WebTrust Audit Applicability (DRAFT)

	RKGC	CA	EV - SSL	Baseline - SSL + Network	EV - CS	Baseline - CS	Additional Microsoft
Private PKI	Optional	Optional	N/A	Optional	N/A	Optional[1]	N/A
Publically-Trusted Commercial PKI - SSL	Required	Required	N/A	Required	N/A	N/A	See footnote 3
Publically-Trusted Commercial PKI - EV SSL	Required	Required	Required	Required	N/A	N/A	See footnote 3
Publically-Trusted Commercial PKI - CS	Required	Required	N/A	Not Required	N/A	Required[1]	See footnote 3
Publically-Trusted Commercial PKI - EV CS	Required	Required	N/A	Not Required	Required	Required[1]	See footnote 3
Publically-Trusted Commercial PKI - All other uses	Required	Required	N/A	Not Required	N/A	N/A	See footnote 3
Publically-Trusted Government PKI - SSL	Required	Required[2]	N/A	Required[2]	N/A	N/A	See footnote 3
Publically-Trusted Government PKI - EV SSL	Required	Required[2]	Required	Required[2]	N/A	N/A	See footnote 3
Publically-Trusted Government PKI - CS	Required	Required[2]	N/A	Not Required	N/A	Required[1,2]	See footnote 3
Publically-Trusted Government PKI - EV CS	Required	Required[2]	N/A	Not Required	Required[2]	Required[1,2]	See footnote 3
Publically-Trusted Government PKI - All other uses	Required	Required[2]	N/A	Not Required	N/A	N/A	See footnote 3
PKI X-Cert with USA Federal Bridge	Required	Required[5]	N/A	N/A	N/A	N/A	N/A

Reporting Requirements

For all WebTrust audit schemes, the intial audit can be either (1) as at a point in time, or (2) over a period of time (minimum period of coverage of 2 months and not to exceed 12 months). All subseq
time (minimum period of coverage of 2 months not to exceed 12 months). NOTE: Point in time audits are not eligible for a WebTrust seal.

Footnotes

[1] Baseline for Code Signing is currently under development. Audits are only required once the requirements and audit criteria have been developed and finalised

[2] Until 15 January 2017, Microsoft will accept an audit equivalency in lieu of a WebTrust audit. Post 2017, Microsoft will still accept an audit equivalency for non-SSL Government PKIs, and for SSL PKIs providing the audit equivalency incorporate
Baseline Requirements. Refer to http://social.technet.microsoft.com/wiki/contents/articles/26675.windows-root-certificate-program-audit-requirements-for-cas.aspx.

[3] Microsoft requires all End-Entity certificates to have OCSP available as a status checking mechanism (regardless of the certificate type) and that all certificates have at least 8 bytes (64 bits) of entropy in the serial number. Refer to http://social.technet.microsoft.com/wiki/contents/articles/1760.windows-root-certificate-program-technical-requirements-version-2-0.aspx

[4] Mozilla does not currently make a distinction between Commerical and Government CAs. Therefore, the requirements for Commerical CAs apply equally to a Government CA if part of the Mozilla Root Programme.

[5] Includes special reporting requirements for the Federal PKI

[6] Specific CP and CPS disclosures required; must map to CP of Federal Bridge

Additional Mozilla	Additional FPKI
N/A	N/A
N/A	N/A
N/A	N/A
N/A	N/A
N/A	N/A
N/A	N/A
See footnote 4	N/A
See footnote 4	N/A
See footnote 4	N/A
See footnote 4	N/A
See footnote 4	N/A
N/A	See footnote 6

uent audits must be over a period of

ɜs the current revision of the CAB Forum SSL