


[About Us »](#)
[Baseline Requirements »](#)
[Extended Validation »](#)
[CA Practices »](#)
[Current Work »](#)
[Resources »](#)
[Home » Information for Developers](#)

## INFORMATION FOR DEVELOPERS

### Information for Developers

This page assumes that developers are familiar with the basics of the X509 certificate system and public key infrastructure (PKI). The PKI as used in web browsers on the Internet is similar but not identical to that described by the relevant RFCs. It may help to review "Information for the Public" and our FAQ for Extended Validation and our FAQ for Baseline Requirements to understand more about certificated used in the Internet PKI.

Here are some useful documents to help developers understand aspects of certificate use:

- Recommendations for the Processing of EV SSL Certificates.v2.0
- **Mozilla's List of Included Root CAs** – <http://www.mozilla.org/en-US/about/governance/policies/security-group/certs/included/> (a detailed spreadsheet of this table is also available here: <https://docs.google.com/spreadsheets/pub?key=0Ah-tHXMawqU3dGx0cGFObG9QM192NFM4UWNBMlBaekE&single=true&gid=1&output=html>)
- Department of Defense (DOD) Class 3 Public Key Infrastructure (PKI) Public Key-Enabled Application Requirements
- W3C's Web Security Context: User Interface Guidelines
- FIPS 186-4, the Digital Signature Standard
- NIST Special Publications on Computer Security, especially:
  - NIST Special Publication 800-21: Guideline for Implementing Cryptography In the Federal Government
  - NIST Special Publication 800-52: Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations
  - NIST Special Publication 800-131A: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths
- NSA Suite B Cryptography

Although the CAB Forum EV Guidelines and Baseline Requirements are requirements for CAs, developers may wish to familiarize themselves with them too.

 to search type and hit enter

### RECENT NEWS

- Ballot 212 – Canonicalise formal name of the Baseline Requirements September 1, 2017
- Ballot 210 – Misc. Changes to the NCSSR August 31, 2017
- 2017-08-03 Minutes August 3, 2017
- 2017-07-20 Minutes July 20, 2017
- Ballot 204 – Forbid DTPs from doing Domain/IP Ownership July 11, 2017
- Ballot 205 – Membership-Related Clarifications July 6, 2017
- Ballot 192 – Notary Revision June 28, 2017
- 2017-06-21 F2F Minutes Meeting 41 in Berlin June 21, 2017
- Ballot 203 – Formation of Network Security Working Group June 19, 2017

### PAST PROCEEDINGS

Past Proceedings

### BY CATEGORY

By Category