Summer 2022 CA/B Forum F2F

Validation Sub-committee
Progress since Spring F2F

• SC-54 (Onion cleanup) passed and became effective late April
• Identification and discussion of several EVG “cleanup” items
  • EV CRL “3-second rule”
  • Enterprise RA language cleanup
• Certificate Profiles
  • Revisiting discussions
  • Establishing a transition plan
  • Pushing back some items to version 2
• Migration from Trello to Github Project for tracking
Certificate Profiles

• Major reformat of BR Section 7.1
• Some normative changes are introduced
  • Every CA should be analyzing this draft ballot to determine impact

• [https://github.com/sleevi/cabforum-docs/pull/36](https://github.com/sleevi/cabforum-docs/pull/36)
Impact Analysis – A few caveats

• The affected Certificate counts are not exact but give a rough estimate
  • Censys.io may not have an accurate, up-to-date calculation of whether a particular Certificate is trusted by at least one Root Program
  • There is double-counting of pre-certificate/final Certificate pairs if the final Certificate is logged to CT and/or ingested by a Censys.io scan
  • Sometimes, an expired Certificate is mistakenly flagged as still valid/trusted
MUST (NOT)-level changes - Validity

• There are now restrictions on backdating for Certificates
  • The exact requirements are dependent on the type of Certificate (Root, Subordinate CA, Subscriber, etc.)

• The are now restrictions on forward-dating for Certificates
  • Prohibited entirely for CA Certificates
  • Allowed for up to 48 hours for Subscriber Certificates

• Root validity period is now capped at 25 years (matches MSFT Root Policy requirement)
MUST (NOT)-level changes - Subject

- There is now a specific, well-defined ordering of attributes that MUST be followed
- Multiple instances of the same attribute are prohibited
  - GRID Certificates are now prohibited. ~13K Certificates affected:
    https://search.censys.io/certificates?q=parsed.extensions.extended_key_usage.server_auth%3A+true+and+tags.raw%3Atrusted+and+parsed.subject.domain_component%3A+%2A
MUST (NOT)-level changes - Subject

- Domain Names and IP Addresses in any attribute must be validated per section 3.2.2.4/3.2.2.5
  - Example: "Co.Ltd" is a Domain Name within "O=ACME Enterprises Co.Ltd", so the Applicant MUST validate "co.ltd" per 3.2.2.4
  - Rough estimate of ~392K certificates may be affected
MUST (NOT)-level changes - KeyUsage

• Subscriber Certificates:
  • All bits MUST be unset except for the following:
  • RSA: digitalSignature (SHOULD), keyEncipherment (MAY) (but both together are NOT RECOMMENDED)
    • 14.31M certs with dataEncipherment:
      https://search.censys.io/certificates?q=parsed.extensions.extended_key_usage.server_auth%3A+true+and+tags.raw%3Atrusted+and+parsed.extensions.key_usage.data_encipherment%3A+true
  • ECDSA: digitalSignature (MUST)
    • 14.01 K ECDSA certs with keyAgreement:
      https://search.censys.io/certificates?q=parsed.extensions.extended_key_usage.server_auth%3A+true+and+tags.raw%3Atrusted+and+parsed.subject_key_info.ecdsa_public_key.curve%3A+%2A+and+parsed.extensions.key_usage.key_agreement%3A+true
MUST (NOT)-level changes - KeyUsage

• OCSP Responders:
  • All bits MUST be unset except for digitalSignature
  • 396 certs with contentCommitment

  https://search.censys.io/certificates?q=%28parsed.extensions.extended_key_usage.ocsp_signing%3A+true+and+parsed.extensions.key_usage.content_commitment%3A+true%29+AND+tags.raw%3A+%22trusted%22&
MUST (NOT)-level changes - KeyUsage

• OCSP Responders:
  • All bits MUST be unset except for digitalSignature
  • 396 certs with contentCommitment
    https://search.censys.io/certificates?q=%28parsed.extensions.extended_key_usage.ocsp_signing%3A+true+and+parsed.extensions.key_usage.content_commitment%3A+true%29+AND+tags.raw%3A+%22trusted%22&
MUST (NOT)-level changes - certPolicies

• All Certificates:
  • userNotice (i.e., explicitText) is prohibited
  • 1.63 million Certificates affected
    https://search.censys.io/certificates?q=parsed.extensions.extended_key_usage.server_auth%3A+true+and+tags.raw%3Atrusted+and+%28parsed.extensions.certificate_policies.user_notice.explicit_text%3A+*+or+parsed.extensions.certificate_policies.user_notice.notice_reference.notice_numbers%3A+*+or+parsed.extensions.certificate_policies.user_notice.notice_reference.organization%3A+*%29
MUST (NOT)-level changes - certPolicies

• OCSP Responders:
  • Effective 2022-11-01, the inclusion of this extension is prohibited
  • 815 affected Certificates
  • https://search.censys.io/certificates?q=parsed.extensions.extended_key_usage.ocspSigning%3A+true+and+tags.raw%3Atrusted+and+parsed.extensions.certificate_policies.id%3A+%2A+and+not+parsed.extensions.basic_constraints.is_ca%3A+true
MUST (NOT)-level changes - EKU

