PoC Certificate Expiration Timelines

Goals

1. Establish a reasonable root certificate expiration period by shortening the EE Enrollment certificate expiration period from previous 30 years as mentioned in the Vehicle Safety Communications Security Studies Project (VSCS)
2. Allow EE to use their existing enrollment certificate for authentication when requesting a rollover enrollment (Re-enrollment) certificate
3. Minimize the number of root certificates that are valid at any time

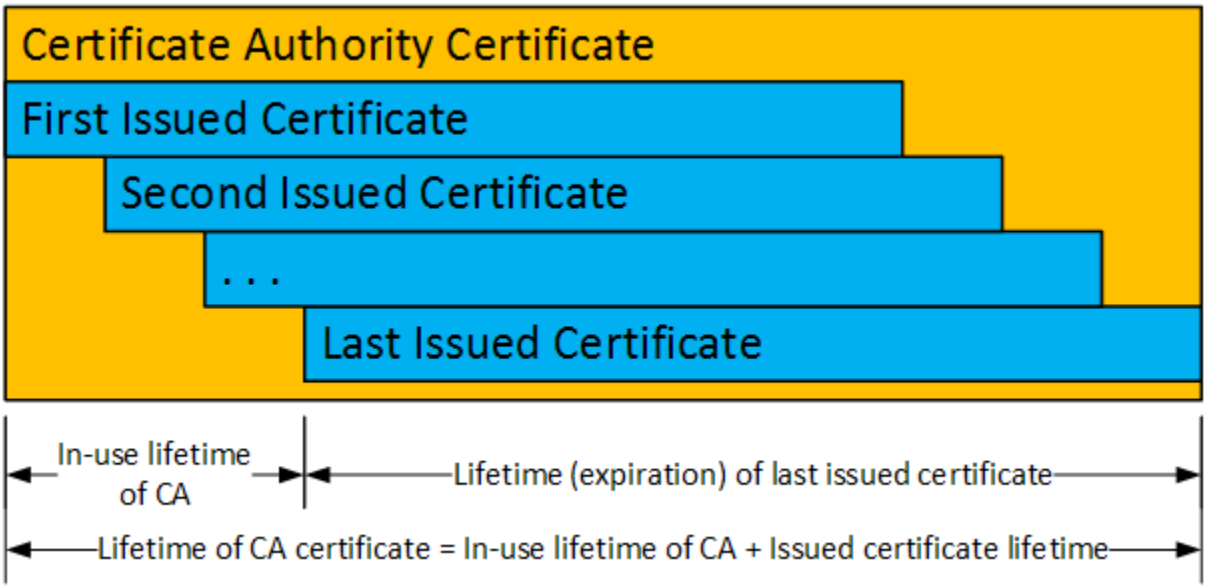
Assumptions

1. Vehicles have an estimated life of up to 30 years
2. EEs may only have connectivity once every three years
3. Initial EE enrollment certificates and rollover certificates are issued by the ECA
4. Only one enrollment certificate for an EE shall be valid at a time
5. EE must request and download the rollover certificate before the current certificate expires
6. Re-enrollment certificates will not be generated or available for download until three years before the expiration of the current enrollment certificate

Factors Influencing Certificate Lifetimes

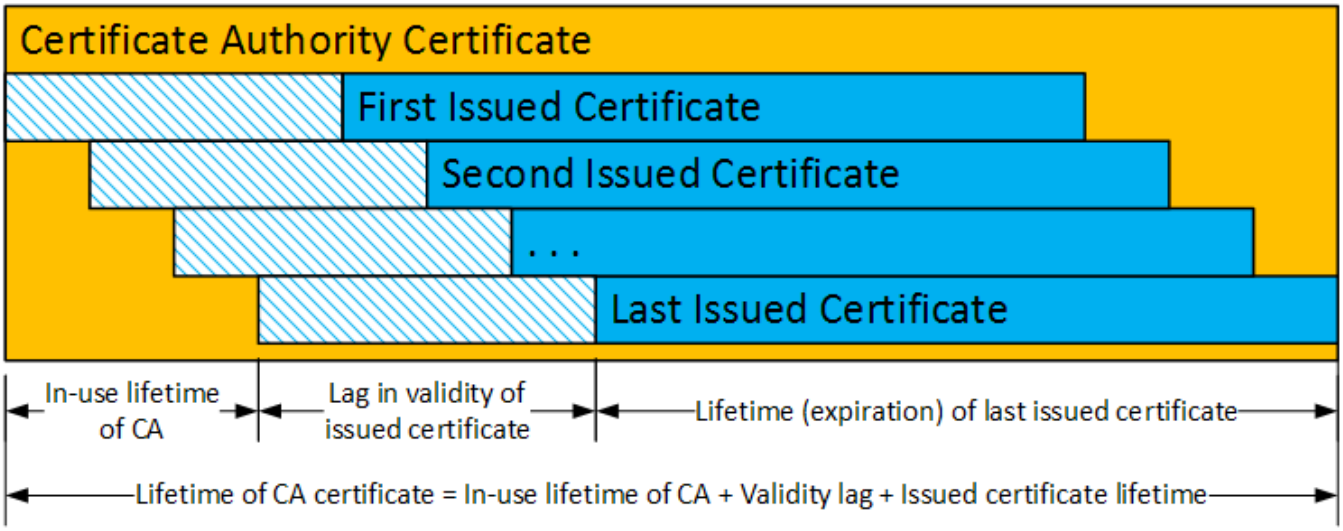
Certificate lifetimes affect the security of PKI infrastructures. The longer a public/private key pair is in use, the greater the chances are that the keys can be compromised. As computing power increases and technologies improve over time, cryptanalysis becomes a risk. For these reasons, excessively long-lived CA certificate lifetimes are undesirable.

