



Discussion on CP vs CPS vs CP/CPS, expectations for RFC 2119 language

F2F#68 23 September 2026 | Vienna, Austria

Presenter: Dimitris Zacharopoulos (HARICA)

Prior discussions

- ▶ CCADB thread <https://groups.google.com/a/mozilla.org/g/dev-security-policy/c/QECjs4bxNQw/m/ibl6lLlgCQAJ>

Multiple terms

Discussion on CP vs CPS vs CP/CPS, expectations for RFC 2119 language, "descriptive" vs "prescriptive", or "vague", "narrative", "non-technical" vs "specific", "detailed", "technical"

- ▶ CP → WHAT

- ▶ *“The CA SHALL inspect any document relied upon under this Section for alteration or falsification.”*
- ▶ The CA MUST inspect documents for alterations/falsifications but doesn't say “HOW”

- ▶ CPS → HOW

- ▶ “check against a source of light, search for the decorative paper, etc”
- ▶ Expands on the “WHAT” and describes the CA's implementation that meets the “HOW”

Multiple terms

Discussion on CP vs CPS vs CP/CPS, expectations for RFC 2119 language, "descriptive" vs "prescriptive", or "vague", "narrative", "non-technical" vs "specific", "detailed", "technical"

- ▶ Prescriptive → “specific”, “detailed”, or “technical”. It says what needs to be done with a high level of specificity that there is very little room for interpretation or customization by the CA.
 - ▶ *“Subscriber Certificates... MUST NOT have a Validity Period greater than 200 days.”*
 - ▶ *“The CA SHALL develop, maintain, and implement documented procedures that identify and require additional verification activity for High Risk Certificate Requests...”*
 - ▶ *“CAs SHALL NOT issue Certificates containing Internal Names...”*
- ▶ Descriptive → "vague", "narrative", or "non-technical“. It says what needs to be done but leaves a lot of room for the CA to decide how to do it. Examples from LE's CPS.
 - ▶ *Validity Period: Up to 100 days*
 - ▶ *CA maintains a list of high-risk domains and blocks issuance of certificates for those domains.*
 - ▶ *The CA Server is periodically updated with the latest version of the Public Suffix List and consults the ICANN domains section for every requested DNS identifier. The CA server rejects issuance requests for DNS identifiers that do not have a Public Suffix in the ICANN domains section.*

Expectations

- ▶ Where should “specific”, “technical”, “detailed” requirements go? In the CP, the CPS or the CP/CPS?
- ▶ It doesn’t matter! Some requirements/practices will be described in “vague”, “narrative”, or “non-technical” and some with “specific”, “technical”, “detailed” language
- ▶ The CABF Baseline Requirements are meant to be a CP (the “WHAT”). However, there is a lot of language describing the “HOW”.
- ▶ The CA’s CP, CPS, CP/CPS is primarily aimed to be read by humans (Subscribers, Relying Parties).
- ▶ Technical language is important and RFC 2119 keywords are supposed to have a special meaning/interpretation. Readers must understand the subtle difference in RFC 2119 keywords
- ▶ What about the interpretation of the words “can”, “will”, and other plain English terms? Can the CABF provide guidance to readers on that?

Guidance for CAs and Readers

- ▶ For CAs when describing the “how”
 - ▶ Avoid the use of certain words that create ambiguity (e.g. “will”, “should”?).
 - ▶ Decide about interpretation of RFC 2119 keywords with capital or lowercase letters (SHALL vs shall)
 - ▶ ...
- ▶ For Readers
 - ▶ “can” to be interpreted as “may”?
 - ▶ ...
 - ▶ ...

Next steps

(brainstorming.... not concrete proposals)

- ▶ CP/CPS editorial guidelines
- ▶ Parse the BRs to
 - ▶ flag “descriptive” vs “prescriptive” language
 - ▶ flag “policy” (WHAT) vs “practice” (HOW)
 - ▶ For the “HOW”, CAs must implement exactly what is described
 - ▶ For the “WHAT”, CAs must expand and describe “HOW” they meet the policy