• Subscriber Certificates:
  • Inclusion of non-TLS–related EKUs is prohibited (e.g., id-kp-emailProtection)

• Cross Certificates:
  • The entirety of the Certificate profile MUST follow the relevant specification that defines the extension, even if deviations from that profile are compliant with the BRs
MUST (NOT)-level changes – Authority Information Access

• Non-HTTP (i.e., LDAP and FTP) OCSP and CA Issuers URIs are prohibited
  • 17.30K affected certificates

• Multiple OCSP and CA Issuers URIs MUST be encoded in order of preference (weight) by the CA
MUST (NOT)-level changes – CRL Distribution Points

• Non-HTTP (i.e., LDAP and FTP) URIs are prohibited
  
• 69.29K affected certificates

MUST (NOT)-level changes – Subject Key Identifier

- MUST be a unique value (within the scope of the Issuing CA) corresponding to the certified Public Key
MUST (NOT)-level changes – Non-TLS ICAs

• The Subject of a non-TLS ICA MUST be validated and encoded according to the TLS BRs
  • Even if another specification (e.g., S/MIME BRs) defines its own validation and encoding requirements, the TLS BRs prevail
• Required conformance to RFC 5280 (RFC 6818 not allowed)
• All IP Addresses and Domain Names in nameConstraints MUST be validated per 3.2.2.4/3.2.2.5
• All dirName NameConstraints MUST be validated per 3.2
• If a rfc822Name Name Constraint contains a Mailbox Address, the CA MUST validate the domain-part per 3.2.2.4
• Subject Public Key types are restricted to those allowed by the BRs (e.g., EdDSA, Brainpool, etc. is prohibited)
• certificatePolicies MUST NOT contain anyPolicy if the Subordinate CA is not issued to an Affiliate (mirrors TLS ICA profile)
SHOULD (NOT)-level changes – Subject

• streetAddress is now a SHOULD NOT
  • 23.78K affected Certificates
    https://search.censys.io/certificates?q=parsed.extensions.extended_key_usage.server_auth%3A+true+and+tags.raw%3Atrusted+and+tags.raw%3Aleaf+and+parsed.subject.street_address%3A+%2A

• postalCode is now a SHOULD NOT
  • 23.5K affected Certificates
    https://search.censys.io/certificates?q=parsed.extensions.extended_key_usage.server_auth%3A+true+and+tags.raw%3Atrusted+and+tags.raw%3Aleaf+and+parsed.subject.postal_code%3A+%2A

• Any attribute not explicitly listed in the ordering table SHOULD NOT be included
SHOULD (NOT)-level changes – KeyUsage

• RSA: digitalSignature and keyEncipherment together is now a SHOULD
  NOT
  614.74 million affected Certificates
  https://search.censys.io/certificates?q=tags.raw%3Atrusted+and+parsed.extensions.extended_key_usage.server_auth%3A+true+and+parsed.extensions.key_usage.digital_signature%3A+true+and+parsed.extensions.key_usage.key_encipherment%3A+true
SHOULD (NOT)-level changes – certPolicies

- The first policy OID SHOULD be a reserved CABF policy OID
SHOULD (NOT)-level changes – Authority Key Identifier

• SHOULD be included in Root Certificates
  • 224 affected Root Certificates
  
  [link to query]
  https://search.censys.io/certificates?q=tags.raw%3Aroot+and+not+parsed.ext
don+extensions.authority_key_id%3A+%2A+and+tags.raw%3Atrusted
SHOULD (NOT)-level changes – Name Constraints

• SHOULD not contain permittedSubtrees or excludedSubtrees that are not of type dirName, iPAddress, or dSName
SHOULD (NOT)-level changes – Other Extensions

• SHOULD NOT contain extensions that are not explicitly listed in the Extensions table
  • MSFT Template Name, etc.
  • QCStatements
  • TLSFeature (OCSP Must-Staple)
Profiles v2

• Tackling some of the items deferred from v1
Who defines OIDs?

• 7.1.2.4 (the “any other extension” requirement) and 7.1.2.3 (a) (Policy OID requirement) refer to an Applicant “owning an OID” or the CA “defining an OID”, respectively

• How is ownership determined?
  • Can use be granted?
Certificate Policies

- V1 of Profiles allows for cPSUri across the board (in all non-Root Certificate types)
  - It has been proposed to disallow all qualifiers for Sub CA Certificates with anyPolicy in v2
- V1 allows for Certificate Policies extension in OCSP responders until the sunset date
Naming

• V1 of Profiles makes OrganizationName in IV certificates “NOT RECOMMENDED”
  • Proposed in v2 to make MUST NOT

• Defining Naming requirements for OCSP responders

• Define requirements for dnQualifier attribute to enable sunset of CN
Other items

• Define requirements for several extensions
  • QCStatements
  • TLSFeature
  • CABFOrganizationId

• Prohibit all non-TLS issuance
Questions?