The below diagram illustrates the calculation of the minimum lifetime of a typical CA certificate.



Calculating In-use Lifetime of a Certificate Authority

Some certificate authorities may issue certificates that are not valid until a significant time in the future. Examples of this within the SCMS are pseudonym certificates and rollover enrollment certificates. As a recommendation, the validity lag for these certificates can be up to 3 years. For example, a pseudonym certificate generated (issued) today may have a "Valid from" date that is up to 3 years from now. The below diagram illustrates the impact of the validity lag on the lifetime of the issuing CA certificate.

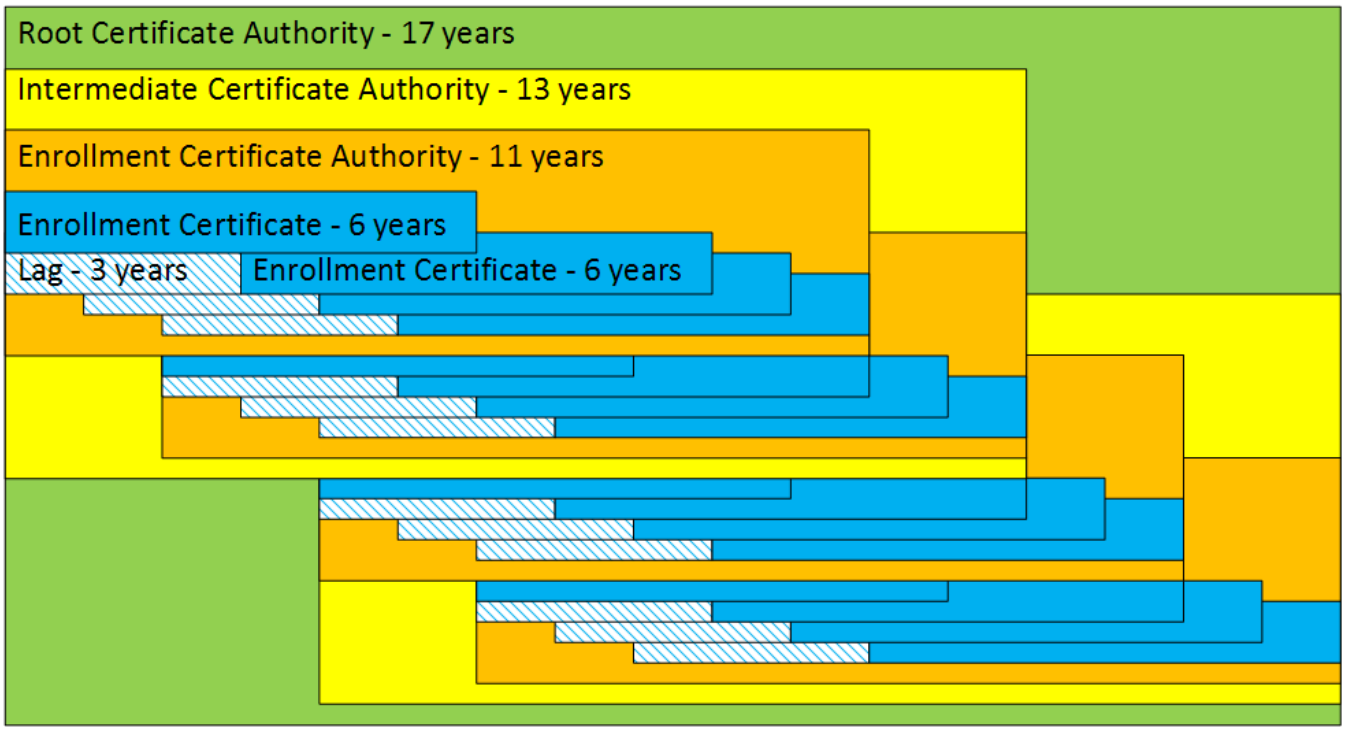


Impact of Lag in Validity of Issued Certificates

As additional layers are added to the certificate hierarchy, this process is repeated up to the root CA. When operational factors and the requirement to have the ability to issue new certificates at any time are considered, the required lifetime of each CA certificate in the trust chain is further increased.

