SC-63: Make OCSP Optional and Incentivize Automation

The ballot is proposed by the Chrome Root Program (Ryan Dickson and Chris Clements) and endorsed by Microsoft (Kiran Tummala) and Sectigo (Tim Callan).

Summary:

This pull request proposes updates to the *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates* related to making Online Certificate Status Protocol (OCSP) services optional for CAs. This proposal does not prohibit or otherwise restrict CAs who choose to continue supporting OCSP from doing so. If CAs continue supporting OCSP, the same requirements apply as they exist today.

Additionally, this proposal introduces changes related to CRL requirements including:

- CRLs must conform with the proposed profile.
- CAs must generate and publish either:
  - a full and complete, or
  - a set partitioned CRLs (sometimes called "sharded" CRLs), that when aggregated, represent the equivalent of a full and complete CRL.
- CAs issuing Subscriber Certificates must update and publish a new CRL...
  - within twenty-four (24) hours after recording a Certificate as revoked; and
  - Otherwise:
    - at least every seven (7) days if all Certificates include an Authority Information Access extension with an id-ad-ocsp accessMethod ("AIA OCSP pointer"), OR
    - at least every four (4) days in all other cases.

Finally, the proposal revisits the concept of a "short-lived" certificate, introduced in Ballot 153. As described in this ballot, short-lived certificates (sometimes called "short-term certificates" in ETSI specifications) are:

- **optional**. CAs will not be required to issue short-lived certificates. For TLS certificates that do not meet the definition of a short-lived certificate introduced in this proposed update, the current maximum validity period of 398 days remains applicable.

- **constrained to an initial maximum validity period of ten (10) days.** The proposal stipulates that short-lived certificates issued on or after 15 March 2026 must not have a Validity Period greater than seven (7) days.

- **not required to contain a CRLDP or OCSP pointer and are not required to be revoked**. The primary mechanism of certificate invalidation for these short-lived certificates would be through certificate expiry. CAs may optionally revoke short-lived certificates. The initial maximum certificate validity is aligned with the existing maximum values for CRL "nextUpdate" and OCSP response validity allowed by the BRs today.

Background and Justification:

- **Make OCSP Optional:** OCSP requests reveal details of individuals' browsing history to the operator of the OCSP responder. These can be exposed accidentally (e.g., via data breach of logs) or intentionally (e.g., via subpoena). Due to privacy concerns, several certificate consumer products represented in the CA/Browser Forum do not perform online OCSP checks by default - or have signaled interest in transitioning to privacy-preserving methods of communicating revocation status. Beyond privacy concerns, OCSP use is accompanied by a high volume of routine incidents and issues (1 and 2). Concern surrounding OCSP is further elevated considering the disproportionately high cost of offering these services reliably at the global scale of the Web PKI.

- **Require CRLs:** Given this ballot makes operating OCSP services optional for CAs, allow relying party software applications and certificate consumer user agents to consistently and reliably evaluate certificate revocation status using a privacy-preserving check. While many certificate consumer user agent installations do not rely on the processing of data contained in the CRL Distribution Points extension by default (i.e., they instead rely on custom status-checking mechanisms like CRLSets or CRLite that aggregate and communicate revocation status), the broader ecosystem impact of making the presence of both OCSP and CRLDP optional in Web PKI certificates is not yet understood and is not being considered at this time.

- **Short-Lived Certificates:** Subscriber certificate expiration is broadly and reliably enforced across major certificate consumers, while the same is not for certificate revocation. From a security perspective, short-lived certificates may reduce the aperture of an attack where subscriber private keys are compromised - limiting the maximum attack window to just a few days. Short-lived certificates also present an opportunity to further reduce the size of Certificate Revocation Lists, which are being relied upon by many certificate consumers represented in the Forum and introduced as required by this proposal.

Proposed Transition Period:

The proposed effective date for this ballot is 2024-03-15. However, CAs must consider the following:

- **OCSP:** CAs must continue supporting existing OCSP services for as long as the corresponding HTTP URI exists within a valid, unrevoked certificate.

