Detailed FPKI

Yongzhe Xu

April 2022

1 Some Words

The document only gives an overview of the design. The data structure might be changed (slightly) during the implementation, and some logics or procedures might be changed during the implementation. However, the main idea will not be changed.

2 Overview

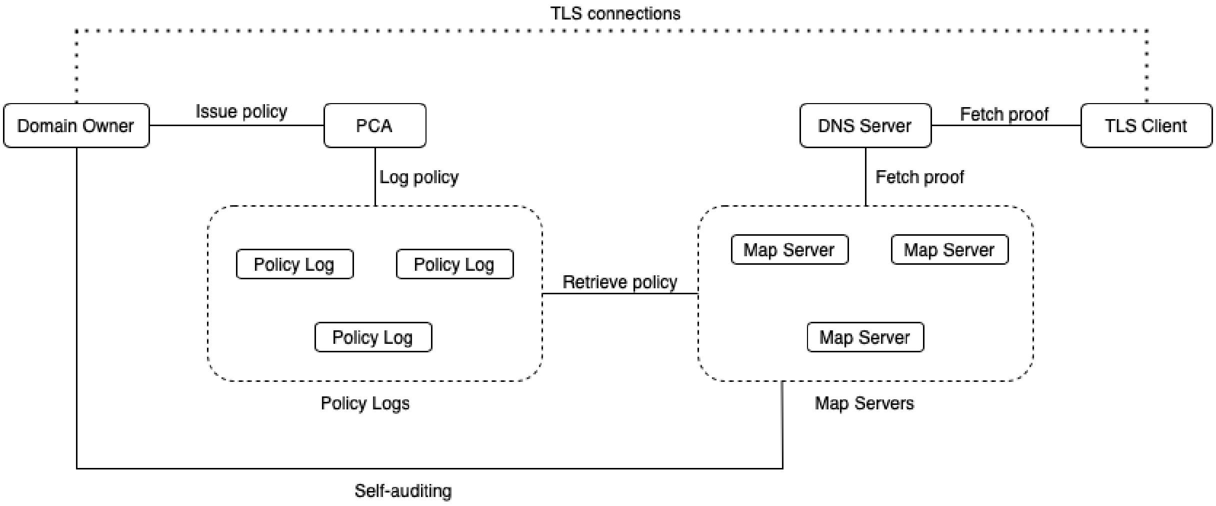


Figure 1: Overview

There are six components in the FPKI:

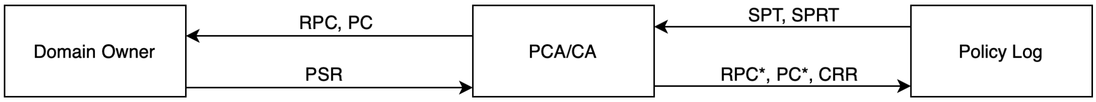
- **Domain owner**: Legitimate owner of the domain.
- **Policy Certificate Authority (PCA)**: Authority which is responsible for issuance and revocation of the Root Policy Certificate (RPC) and Policy Certificate (PC). PCA will be an additional department in the normal CA, and PCA will not influence the existing functionalities of the CA. To support FPKI, CA should have at least one PCA.
- **Policy log**: A group of logs that record all the RPCs, PCs, and revocations.
- **Map server**: A group of servers that collect RPCs, PCs, and revocations from all the policy logs, then categorise them according to domain names and CAs. It is similar to a Certificate Transparency monitor.
- **DNS server**: Except for the DNS server's standard functionalities, it is also responsible for collecting proofs of certain domains from map servers and distributing them to the TLS client.
- **TLS client**: TLS clients which use the FPKI.

The domain owner contacts PCA to issue or revoke RPC and PC for its domain. Then the PCA logs the RPC, PC, and revocations in the policy logs, and returns them to the domain owner. The map server will periodically fetch the RPC, PC, and revocations from all the policy logs, and updates its database. DNS server will periodically fetch the policies of domains and distributes them to the TLS clients. During the establishing of the TLS connection, the TLS client will query the DNS server for policies and verify the policies. Based on the policies, the TLS client will decide whether to accept the certificate from the web server. All these operations will run asynchronously.

3 Data Structure

This section defines seven data structures. Details of each data structure will be introduced in the following sections.

- **Proof**: Data structure which is returned from the map server. It contains all the RPCs, PCs and revocations of the target domain and its parent domains. Proof of Inclusion (PoI) and Signed Tree Head (STH) are also included, thus the proof is verifiable.
- **Policy Certificate (PC)**: Policy certificate defines the current policies of the domain. It is issued by PCA. Every PC must have a valid signature from RPC.
- **Root Certificate Signing Request (RCSR)**: It is generated by the domain owner and sent to the PCA. PCA will generate a RPC according to the PCSR.
- **Root Policy Certificate (RPC)**: The certificate which is issued by PCA and owned by the domain owner. At any time, there will only be one valid RPC from every PCA for every domain.
- **Signed Policy Timestamp (SPT)**: It is generated by the policy log when the new policy or RPC is logged by the policy log. It records the STH of the policy log and PoI of the PC or RPC. Everyone can audit the policy log using the SPT.
- **Signed Policy Revocation TimeStamp (SPRT)**: It is generated by the policy log when the CRR is logged by the policy log. It records the STH of the policy log and PoI of the CRR. Everyone can audit the policy log using the SPRT.
- **Policy Signing Request (PSR)**: It is generated by the domain owner when the domain owner wants to issue a new PC. The PSR will be sent to a specific PCA.
- **Certificate Revocation Request (CRR)**: It is used to revoke one specific PC or RPC. CRR is generated by PCA. Revocation of domain certificate is also possible by submitting a CRR (Assume every CA has one PCA).



* The RPC and PC from CA to Policy log do not contain SPTs. Once the Policy Log returns the SPTs, the SPTs will be attached to RPC and PC.

Figure 2: Information Flow

Figure 2 illustrates the information flow between domain owner, PCA and policy log.

4 General Rules

Some general rules:

- If the RPC is revoked, the PC signed by this RPC will also become invalid.

- When a domain owner wants to issue a new RPC, he must issue a PC at the same time. Once the old RPC is replaced by the new RPC, the old policy will also become invalid. It's possible to make this optional (issue RPC without new PC). But human is prone to mistakes, so it is recommended to make this mandatory.
- RPC and PC in the Merkle Tree of policy log do not contain SPTs. SPT will be generated and attached to the RPC or PC, and then the complete RPC and PC will be delivered to PCA and map server. In short, the RPC and PC in the Merkle Tree do not contains SPT, but the RPC and PC received by PCA, domain owner, map server and TLS client will have SPTs.
- RPC can not be used between different CAs. For example, if RPC is issued by CA1, it can not be used for signing Policy for CA2.
- Every Max Merge Delay (MMD), every PCA can issue at most one RPC for every domain.

