Possible conflict between Microsoft Root Certification Technical Requirement V 2.0 and CABF Baseline Requirement about extendedKeyUsage

Chunghwa Telecom Co., Ltd.
Li-Chun CHEN,
Engineer, CISSP, CISM, CISA, PMP
realsky@cht.com.tw

CA/Browser Forum Meeting 33
September, 16 , 2014

RFC 5280 about Extend Key Usage

- 4.2.1.12. Extended Key Usage
- This extension indicates one or more purposes for which the certified public key may be used, in addition to or in place of the basic purposes indicated in the key usage extension. In general, this extension will appear only in end entity certificates. This extension is defined as follows:

  id-ce-extKeyUsage OBJECT IDENTIFIER ::= { id-ce 37 }

  ExtKeyUsageSyntax ::= SEQUENCE SIZE (1..MAX) OF KeyPurposeId

  KeyPurposeId ::= OBJECT IDENTIFIER

CABF BR about Extended Key Usage

- CABF try the best to conform the BR to RFC 5280
- In Appendix B – Certificate Extensions
  - (a) Root CA Certificate
    - D. extendedKeyUsage

      This extension MUST NOT be present.
  - (b) Subordinate CA Certificate
    - G. extkeyUsage (optional)
      - Only "Technically Constrained Subordinate CA Certificate" MUST include an Extended Key Usage (EKU) extension.

      ** Generally Extended Key Usage will only appear within end entity certificates (as highlighted in RFC 5280 (4.2.1.12)), however, Subordinate CAs MAY include the extension to further protect relying parties until the use of the extension is consistent between Application Software Suppliers whose software is used by a substantial portion of Relying Parties worldwide.
  - (c) Subscriber Certificate
    - F. extKeyUsage (required)
      - id-kp-serverAuth or id-kp-clientAuth or both values MUST be present
      - id-kp-emailProtection MAY be present

CABF BR about Technically Constrained Subordinate CA Certificate

- Technically Constrained Subordinate CA Certificate:
  - A Subordinate CA certificate which uses a combination of Extended Key Usage settings and Name Constraint settings to limit the scope within which the Subordinate CA
- In section 9.7 of CABF BR
  - For Technically Constrained Subordinate CA Certificate
    - the certificate MUST include an Extended Key Usage (EKU) extension specifying all extended key usages that the Subordinate CA Certificate is authorized to issue certificates for.
    - if the Subordinate CA Certificate includes the id-kp-serverAuth extended key usage, then the Subordinate CA Certificate MUST include the Name Constraints X.509v3 extension with constraints on dNSName, iPAddress and DirectoryName…

Microsoft Root Certificate Program – Technical Requirement V2.0 (Microsoft TR V2.0)

- In "INTERMEDIATE / ISSUING CA CERTIFICATES" section:
  - Intermediate CA certificates under root certificates submitted for distribution by the Program must be configured to separate server authentication (SSL) from code signing and time stamping uses. A single issuing CA must not be used to issue both server authentication and code signing certificates.
  - Rollover root certificates will not be accepted that combine server authentication with code signing uses unless the uses are separated by application of EKUs at the intermediate CA certificate level that are reflected in the whole certificate chain.
- Does that means Microsoft will only accept a new root certificate if all its subordinate CA certificates contain the extendedKeyUsage extension? It seems Microsoft TR 2.0 intends to require the extendedKeyUsage extension present in all subordinate CA certificates even if they are not "technically constrained".

Microsoft Root Certificate Program – Technical Requirement V2.0 (Microsoft TR V2.0)

- In "INTERMEDIATE / ISSUING CA CERTIFICATES" section:
  - Intermediate CA certificates under root certificates submitted for distribution by the Program must be configured to separate server authentication (SSL) from code signing and time stamping uses. A single issuing CA must not be used to issue both server authentication and code signing certificates.
  - Rollover root certificates will not be accepted that combine server authentication with code signing uses unless the uses are separated by application of EKUs at the intermediate CA certificate level that are reflected in the whole certificate chain.
- Does that means Microsoft will only accept a new root certificate if all its subordinate CA certificates contain the extendedKeyUsage extension? It seems Microsoft TR 2.0 intends to require the extendedKeyUsage extension present in all subordinate CA certificates even if they are not "technically constrained".

Suggest more Application Software Providers to join CA/Browser Forum

- We suggest more Application Software Providers to join CA/Browser Forum to promote B.R. Code signing and E.V. code signing
  - Oracle’ s Java Root Certificate program
  - IBM (IBM’ s JAVA SDK)
  - Adobe (They charged USD$7,500 annual fee for Adobe Approved Trust List)


Value Creator for
Investors, Customers, Employees, and Society
Thank you!