It will be necessary to renew the enrollment certificate multiple times for an estimated vehicle lifetime of 30 years. An enrollment certificate lifetime of 6 years greatly reduces security concerns due to certificate longevity, but it requires an automatic renewal mechanism that can accommodate the EEs with infrequent network connectivity. As better and more frequent network connectivity becomes available to the EEs, it may be possible to further reduce these lifetimes.

The below diagram illustrates the impact of issued certificate lifetime, certificate validity lag and operational factors on the PKI hierarchy.

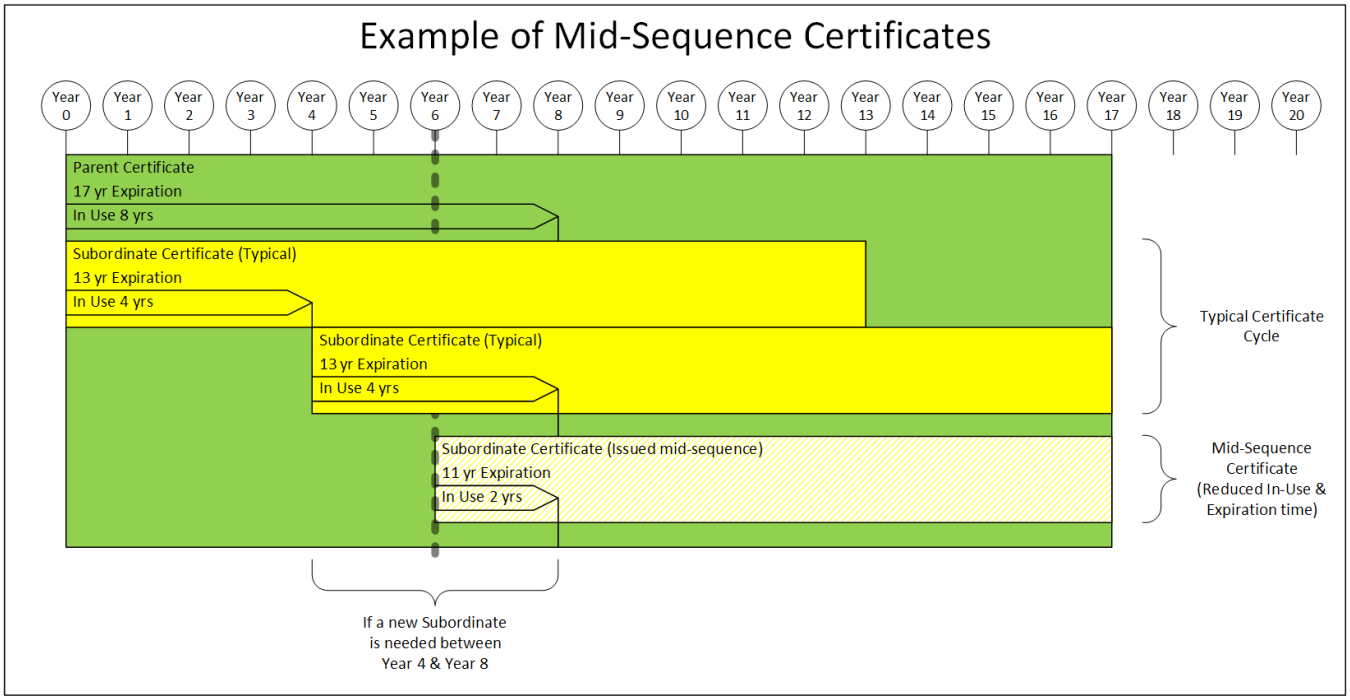


Relationship Between Enrollment and CA Certificate Lifetimes

Establishing a fixed schedule for the expiration of elector certificates, root CA certificate(s), intermediate CA certificates and enrollment CA certificates is recommended to reduce operational complexities. For offline CAs, this procedure increases security by minimizing the frequency of required access. Certificates issued in the middle of this fixed schedule, due to revocation or new instances, will expire according to the defined schedule and will have a reduced overall lifetime due to a shorter in-use lifetime.