4.1 Proof

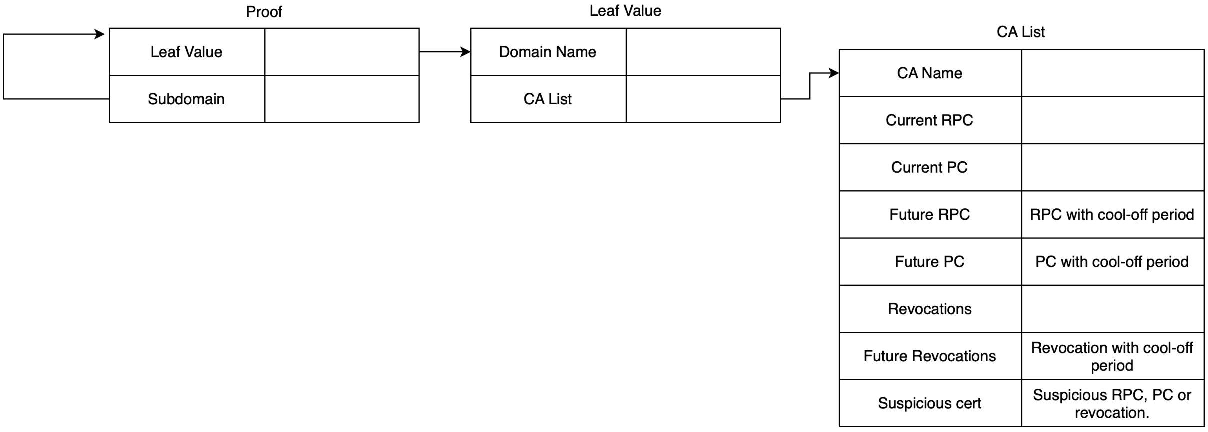
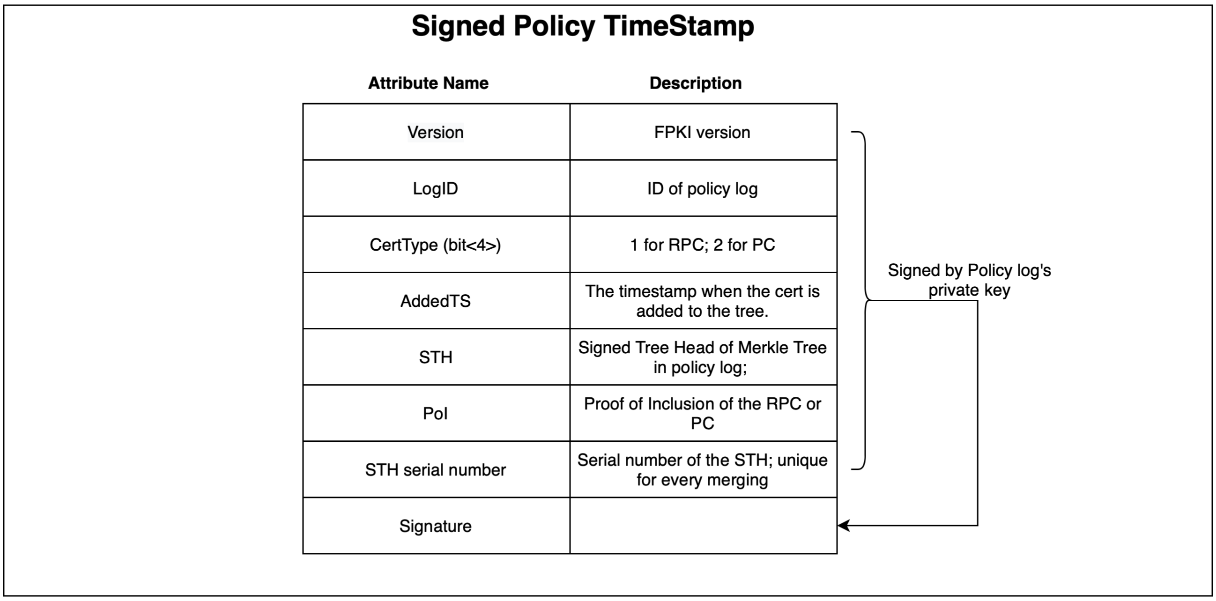


Figure 3: Proof

Figure 3 illustrates the simplified structure of the Proof (Omit the STH and PoI. Details will be added during the implementation). One proof will contain one or several leaves, and every leaf represents the policies of one domain or its parent domain. Every leaf will have a list of CAs, and every element in the list contains the RPC, PC, and revocation for this domain. Every field whose name contains "future" is used for the cool-off period. The suspicious cert field records all the suspicious certificates.

For the client, only the "Current RPC", "Current PC" and "Revocations" are valid. All other fields should be omitted. The client can also monitor the "future" field, but this is optional.

4.2 Signed Policy Timestamp



Signed Policy TimeStamp

Attribute Name	Description
Version	FPKI version
LogID	ID of policy log
CertType (bit<4>)	1 for RPC; 2 for PC
AddedTS	The timestamp when the cert is added to the tree.
STH	Signed Tree Head of Merkle Tree in policy log;
PoI	Proof of Inclusion of the RPC or PC
STH serial number	Serial number of the STH; unique for every merging
Signature	

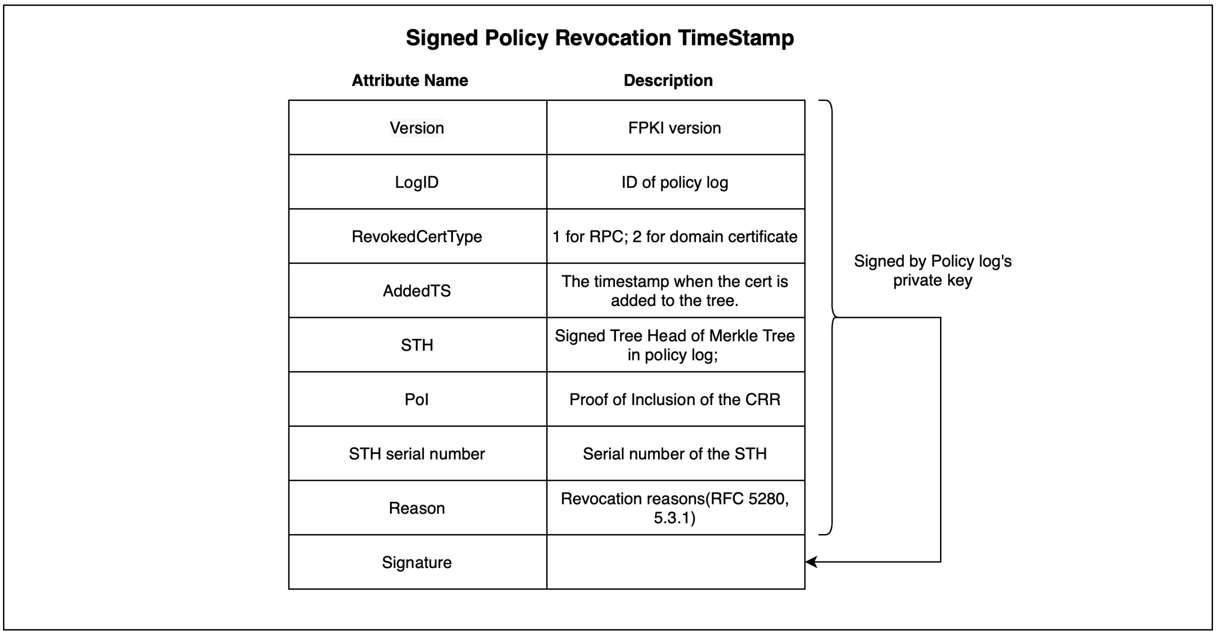
Figure 4: Signed Policy Timestamp

SPT will be generated by the policy log after the policy log adds the RPC or Policy. Different from the Signed Certificate Timestamp (SCT) in Certificate Transparency (CT), the SPT is proof that the RPC or Policy is already added to the policy log. Figure 4 illustrates the structure of SPT. The field "STH serial number" should be increased by one after every merging, and every merge will have a unique serial number. The field "Signed Tree Head (STH)" and "Proof of Inclusion (PoI)" include the necessary data to verify the inclusion of the certificate. Using "STH" and "PoI", one can easily verify that the certificate is added to the log.

One idea is to make SPT similar to SCT. After the policy log sees the RPC or PC, the policy log will immediately return an SPT, rather than after adding the RPC or PC. In this case, the SPT will not contain STH and PoI. However, SPT with STH and PoI will have the following benefits:

- The TLS client can verify the RPC or PC without privacy issues since the SPT contains the STH and PoI. The policy log will not know who is trying to verify what certificate.
- Malicious policy log can issue an SPT without actually adding the RPC or PC to the tree. The misbehavior will not be discovered until the promised time. However, if the STH and PoI are added, the policy log can not do this, because it needs to add the RPC or PC to generate the SPT.

