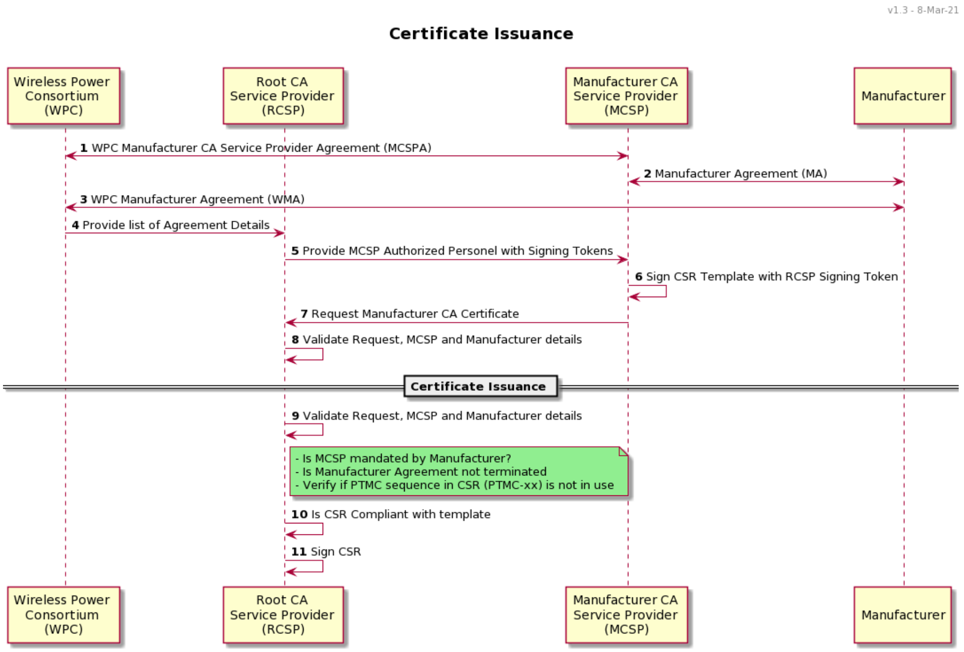
The Root CA establishes controls to assure that certificates are issued securely, to maintain their authenticity and to implement measures against forgery of certificates. The key generation and management requirements are specified in Section 6.

For the certificate issuance, the Root CA operator performs the following verifications, in addition to those described in Certificate Application Processing to validate that the certificate being requested is valid:

- Verify that the Certificate Signing Request is compliant with the MCSP Certificate template;
- Verify that the Manufacturer CA Service Provider is mandated to perform the certificate request on behalf of the Manufacturer CA (the subject, identified by the PTMC) in the Manufacturer Agreement;
- Verify that the Manufacturer Agreement is not terminated;
- Verify that the PTMC-sequence number PTMC-xx in the CSR is not in use.

The purpose of the of the sequence numbers in use is to ensure that no duplicate sequence numbers are in operation. The sequence number is part of the certificate and is flagged as being unique. The Root CA will automatically fail a request for a certificate with a duplicate sequence number. This list is maintained by the Root CA.

The certificate issuance process is the following:


v1.3 - 8-Mar-21
Certificate Issuance
Wireless Power Consortium (WPC)
Root CA Service Provider (RCSP)
Manufacturer CA Service Provider (MCSP)
Manufacturer
1 WPC Manufacturer CA Service Provider Agreement (MCSPA)
2 Manufacturer Agreement (MA)
3 WPC Manufacturer Agreement (WMA)
4 Provide list of Agreement Details
5 Provide MCSP Authorized Personel with Signing Tokens
6 Sign CSR Template with RCSP Signing Token
7 Request Manufacturer CA Certificate
8 Validate Request, MCSP and Manufacturer details
Certificate Issuance
9 Validate Request, MCSP and Manufacturer details
- Is MCSP mandated by Manufacturer?
- Is Manufacturer Agreement not terminated
- Verify if PTMC sequence in CSR (PTMC-xx) is not in use
10 Is CSR Compliant with template
11 Sign CSR
Wireless Power Consortium (WPC)
Root CA Service Provider (RCSP)
Manufacturer CA Service Provider (MCSP)
Manufacturer

The WPC agreements in place for the MCSP require that the MCSP generates and manages the private keys associated with the MCSP certificate in accordance with this CP/CPS. The key generation and management requirements are specified in Section 6.

The issued certificate shall include the WPC Root CA Certificate Policy identifier specified in Section 2.3. If not present in the Certificate Signing Request, the WPC Root CA will add the Policy Identifier to the MCSP certificate.

The Root CA certificate validity is set to not expire.

4.4 Certificate Acceptance

The WPC communicates the certificate policy, terms and conditions to the MCSP. The Certificate Acceptance terms and conditions are defined in the MCSP Agreement and Annexes.

4.5 Key Pair and Certificate Usage

The subscriber's obligations are defined in Annex A of the MCSP Agreement.

4.6 Certificate Renewal

Certificate renewal is not permitted.

4.7 Certificate Re-key

Certificate Re-key is not permitted.

4.8 Certificate Modification

Certificate modification is not permitted.

4.9 Certificate Revocation and Suspension

The Subject certificate revocation conditions are defined in Annex B of the MCSP Agreement.

Certification Authority Revocation List (CARL) is not used.

4.10 Certificate Status Services

A custom CRL is supported. The custom CRL is described in Annex 1 of the CPS.

4.11 End of Subscription

No compliance requirements.

4.12 Key Escrow and Recovery

The subject certificate keys are not escrowed.

5. Facility, Management, and Operational Controls

5.1 General

No stipulations.

5.2 Physical Security Controls

The Root CA services are housed in a secure area, protected by a defined security perimeter, with appropriate security barriers and entry controls to prevent unauthorised access, damage, and interference. This area is monitored by a permanent-duty guard service and online security alarms are established.

- Power supply and air conditioning for the Root CA systems are appropriate and redundancy is established.
- The Root CA systems and storage media used to store confidential information, such as hard disks, smart cards and HSMs, are protected against unauthorised or unintended use, access, disclosure, or damage by people or other threats (e.g. fire, water).
- Backup and installation media are be stored in a separate location that is physically secured and protected against unauthorised or unintended use, access, disclosure, or damage by people or other threats (e.g. fire, water).
- Procedures for the disposal of waste are implemented to avoid unauthorised use, access, or disclosure of confidential data.

The Root CA operations take place in one secure facility located in Finland. The Root CA key generation and management, MCSP certificate and CRL signing systems are hosted in the secure facility. The Root CA service provider’s operational site is responsible for the security operations of the facility.

The physical protection plan is not publicly available. The information presented below summarises the contents of the physical protection plan.

5.3 Site location and construction

The primary site in Finland is a security operations facility with a production-area vault.

The structures of doors, windows and hatches are anti-burglary.

The door window of the storage compartment of the production facility is equipped with a black film that prevents visibility.

The upper hatches of the production room (smoke extraction) are kept locked.

Structural safety will be updated as necessary.

The site is located in a geographical low risk area, and has strong perimeter protection and an advanced access control. Security design is based on the concept of layers of defence. Multiple mutually independent consecutive layers of protective measures are deployed in concentric circles around the building, and around each access point.