- **CRLs:** CAs may begin including the CRL Distribution Points extension in subscriber certificates at any time. However, all non-short-lived subscriber certificates issued after the effective date MUST include the CRL Distribution Points extension as described in the ballot text.

- **Short-Lived Certificates:** May optionally be issued without CRLDP or OCSP pointers, as described in this proposed ballot, once these changes have been made effective.

Additional Areas Considered:

- **Impact on Certificate Transparency Log Operators**: Depending on the number of short-lived certificates issued, Certificate Transparency log operators may need to reduce the temporal sharding period of logs from one year to a shorter period. Although log operators already have to manage the size and capacity of their CT logs, short-lived certificates would be an additional growth factor that needs to be considered. Since presenting this proposal in October 2022, we have not heard concerns from CT log operators related to the impact of short-lived certificates on logs.

- **Impact on Certificate Consumers/Relying Party Software:** It's possible that not all user agents that rely on certificates issued from the Web PKI support CRLs, given the expectation that the Baseline Requirements require OCSP. Since presenting this proposal in October 2022, we have not heard concerns from certificate consumers or relying party software developers regarding CRL support.

- **Opportunity for OCSP Stapling / "must-staple":** In the months leading to this ballot, Server Certificate Working Group discussion focused on the value of OCSP Stapling and future opportunity for usage of the "must-staple" extension to contend with the privacy concerns related to "online" OCSP checks. At that time (February 2023) it was estimated that:
    - the "must-staple" extension was only present in approximately .0622% of time-valid TLS server certificates that assert a CA/Browser Forum policy OID.
    - that approximately 8% of connections in Firefox 110 Beta served a stapled response (only known public telemetry).

Independent of usage statistics, relying parties can't consistently depend on OCSP stapling for security unless responses are stapled on all connections. Further, even if the web server ecosystem had improved support for OCSP-stapling and we could require the use of the "must-staple" extension, we'd remain dependent upon robust and highly-reliable OCSP services, which have been an ongoing ecosystem challenge (1 and 2).

- **Adoption of SC-61:** SC-61 introduced requirements related to revocation reason codes into Section 7.2.2 of the Baseline Requirements. These requirements were integrated into the proposed updates to Section 7.2 (CRL Profile). This doc presents a mapping of the SC-61 language as it is presented in this proposal, given some language was changed.

Summarizing Comments and Questions Resulting from Server Certificate Working Group Public Discussion

(last updated May 3, 2023 at 7:30 AM ET):

Comments:

1. Dimitris:
    - emphasized the ballot changes existing CRL requirements, and that CAs should be aware of these changes.
    - questioned whether the newly proposed issuance frequency (at least once every 24 hours) makes sense for CAs that aren't actively issuing certificates.
    - questioned whether the newly proposed issuance frequency (at least once every 24 hours) makes sense for CAs that are actively issuing certificates, given the Apple Root Store Policy implies Apple checks for new CRLs every 4 hours.
    - proposed changes to the issuance frequency depending on whether or not leaf certificates were revoked during the period between the last CRL's "thisUpdate" time and the expected subsequent publication (which may not be the same time as described in the last CRL's "nextUpdate" time.)
    - Aaron proposed an alternative approach to address the concerns related to CRL issuance frequency, and indicated, instead, a preference for a "carve-out" for CAs that have not issued any certificates
    - Dimitris offered clarification on prior comments (re: new CRLs every 4 hours), and appeared to agree with Aaron's carve-out proposal.

- Aaron requested further clarification related to the 4 hour requirement and how it would be meaningfully measured.
- Dimitris offered clarification. He also reinforced that increasing CRL issuance frequency when there are no changes to the contents of the revoked certificates list does not increase security.
- Aaron emphasized the value of automation, and described how a set schedule is easier, safer, and more reliable than a variable schedule based on additional criteria. Aaron expressed a preference for the 24 hour timeline.
- Dimitris emphasized the BRs are the minimum requirements and are not meant to be overly prescriptive. CAs should be free to choose how they satisfy the minimum requirements. Agrees that CRL issuance frequency is meant to be automated.
- [Ryan attempted to address the concerns above in an updated branch [PR with diffs].]