4.3 Signed Policy Revocation TimeStamp



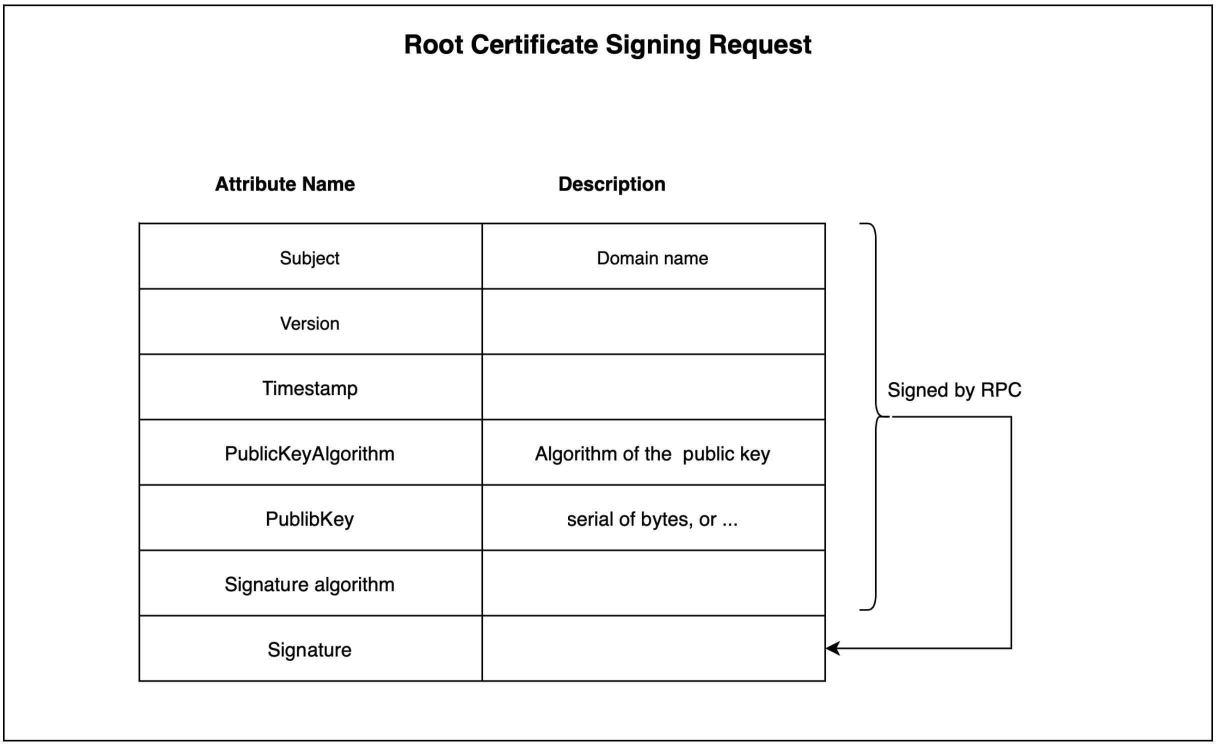
Signed Policy Revocation TimeStamp

Attribute Name	Description
Version	FPKI version
LogID	ID of policy log
RevokedCertType	1 for RPC; 2 for domain certificate
AddedTS	The timestamp when the cert is added to the tree.
STH	Signed Tree Head of Merkle Tree in policy log;
PoI	Proof of Inclusion of the CRR
STH serial number	Serial number of the STH
Reason	Revocation reasons(RFC 5280, 5.3.1)
Signature	

Figure 5: Signed Policy Revocation TimeStamp

Signed Policy Revocation TimeStamp (SPRT) is similar to SPT, while it has an extra field ”reason”, which records the reason for the revocation. The possible values of ”reason” field will follow the RFC 5280 Section 5.3.1. There is no SPRT for the PC, because PC can not be revoked.

4.4 Root Certificate Signing Request



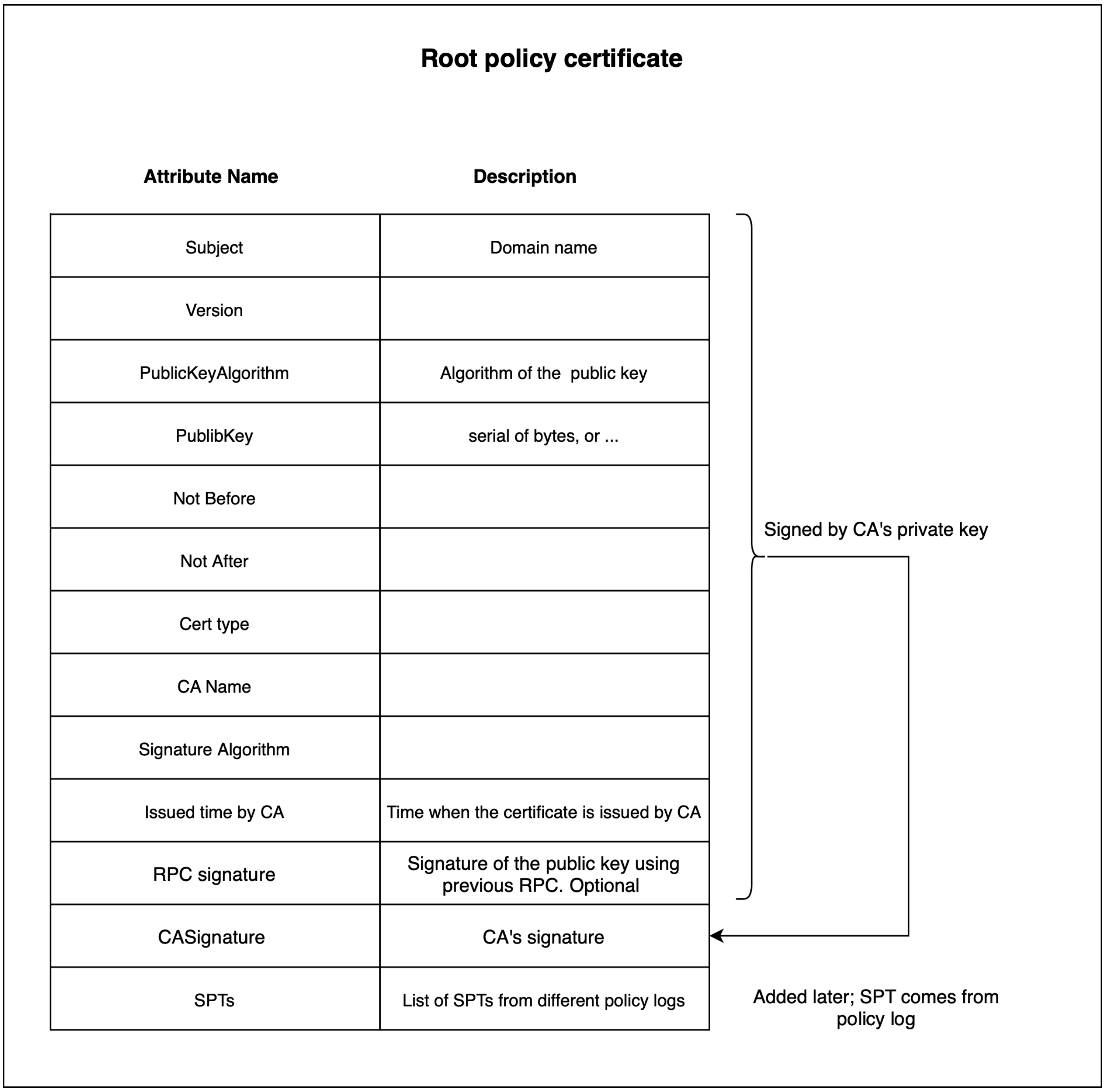
Root Certificate Signing Request

Attribute Name	Description
Subject	Domain name
Version	
Timestamp	
PublicKeyAlgorithm	Algorithm of the public key
PublibKey	serial of bytes, or ...
Signature algorithm	
Signature	

Figure 6: Root Certificate Signing Request

RCSR will be generated by domain owner, and sent tot PCA.

4.5 Root Policy Certificate



Root policy certificate

Attribute Name	Description
Subject	Domain name
Version	
PublicKeyAlgorithm	Algorithm of the public key
PublibKey	serial of bytes, or ...
Not Before	
Not After	
Cert type	
CA Name	
Signature Algorithm	
Issued time by CA	Time when the certificate is issued by CA
RPC signature	Signature of the public key using previous RPC. Optional
CASignature	CA's signature
SPTs	List of SPTs from different policy logs