5.3.1 Surveillance

The purpose of technical surveillance is to support day-to-day operations and to detect changes in the desired state of being, giving alarm information to a place that is constantly occupied and has instructions for action. Technical supervision has been provided by a contracted security services organisation.

The outer perimeter of the property is monitored by cameras so that it and the activity taking place along it can be detected.

The monitoring of passenger traffic has been implemented in such a way that when a person enters the property, the person is certainly recorded in the camera image.

When entering the production room, the camera is set up so that the person entering can be identified.

The production area and the High Security Area (HSA) area are entirely subject to camera surveillance.

Freight traffic is fully camera-monitored.

Digital camera surveillance recorders are located in an area that can only be accessed by authorised persons. Images can be used to illustrate and confirm a security incident. The retention period of the recording is one year.

5.3.2 Burglary and Fire Alarms

The property is equipped with an automatic fire alarm system. The HSA area also has a separate automatic gas extinguishing system. The premises must comply with the applicable fire regulations. Therefore, a fire inspection by the authority must be carried out annually. The shortcomings identified need to be remedied.

Staff must be instructed and trained in the event of a fire. Exit drills must be held at regular intervals.

5.3.3 Cleanliness enforcement

The cleanliness of the premises is an important factor in, for example, fire prevention and comfort in the workplace. Unnecessary storage of papers contributes to increasing the fire load and takes up storage space. Unnecessary papers should be destroyed taking into account their classification and method of destruction.

5.3.4 Physical access

The physical access to the location is protected using electro-mechanic locking with access controls. The access is secured using personal ID access badges. Access badges can only be ordered at the request of the Security Officer.

The Security Management Group (SMG) maintains an up-to-date access badge and key registry. Only the security manager can hand over the access badges and keys to the staff representative against acknowledgment.

The property is equipped with a burglar alarm system. The doors of the shell and compartmentation are equipped with a motion detector. In addition, the areas are equipped with motion detectors.

The vault and HSA area have seismic detectors and motion detectors.

The emergency call buttons are located in critical locations.

The system's shell protection is on outside of normal hours.

The alarm is routed to a 24/7 alarm centre, from where the information is further transferred to a line organization that is constantly on standby.

The operations site is divided in the following areas:

1. Open Access Area, where guests will be received in this area and will be escorted to the following areas. The guest cannot move unaccompanied after this. There is no direct connection from there to the premises inside.
2. Controlled Access Area, which includes corridors and office space inside the building. In this area, the doors only open with a personal ID access badge.
3. Raised Security Area, where only authorised persons will be allowed to enter. A visit to this area will only take place in the presence of an escort. This is protected area where access happens only through a Single Access Systems (SAS) controlled by an automated access control system linked to an active alarm system, which reacts to defeat attempts.The identities of the persons present in the protected area is known at all times.
4. High Security Area (HSA), where Root CA operator functions are conducted. Access to these areas is via a Euro VII vaulted door, which requires two people to open, with personal identification badge and code. One person can work in the area at a time.
5. The Vault is a storage area inside the HSA for hosting the Hardware Security Modules (HMS) used for Root CA operations. The vault is a separate locked space inside the HSA area that is only accessible to authorised persons. Two authorised persons are required to

enter the vault. Guests entering Security Area 4 must be approved by the Security Officer prior to the visit. No visits to area 5 are allowed. Maintenance work is always carried out under supervision.

5.3.5 Power and air conditioning

At the production site, backup electrical power is provided by the local energy company.

The backup power systems are tested periodically.

5.3.6 Water exposures

The site facility is designed to prevent exposure to water. The risk of exposure of the Root CA systems and operations is considered to be minimal.

5.3.7 Fire prevention and protection

The site facility uses a high-sensitivity smoke detection system, and the production area fire-suppression system is based on an inert fire-suppressing gas. This is used instead of water or foam to not cause damage to the production equipment or harm for persons. The fire prevention and protection are periodically tested.

5.3.8 Media storage

On-site media for the Root CA system are held in safes.

5.3.9 Waste disposal

Prior to disposal, paper waste and other media are shredded. Security-waste is disposed in purpose-designed waste bins, which are removed by a specialised security-waste removal contractor. Ordinary office waste is removed by a cleaning contractor.

Magnetic storage media are erased by degaussing. Solid State Drives are erased by physical destruction.

5.3.10 On-site backup

The IT environment backups are done with appropriate backup software.

Backups are done both to tape and disk. This method provides the fastest possible recovery from data on disk and long archival possibilities of tape backup. the backup software is used to backup all virtual machines using reverse incremental backups. This means that the latest backups are always full and the rest are incremental. This provides the possibility of granular recovery or full recovery of a system. File level-restore can be performed from the backup server and also restore to virtual disks in case of disaster and virtual disks can be restored to VMWare hypervisor.

Data is backed up automatically and the functionality of backups is checked and verified during periodic system checks. Only domain administrators and backup server local administrators can access the backup software interface.

5.3.11 Off-site backup

Tape backups are stored outside the production environment in a safe location.

5.4 Procedural Controls

5.4.1 Trusted roles

The Root CA operations are conducted by authorised and vetted staff assigned to one of the following roles:

- Administrator/Operator;
- Security Officer;
- Auditor (internal).

The operator role is incorporated in the administrator role.

The administrator / operator role is authorised to:

- login to the Root CA certificate management system;
- access to the Root CA signing function;
- operate the signing function using the Root CA signing key.

The security officer role is authorised to:

- install, configure and maintain the Root CA PKI system;
- update, maintain and run system and performance diagnostics on the Root CA HSM system

- perform system backup and recovery.

The internal auditor role is authorised to:

- produce, view and maintain archives and audit logs of the Root CA operation system;
- perform tests and checks on the Root CA system on demand;
- quarantine the Root CA system on detection of an incident;
- report incidents to higher management.

5.4.2 Number of persons required per task

The Root CA private key generation and backup is performed according to the Key Ceremony secure operation procedure. This process is witnessed by the Nordic Trust Services (NTS) management team and the WPC representatives. Minutes of the Key Ceremony are documented and approved by the WPC.

The Root CA system installation and configuration requires one Administrator and one Security Officer. The Administrator carries out the installation and configuration operations. The Security Officer verifies these operations and performs the baseline system integrity check prior to entry into service.

Root CA system maintenance operations require one Security Officer. Any changes are detected and verified by system integrity checks performed by the internal auditor.

Root CA PKI system backup requires one administrator. The PKI system recovery requires one administrator and one internal auditor.

Security officer tasks require one security officer.

Root CA certificate signing operations are recorded in the system logs controlled by the internal auditor.

Root CA certificate signing operations require two administrators / operators. The Root CA PKI system start-up requires the intervention of one operator.

Root CA administrators / operators are set during the Key Ceremony. A minimum of two operators are assigned to perform signing operations by the operations team leader.

Root CA system auditing requires the intervention of one administrator and one internal auditor. The audit consists of system integrity checking using software held on read-only media. The administrator configures the system to permit the auditor to execute the integrity checks. Test results are maintained by the internal auditor.

Incident reports are prepared by the internal auditor and sent directly to higher management, with a copy to the Chief Security Officer.

5.4.3 Identification and authentication for each role

Staff assigned to all roles are identified in the course of passage through the physical access controls surrounding the Root CA system.

The system login process requires a certificate smart card, and roles are mapped to user groups.

