Suggestions about Draft of Baselines for Code Signing and Microsoft Root Certification Technical Requirement V 2.0

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
```

- *: it is also the same in RFC 3280

Code sign B.R. Draft vs. Microsoft R.C.P. T.R. V2.0 (1/2)

Code Signing B.R. Draft	Microsoft Root Certificate Program Technical Requirement V.2.0
Appendix B **Certificate Extensions (Normative)** **(2) Subordinate CA Certificates** F. extkeyUsage (optional) The id-kp-codeSigning value MUST be present. Other values SHOULD NOT be present. This extension SHOULD be marked non-critical.	Separation of SSL and Code Signing Key Uses 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.[11]

Code sign B.R. Draft vs. Microsoft R.C.P. T.R. V2.0 (2/2)

Code Signing B.R. Draft	Microsoft Root Certificate Program Technical Requirement V.2.0
(3) Subscriber Certificates F. extKeyUsage (required) The value id-kp-codeSigning [RFC5280] MUST be present. The value anyExtendedKeyUsage (2.5.29.37.0) MUST NOT be present. Other values SHOULD NOT be present. If any other value is present, the CA MUST have a business agreement with the platform vendor to issue the platform specific code signing certificate.	[11] SEPARATION OF SSL AND CODE SIGNING USES Example 1. Fabrikam CA issues SSL and code signing certificates, and wants to issue from a new or rollover root certificate. The root certificate may be enabled with both the server authentication and code signing EKU, provided that their CPS adequately reflect that SSL certificates are issued from an intermediate CA with the server authentication EKU enabled, and code signing certificates are issued from a separate intermediate CA with the code signing authentication EKU enabled. Example 2. Contoso CA also sells SSL and code signing certificates. Their certificate operations allow them to issue from separate root certificates (best practice). One root certificate will be enabled for server authentication, and the other root will be enabled for code signing.

Please suggest IETF PKIX Working Group to modify RFC 5280 about EKU first

- We don’ t know the reason why Microsoft asks an intermediate CA configured to separate sever authentication (SSL) from code signing and time stamping uses.
- We think it is adequate if an intermediate CA following Code signing B.R. and is audited. For example:
  - 9.2.1. Subject Alternative Name Extension
    - This field MUST be present, MUST contain a permanentIdentifier (1.3.6.1.5.5.7.8.3) name form as defined in RFC 4043, and MUST NOT contain a Domain Name or IP Address.
- We wish Microsoft to suggest IETF PKIX Working Group to modify RFC 5280 about EKU first.

Another way about code signing in windows

- For a pki, if its Root CA is already in Microsoft Root Certificate Program , the end entity certificate of that PKI can sign a code with its digital signature key usage.
  - Relying party can verify the code signer of above entity certificate.

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!