**Validation Working Group – Validity Period Options for discussion**

**(Aug. 11, 2015)**

(Based on discussion at Zurich CAB Forum meeting June 2015)

|  |  |  |  |
| --- | --- | --- | --- |
| **Option** | **Max. Validity Periods (Years)** | **Pros** | **Cons** |
|  | **DV** | **OV** | **EV** |  |  |
| *Current* | 3 | 3 | 2 | Well understood, years of implementation, EV validity period should be shorter because identity, domains for EV certs should be made the most accurate (and re-vetting for new EV certs occurs every 13 months). Very few certs go “bad” during a 2-3 year period, no need to make customers buy, install certs more frequently (plus revocation deals with bad certs in interim) | May be too long for DV and OV (especially if domain confirmation occurs only every 39 months). If vetting data used for 3 years and at the end a 3 year DV/OV cert is issued, it’s good for 6 years after vetting.EV validity period may be too long given EV’s special nature (“more secure”) – up to (12+24) = 36 months after last EV vetting. |
| A | 1 | 2 | 3 | Because DV vetting confirms the least, it should be repeated annually. [Note: if we only change the validity period but allow DV and OV data to be used for 39 months as today, may not be a lot of benefit in shortening DV and OV cert validity period – certs can be reissued using the same data, no re-authentication required.]Organization data rarely changes from year to year for a customer, so allow longer period for OV/EV certs (plus, more is known about OV/EV customers than for DV customers, so less likely to be hacker). EV users are more stable than DV and maybe OV users, and EV certs are the safest certs, so should be able to get longer lived EV certs. Same for OV certs versus DV certs. | Many customers use DV certs, and this would make them replace the certs every year without adding value. Most hackers using DV certs do most damage in the first 48-72 hours, and certs can be revoked, so no benefit to shortening maximum validity period from 3 years to 1 year (same for OV from 3 years to 2 years). [Note: if we only change the validity period for DV and OV certs but allow DV and OV authentication data to be used for 39 months as today, may not be a lot of benefit in shortening DV and OV cert validity period – certs can be reissued using the same data, no re-authentication required.] |
| B | 2 | 3 | 3 | Similar arguments to Option A, but avoids making DV certs be replaced every year. OV and EV certs, with more validation are safer because of validations, would be available for a longer period, which encourages website owners to complete the identity validation process. | Similar arguments to Option A, but avoids making DV certs be replaced every year. |
| C | 3 | 3 | 3 | Keeps the customer focused on the differences in validation levels and browser UI when choosing a cert, not distracted in choice by maximum validity period. More convenient for customers, who may be more willing to upgrade to EV certs with a 3 year validity period. Organization data seldom changes from year to year, so longer period for EV certs is justified. | 3 years is too long for certificates, as authentication information for both the organization and domain can change. This effectively allows DV and OV certs that are good for up to 6 years after vetting, and EV certs that are good for up to 4 years after vetting (using current data reuse rules of 39 months for DV and OV and 13 months for EV) |
| D | 2 | 2 | 2 | Same arguments as for 3-3-3 (Option C), but with shorter period maximum validity period after vetting.  | Same arguments as for 3-3-3 (Option C), but with shorter period maximum validity period after vetting is one year less. More work for customers to replace certs after shorter validity period. |