Root CA signing operations require positive authentication, credential validation and access authorisation of two administrator / operator smart cards to the system.

5.4.4 Roles requiring separation of duties

No single person is permitted to cover more than one role simultaneously.

5.5 Personnel Controls

5.5.1 Qualifications, experience, and clearance requirements

1. The Security Officer is responsible for:

- establishing the Root CA operations schedule;
- accommodating auditor-initiated requests for system checks;
- authorizing system maintenance activities;
- installation, configuration and maintenance of the Root CA cryptographic hardware (HSM);
- installation, configuration and maintenance of Root CA PKI system general-purpose IT equipment and operating systems;
- installation, configuration and maintenance of Root CA certificate and CRL signing systems;
- maintaining relationships between the Root CA operations and the WPC.

The Security Officer requires general knowledge in the following areas:

- maintenance of auditable records of Root CA operations;
- Root CA CSR and CRL processing and administrative procedures.

The Security Officer is not required to handle sensitive information. This CP/CPS does not stipulate clearance, but persons assigned to this role are subject to security clearance and vetting procedures defined in the Root CA operator ISMS.

2. The administrator / operator is a trusted role in the Root CA system. Administrators / operators require detailed knowledge in the following areas:

- Root CA secure operating procedures;
- key management processes specific to the Root CA certificate and CRL signing operations;
- Root CA secure operating procedures;
- operation of the Root CA CSR and CRL validation software and processes.

Administrators require general knowledge in the following areas:

- principles of IT security;
- the key management processes specific to the Root CA HSM system;
- Root CA signing and security operating procedures

The administrator role is required to handle the root keys. This CP/CPS does not stipulate clearance, but persons assigned to this role are subject to security clearance and vetting procedures defined in the Root CA operator ISMS.

3. The internal auditor is a trusted role in the Root CA system. Internal auditors require detailed knowledge in the following areas:

- the Root CA secure operating procedures;
- IT security auditing, with emphasis on system integrity checking;
- the operation of the Root CA CSR and CRL validation and processes;
- CardPlus ISMS and Quality Management System (QMS)

Auditors require general knowledge in the following areas:

- IT forensics;
- principles of cryptography and issues involved in cryptographic key management.

The internal auditor role is not required to handle sensitive information, and therefore no clearance requirements are stipulated.

To ensure the audit report's independence, the Root CA event logs and internal audit reports are included in the annual Root CA operator ISMS audit report, audited by an accredited external auditor.

5.5.2 Background check procedures

Any background checks are performed in accordance with the Root CA operator ISMS security policy.

5.5.3 Training requirements

The personnel training plan is managed by the Root CA operator HR Group.

Trainees are required to familiarise themselves with the documentation issued to the appropriate role.

Trainees are required to observe a number of Root CA signing operations performed according to the schedule established by the Security Officer. Training is performed using the Root CA Test environment.

Trainees are subjected to a number of practical tests on the development / test systems under the supervision of a staff member appointed to the appropriate role.

A trainee is deemed qualified by a staff member appointed to the appropriate role.

5.5.4 Retraining frequency and requirements

Retraining is required in case of changes to the Root CA policies, procedures, or operations.

5.5.5 Job rotation frequency and sequence

Appointment to the administrator / operator and security officer roles are proposed by the NTS management authorised by the WPC PKI Policy Authority.

Appointments to the internal auditor role are proposed by the NTS management in accordance with the HR Group.

Operator smart card certificates and associated key activation data (i.e. PIN values) are changed on job rotation or new appointments.

No frequency or sequence for job rotation are stipulated.

5.5.6 Sanctions for unauthorized actions

Articles engaging the responsibility of Root CA operational personnel for their actions in carrying out their duties are defined in the NTS work contracts.

Articles engaging the responsibility of contractual staff for their actions in carrying out their duties are defined in their contract of employment.

5.5.7 Contracting personnel requirements

Only persons covered by the employment contracts are involved in the Root CA operations.

5.5.8 Documentation supplied to personnel

The Root CA operation staff are provided with the following documentation:

- NTS (Root CA operator) ISMS Policy;
- The WPC Root CA CP/CPS (this document);
- Root CA Secure operating procedures guidance;

The Root CA Security Officer is responsible for ensuring that staff are provided with up-to-date versions of the documentation.

5.6 Audit Logging Procedures

5.6.1 Types of event recorded

All significant security events in the Root CA system are automatically time stamped and recorded in the system log files. These include events such as:

- successful and failed attempts to initialise, remove, update, and recover public keys and data;
- successful and failed attempts to create, remove, login as, set, reset, and change passwords of, revoke privileges of, create, update, and recover access keys of Root CA operational personnel;
- successful and failed interactions with the Root CA database including connection attempts, read, update, and write operations made by the Root CA system and PKI software;
- all events related to certificate status information, security policy modification and validation, Root CA PKI software start-up and stop, database backup, certificate requests, key management, and audit trail;
- management and other miscellaneous events;
- system start-up and shutdown.

The Root CA Security Officer maintains information concerning:

- system configuration changes and maintenance;
- administrator privileges.

The internal auditor maintains:

- system integrity checking software;
- system integrity checking results;
- discrepancy and compromise reports.

The Root CA facility has an electronic monitoring and access control system that records physical access to the Root CA operational environment.

5.6.2 Frequency of system integrity checks

The operations schedule foresees that the internal auditors perform system integrity checks before starting and after completion of each Root CA certificate signing session.

The internal auditors investigate any alerts or irregularities in the integrity checks, and may quarantine the system, suspending operations until the alerts or irregularities are resolved.

The internal auditors have the right to request performance of system integrity checks outside the established operations schedule. Such “out of band” requests are submitted to the Security Officer who is required to make the necessary arrangements with the shortest possible delay.

Security incidents detected by the system integrity checks are defined in the Information Security Incident Management plan provided to the internal auditors.

5.6.3 Frequency of processing system logs

The operations schedule foresees that the internal auditors inspect system logs after completion of each signing session.

The auditors investigate any alerts or irregularities in the logs, and may quarantine the system, suspending operations until the alerts or irregularities are resolved.

The internal auditors have the right to inspect system logs outside the established operations schedule. Such “out of band” requests are submitted to the Security Officer who is required to make the necessary arrangements with the shortest possible delay.

Security incidents resulting from system log inspection are defined in the Information Security Incident Management plan provided to the internal auditors.

5.6.4 Retention period for audit log

The audit trails are retained indefinitely.

5.6.5 Protection of audit log

The audit logs are written to disk and tape media. The audit logs are backed up in the same process and same way as the production system environment and data.

5.6.6 Audit log backup procedures

The Root CA audit log consists of two parts:

1. system integrity check results;
2. dataset of signing session records.

The dataset of signing session records consists of:

1. the Root CA signature and CRL request database;
2. the Root CA signature request system log file;
3. Root CA cryptographic hardware log file.

This dataset is backed up in the same process and same way as the production system environment.

5.6.7 Audit collection system

Audit trail information is generated by the Root CA hardware, the Root CA PKI software, and the underlying operating system.

Information security incidents are recorded, reported and managed in the NTS RMA system, which collects incident information from all NTS operated systems.

5.6.8 Notification to event-causing subject

Event-causing subjects are not notified of logging and auditing events. Actions are logged and audited, but audit records are retained within the Root CA system.

