Timing Matrix - Baseline Requirements

Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, Version 1.7.1, August 20, 2020

Category	Activity	Timing	Measured From/By	Reference
Next Update				
OCSP Responses	Update information provided via an OCSP at least every four (4) days. Responses from this service have a maximum expiration of ten (10) days.	At least every 4 days Not to exceed 10 days Before September 30, 2020 00:00:00 UTC	From OCSP update	BR Section 4.9.10
OCSP Responses	Set OCSP validity periods • If validity periods less than 16 hours, update information • If validity periods greater than or equal to 16 hours, update information	Greater than or equal to 8 hours and less than or equal to 10 days • Prior to one half the validity period before nextUpdate • No later than 4 days after thisUpdate **After September 30, 2020 00:00:00 UTC**	From thisUpdate to nextUpdate • From current time to nextUpdate • From thisUpdate	BR Section 4.9.10
Phase Outs				
Certificate Validity Period	Issue subscriber certificates with validity periods of not greater than 398 days	398 days After September 1, 2020 00:00:00 UTC	From issuance date	BR Section 6.3.2
Certificate Validity Period	Issue subscriber certificates with validity periods of not greater than 825 days	825 days After March 1, 2018 AND prior to September 1, 2020	From issuance date	BR Section 6.3.2
Certificate Validity Period	Issue subscriber certificates with validity periods of not greater than 39 months	39 months After July 1, 2016 AND prior to March 1, 2018	From issuance date	BR Section 6.3.2
Deprecated Validation Method	Cease *Agreed-Upon Change to Website* validation method, except if re-using within the data reuse period	After March 3, 2020	Specific date	BR Section 3.2.2.4.6
Deprecated Validation Method	Cease *Phone Contact with Domain Contact* validation method, except if re-using within the data reuse period	After May 31, 2019	Specific date	BR Section 3.2.2.4.3
Program Documentation	Update the CP/CPS	Annually	From the last CP/CPS version date	BR Section 2
Program Documentation	Perform a security risk assessment	Annually	From the date the last risk assessment was performed	BR Section 5
Program Documentation	Test, review and update incident and compromise handling procedures	Annually	From the last test, review or update date, respectively	BR Section 5.7.1
Program Documentation	Modify requirements in the CP/CPS that conflict with laws, including a detailed reference to the law and required modifications in section 9.16.3, and notify the CA/B Forum	Before issuing a certificate under the modified requirement	Issuance date of first certificate issued	BR Section 9.16.3
Program Documentation	Discontinue activities in section 9.16.3 when the law no longer applies or the requirements are modified to no longer conflict, and update the CP/CPS	Within 90 days of change in the law or requirements	Effective date of the law or requirements	BR Section 9.16.3
Personnel	Verify the identity and trustworthiness of personnel engaged in the certificate management process	Prior to engagement in the certificate management process	Hire date or contract start date	BR Section 5.3.1
Operational Requirements	Ensure the CP/CPS is publicly accessible	24 x 7	Up-time of repository	BR Section 2.2
Operational Requirements	Maintain a continuous ability to respond internally to high-priority certificate problem reports, and where appropriate, forward such a complaint to law enforcement authorities and/or revoke a certificate that is the subject of such a complaint	24 x 7	Personnel coverage	BR section 4.10.2
Operational Requirements	Maintain an online repository that application software can use to automatically check the current status of all unexpired certificates issued by the CA (Online Certificate Status Protocol - OCSP)	24 x 7	Up-time of OCSP	BR section 4.10.2
Operational Requirements	Operate and maintain a certificate revocation list (CRL) and OCSP capabilities with resources to provide a response time of 10 seconds or less under normal operating conditions	10 seconds or less	Call to response	BR section 4.10.2
OCSP Responses	Update the status of Subordinate CA certificates via OCSP	At least every 12 months Within 24 hours after revoking a Subordinate CA	From thisUpdate field From revocation	BR Section 4.9.10