The following guidelines shall be followed when component certificates are issued mid-sequence:

- This concept is mandatory for all certificates issued by the root CA and intermediate CA
- The certificate's in-use and expiration shall be reduced by the same amount



Example of Mid-Sequence Certificates

To ensure the overall integrity of the SCMS, the minimum and maximum lifetime of each certificate type will be defined and enforced by the SCMS manager policy. Operators will have some amount of flexibility in defining the actual certificate lifetimes.

Certificate Lifetime Overview

The following table provides the certificate expiration and renewal periods to be used in a SCMS that supports EE enrollment certificate rollover.

Certificate Type	Issuing CA	Expiration	In Use	Request for Renewal	Start of Validity for Renewal	Number of Concurrently Valid Certificates (In-Use [+ Legacy])	Example Size in Bytes (Certs are Not Fixed Size)	Notes
OBE Enrollment	ECA	6 years	6 years	Anytime (see notes)	6 years	1	87	Rollover certificate will be available no more than 3 years before start of validity.
OBE Pseudonym	PCA	1 week + 1 hour	1 week	Anytime	1 week	20 + 20 (for just 1 hour)	86	
OBE Identification	PCA	1 month + 1 hour	1 month	Anytime	1 month	1 + 1 (for just 1 hour)	89	
RSE Enrollment	ECA	6 years	6 years	Anytime (see notes)	6 years	1	87	Rollover certificate will be available no more than 3 years before start of validity.
RSE Application	PCA	1 week + 1 hour	1 week	Anytime	1 week	1 + 1 (for just 1 hour)	89	
DCM	ICA	3 years + 1 week	3 years	3 months before end of In-Use	3 years	1 + 1 (for just 1 week)	219	
ECA	ICA	11 years	2 years	3 months before end of In-Use	2 years	1 + 5	150	
RA	ICA	3 years + 1 week	3 years	3 months before end of In-Use	3 years	1 + 1 (for just 1 week)	217	
LA	ICA	3 years + 1 week	3 years	3 months before end of In-Use	3 years	1 + 1 (for just 1 week)	205	
PCA	ICA	4 years	1 year	3 months before end of In-Use	1 year	1 + 3	216	
ICA	Root CA	13 years	4 years	3 months before end of In-Use	4 years	1 + 3	195	
MA	Root CA	4 years + 1 week	4 years	3 months before end of In-Use	4 years	1 + 1 (for just 1 week)	205	

CRLG	Root CA	4 years + 1 week	4 years	3 months before end of In-Use	4 years	1 + 1 (for just 1 week)	190	
Policy Generator (PG)	Root CA	4 years + 1 week	4 years	3 months before end of In-Use	4 years	1 + 1 (for just 1 week)	172	
Root CA (RCA)	Self	17 years	8 years	3 months before end of In-Use	8 years	1 + 2	211	
Elector	Self	12 years	12 years	3 months before end of In-Use	12 years	3	166	The initial elector certificates have an expiration and "in use" time of 4, 8 and 12 years, respectively.

PoC Certificate Expiration Timelines - Certificate Expiration and Renewal

Expiration, In-use, and Overlap Requirements

Key	Summary	Description	Justification	Notes	Component/s
SCMS-1412	Destroy certificate's private key	The certificate's private key shall be destroyed at the end of the "In-use" life of a certificate. The in-use lifetime of certificates shall be defined either by SCMS policy and/or based on the expiration and In-use lifetime of subordinate certificates.	To prevent the usage of certificates that have reached the end of defined In-use lifetime.	Out of scope as this needs to be implemented as operational policy.	CRL Store, CRLG, DCM, ECA, ICA, LA, MA, PCA, PG, RA
SCMS-1725	Component certificate FQDN match	The SCMS component shall have a certificate with a certificateId field that matches the FQDN of the component.	FQDN of each component must match the official ID of the component.		CRLG, DCM, ECA, LA, MA, PCA, PG, RA
SCMS-1581	Component certificate in-use period	The SCMS component shall use its certificate for an in-use period of 3 years.	Use 3 years for standard SCMS components	Out of scope as this needs to be implemented as operational policy. This is for POC & CV-Pilot only.	CRLG, DCM, LA, MA, PG, RA
SCMS-1319	Component certificate expiration	The component shall request a certificate with a validity of 3 years and 1 week.	Use 3 years for standard SCMS components	This is for POC & CV-Pilot only.	CRLG, DCM, LA, MA, PG, RA
SCMS-1591	ECA certificate validity	ECA shall request an ECA certificate with a validity of 11 years.	To support issuing of subordinate certificates.	This is for POC only.	ECA
SCMS-1307	Enrollment certificate lifetime	ECA shall issue Enrollment Certificates with a lifetime of 6 years.	For PoC, enrollment certificates use a life span of 6 years	This is for PoC only	ECA
SCMS-1809	Elector certificate validity	Elector certificates validity period shall be set to 12 years.	Elector certificates must have an expiration date.	Certificate types and expiration periods are defined in the Certificate Types common requirements section. This is for PoC and CV-Pilot only.	Elector
SCMS-1590	Elector Certificate In-Use period	The Elector certificate In-Use period shall be the same as the Expiration period.	Out of scope as this needs to be implemented as operational policy. To maintain a fixed number of valid Elector at all times.		Elector