5.6.9 Vulnerability assessments

The auditor role is provided with a baseline integrity check of Root CA system PKI software on entry into service of a new signing system. This provides integrity checking data on the immutable system files (e.g., operating system and application binaries, configuration files etc.).

The internal auditor role builds up a collection of session records and integrity checks in the course of system operation.

The internal auditor role is authorised to implement and perform any tests and checks on copies of the session records and integrity check data which it sees fit, in order to investigate susceptibility of the Root CA system to published vulnerabilities.

The Security Officer and auditor roles are encouraged to monitor on-line information sources (e.g. http://www.cert.org) for advisories and incident notes, and to evaluate whether these may have an impact on Root CA operations.

Tests may be performed on the Root CA Test system, using copies of Root CA data from the audit log sources.

5.7 Records Archival

5.7.1 Types of data archived

Different documents are provided in the execution of Root CA operations. These documents include:

- documents related to public key certification signing requests and their validation;
- CRL signing requests and their validation.

Some information provided is personal information and falls under the GDPR. This information is not stored in the Root CA systems. It is managed by the WPC, according to the WPC policy.

The types of events recorded in the Root CA system database include:

- data reception events;
- data preparation events;
- certificate issuance events;
- CRL signing request events.

5.7.2 Retention period for archive

Audit information, certificate signing requests and CRL signing request events are archived indefinitely.

Personal identification information related to CSR and CRL request validation is archived in accordance with GDPR regulation.

5.7.3 Protection of archive

The Root CA certificate signature request database is stand-alone and protected by physical security. Protection of the audit trail is as described in the corresponding section. The database archive media are protected by physical security in that they are retained in the same restricted access facility as the system, to which only the authorised Root CA operational staff have access.

5.7.4 Archive backup procedures

The Root CA certificate signature request system database, system logs, and cryptographic hardware logs are backed up regularly, as specified in corresponding sections.

The backup copies of the Root CA database require no assurances of confidentiality, as no sensitive data are held in that database.

The Root CA database may be copied from the backup held by the NTS management for the following purposes:

1. as the source of certificate signature request information for the Root CA quality assurance processes;
2. maintenance of copies used for training / documentation / operations analysis.

5.7.5 Requirements for time-stamping of records

The Root CA certificate signature request system clock is adjusted in the course of the system integrity checks performed on the day before signing operations. The system clock shall be adjusted to compensate for deviations greater than 5 minutes from local time.

System clock adjustments shall be notified to, and recorded by the internal auditor.

5.7.6 Archive collection system

The Root CA archive collection is a function of the Root CA PKI software. The backup facility for the system log files is described in corresponding sections, and is external to the Root CA PKI software. These data stores are archived on to separate media, copies of which are stored outside the Root CA operational protected area.

5.7.7 Procedures to obtain and verify archive information

Once per year, the archive media are retrieved by the Root CA Security Officer and internal auditor and verified to ensure that no damage or loss of data has occurred, by attempting a data recovery operation to the Root CA development / training test system. If any irregularity occurs during this operation, a new data backup is produced in the shortest possible delay.

5.8 Key Changeover

This section is not applicable to the CP/ CPS.

5.9 Compromise and Disaster Recovery

5.9.1 Incident and compromise handling procedures

Security incidents and compromise handling procedures are defined in the Information Security Incident Management plan provided to the Root CA administrators/operators and Security Officers.

Information security incidents are communicated in a manner allowing timely corrective action to be taken. Formal incident reporting and escalation procedures are established and communicated to all personnel. Responsibilities and procedures are established to handle information security incidents once they have been reported. Incident reporting is done in the NTS RMA system, which is used to collect, record and manage all incidents and incident related information from all NTS operated systems.

On detection of an incident, the Root CA certificate signature request system may be quarantined, and Root CA operations suspended, until the level of compromise has been established.

If data is lost on a virtual server or a granular file level recovery is needed, the NTS IT-administrator will contact the IT-partner and request the recovery. The IT-partner will perform the requested recovery and inform the NTS IT- administrator that the task has been completed. For a remote recovery to be possible, the NTS IT- administrator has to connect the “remote access” cable to the firewall prior to the restore operation to allow remote connections.

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

The steps for recovering a secure environment, depending on the nature of the disaster, are as follows:

1. Immediate replacement of certificate signature request system with backup or development systems;
2. Regeneration of Root CA PKI software from source code backups;
3. Recovery of Root CA database from backups;
4. Generation of new Security Officer and Administrator access keys;
5. Recovery and activation of Root CA secret key from backups;

If data is lost on physical servers, the recovery process is the same as above.

In case of a physical component failure, the NTS IT- administrator will inform the IT-partner of the issue. This will start the following process:

Notify IT-partner of the problem

1. IT-partner will notify IT vendor support about the faulty component
2. Connect the “remote access” cable to enable IT partner remote support
3. After the component has been changed, a system check is performed on the systems

If the IT-partner notices the component failure, it will start the following process:

1. Notify NTS IT- administrator of the problem
2. IT-partner will notify IT vendor support about the faulty component
3. Connect the “remote access” cable to enable IT partner remote support
4. After the component has been changed, a system check is performed on the systems

In case all data has been lost due for example to a RAID failure, all the data will be recovered from physical server disk backups. If the data from server disk backups is unavailable (for example a fire or flood situation), the whole infrastructure will be rebuilt and recovered from the last tape backup. To perform this recovery the following process will be started:

1. Purchase identical or nearly similar hardware from the selected IT-vendor / partner
2. Agree a date and time for the restore operation with the IT-partner
3. Install virtualisation environments on the selected host servers
4. Perform a “Bare Metal Recovery” recovery on the new server
5. After the server has been recovered, perform recovery of other infrastructure computers from the server tape backups using the backup software
6. Perform system check on all recovered servers

After these steps the infrastructure is in the state of the last functional tape backup.

Backup restorations are tested twice per year.

The risks for failure and the planned recovery methods are listed and maintained in the system documentation, which is regularly reviewed as part of the ISO/IEC 27001 certification process.

5.9.3 Root CA private key compromise procedures

In case of Root CA key compromise, the NTS team shall notify the WPC PKI Authority.

The NTS team and WPC PKI Authority shall convene an emergency meeting to identify a course of action.

Root CA key compromise is a critical incident which requires the resetting of the Root CA key ceremony and the Root CA operational system. The full action plan is defined in a subsequent risk management plan approved by the WPC PKI Authority.

5.9.4 Business continuity capabilities after a disaster

In case of a physical failure of the Root CA PKI system, the failure will always be reported to the IT vendor support who will provide a replacement part or server.

In case of a physical failure of the Root CA HSM system, the failure will always be reported to HSM vendor support who will provide a replacement device.

If the whole environment is lost for example in a fire, the whole environment will be rebuilt from the latest Tape backup which is stored in another location. In case of a fire would destroy the current secure environment, a compliant secure environment is identified. Once the new secure environment is in place, the recovery from backup can proceed. Reconstruction of a secure Root CA operational environment from off-site data backups, and most recent system image will be deployed in an alternative restricted access area.

5.10 Certification Authority or Registration Authority termination

The WPC is the owner of the WPC Root CA key material. On contract termination with NTS, key material shall be handed over to the WPC or WPC designated service provider.

The de-commissioning process will be specified in detail by the NTS security team together with the WPC PKI Policy Authority if or when contract termination with NTS is planned.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

The Key Pair Generation and Installation is defined in the Qi Specification – Authentication Protocol – Certificates.