CRL	If the CA publishes a CRL, update and reissue CRLs Set the value of the nextUpdate field	Every 7 days Not more than 10 days	From last CRL publish date From thisUpdate field to nextUpdate field	BR Section 4.9.7
CRL	Update and reissue CRL's for status of Subordinate CA Certificates Set the value of the nextUpdate field	Every 12 months AND Within 24 hours after revoking a Subordinate CA certificate Not more than 12 months	From last CRL publish date From revocation date of Subordinate CA certificate From thisUpdate field to nextUpdate field	BR Section 4.9.7
CRL/ OCSP	Do not remove revocation entries on CRL or OCSP response before the expiry date of the revoked certificate	Daily	Expiry date of the revoked certificate	BR Section 4.10.1
Validation	Validate the Fully Qualified Domain Name (FQDN) for each certificate	Prior to certificate issuance	Issuance date in the CT log	BR Section 3.2.2.4
Validation	Verify subject information is accurate in a Subordinate CA certificate	Date of certificate issuance	Issuance date in the CT log	BR Section 7.1.4.3
Data Used in Validation	Use random values for validation	No more than 30 days (or the time frame permitted for reuse of validated information for sections to the right denoted with an *)	From the random value creation date	BR Sections 3.2.2.4.2, 3.2.2.4.4, 3.2.2.4.6*, 3.2.2.4.7*, 3.2.2.4.13, 3.2.2.4.14, 3.2.2.4.15, 3.2.2.4.16, 3.2.2.4.17, 3.2.2.4.18, 3.2.2.4.19, 3.2.2.5.1*, 3.2.2.5.2, 3.2.2.5.5, Appendix C
Data Used in Validation	Use a request token containing a timestamp for validation	No more than 30 days	From token's creation	BR Section 1.6.1
Data Used in Validation	Obtain a certificate request and an executed subscriber agreement or terms of use	Prior to certificate issuance	Issuance date in the CT log	BR Section 4.1.2
Data Used in Validation	Reuse documents and data provided in section 3.2 or prior validations	No more than 825 days	Date on the document or date information was obtained, whichever is sooner	BR Section 4.2.1
Certificate Issuance	Issue a certificate	Within the TTL of the CAA record, or 8 hours, whichever is greater	The TTL of the CAA record OR from the CAA record check time	BR Section 3.2.2.8
Problem Reporting	Investigate a certificate problem report, provide a preliminary report to the subscriber and entity that filed the problem report, determine whether to revoke If applicable, revoke the certificate(s)	24 hours Within 24 hours or 5 days (refer to 4.9.1.1 below)	From problem report receipt	BR Section 4.9.5
Certificate Revocation	Revoke a subscriber certificate for the following reasons: 1. Subscriber requests in writing 2. Subscriber notifies request was not authorized 3. CA obtains evidence subscriber's private key was compromised 4. CA obtains evidence domain validation should not be relied upon	Within 24 hours	From revocation-related notice to published revocation	BR Section 4.9.1.1, 4.9.5
Certificate Revocation	Revoke a subscriber certificate for the following reasons: 1. Certificate no longer complies with 6.15 and 6.16 2. CA obtains evidence of misuse 3. Subscriber agreement or terms of use violation 4. Domain authorization or control is no longer legally permitted 5. Wildcard certificate used to authenticate fraudulently misleading Subordinate FQDN 6. Material change in certificate information 7. Certificate issuance not compliant with BRs or CP/CPS 8. Certificate information is inaccurate 9. Right to issue certs is revoked, unless CRL/OCSP maintained 10. Revocation required by CA's CP/CPS 11. Method exists to expose subscriber's private key to compromise	Should revoke within 24 hours, must revoke within 5 days	From revocation-related notice to published revocation	BR Section 4.9.1.1, 4.9.5
Certificate Revocation	Revoke a Subordinate CA's certificate for the following reasons: 1. Subordinate CA requested revocation in writing 2. Subordinate CA notifies issuance was not authorized 3. Issuing CA obtains evidence of key compromise 4. Issuing CA obtains evidence of misuse 5. Certificate issuance not compliant to BR's or CA's CP/CPS 6. Issuing CA determines certificate information is inaccurate or misleading 7. Subordinate CA or Issuing CA cessation of operations 8. Right to for Subordinate or issuing CA to issue certs is revoked, unless CRL/OCSP maintained 9. Revocation required by CA's CP/CPS	Within 7 days	From revocation-related notice to published revocation	BR Section 4.9.1.2 (4.9.5 implied)

Audit Reporting	Conduct a point-in-time readiness assessment	No earlier than twelve (12) months prior to issuing Publicly-Trusted Certificates	Issuance date of first publicly-trusted certificate	BR Section 8.1
Audit Reporting	Conduct a complete external audit	First, within ninety (90) days of issuing Publicly-Trusted Certificate Ongoing, not to exceed one (1) year	Issuance date of first publicly-trusted certificate From the previous period-end date (not the report date)	BR Section 8.1
Audit Reporting	Obtain an audit report for any delegated third parties to verify the delegated third party complies with these requirements for an audit period not to exceed one year	One year	From period-start to period-end	BR Section 8.4
Audit Reporting	Publish external audit report	Within three (3) months of the period-end *May exceed 3 months w/ explanatory letter from the auditor	Period-end date of the audit (not the report date)	BR Section 8.6
Internal Audits	Conduct audits of 3% or greater of the certificates issued based on a randomly selected sample, including: • Certificates issued by the CA (self-audit) • Certificates issued by a Subordinate CA • Certificates issued by a delegated third party employed by the CA, except those that undergo an annual audit meeting specified criteria in section 8.1 (also see section 8.4)	Quarterly	From the date the previous self-audit was completed	BR Section 8.7
Internal Audits	Perform an audit of delegated third parties to ensure compliance with the BR	Annually	From last period-end	BR Section 8.4 and 8.7
Retention	Retain audit logs	7 years	Date of oldest entry/ log file	BR Section 5.4.3
Retention	Retain all documentation related to • Certificate requests and verification thereof • Certificates and revocation thereof	7 years	After any certificate based on that documentation ceases to be valid	BR Section 5.5.2

***Only including effective dates for active certificates**