SCMS-1423	Elector Certificate Expiration	The Technical Component of the SCMS Manager (TCotSCMSM) shall issue Elector certificates with an expiration of 12 years.	Component 1609 certificates shall have a defined expiration.	In the case of the certificate being revoked, the new certificate may have a different expiration to align with predefined replacement schedules (if any exist). For the initial system deployment, 1 of the 3 Electors shall have a certificate expiration of 4 years, another one a certificate expiration of 8 years, to prevent multiple elector certificates from expiring at the same time. These durations are for the SCMS PoC and CV-Pilot only. For other SCMS instances, this duration should be reevaluated.	Elector
SCMS-1597	ICA certificate in-use period	ICA shall use its ICA certificate for an in-use period of 4 years.	The in-use period shall be short to minimize impact, if revocation is required.	Out of scope as this needs to be implemented as operational policy. This is for POC only.	ICA
SCMS-1596	ICA certificate validity	ICA shall request an ICA certificate with a validity of 13 years.	To support issuing of subordinate certificates.	This is for POC only.	ICA
SCMS-1595	PCA certificate in-use period	PCA shall use its certificate for an in-use period of 1 years.	The In-use period shall be short to minimize impact if revocation is required.	Out of scope as this needs to be implemented as operational policy. This is for POC & CV-Pilot only.	PCA
SCMS-1594	PCA certificate expiration	PCA shall request a certificate with a validity of 4 years.	The expiration must be sufficiently long to issue pseudonym certificates for 3 years in the future.	This is for POC only.	PCA
SCMS-1416	Certificate Overlap: OBE Identification Certificates	RA shall request PCA to generate OBE identification certificates with an overlap $t_{\_overlap}$ of one hour.	This is in line with pseudonym certificates. $t_{overlap}$ of 1 hour (60 minutes) reduces the risk of a vehicle operating without a valid certificate.	This is for POC & CV-Pilot only.	RA
SCMS-1415	Certificate Validity: OBE Pseudonym Certificates	RA shall request PCA to generate OBE pseudonym certificates with validity period $t_{\_validity}$.	This allows flexible certificate handling.	Validity period $t_{\_validity}$ is currently set to 1 week + 1 hour for POC & CV-Pilot.	RA
SCMS-1370	Certificate Validity: OBE Identification Certificates	RA shall request PCA to generate OBE identification certificates with validity period $t_{\_validity}$.	This is in line with pseudonym certificates. It allows revocation by not renewing certificates, and does not require a permanent but only regular online connection to renew certificates.	Validity period $t_{\_validity}$ is currently set to 1 month + 1 hour for POC & CV-Pilot.	RA
SCMS-1213	Certificate Validity: RSE Application Certificates	RA shall request PCA to generate RSE application certificates with validity period $t_{\_validity}$ as defined in rse_application_cert_validity.	As per communications with USDOT, RSEs will have frequent connectivity. Therefore, a short validity period is justified for RSE application certificates.	Validity period $t_{\_validity}$ is currently set to 1 week for POC & CV-Pilot.	RA
SCMS-1212	Certificate Overlap: RSE Application Certificates	RA shall request PCA to generate RSE application certificates with an overlap $t_{\_overlap}$ as defined in rse_application_cert_overlap	$t_{overlap}$ of e.g. 1 hour (60 minutes) reduces the risk of a vehicle having to verify another RSE certificate during a critical time period.	This is for POC & CV-Pilot only.	RA
SCMS-526	Certificate Overlap: OBE Pseudonym Certificates	RA shall request PCA to generate OBE pseudonym certificates with an overlap $t_{\_overlap}$ of one hour.	The original value for $t_{overlap}$ was 1 minute but there are safety concerns with such a small overlap. For example, a device could be in an alert state for more than 1 minute. Extending $t_{overlap}$ to 1 hour (60 minutes) reduces the risk of a vehicle operating without a valid certificate.	This is for POC & CV-Pilot only.	RA