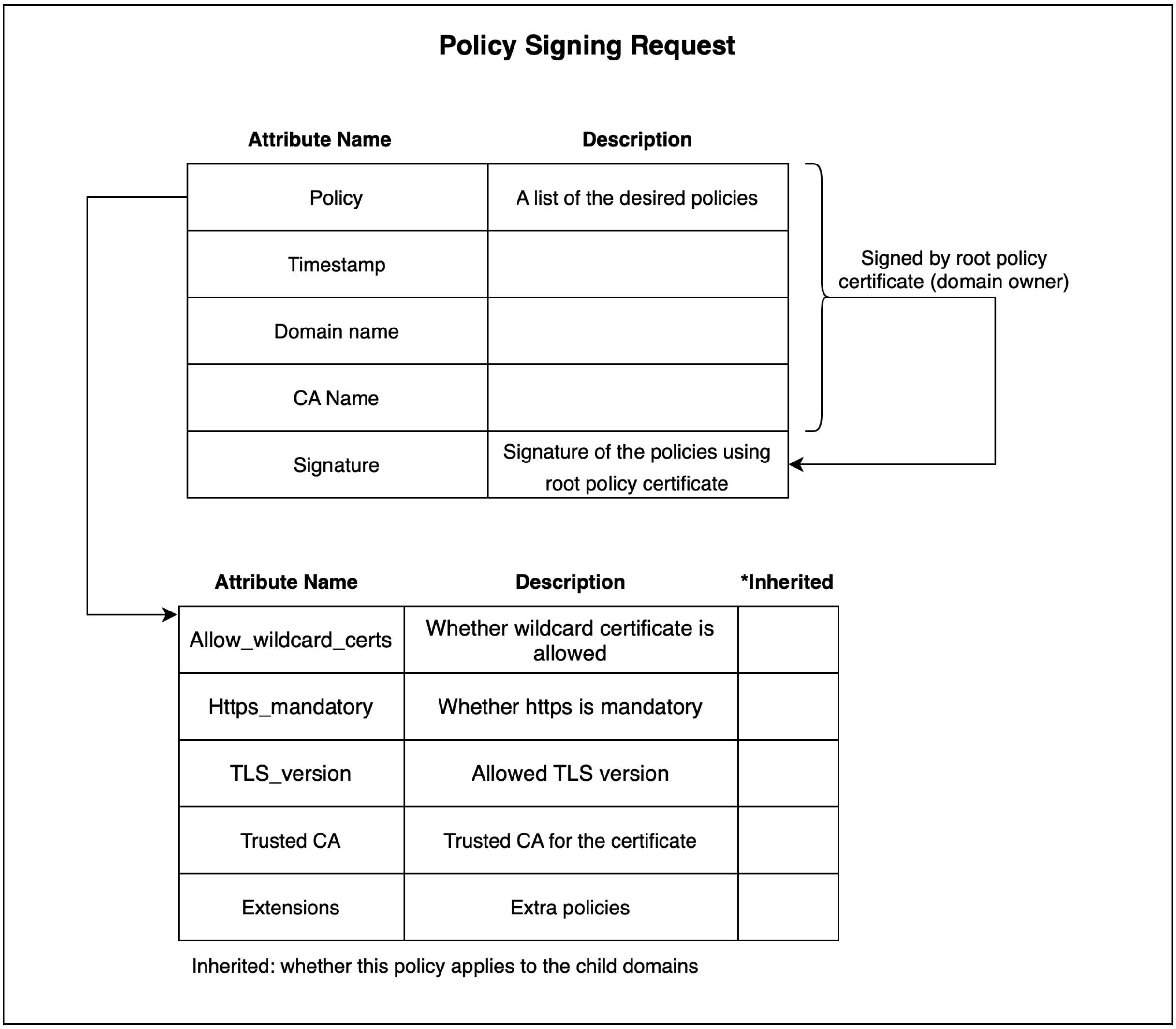
Signed by CA's private key
Added later; SPT comes from policy log

Figure 7: Root Policy Certificate

Figure 7 illustrates the structure of RPC. Except for normal X509 certificate fields, RPC will contain a list of SPTs and the issued time by CA. The later field is used to avoid the race condition between policy logs when PCA registers RPC and PC at different policy logs in different orders. SPT will be returned from the policy log after the RPC (without SPT) is logged. Then the SPT will be added to the final RPC by PCA. The RPC distributed by policy log will also have SPTs.

”RPC signature” field will contains the signature using previous RPC. If the signature is correct, the RPC can bypass cool-off period.

4.6 Policy Signing Request



Policy Signing Request

Attribute Name	Description
Policy	A list of the desired policies
Timestamp	
Domain name	
CA Name	
Signature	Signature of the policies using root policy certificate

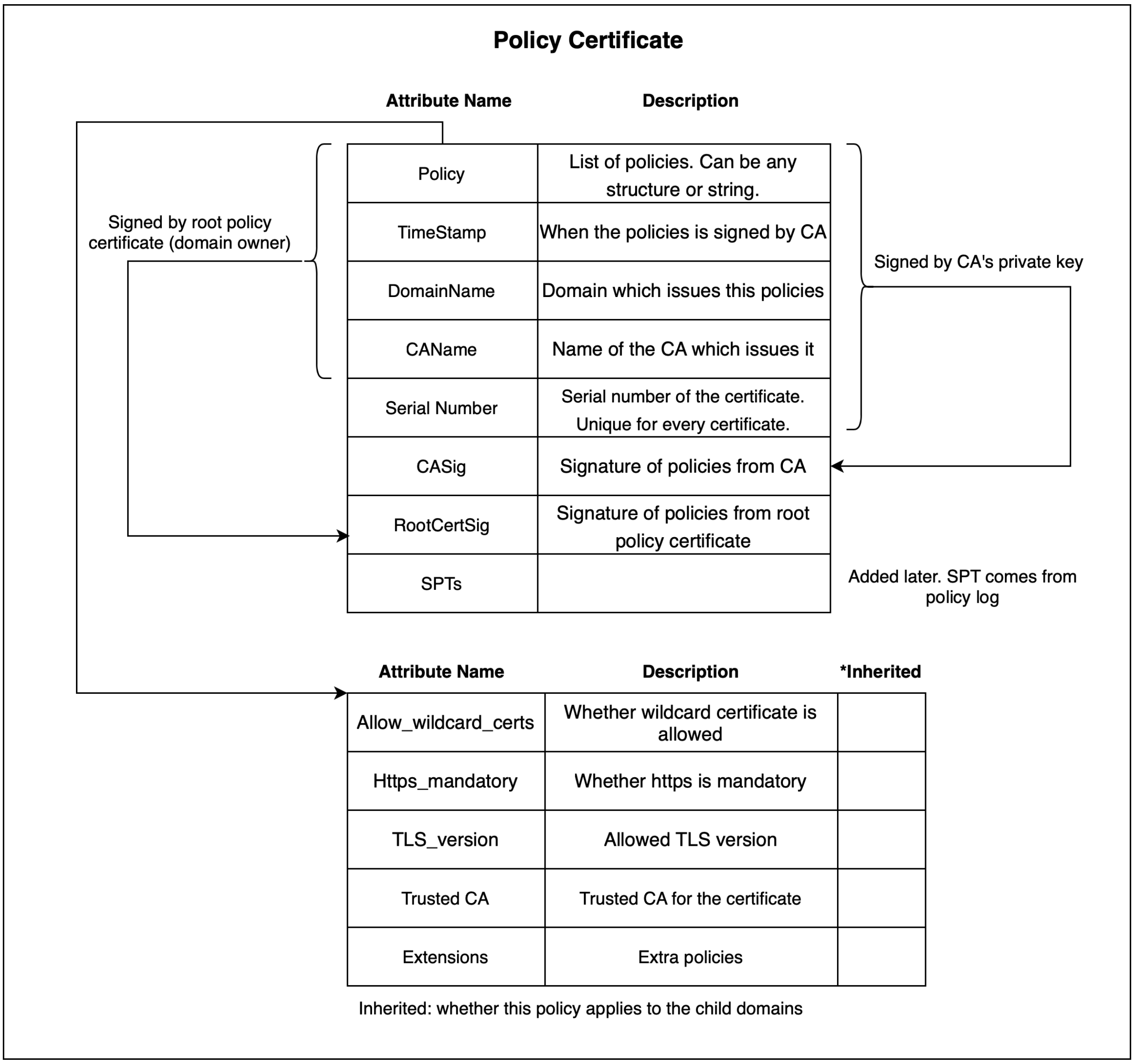
Attribute Name	Description	*Inherited
Allow_wildcard_certs	Whether wildcard certificate is allowed	
Https_mandatory	Whether https is mandatory	
TLS_version	Allowed TLS version	
Trusted CA	Trusted CA for the certificate	
Extensions	Extra policies	

Inherited: whether this policy applies to the child domains

Figure 8: Policy Signing Request

PSR will be generated by the domain owner. It contains the new policies and a signature from the RPC. The signature from RPC is mandatory.

