



Validation Subcommittee

Tim Hollebeek

October 20, 2020

Agenda

- Review since June
- Certificate Profiles
- OU Discussion
- Priorities for Winter 2020

Review since June

Review since June Virtual F2F

- Acceptable redirect codes (“Clarifying acceptable status codes ...” June 2020)
- Ballot SC30 (**PASSED**): Disclosure of Registration / Incorporation Agency
- Validation Re-use (2020-07-20 minutes)
- Using github instead of Trello (2020-07-16 minutes)
- Ballot SC33 (**PASSED**): ALPN / 8737 ballot
- OU Requirements (“Revision to OU requirements”)

- ONGOING: Certificate profiles – work on capturing existing requirements in more useful format; fill in gaps and omissions

Certificate Profiles

Certificate Profiles

- First pass of review through all the fields has been completed
- Path forward?

OU Discussion

Overview

There seems to be a consensus that the current OU requirements are bad and need to be improved.

Two approaches:

1. Fix the rules to match the original intent, or
2. Simply sunset and move away from OUs as an allowed field.

Entrust Proposal (1/3)

3.2.2.1.1 Organizational Unit

If the Subject Identity Information is to include an organizational unit, then it SHALL NOT include a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless the CA has verified this information in accordance with Section 3.2.

The usage of commonly recognized organizational unit names is permitted and the CA is not required to verify the existence of and affiliation with the Applicant as long the value is included on a publicly disclosed list of CA has pre-approved values (disclosure of this list SHALL be through an appropriate and readily accessible online means).

Self reported values SHALL be preceded or followed by a whitespace and the word “department”, “division”, “unit” or the equivalent in a language other than English. The CA may extend these options using a publicly disclosed list containing the preceded or followed values which the CA has approved; as long it's disclosed through an appropriate and readily accessible online means.

Entrust Proposal (2/3)

The CA SHALL verify the existence of and affiliation of the organizational unit with the Applicant using at least one of the following:

1. A government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
2. A government agency responsible for the management of such organizational units, DBAs or tradenames;
3. A third party database that is periodically updated and considered a Reliable Data Source;
4. A site visit by the CA or a third party who is acting as an agent for the CA;
5. An Attestation Letter;
6. A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the CA determines to be reliable;
7. A connection with the Applicant's directory system;
8. An Organizational Chart or public directory of the Applicant; or
9. Communication with an authoritative source within the Applicant's organization, such as the Applicant's main business offices, corporate offices, human resource offices, information technology offices, or other department that the CA deems appropriate.

Entrust Proposal (3/3)

The value SHALL not be abbreviated unless this would exceed the maximum length of the `subject:organizationalUnitName` field, in which case it SHALL only use locally accepted abbreviation.

Alternatively, the CA MAY allow values or series as defined by a Government, standard, or regulatory body; or a series of at least five numerals, optionally preceded or followed by two alphabetical characters. The CA is not required to verify the accuracy of these non descriptive identifiers.

Until June 30, 2023, CA's are permitted to include other types of data in the OU field on a case by case basis to allow legacy applications to adjust to the above rules.

Priorities for Winter 2020

Summer Winter 2020 Priorities

- Continue work on certificate profiles
- Continue work on Incorporation Agencies and Registration Agencies
- Fix requirements for validation of OUs (?)
- Other priorities



Tim Hollebeek
tim.hollebeek@digicert.com