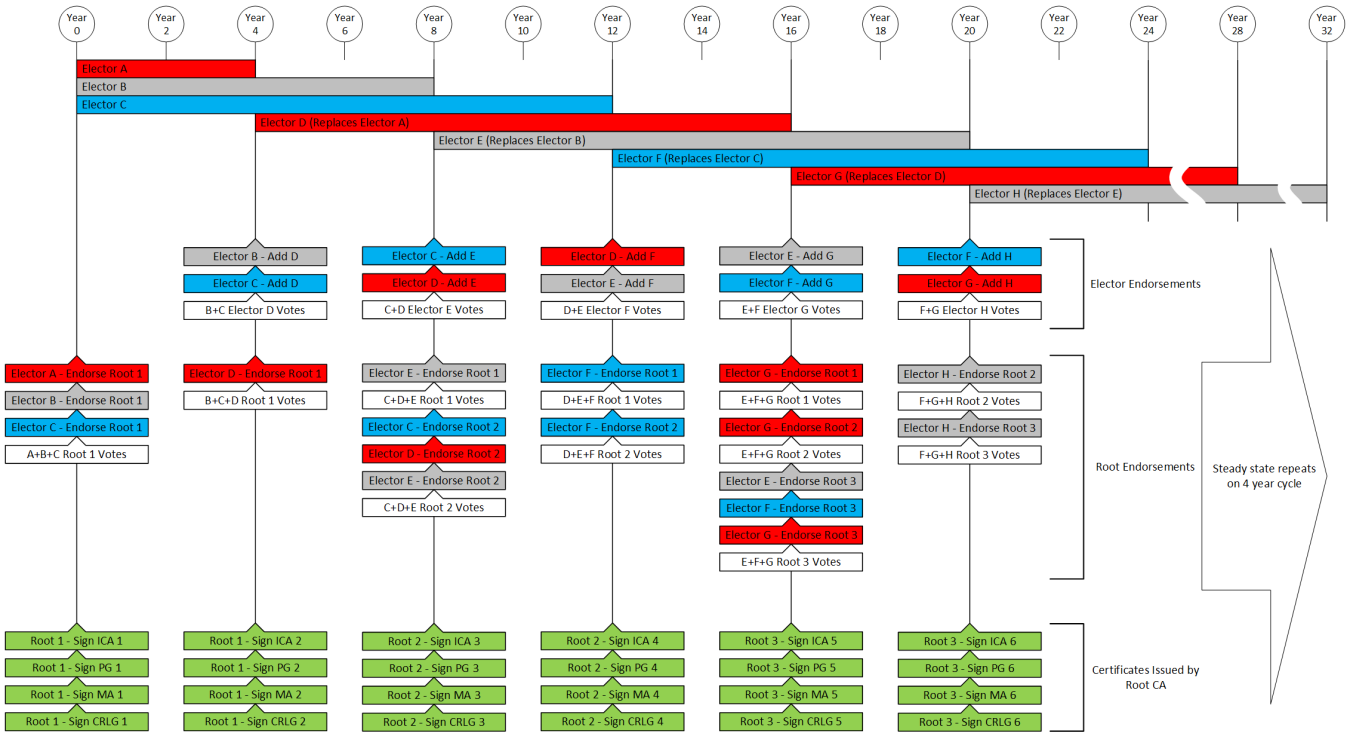
SC MS-1332	Root CA certificate overlap	Root CA certificates shall have an overlap of 9 years (an in-use period of 8 years).	The overlap is necessary to allow rollover.	This is for POC & CV-Pilot only.	RCA
SC MS-1318	Root CA certificate validity	The root CA certificate validity period shall be set to 17 years.	Root CA certificates must have an expiration date. The root CA certificate must be valid at least as long as the longest issued enrollment certificate.	Certificate types and expiration periods are defined in the Certificate Types common requirements section. This is for PoC only.	RCA

