

WebTrust Engagement Applicability
Based on current CA/Browser Forum and Other Requirements

Last Updated: 31-August 2023

	RKGC ⁷	Key Protection ⁸	CA	EV SSL	SSL Baseline + Network	CS Publicly Trusted	S/MIME ¹¹	Network Security ¹⁰	VMC	Additional Browser	Additional FPKI	RA
Private PKI	Optional	Optional	Optional	N/A	Optional	Optional ¹	N/A	Optional	N/A	See footnote 3	N/A	See footnote 9
Publicly-Trusted Commercial PKI - SSL	Required	Required	Required	N/A	Required	N/A	N/A	Required	N/A	See footnote 3	N/A	See footnote 9
Publicly-Trusted Commercial PKI - EV SSL	Required	Required	Required	Required	Required	N/A	N/A	Required	N/A	See footnote 3	N/A	See footnote 9
Publicly-Trusted Commercial PKI - CS	Required	Required	Required	N/A	Not Required	Required ¹	N/A	Required	N/A	See footnote 3	N/A	See footnote 9
Publicly-Trusted Commercial PKI - S/MIME	Required	Required	Required	N/A	Not Required	N/A	Required	Required	N/A	See footnote 3	N/A	See footnote 9
Publicly-Trusted Commercial PKI - All other uses	Required	Required	Required	N/A	Not Required	N/A	N/A	Not Required	N/A	See footnote 3	N/A	See footnote 9
Publicly-Trusted Government PKI - SSL	Required	Required	Required ²	N/A	Required ²	N/A	N/A	Required ²	N/A	See footnote 3 and 4	N/A	See footnote 9
Publicly-Trusted Government PKI - EV SSL	Required	Required	Required ²	Required ²	Required ²	N/A	N/A	Required ²	N/A	See footnote 3 and 4	N/A	See footnote 9
Publicly-Trusted Government PKI - CS	Required	Required	Required ²	N/A	Not Required	Required ^{1,2}	N/A	Required ^{1,2}	N/A	See footnote 3 and 4	N/A	See footnote 9
Publicly-Trusted Government PKI - All other uses	Required	Required	Required ²	N/A	Not Required	N/A	N/A	Not Required	N/A	See footnote 3 and 4	N/A	See footnote 9
PKI X-Cert with USA Federal Bridge	Required	Required	Required ⁵	N/A	N/A	N/A	N/A	N/A	N/A	See footnote 3	See footnote 6	See footnote 9
Publicly-Trusted Commercial PKI - Verified Mark Certificates	Required	N/A	Required ⁵	N/A	N/A	N/A	N/A	Required	Required	N/A	N/A	N/A

Reporting Requirements

For all WebTrust assurance schemes, the initial engagement 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 subsequent engagements must be over a period of time (minimum period of coverage of 2 months not to exceed 12 months), with the engagement period commencing on the day following the end of the previous audit period to ensure continuous coverage. NOTE: Point in time engagements are not eligible for a WebTrust seal. WebTrust seals expire 15 months after the end of the engagement period. Current report templates are available in WebTrust for CA - Illustrative Reports v2.0.

WebTrust for CA

WebTrust for CA is considered to be the 'base' assurance scheme and is therefore required to be completed in all instances. Additional engagements for Extended Validation (SSL or Code Signing) and Baseline Requirements are designed to be conducted concurrently with a WebTrust for CA engagement.

Footnotes

- 1 Issuance and Management of Publicly-Trusted Code Signing Certificates is required for periods starting on or after February 1, 2017 for code signing certificates trusted by Microsoft Windows. Refer to <http://aka.ms/auditreqs>. See section 3.14.
- 2 Microsoft accepts an 'equivalent' audit for Government CAs in lieu of a WebTrust engagement, with certain restrictions. For more information, refer to <https://aka.ms/auditreqs>.
- 3 Microsoft publishes specific technical requirements for Roots and certificates that are part of its root programme. Refer <http://aka.ms/auditreqs> for the most up to date version of the technical requirements.
- 4 Mozilla does not currently make a distinction between Commercial and Government CAs. Therefore, the requirements for Commercial 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.
- 7 RKGC refers to assurance reports to be issued in conjunction with a WebTrust Practitioner's witnessing of CA's Root Key Generation Ceremony.
- 8 Key Protection refers to assurance reports to be issued in conjunction with a WebTrust Practitioner's witnessing of the migration, transportation or destruction of a CA's Root or Sub CA.
- 9 WebTrust for Registration Authorities (RA) can be performed by any entity that performs outsourced RA activities. This report may also be required as part of the contractual obligations by the CA, or by an oversight body such as the CA / Browser Forum.
- 10 Effective July 1 2023 Network Security is being separated from BS+NSR, CS, S/MIME and VMC engagements to a separate offering that needs to be conducted for each.
- 11 Although CA/Browser S/MIME is not effective until September 2023 (at present time) - earlier implementation is facilitated.

Audit Scheme Versions

Scheme	Version	Release Date	Effective Date
WebTrust for CA	2.2.1	01-Nov-20	01-Nov-20
WebTrust for CA	2.2.2	01-Jun-21	01-Jun-21
WebTrust for CA - Extended Validation - SSL	1.7.8	31-Jan-22	01-Feb-22
WebTrust for CA - Extended Validation - SSL	1.8	31-Mar-23	01-Apr-23
WebTrust for CA - SSL Baseline with Network Security	2.6	31-Jan-22	01-Feb-22
WebTrust for CA - SSL Baseline with Network Security	2.7	31-Mar-23	01-Apr-23
WebTrust for CA - Code Sign Baseline Requirements	2.7	31-Jan-22	01-Feb-22
WebTrust for CA - Code Sign Baseline Requirements	3.2	31-Mar-23	01-Apr-23
WebTrust for CA - S/MIME11	1.01	31-Aug-23	01-Sep-23
WebTrust for CA - S/MIME11	1.0	31-Mar-23	01-Apr-23
WebTrust for CA - Network Security10	1.0	31-May-23	01-Jul-23
WebTrust for CA- Verified Mark Certificates	1.0	01-Dec-21	01-Dec-21
WebTrust for CA- Verified Mark Certificates	1.4	31-Mar-23	01-Apr-23
WebTrust for RA	1.1	01-Nov-20	01-Nov-20