4.7 Policy Certificate



Policy Certificate

Attribute Name	Description
Policy	List of policies. Can be any structure or string.
TimeStamp	When the policies is signed by CA
DomainName	Domain which issues this policies
CAName	Name of the CA which issues it
Serial Number	Serial number of the certificate. Unique for every certificate.
CASig	Signature of policies from CA
RootCertSig	Signature of policies from root policy certificate
SPTs	

Attribute Name	Description	*Inherited
Allow_wildcard_certs	Whether wildcard certificate is allowed	
Https_mandatory	Whether https is mandatory	
TLS_version	Allowed TLS version	
Trusted CA	Trusted CA for the certificate	
Extensions	Extra policies	

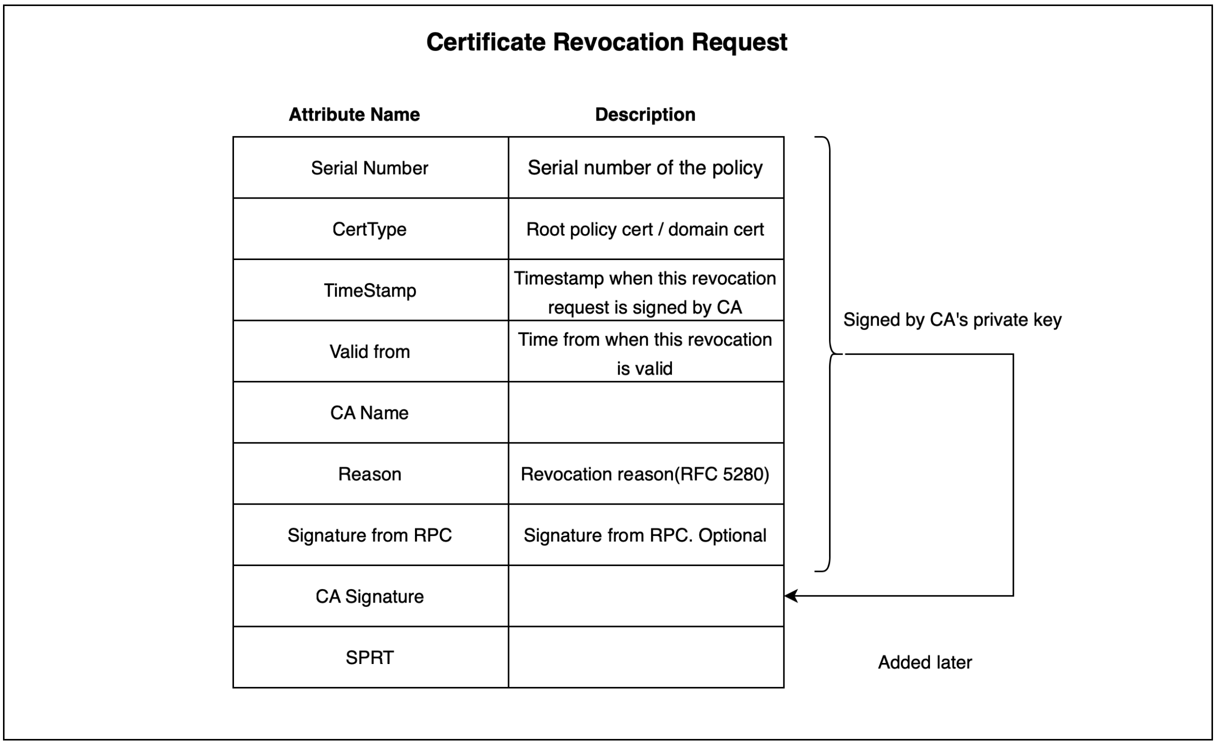
Inherited: whether this policy applies to the child domains

Signed by root policy certificate (domain owner)
Signed by CA's private key
Added later. SPT comes from policy log

Figure 9: Policy Certificate

Figure 9 illustrates the structure of the PC. Every PC will have two signatures. One from the PCA, and the other from the RPC. The policy also has an ”SPTs” field to contains multiple SPTs from different policy logs. SPTs will be added later.

4.8 Certificate Revocation Request



Certificate Revocation Request

Attribute Name	Description
Serial Number	Serial number of the policy
CertType	Root policy cert / domain cert
TimeStamp	Timestamp when this revocation request is signed by CA
Valid from	Time from when this revocation is valid
CA Name	
Reason	Revocation reason(RFC 5280)
Signature from RPC	Signature from RPC. Optional
CA Signature	
SPRT	

Figure 10: Certificate Revocation Request

The CRR will be generated by CA and logged by policy log. Signature of RPC is optional.

5 Issuance and Update

It is not necessary to revoke a PC, because the compromise of the PC is not an attack (it does not have a private key). In other words, a PC can not be ”compromised”. The domain owner can simply issue a new PC and overwrite the previous one. So to standardise the management of PC, the PC can only be updated. If the domain owner has the private key of RPC, then the updating of the PC will become valid immediately.

The RPC can be revoked or updated. Because if the RPC is compromised, the attacker can issue a PC in certain circumstances. Once the RPC is revoked, the PC signed by the RPC will also become invalid. There is no specific protocol for updating. The new one will overwrite the previous one.

For the issuance and updating of RPC, a cool-off period might apply. One RPC that has a signature from the current RPC can bypass the cool-off period. More information in Appendix A.

5.1 Issuance of Root Policy Certificate

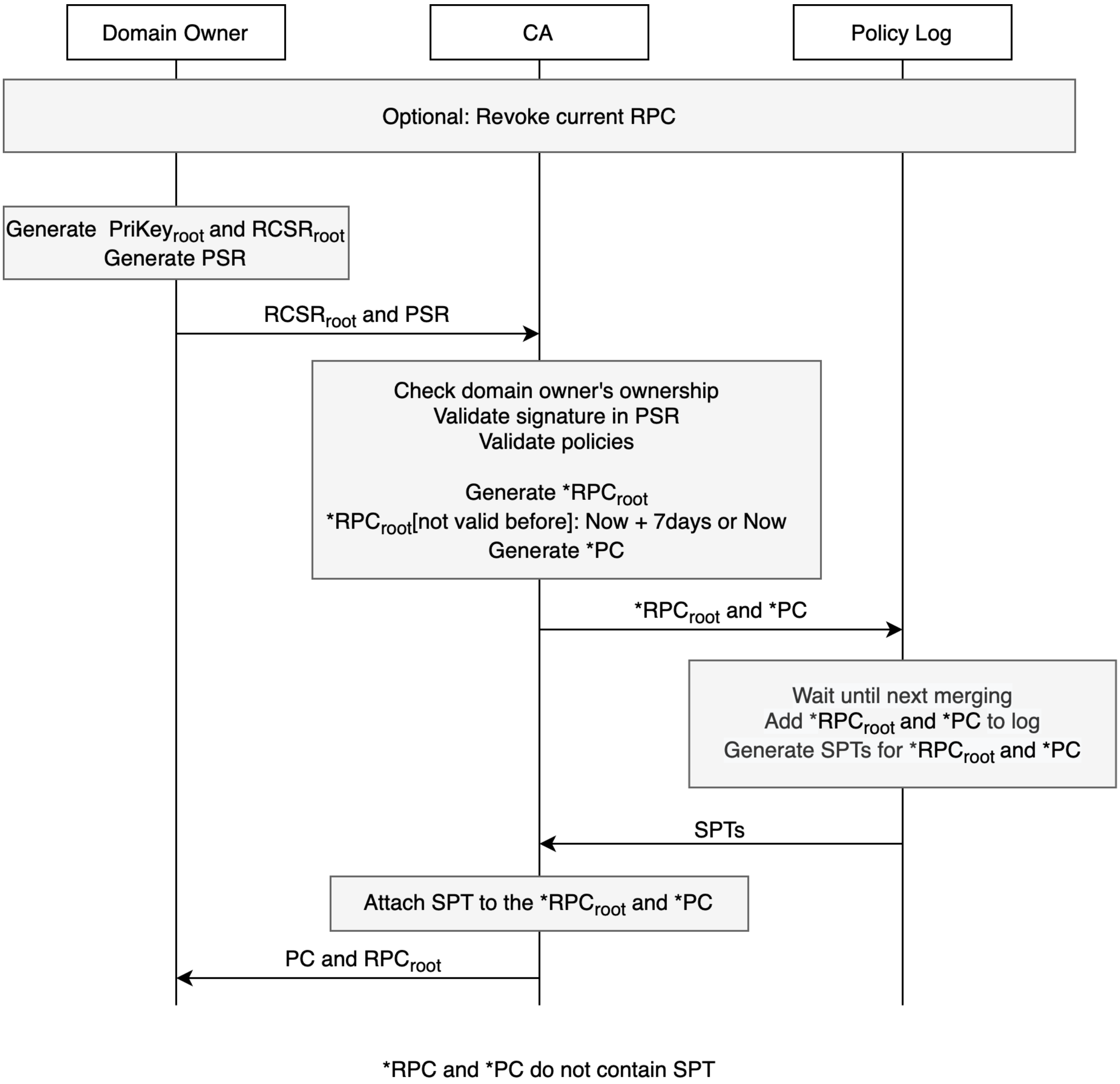

Domain Owner
CA
Policy Log
Optional: Revoke current RPC
Generate PriKey$_{root}$ and RCSR$_{root}$
Generate PSR
RCSR$_{root}$ and PSR
Check domain owner's ownership
Validate signature in PSR
Validate policies
Generate *RPC$_{root}$
*RPC$_{root}$[not valid before]: Now + 7days or Now
Generate *PC
*RPC$_{root}$ and *PC
Wait until next merging
Add *RPC$_{root}$ and *PC to log
Generate SPTs for *RPC$_{root}$ and *PC
SPTs
Attach SPT to the *RPC$_{root}$ and *PC
PC and RPC$_{root}$
*RPC and *PC do not contain SPT

Figure 11: Issuance of new RPC

Figure 11 illustrates the issuance of the RPC. In the beginning, the domain owner can choose whether to revoke the current RPC. If the RPC is lost but not compromised, or it is a regular updating of the RPC, the domain owner can choose not to revoke the current RPC.