Key pair generation and installation are performed by two entities:

1. the WPC Root CA
2. the MCSP

Both entities generate their respective entity public and private key pairs using methods and parameters defined in this section of the CP/CPS.

In all cases, key generation is performed on a secure hardware element which meets the requirements specified in this section of the CP/CPS.

The private keys are not provided to other entities as all entities generate their own key pairs and maintain the corresponding private key parts within the secure element.

The WPC Root CA public key is provided to the MCSP and Relying Parties using the TLS/SSL protected WPC website.

The MCSP public key is provided to the WPC Root CA in a Certificate Signing Request message signed by the MCSP applying for a certificate.

The WPC Root CA certificate key size is 256-bit elliptic curve and ECDSA with SHA-256 digest hash algorithm.

The Manufacturer CA certificate key size is a is 256-bit elliptic curve and ECDSA with SHA-256 digest hash algorithm.

The parameters, algorithms and identifiers are as follows:

- NIST-P256 (secp256r1) elliptic curve key, in accordance with specification Certicom-SEC-2 and NIST-SP800-186 with reference to RFC 5480, using the ASN1 object identifier 1.2.840.10045.3.1.7 (secp256r1);
- Certificate signatures use ECDSA-based digital signatures, as specified in ANSI-X9.62 and NIST-FIPS-186-4, using the ASN1 object identifier 1.2.840.10045.4.3.2 (ecdsa-with-SHA256)
- The digital signature secure hash is based on SHA-256 digest hash algorithm, as specified in NIST-FIPS-180-4 and ISO/IEC-10118-3 (Dedicated hash-functions Clause 10).

Parameters are generated and checked for quality by the certified hardware security module (HSM), which is parameterised to generate NIST P-256 ECC keys.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The WPC Root CA uses a certified cryptographic hardware security module for the generation and storage of the Root CA certificate keys, for signing of MCSP certificates and for signing of Certificate Revocation Lists.

The HSM operation is verified by means of internal tests prior to any cryptographic operations.

The HSM firmware upgrade status is checked once per year by the administrator.

The hardware security module (HSM) device the WPC Root CA utilises is a HSM system with a cryptographic module which meets the overall requirements applicable to Level 3 security in FIPS 140-2.

The table here below specifies the HSM security level:

NIST FIPS 140-2 Security Requirements Section	Level
Cryptographic Module Specification	3
Module Ports and Interfaces	3
Roles, Services and Authentication	3
Finite State Model	3
Physical Security	3
Operational Environment	N/A
Cryptographic Key Management	3
EMI/EMC	3
Self-Tests	3
Design Assurance	3
Mitigation of Other Attacks	3

The WPC Root CA private key is under n out of m multi-person control where at least two authorised operators are required to perform signing operations and at least two authorised administrators and Security Officers are required to perform HSM management operations.

WPC Root CA private key is not escrowed.

WPC Root CA private key is not archived.

The private key is backed up in an encrypted format. The key is encrypted using the HSM Master key and de-crypted using two-person control.

The private key is stored in the module in an encrypted form using the HSM Master Key.

The use of the private key is authorised to named operators, which use PKI smart cards and access credentials to authenticate the session. The HSM system is on stand-by mode and connected to a local management PC with two smart card readers. Once the key is activated by the operators, the key is active for the duration of the activation purpose (i.e. a signing ceremony. The deactivation of the private key includes logging out, turning the power off, removing the smart card and automatic deactivation due to time expiration or defined period of inaction.

In order to manage the WPC Root CA, authorised operators and WPC representatives are provided personalised smartcards with certificates. The WPC representatives are issued administration certificates and operators are issued management and operator certificates during the WPC Root CA Key Ceremony. The operator certificates are used to:

- Sign validation data
- Revoke MCSP CA certificates
- Request WPC agent certificates
- Revoke registration agent certificates
- Sign and encrypt files and messages

The Root CA operator shall also issue operator certificates on smartcards to authorised MCSP Personnel. These are called Registration Agent certificates and they are used to:

- Request Root CA certificates
- Sign and encrypt files and messages

The WPC Root CA private key shall not be destroyed in any other situation than when the HSM device is decommissioned. A written confirmation is requested from the WPC PKI Policy Authority before the private key is destroyed. The private key is destroyed using the overwriting mechanism provided by the certified HSM system.

6.3 Other Aspects of Key Pair Management

The WPC Root CA public key is archived by the Root CA Service Provider, on behalf of the WPC PKI Policy Authority. The public key is archived in the Root CA database under the PKI system control mechanisms and procedures. The CA database is signed for integrity assurance and is under the two-person control procedure for tamper protection and data integrity.

6.4 Activation Data

Activation data refers to data values other than whole private keys that are required to operate private keys or cryptographic modules containing private keys. These are PIN codes, passwords, portions of a private key used in a key-splitting scheme. Protection of activation data prevents unauthorized use of the private key during the entire life-cycle of the activation data from generation through archival and destruction.

The operator smart cards are protected using PIN codes, which are issued to the operators separately from the handing out of the smart card. The delivery of the card and the PIN code is done only after positive identification of the authorised operator. The operator shall not modify the PIN code and in case the PIN code is blocked, the card issuing authority is only authorised to unblock the PIN code after positive identification of the authorised card holder. The card issuing authority is the Root CA service provider hosting and managing the WPC Root CA environment.

The activation data for the HSM and PKI system accounts and roles defined and assigned during the Root CA Key Ceremony, are recorded in the Key Ceremony artefacts and sealed in tamper-evident security bags in a split-mode. The split-mode means that one part of the artefacts are stored in the safe at the Root CA service provider and another at the WPC PKI Policy Authority.

6.5 Computer Security Controls

The Root CA PKI specification is made available to the WPC. The PKI system is setup using the NTS security policy guidelines, which are part of the certified and audited ISMS.

The NTS IT systems, including the Root CA PKI system, use general-purpose, commodity IT hardware.

Security sensitive information is stored in FIPS 140-2 Level 3 approved hardware security modules. NTS may also use hardware security modules which are Common Criteria-certified according to the eIDAS Protection Profile (PP) EN 419 221-5 “Cryptographic Module for Trust Services”.

6.6 Life Cycle Security Controls

Access to the PKI system source code is limited to designated software developers.

Prior to accepting software for NTS operations, the Administrator:

- reviews source code for conformity with functional specifications;
- reviews the results of acceptance tests performed according to the acceptance test specification.

System software developers are excluded from NTS trusted roles.

6.7 Network Security Controls

The Root CA key management system is an HSM system connected to the secure production IT network. NTS has segregated and implemented the network architecture in such a way that access from the internet to the internal network domain, and from the internal network domain to the systems used to generate, manage and store cryptographic keys (including the HSMs), can be effectively controlled. The operational production environment where the Root CA HSM is operated, is physically segregated from any communications lines, wired or wireless, that may be connected to an outside network.

The NTS network architecture, including the use of firewalls and IDS/IPS is documented in confidential system specifications, which are a part of the ISMS and available only upon request.

6.8 Timestamping

Not applicable.

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

7.1.1 Root CA Certificate Profile

The WPC Root CA certificate profile shall be specified in Annex 1 of this CP/CPS.

