Agenda

- News
  - New policy version 1.2
  - New UIs

- CA Root inclusion process
  - List of accepted CAs
  - Issues with CAs documentation
News
Root program policy

- New policy, version 1.2
  - Modified procedure for inclusion.
  - New CA form
  - New policy requirements, requesting specific and adequate information in the CP/CPS about the validation methods
New UIs

- **For CAs included in the 360 root store**
  - No problem: prompts the green lock 🟢
  - Expired certificate: prompts the grey lock ✗, blocks the page directly
  - Error host: prompts the grey lock ✗

Certificate was revoked: revise to prompt the grey lock ✗, and blocks the page

- **For CAs NOT included in the 360 root store**
  - In MS windows root store, non-government and other special sites——poor security
    - Prompt ⚠ in early period
    - Prompt ⚠ in mid period
    - Prompt ✗ in later period
  - Not in MS windows root store, non-government and other special sites——insecurity
    - prompt ✗, blocks the page directly
  - Government and other special websites: prompt ⚠ always
CA root inclusion
Root inclusion process

- New list of accepted CAs
  - In “caprogram” website (caprogram.360.cn) will be published the list of the included CAs in the 360 root store
  - This site will be updated quarterly and will be listed in the CABF wiki as well, for people to check.
  - At the end of October a new (beta) version (kernel 69) with the first list of admitted CAs in the root store. This will become definitive in November.
Issues with CAs documentation

- Don’t “copy-paste” the BRs:
  - The CP/CPS is about your CA, there can’t be terms like “the CA” when is referring to your own CA.
  - Regarding validation methods, is hard to understand that the CA has implemented all methods available.
  - Use your words in the revocation section.
- Please, review some “typos”, i.e. RFC 3280. Also, review section 1.6 there are terms and acronyms included that are not used in the document.
- Be explicit, the CPS is a “binding” document and would like to read all the minimal requirements: what to do in case of discrepancy, what to do when validating a cert that has not been issued, what about vulnerability scans and penetration tests, etc.
- BTW, the CP/CPSs have to be updated yearly

Question for CAs: we’d like to know why it takes so long to update a CP/CPS when there are some issues to be addressed.
Thank You!