The domain owner will send a RCSR for RPC and a PSR for PC to the PCA. Then the PCA will check the ownership of the domain owner and issue an RPC. The "validate from" field in the RPC depends on whether the domain owner provides a signature using the current RPC. If the domain owner does not provide a signature using current RPC, the "validate from" field will be seven days later (cool off period). Besides, PCA will also validate the PSR using the public key in the RCSR. Then the PCA will send the RPC and new PC to the policy log. The "SPTs" field of RPC and PC is empty. The policy log will wait until the next merging and add the RPC and PC to the Merkle Tree. Then the policy log will generate SPTs and return the SPTs to the PCA. When PCA receives the SPTs, it will attach the SPT to the corresponding RPC and PC, and return the RPC and PC to the domain owner.

5.2 Issuance of PC

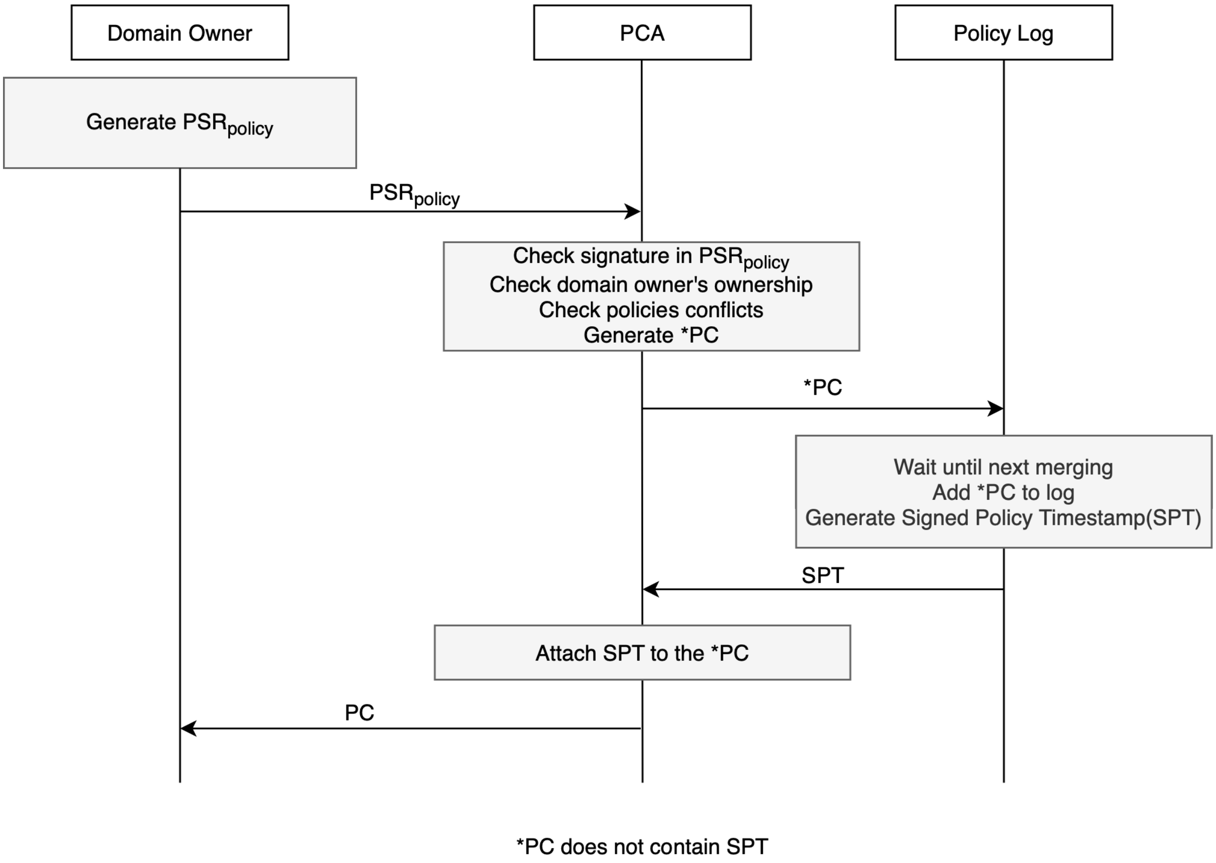


Figure 12: Issuance of Policy

Figure 12 illustrates the issuance of Policy. Issuance of PC is similar to the issuance of RPC. A PSR will be generated by the domain owner. Then the PSR will be processed by PCA. PCA will validate the signature and check the policies. If the new policies violate the previous policies or might cause the unavailability of the domain, the PCA will communicate with the domain owner. However, only the domain owner can do the final decision. PCA can not refuse to issue the PC only because of the policies conflicts. Then the PC without SPT will be sent to the policy log. When the SPT is returned by policy log, the PCA will attach the SPT to the PC, and return the complete PC to the domain owner.

6 Revocation

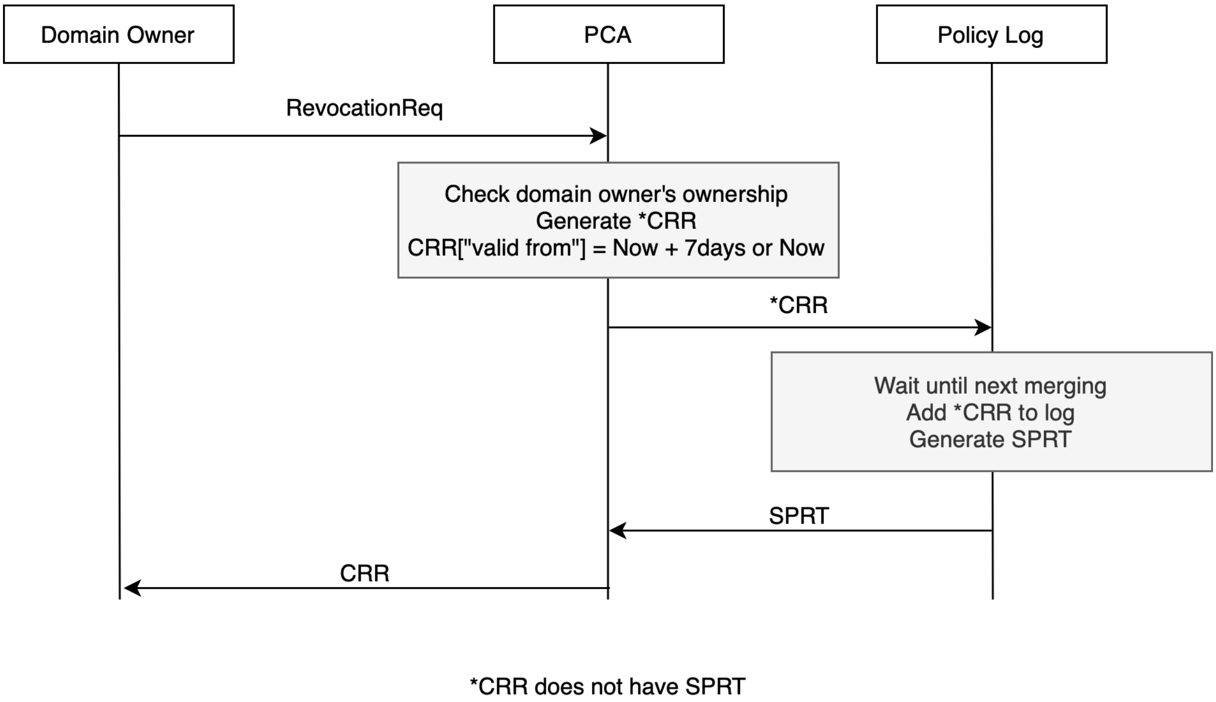
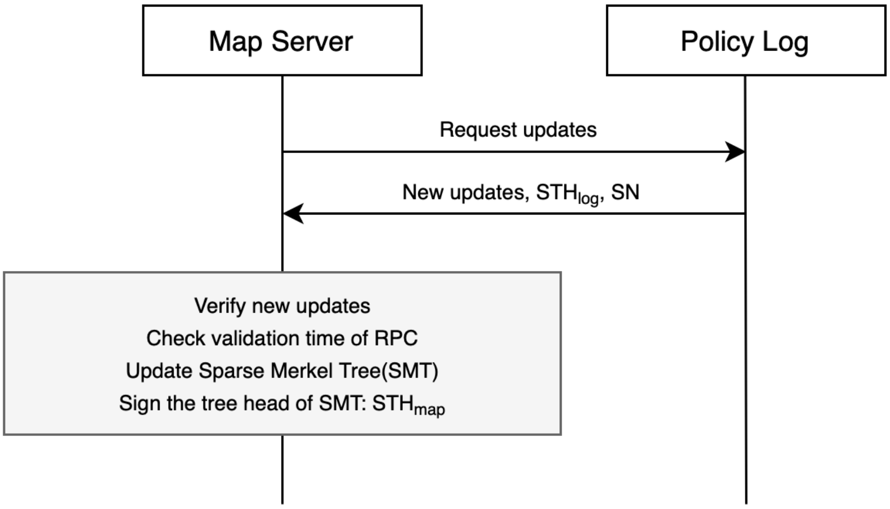