21 issues

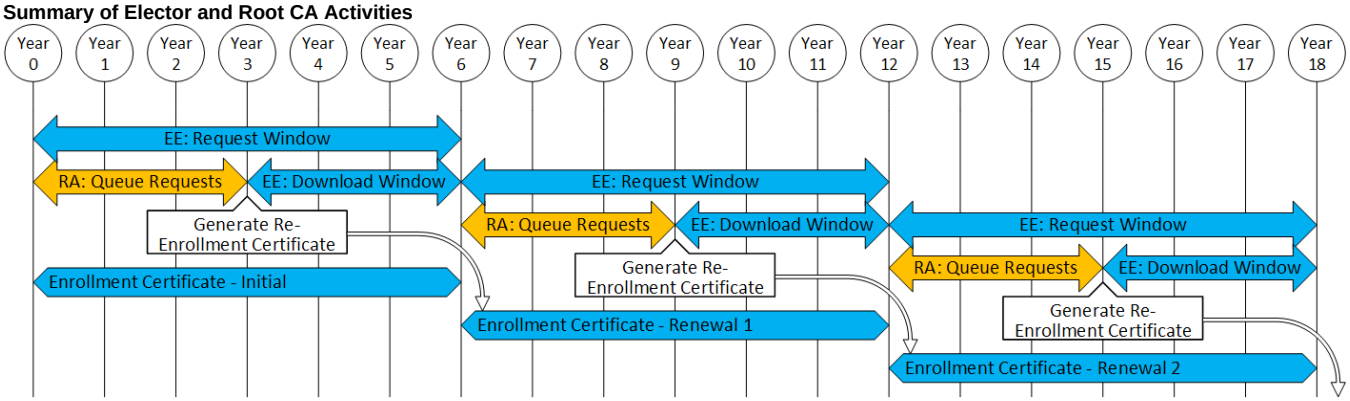
Expiration, In-use, and Overlap Requirements

Overview Diagrams

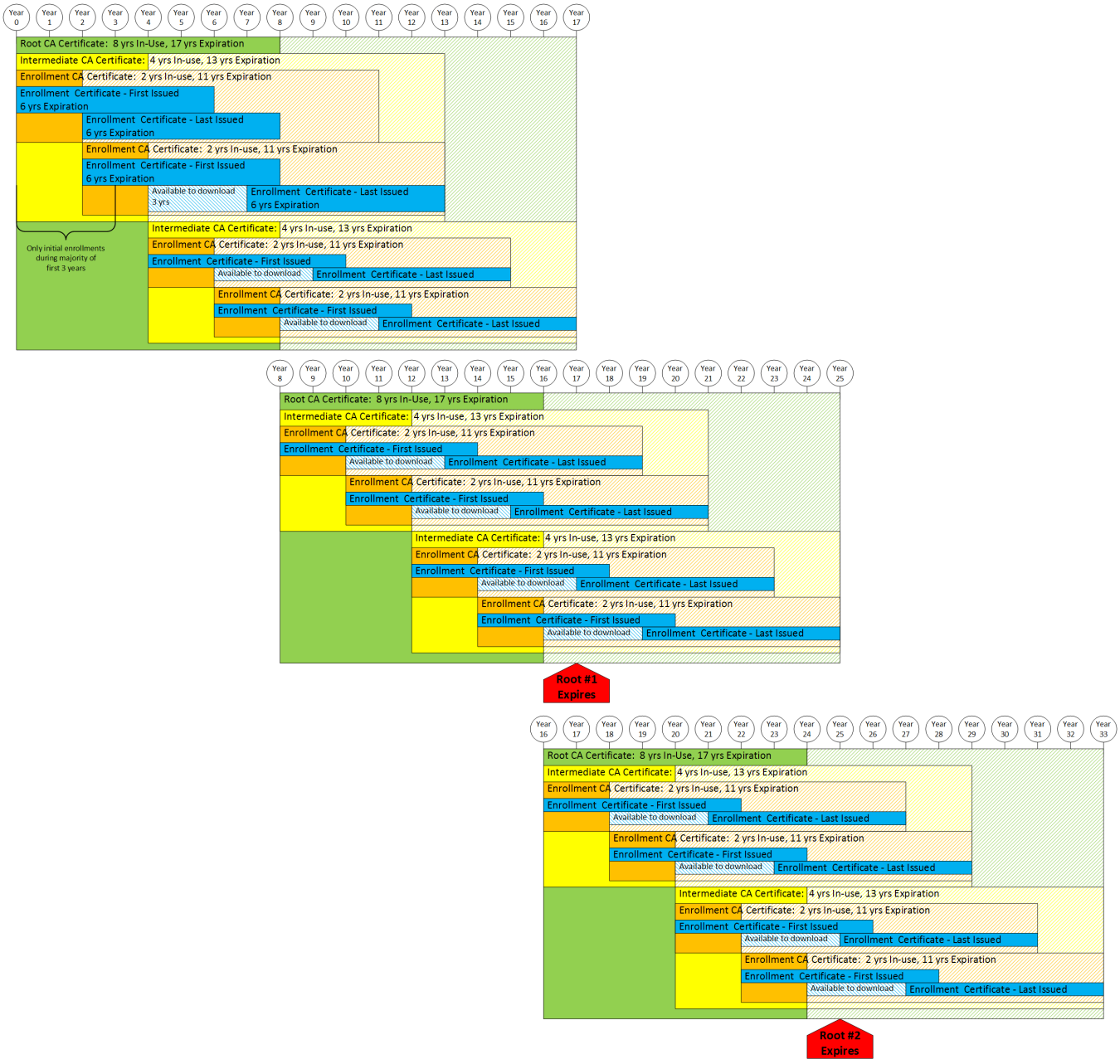
The following diagrams illustrate the expiration period of various certificate types. The diagrams show the specific duration of the certificate (valid from and to dates) only and do not account for setup time (request generation, signing ceremony, distribution, etc.). Each section shows the life of a single instance of a component under typical (non-compromised) conditions. If multiple instances exist, they would follow a similar pattern but the specific dates may be shifted within the validity period.