7.1.2 MCSP CA Certificate Profile

The WPC MCSP CA certificate profile shall be specified in Annex 1 of this CP/CPS.

7.2 CRL Profile

The custom CRL profile is described in Annex 1 of this CP/CPS.

7.3 OCSP Profile

Not applicable: OCSP is not used.

8. Compliance Audit and Other Assessment

8.1 Compliance with legal provisions

The WPC Root CA service is operated in conformity with applicable requirements of the following European regulations:

- Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS);
- Regulation (EU) 2016/679 protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR).

The WPC Root CA provider ensures that personal data is processed in accordance with Regulation (EU) 2016/679 on General Data Privacy. In this respect, the WPC Root CA service processes only those personal identification data which are adequate, relevant and not excessive to conducting the service. The data protection practices are defined in the NTS privacy policy.

8.2 Frequency or circumstances of assessment

A full internal audit on the WPC Root CA operations is performed annually.

A formal Compliance audit of the WPC Root CA operations is included in the ISO/IEC 27001 and ISO 9001 maintenance audits, performed in intervals approved by the NTS Security Management Group.

The Compliance audit shall establish whether the requirements on the organisation and role to be audited, as described in this CPS, are being maintained.

The first Compliance audit shall be performed within 12 months of the start of the operations the Root CA.

If a Compliance audit finds no evidence of non-conformity, the next Compliance audit shall be performed within 24 months.

If a Compliance audit finds evidence of non-conformity, a follow-up Compliance audit shall be performed within 12 months to verify that the non-conformities have been solved.

8.3 Identity / Qualifications of Assessor

The Compliance audit shall be performed by an independent auditor.

The SMG shall appoint and approve the person to perform a Compliance audit.

The names of the auditors which will perform the audits shall be registered by the SMG.

The auditor shall possess significant knowledge of, and preferably be accredited for:

- performance of information system security audits;
- data protection regulation (privacy);
- PKI and cryptographic technologies;
- the operation of PKI software;
- the relevant industry good practices.

8.4 Assessor's Relationship to Assessed Entity

The auditor shall be independent and not connected to the organisation being the subject of the Compliance audit.

8.5 Topics Covered by Assessment

A Compliance audit shall cover compliance to this CPS and the associated procedures and techniques documented by the organisation shall be audited.

The scope of the Compliance audit shall be the implementation of the technical, procedural and personnel practices described in this CPS.

Some areas of focus for the Compliance audits shall be:

- identification and authentication;
- operational functions/services;
- physical, procedural and personnel security controls;
- technical security controls.

The Compliance audit shall assess the system logs/audit logs to be determined whether weaknesses are present in the security of the systems of the organisation to be audited.

Determined (possible) weaknesses shall be mitigated by the Assessed role and organisation.

The Compliance audit including the assessment and possible weaknesses shall be recorded and documented in the audit report.

8.6 Actions Taken as a Result of Deficiency

If deficiencies for non–conformity are discovered by the auditor, corrective actions shall be taken immediately by the Root CA operator.

The corrective actions shall be reported to the auditor who will approve them.

After the corrective actions have been fulfilled a follow-up audit shall take place within 12 months.

8.7 Communication of Results

The auditor shall report the full results of the Compliance audit to the NTS SMG, which will report to the Wireless Power Consortium PKI Policy Authority.

9. Other Business and Legal Matters

9.1 Fees

No stipulations.

9.2 Financial Responsibility

No stipulations.

9.3 Confidentiality of Business Information

All information that is not considered by the Wireless Power Consortium PKI Policy Authority to be public domain information is for Root CA service provider internal use only.

Information held in audit trails is restricted to the Root CA service provider and shall not be released outside the organisation, unless required by law, regulations, or provisions of this CPS.

The results of annual audits are restricted to the Root CA operator and the WPC PKI Policy Authority, with exceptions as outlined in Section 8.7 of this CPS.

Audit logs and archived records are not confidential to the Root CA provider.

The following information is public:

- WPC Root CA CPS redacted public version (this document)
- WPC Root CA CPS redacted public version Annex 1

9.4 Privacy of Personal Information

The Root CA service provider does not archive personal information subject to the collection, maintenance, retention and protection requirements of Regulation 2016/679 (General Data Protection Regulation - GDPR).

Personal identification information, contact information, and authorisations of the couriers transporting data between the WPC, MCSPs and the Root CA service provider are private.

Personal identification information, contact information, and authorisations of the Root CA service provider staff are private.

The public key certificates of MCSPs are not deemed private, but they are treated as business-confidential.

Personal information stored locally by the Root CA is restricted, and access is only granted to those with an official need-to-know.

9.5 Intellectual Property Rights

The software developed by NTS for the Root CA service provider is the property of CardPlus Group and CardPlus Sverige AB, which operates the Nordic Trust Services (NTS).

9.6 Representations and Warranties

The Root CA service provider warrants and promises to:

- provide WPC Administrator and MCSP Agent smartcards and related services (PIN code generation) consistent with this CPS;
- provide key management services including certificate signature request and certificate revocation list distribution in accordance with this CPS.

The Root CA service provider and its staff make no representations, warranties or conditions, express or implied, other than as expressly stated in this CPS.

9.7 Disclaimers of Warranties

The Root CA service disclaims all warranties and obligations of any type, including any warranty of merchantability, any warranty of fitness for a particular purpose, and any warranty of accuracy of information provided (except that it came from an authorised source), and further disclaims any and all liability for negligence and lack of reasonable care on the parts of subscribers and relying parties.

9.8 Limitations of Liability

The Root CA service provider, CardPlus Sverige AB, CardPlus Group or NTS, are not liable for any loss:

- of service due to war, natural disasters or other uncontrollable forces;

- incurred between the time certificate status changes and the next scheduled issuance of certificate status information;
- due to unauthorised use of keys issued by the Root CA provider, and use of keys beyond the prescribed use defined by this CPS;
- caused by fraudulent or negligent use of keys issued by the Root CA.

The Root CA service provider disclaims any liability of any kind whatsoever for any award, damages or other claim or obligation of any kind arising from tort, contract or any other reason with respect to any service associated with the issuance, use of, or reliance upon:

- the public/private key pair used by a subscriber or relying party;
- the administration or agent smartcard or encryption certificate used by a subscriber, relying party or other recipient.

Issuance of public keys by the Root CA service provider does not make CardPlus Sverige AB or CardPlus Group an agent, fiduciary, trustee, or other representative of requesters or relying parties, or others using the Root CA service.

Requesters are not eligible for compensation claims for losses resulting from inappropriate or fraudulent use of the provided services.

In addition, the Root CA service provider is not an intermediary to transactions between subscribers and relying parties. Claims against the Root CA service provider are limited to showing that it operated in a manner inconsistent with this CPS.

9.9 Indemnities

No stipulations.

9.10 Term and Termination

The Wireless Power Consortium PKI Policy Authority shall approve the Root CA service provider before it is allowed to commence operations.

The Wireless Power Consortium PKI Policy Authority shall approve this CPS before the Root CA service provider is allowed to commence operations.

Before the start of the operations of the Root CA service provider, the Wireless Power Consortium PKI Policy Authority shall carry out a preoperational assessment to obtain evidence that the organisation is able to operate in conformance to the requirements defined in the Service Agreement signed between the Wireless Power Consortium and CardPlus Group. The Wireless Power Consortium PKI Policy Authority shall ensure that this CPS complies with the Wireless Power

Consortium policies and standards. A Compliance audit shall be performed, as specified in Section 8.