Figure 13: Revocation of Policy

Revocation is similar to the issuance. The PCA will generate a CRR and log the CRR in the policy log. Then the policy log will return an SPRT after the CRR is added. The ”valid from” field in the CRR depends on whether the domain owner provides a signature from current RPC.

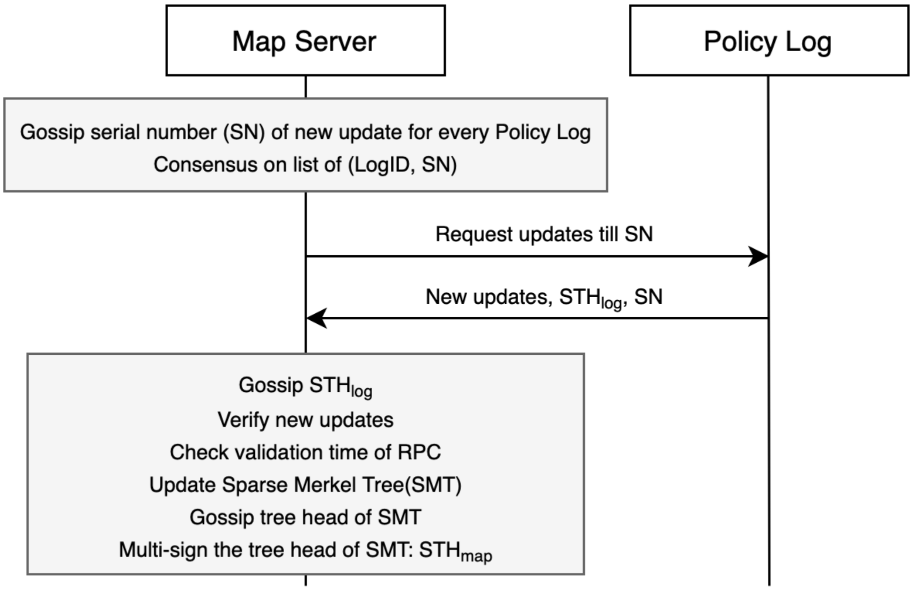
7 Updates of Map Server



Map Server
Policy Log
Request updates
New updates, STH$_{log}$, SN
Verify new updates
Check validation time of RPC
Update Sparse Merkel Tree(SMT)
Sign the tree head of SMT: STH$_{map}$

Figure 14: Updates of map server. Single map server model

Figure 14 illustrates the update of the map server. Periodically, map server will fetch the new updates from all the policy logs. Then the map server will validate the new updates and update the Sparse Merkle Tree (SMT). Finally, map server will sign the tree head of SMT.



Map Server
Policy Log
Gossip serial number (SN) of new update for every Policy Log
Consensus on list of (LogID, SN)
Request updates till SN
New updates, STH_{log}, SN
Gossip STH_{log}
Verify new updates
Check validation time of RPC
Update Sparse Merkel Tree(SMT)
Gossip tree head of SMT
Multi-sign the tree head of SMT: STH_{map}

Figure 15: Updates of map server. Federation model

To prevent single point of failure, several map servers can also form one federation. Figure 15 illustrates the update of the map server. Periodically, all the map servers will run a consensus protocol to decide the newest Serial Number(SN) of every policy log. In most cases, all the map servers are well-synchronised and they only need to fetch the newest one. However, if using quorum, some map servers might not be updated in the previous synchronisation. In this case, the lagging map servers will fetch all the missing updates till the agreed SN.

Once the consensus is reached, every map server will query all the policy logs and download the newest updates till SN. After validating all the new RPCs and Policies, the map server will update their hierarchical SMT, and gossip the tree head of the hierarchical SMT. If the tree head is identical, they will multi-sign the tree head and release the signed tree head.

7.1 Logic of Updating

Once the map server collects the daily updates, it will retrieve all the relevant leaves in the hierarchical SMT and update the leaves.

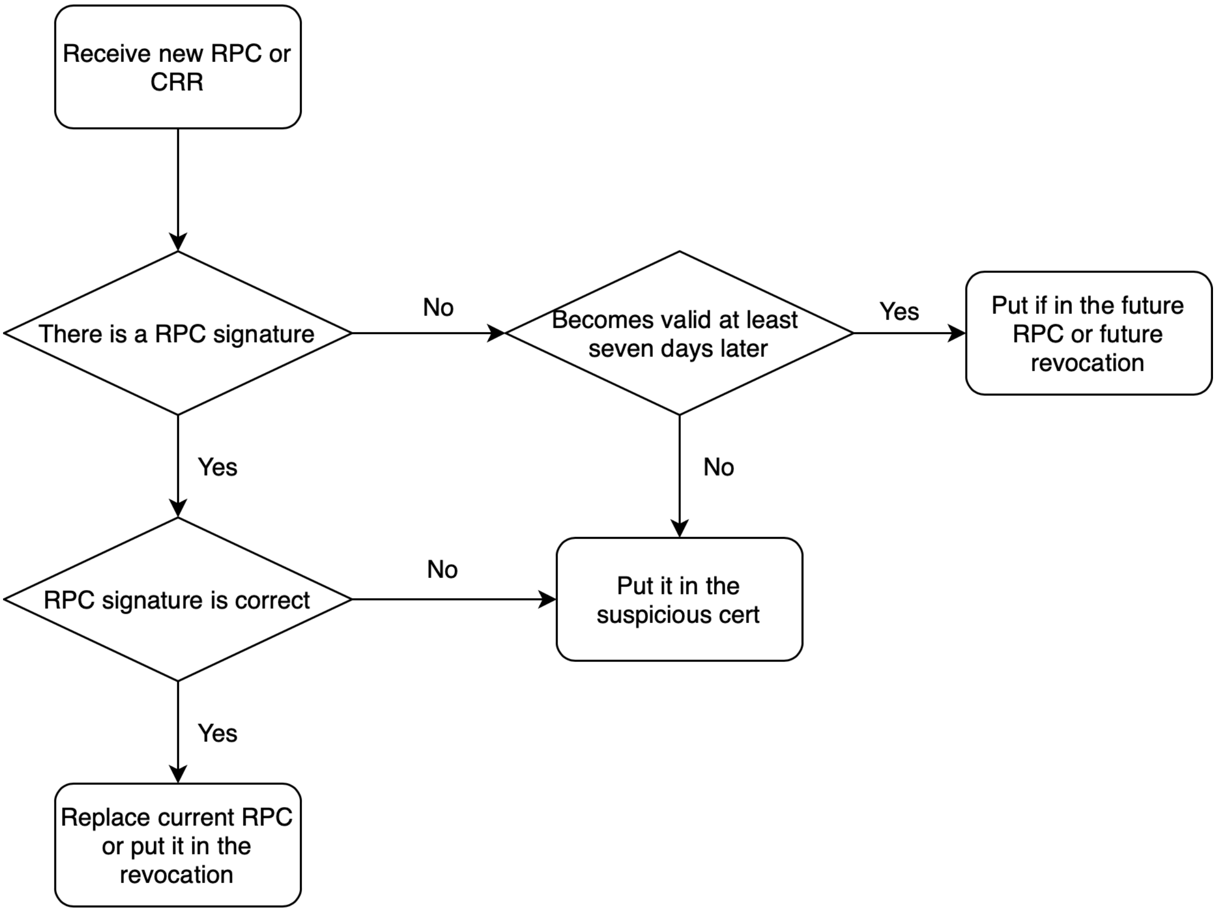

Receive new RPC or CRR
There is a RPC signature
No
Becomes valid at least seven days later
Yes
Put if in the future RPC or future revocation
Yes
No
RPC signature is correct
No
Put it in the suspicious cert
Yes
Replace current RPC or put it in the revocation

Figure 16: Updates new RPC or revocation

When a map server receives a new RPC or CRR, it will check if there is an RPC signature. If there is an RPC signature and the RPC signature is valid using the "current RPC", then the RPC or CRR will take into effect immediately. If the signature is not correct, the RPC or CRR will be put into the "suspicious cert".