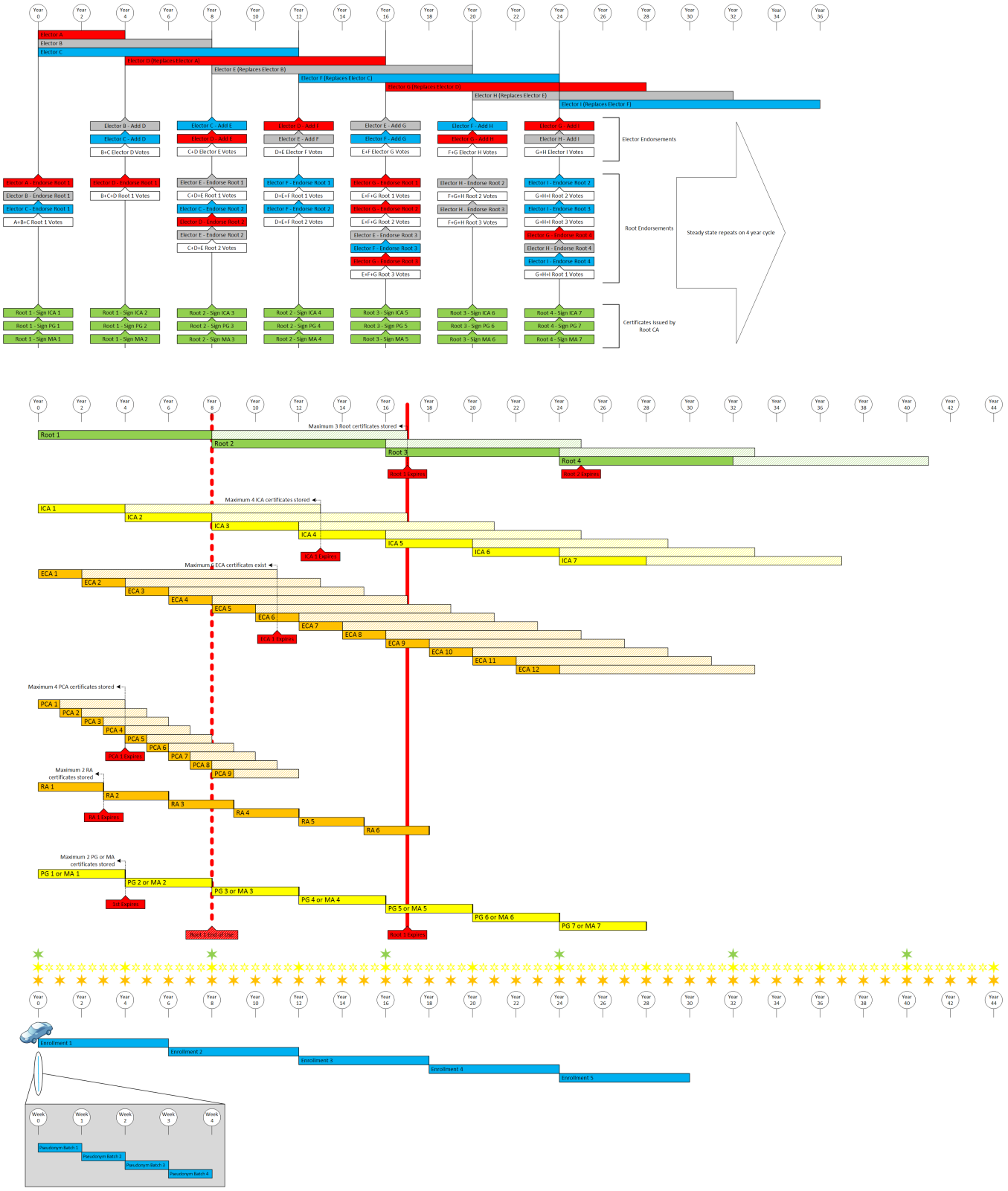
Summary of Elector and Root CA Activities



EE Enrollment Rollover Timeline



PoC Certificate Expiration Timelines - Overview Diagram



PoC Certificate Expiration Timelines - Stackup