2. Aaron:
   - added some editorial comments on the PR
     i. [ryan still needs to address these]
   - expressed concern related to the required inclusion of the CRLDistributionPoints extension in subscriber certificates, specifically related to how its inclusion will result in "a number of certificate consumers will begin executing old codepaths and downloading them directly."

3. Wayne:
   - re-highlighted past concern re: potential effects on the broader ecosystem, specifically clients that rely only on OCSP for revocation checking.
   - expressed concern that the ballot does not prevent CAs from sharding CRLs to the point that individual sites are easily or exclusively identified, so even allowing cRLDPs in end-entity certificates seems to violate the purpose of this ballot.
   - Asked Is there some other reason to begin requiring cRLDPs if the CA chooses to operate an OCSP service after this ballot goes into effect?

Unanswered Questions:

1. [Aaron] Can CA owners share:
   - How many certificates you have which embed a CRLDP?
     i. While not a CA, Chrome Root Program shared some data via Censys query re: use of CRLDP today. Interpretation of the results is that ~35% of all time-valid leafs asserting a BR certificate policy OID contain a CRLDP, and that ~88% of the issuing CAs issuing those leafs include CRLDP by

default on 100% of certs issued (that contain a BR policy OID). Feedback on the queries to offer more accurate results are welcome.

- How many requests-per-second you receive for that CRLDP as a result?

Summarizing GitHub Comments & Adjudication

Date	Commenter	Comment Type	Comment	Resolution	Status
5/3/2023	Aaron	Editorial	**From: "***partitioned (i.e., "sharded") CRLs, that when aggregated, represent the equivalent of the full and complete CRL."* **To:** *"partitioned (i.e., "sharded") CRLs that, when aggregated, represent the equivalent of a full and complete CRL."*	Accepted suggestion.	Closed.
5/3/2023	Aaron	Editorial	**From: "***the corresponding CA Private Key is destroyed"* **To:** *"the corresponding CA Private Key is destroyed."*	Accepted suggestion.	Closed.
5/3/2023	Aaron	Substantive	On CRL Issuance Frequency Table: ☐ 1) Can we avoid using the phrase "has revoked?" (How can a CA be said to "have revoked" something if they haven't published a CRL containing it yet?) ☐ 2) Need to clean up "last CRL" / "thisCRL" language, because as currently described, satisfying these requirements may be impossible in some conditions. ☐ 3) Is it intentional that the SHOULD here is also 4 hours, and not 24 hours as suggested in Dimitris' latest message? Still prefers "CAs issuing Subscriber Certificates SHALL update and reissue CRLs at least once every 24 hours". Comment applies to both subject CA categories. Related, on thread, Dimitris recommended "The CA MUST update and reissue CRLs at least 1) once every 7 days; or 2) within 24 hours after recording that a certificate must be	Addressed in https://github.com/ryancdickson/staging/blob/make-ocsp-optional-updates/docs/BR.md#497-crl-issuance-frequency Removes table and converts back to a simpler bulleted list borrowing Dimitris' latest proposal.	Closed.