If the signature is missing, the map server will check the validation time of the certificate. If the validation time is at least seven days later, the map server will add it to the "future RPC" or "future revocations". Otherwise, it will be added to the "suspicious cert."

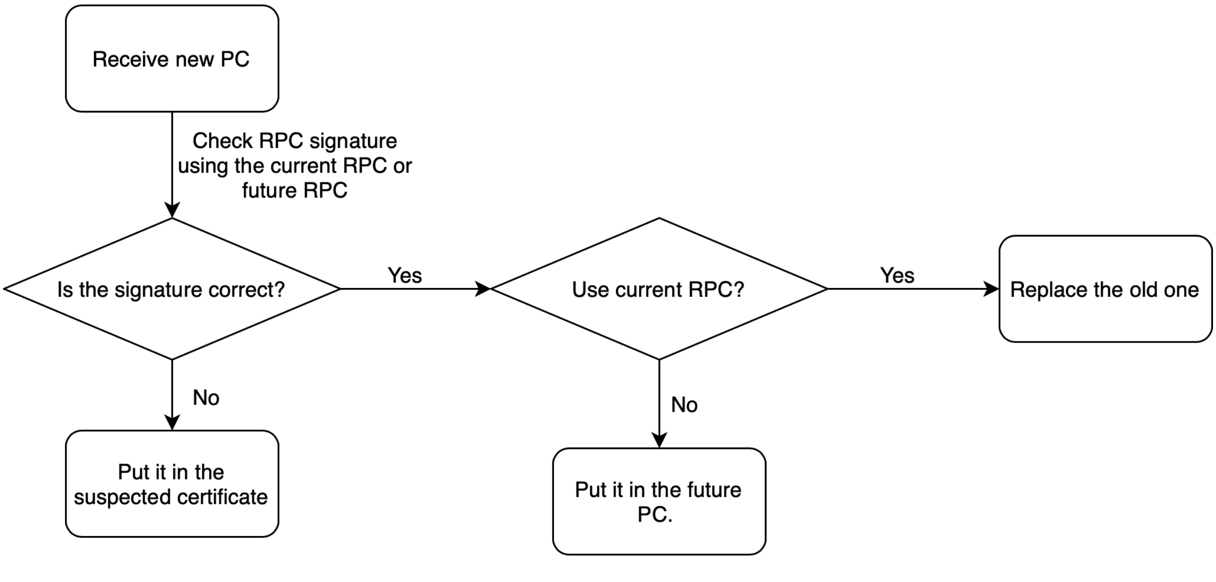

Receive new PC
Check RPC signature using the current RPC or future RPC
Is the signature correct?
Yes
Use current RPC?
Yes
Replace the old one
No
Put it in the suspected certificate
No
Put it in the future PC.

Figure 17: Updates new PC

When a map server receives a new PC, it will check the signature of the PC. If the signature is valid using current RPC or future RPC, the PC will be added to "current PC" or "future PC" according to the type of RPC (future or current). However, if the signature is incorrect or missing, the PC will be added to the "suspicious cert".

A Cool-off Period

A.1 Definition

During the cool-off period, the new certificate will be publicly shown in the proof of one domain in the map server. However, the certificate will not be valid before the cool-off period expires. The cool-off period is mainly used for limiting the power of CA. Without cool-off period, any trusted CA can issue or revoke any RPC for one domain freely without being noticed by domain owner. Although the misbehaviour can be detected eventually, the attacks are still possible. With the help of cool-off period, there will be plenty of time for the domain owner to react to the attack, thus preventing the attack from happening.

A.2 Use Cases of Cool-off Period

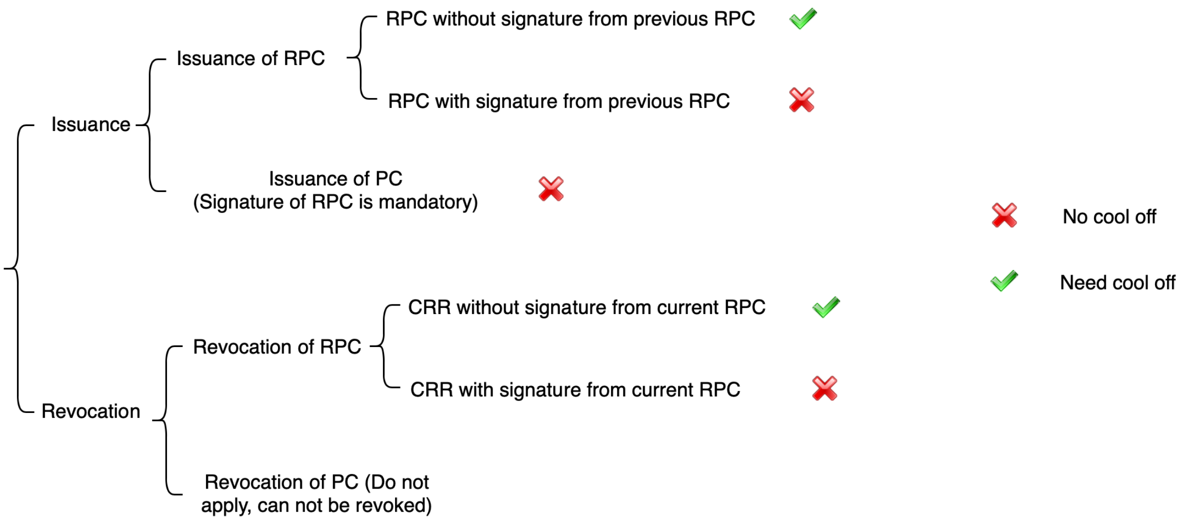

RPC without signature from previous RPC ✓
Issuance of RPC
RPC with signature from previous RPC ✗
Issuance
Issuance of PC
(Signature of RPC is mandatory) ✗
✗ No cool off
✓ Need cool off
CRR without signature from current RPC ✓
Revocation of RPC
CRR with signature from current RPC ✗
Revocation
Revocation of PC (Do not
apply, can not be revoked)

Figure 18: Use cases of cool off period

Generally speaking, any issuance and revocation with the signature of the previous RPC (which already passes the cool-off period) will take into effect immediately. The ownership of RPC is already checked by the domain owner if the RPC has gone through the cool-off period. Because the domain owner will detect the malicious RPC and report it during the cool-off period. So if the new RPC and CRR have a signature of a valid RPC, the cool-off period can be skipped. If the private key of the RPC is not compromised, the trusted CA can not issue any malicious policy, or maliciously revoke any valid PC or RPC. The availability will not be harmed either, as issuance and revocation of RPC and PC will take into effect immediately.

If the private key of RPC is compromised, and the trusted CA is not compromised, the attacker can not modify the policies of one domain. Because the issuance and revocation of RPC and PC will also be checked by CA. Besides, the legitimate domain owner can revoke the compromised RPC without a cool-off period. If the CA is not compromised and the ownership checking is reliable (two-factor authentication for example), the domain owner can even issue a new RPC without revoking the compromised one. During the cool-off period, the domain owner can still use the compromised RPC to issue a new PC.

If the private key of RPC is lost, then the domain owner needs to issue a new one. Although the domain owner can not issue any new PC during the cool-off period, the previous PC is still valid and the domain is still protected by the previous PC.

If the private key of RPC is compromised and the trusted CA is compromised as well, then the attacker can modify the domain's policies freely. This attack can only be prevented if the issuance and revocation of PC is mandatory. However, this will dramatically harm the availability, since every PC will go through a cool-off period.

In conclusion, modification of policies by the attacker is only possible if the attacker gets the private key of the RPC and the trusted CA colludes with the attacker. For the availability, as long as the domain owner does not lose the private key, it can issue or revoke any RPC and PC without any cool-off period (Assume the trusted CA is honest. If the trusted CA is malicious, it can always refuse to provide service).