This CPS becomes effective from the date of approval, and remains in force until amended, according to the amendment procedure of Section 9.12, or terminated.

The maximum term for the CPS corresponds to the lifetime of the WPCCA1 Root keys, defined in Annex 1 of this CPS.

Service agreements become effective from the date of signature by the two parties to the agreements and remain in force for the duration defined in the agreement, unless amended according to the procedure defined in the agreement itself.

9.11 Individual notices and communications with participants

Official notices and communications with MCSPs shall be in written form, and subject to the registration procedures for correspondence in force within the CPS.

Notice of severance or merger may result in changes to the scope, management and/or operation of the CPS. In such an event, this CPS may require modification as well.

Changes to the operations will occur consistent with the administrative requirements stipulated in Section 9.12 of this CPS.

9.12 Amendments

This CPS shall be reviewed in its entirety every year. Errors, updates, or suggested changes to this document shall be communicated to the NTS Security Management Group.

The procedure for amendment is the following:

a) Requests for changes to the CPS are reserved to the Wireless Power Consortium PKI Policy Authority.
b) Requests for changes shall be directed to the NTS Security Management Group. Such communication must include a description of the change with a rationale.
c) Notification of change requests will be communicated to the requestor by the NTS Security Management Group. The notification shall include the change request and the proposed effective date of change.
d) The Root CA service provider shall implement the requests with or without modifications, based on the comments received from the Wireless Power Consortium PKI Policy Authority.
e) Changes will be posted to the Wireless Power Consortium PKI Policy Authority. The amended CPS shall include the effective date of change.

The only changes that may be made to this CPS with no change to the document version number and no notification to the Wireless Power Consortium PKI Policy Authority are editorial or typographical corrections.

The Root CA service provider may change the contact information in section 2.4 with notification to the Wireless Power Consortium PKI Policy Authority but without change to the document version number.

All other changes to this CPS shall be made according to the amendment procedure.

9.13 Dispute Resolution Procedures

No stipulation.

9.14 Governing Law

No stipulation.

9.15 Compliance with Applicable Law

No stipulation.

9.16 Miscellaneous Provisions

No stipulation.

10. Other Provisions

10.1 Organizational

No stipulation.

10.2 Additional testing

No stipulation.

10.3 Disabilities

No stipulation.

10.4 Terms and conditions

No stipulation.

11. References

This WPC Root CA CPS is structured in accordance with the ETSI EN 309 411-1 standard and it draws its inspiration and good practices in part from the following industry and public standards:

- CA/Browser Forum (V1.7.3): " Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates"
- Certicom Research Standards for Efficient Cryptography v.2.0 (2010): “SEC 2: Recommended Elliptic Curve Domain Parameters”
- ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites".
- ETSI EN 319 401: "Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers".
- ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing certificates; Part 1: General requirements".
- IETF RFC 3647: “Internet X.509 Public Key Infrastructure – Certificate Policies and Certification Practices Framework” (obsoletes RFC 2527)
- IETF RFC 5280: “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL)”
- ISO/IEC 27002:2013: "Information technology - Security techniques - Code of practice for information security management"
- NIST FIPS PUB 140-2 (2001): "Security Requirements for Cryptographic Modules"

12. Definitions

12.1 Used Abbreviations

CA: Certification Authority

CP: Certificate Policy

CPS: Certification Practice Statement

ETSI: European Telecommunications Standards Institute

HSA: High Security Area

HSM: Hardware Security Module

IETF: Internet Engineering Task Force

ISMS: Information Security Management System

ISO: International Standards organization

ITU: International Telecommunications Union

MCSP: Manufacturer Certificate Authority Service Provider

MSCPA: Manufacturer CA Service Provider Agreement

PKI: Public Key Infrastructure

PTMC: Power Transmitter Manufacturer Code

QMS: Quality Management System

RA: Registration Authority

RCSP: Root Certificate Authority Service Provider

RFC: Request for Comments

SMG: Security Management Group

12.2 Used Terminology

ACCEPT (A CERTIFICATE)

- To approve of a digital certificate by a certificate applicant within a transactional framework.

ACCREDITATION

- A formal declaration by an approving authority that a certain function/entity meets specific formal requirements

APPLICATION FOR A CERTIFICATE

- A request sent by a certificate applicant to a CA to issue a digital certificate

ARCHIVE

- To store records for period of time for purposes such as security, backup, or audit.

ASSURANCES

- A set of statements or conduct aiming at conveying a general intention.

AUDIT

- Procedure used to validate compliance with formal criteria or controls.

AUTHENTICATION

- A process used to confirm the identity of a person or to prove the integrity of specific information by placing them within the right context and verifying such relationship.

AUTHORISATION

- Granting of rights.

AVAILABILITY

- The rate of accessibility of information or resources.

CERTIFICATE

- The public key of a subject and the associated information, digitally signed with the private key of the issuer of the certificate. Unless explicitly specified, the certificates described here are the subscriber's certificates.

CERTIFICATE REVOCATION LIST OR CRL

- A list maintained by the CA of certificates that are revoked before their expiration time.

CERTIFICATION AUTHORITY OR CA

- An entity that is trusted to associate a public key to the information on the subject, contained in the certificate. Unless explicitly specified, the CA described herein is the [COMPANY CA].

CERTIFICATION PRACTICE STATEMENT OR CPS

- A statement of the practices in the management of certificates during all life phases.

CERTIFICATE CHAIN

- A hierarchical list certificates containing a subscriber certificate and CA certificates.

CERTIFICATE EXPIRATION

- The end of the validity period of a digital certificate.

CERTIFICATE EXTENSION

- A field in the digital certificate used to convey additional information on issues that include: the public key, the certified subscriber, the certificate issuer, and/or the certification process.

CERTIFICATE HIERARCHY

- A level-based sequence of certificates of one (root) CA and subordinate entities that include, CAs and subscribers.

CERTIFICATE MANAGEMENT

- Actions associated with certificate management include storage, dissemination, publication, revocation, and suspension of certificates.

CERTIFICATE REVOCATION LIST (CRL)

- A list issued and digitally signed by a CA that includes revoked and suspended certificates. Such list is to be consulted by relying parties at all times prior to relying on information featured in a certificate.

CERTIFICATE SERIAL NUMBER

- A sequential number that uniquely identifies a certificate within the domain of a CA.

CERTIFICATE SIGNING REQUEST (CSR)

- A machine-readable application form to request a digital certificate.

CERTIFICATION

- The process to issue a digital certificate.

CERTIFICATION AUTHORITY (CA)

- An authority (WPC Root CA) that issues, suspends, or revokes a digital certificate.

CERTIFICATE POLICY (CP)

- A statement of the practices of a CA and the conditions of issuance, suspension, revocation etc. of a CA certificate.

CERTIFICATE ISSUANCE

- Delivery of X.509 v3 digital certificates.

CERTIFICATE SUSPENSION

- Online service used to temporarily disable a digital certificate and to automatically revoke it if no request for re-activating it is submitted within a certain time period

CERTIFICATE REVOCATION

- Online service used to permanently disable a digital certificate before its expiration date

CERTIFICATE REVOCATION LISTS

- Online publication of complete and incremental digital certificates revocation lists compliant with RFC 2459

REGISTRATION AUTHORITY OR RA

- An entity that has the responsibility to identify and authenticate subscribers. The RA does not issue certificates. It merely requests the issuance of a certificate on behalf of applicants whose identity it has verified.