			revoked." Adopting this language would allow us to go back to the bulleted list, which is a bit more streamlined than the table. Ryan will try that approach.		
5/3/2023	Aaron	Clarification	**From:** *"If the CA supports OCSP, the following requirements SHALL apply:"* **To:** *"If the CA signs OCSP responses either directly or through a delegated OCSP responder, the following requirements SHALL apply."* Clarify: Is it acceptable for a CA to operate an OCSP service for only some of the non-expired certificates it has issued? Corey shared language used in another PKI based on the BRs and EVGs where OCSP is optional for subscriber certificates. : "For the status of Subscriber Certificates which include an Authority Information Access extension with a id-ad-ocsp accessMethod ("AIA OCSP pointer")"	Accepted suggestion with modifications. **From:** "*If the CA signs OCSP responses either directly or through a delegated OCSP responder, the following requirements SHALL apply."* **To:** "*The following SHALL apply for communicating the status of Certificates which include an Authority Information Access extension with an id-ad-ocsp accessMethod ("AIA OCSP pointer")."*	Closed.
4/27/2023	Aaron	Clarification	Summarized: Move the effective dates for short-lived certificates referenced in 6.3.2 to the definitions table. It's somewhat confusing here.	Accepted with slight modification. "For Certificates issued on or after 15 March 2024 and prior to 15 March 2026, a Subscriber Certificate with a Validity Period less than or equal to 10 days (864,000 seconds). For Certificates issued on or after 15 March 2026, a Subscriber Certificate with a	Closed.

				Validity Period less than or equal to 7 days (604,800 seconds).”	
4/27/2023	Aaron	Editorial	Summarized: Reference the term Short-Lived Subscriber Certificate rather than describing it in most instances.	Accepted.	Closed.
4/27/2023	Aaron	Editorial	From: Minimally, CAs MUST issue either a "full and complete" CRL - or "partitioned" CRLs. Aside from the presence of the `IssuingDistributionPoint` extension (OID 2.5.29.28) in partitioned CRLs, both CRL formats are syntactically the same from the perspective of this profile. to : Minimally, CAs MUST issue either a "full and complete" CRL or "partitioned" CRLs. Aside from the presence of the `IssuingDistributionPoint` extension (OID 2.5.29.28) in partitioned CRLs, both CRL formats are syntactically the same from the perspective of this profile.	Accepted.	Closed.
4/27/2023	Aaron	Editorial	Re-phrashing the introduction to 4.9.7 where we describe full and complete and partitioned CRLs may improve clarity.	Accepted.	Closed.
4/27/2023	Aaron	Clarification	Clarify use of “monotic” in the CRL profile. From: `contain an INTEGER greater than or equal to zero (0) and less than 2¹⁵⁹, and convey a monotonically increasing sequence.` To: `contain an INTEGER greater than or equal to zero (0) and less than 2¹⁵⁹, and convey a strictly increasing sequence.`	Accepted.	Closed.
4/27/2023	Aaron	Clarification	The description of the revokedCertificates extension is too strict. “This description is too strict. CRL entries are required to remain on a CRL for one CRL issuance cycle *after* they expire (so that a cert which is revoked seconds before it expires appears on at least one CRL anyway). This requirement would force a CA to violate *that* requirement if the CA has only expired-and-revoked certificates left, which is a common scenario for the very last CRL published at the end of a CA's issuing lifetime.”	Addressed in https://github.com/ryancdickson/staging/commit/5cc135f2eec7241dd3868369e50b200b641cf813	Closed.
5/15/2023	Rob	Clarification	In BR v2.0.0, this note refers to the paragraph immediately preceding it (that begins "When a CA obtains verifiable evidence of Key Compromise..."). Moving the note (so that it becomes a footnote for this table) without also moving that paragraph loses (or at least confuses) essential context and creates an apparent contradiction. i.e., "The date and time which revocation occurred"		

			is NOT "Backdating the revocationDate field". To resolve this, I suggest moving the "When a CA obtains..." paragraph to the beginning of this footnote, and then updating the first part of the revocationDate description to say something like "Normally the date and time at which revocation occurred, although see footnote for circumstances under which backdating is permitted." Also, I'm curious: Do there really exist "TLS implementations that process the revocationDate field as the date when the Certificate is first considered to be compromised"? Or has this language accidentally been imported from the Code Signing BRs, which permit the RFC5280-non-compliant backdating of the revocationDate field as a workaround for the fact that Microsoft's stack doesn't support the RFC5280 Invalidity Date extension? ISTM that TLS implementations only care about the revocation status of a certificate and pay no heed to any timestamps that indicate how far in the past the revocation occurred, whereas Code Signing does care about the "revocation time" and "invalidity date".		