RELYING PARTY

- Any entity that relies on a certificate for carrying out any action.

REPOSITORY

- A database and/or directory listing digital certificates and other relevant information accessible on-line.

REVOKE A CERTIFICATE

- To permanently end the operational period of a certificate from a specified time forward.

SIGNATURE

- A method that is used or adopted by a document originator to identify himself or herself, which is either accepted by the recipient or its use is customary under the circumstances.

SIGNER

- A person who creates a digital signature for a message, or a signature for a document.

SMARTCARD

- A hardware token that contains a chip to implement among others cryptographic functions.

SUBJECT OF A DIGITAL CERTIFICATE

- The named party to which the public key in a certificate is attributable, as user of the private key corresponding to the public key.

SUBSCRIBER

- The subject of a digital certificate, or a party designated by the subject to apply for the certificate.

SUBSCRIBER AGREEMENT

- The agreement between a subscriber and a CA for the provision of public certification services.

TRUSTED ROLE

- A role within a CA that includes access to or control over cryptographic operations that may allow for privileged access to the issuance, use, suspension, or revocation of certificates, including operations that restrict access to a repository.

TRUSTED SYSTEM

- Computer hardware, software, and procedures that provide an acceptable level against security risks, provide a reasonable level of availability, reliability, and correct operation and enforce a security policy.

WPC ROOT CA PRIVATE CERTIFICATION SERVICES

- A private digital certification system made available by WPC as well as the entities that belong to the Consortium domain as described in this CPS.

WPC ROOT CA PROCEDURES

- A document describing the WPC Root CA's internal procedures with regard to registration of Manufacturers and Manufacturer CA Service Providers, and information security practices.

X.509

- The standard of the ITU-T (International Telecommunications Union-T) for digital certificates.

Annex 1: Description of the Certificate and CRL Profiles

WPC Root CA Certificate Profile

Field	OID	Data type	Value*	Example
Version		INTEGER	0x02 {=X.509v3}	0x02
serialNumber		INTEGER	A unique number up to 9 bytes in length	0x01 10 20 30 40 50 60 70
signature	1.2.840.10045.4.3.2 {ecdsa-with-SHA256}		n/a	
issuer	2.5.4.3 {Common Name}	'UTF8String'	"WPCCA"+ one character suffix denoting different root CA instances	"WPCCA1"
validity.notBefore		Either GeneralizedTime for any year, or UTCTime for years prior to 2050	Any value (not used by PRx)	
validity.notAfter		GeneralizedTime	9999-12-31 23:59:59	9999-12-31 23:59:59
subject	2.5.4.3 {Common Name}	UTF8String	Same as "issuer"	"WPCCA1"
subjectPublicKeyInfo.algorithm	1.2.840.10045.2.1 {ecPublicKey}		n/a	
	1.2.840.10045.3.1.7		n/a	

Field	**OID**	**Data type**	**Value***	**Example**
	{secp256r1}			
subjectPublicKeyInfo.subjectPublicKey		BIT STRING	(Public Key value; optionally may use compressed point representation)**	
Extensions.1	2.5.29.19 {basicConstraints}		n/a	
Extensions.1.critical		BOOLEAN	TRUE	TRUE
Extensions.1. extnValue.cA		BOOLEAN	TRUE	TRUE
Extensions.1. extnValue.pathLenConstraint	this shall not be present	n/a	n/a	n/a

Manufacturer CA Service Provider Certificate Profile

Field	OID	Data type	Value*	Example
Version		INTEGER	0x02 {=X.509v3}	0x02
serialNumber		INTEGER	A unique number up to 9 bytes in length	0x01 10 20 30 40 50 60 70
signature	1.2.840.10045.4.3.2 {ecdsa-with-SHA256}		n/a	
issuer	2.5.4.3 {Common Name}	UTF8String	"WPCCA"+ one character suffix denoting different root CA instances	"WPCCA1"
validity.notBefore		Either Generalized Time for any year, or UTCTime for years prior to 2050	Any value (not used by PRx)	
validity.notAfter		Either Generalized Time for any year, or UTCTime for years prior to 2050	Any value (not used by PRx)	9999-12-31 23:59:59

Field	OID	Data type	Value*	Example
subject	2.5.4.3 {Common Name}	UTF8String	7 bytes string consisting of: · Four upper-case characters containing a PTMC hex value · one character containing a dash · two arbitrary alpha-numeric characters	"CACA-1A"
subjectPublicKeyInfo.algorithm	1.2.840.10045.2.1 {ecPublicKey}		n/a	
	1.2.840.10045.3.1.7 {secp256r1}		n/a	
subjectPublicKeyInfo.subjectPublicKey		BIT STRING	(Public Key value; optionally may use compressed point representation)**	
Extensions.1	2.5.29.19 {basicConstraints}		n/a	
Extensions.1.critical		BOOLEAN	TRUE	TRUE
Extensions.1. extnValue.cA		BOOLEAN	TRUE	TRUE
Extensions.1. extnValue.pathLenConstraint		INTEGER	0	0x00
Extensions.2	2.23.255.1.1 {wpc-qi-policyFlags}		n/a	
Extensions.2.critical		BOOLEAN	TRUE	TRUE
Extensions.2. extnValue		OCTET STRING	4 bytes reserved for future use	0x00 00 00 00

Certificate Revocation List Structure

The CRL used by WPC and signed by the Root CA is a custom CRL with the below structure.

```
<?xml version="1.0"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">
<xs:element name="WPCCRL">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="issuer" type="xs:string"/>
      <xs:element name="sequence-no" type="xs:integer"/>
            <xs:element name="date-issued" type="xs:date"/>
            <xs:element ref="CRL"/>
    </xs:sequence>
            <xs:attribute name="crl-version" type="xs:string"/>
  </xs:complexType>
</xs:element>
<xs:element name="CRL">
  <xs:complexType>
            <xs:choice maxOccurs="unbounded" minOccurs="0">
              <xs:element ref="revoke-qi-id"/>
              <xs:element ref="revoke-manufacturer-certificate"/>
              <xs:element ref="revoke-batch-certificates"/>
            </xs:choice>
  </xs:complexType>
</xs:element>
<xs:element name="revoke-qi-id">
  <xs:complexType>
    <xs:sequence>
                        <xs:element name="qi-id" type="xs:integer"/>
            <xs:element name="reason" type="xs:string"/>
            <xs:element name="decision" type="xs:integer"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="revoke-batch-certificates">
  <xs:complexType>
    <xs:sequence>
    <xs:element name="issuer-id" type="xs:string"/>
            <xs:element name="rsid min" type="xs:string"/>
    <xs:element name="rsid max" type="xs:string"/>
            <xs:element name="reason" type="xs:string"/>
            <xs:element name="decision" type="xs:integer"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="revoke-manufacturer-certificate">
  <xs:complexType>
    <xs:sequence>
            <xs:element name="manufacturer-serial" type="xs:integer"/>
            <xs:element name="reason" type="xs:string"/>
            <xs:element name="decision" type="xs:integer"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
</xs:schema>
```