SwissSign

Organization identifier: setting some fields to optional if set

We would like to discuss the following topic "setting some fields to optional if Organizational identifier is set“ in *EV* certificates

29 May 2024, CABF F2F Meeting, Bergamo

Adrian Mueller, SwissSign
Sandy Balzer, SwissSign

Suggestion Overview

- Topic is about naming fields of *EV certificates*, i.e.
  - CABFOrganizationIdentifier extension and
  - Subject Distinguished Name (SDN) attributes (OrganizationIdentifier, JoI-fields and serialNumber)
- If the OrganizationIdentifier is included in the Subject Distinguished Name of a certificate the CABFOrganizationIdentifier extension should be *optional* only.
- The OrganizationIdentifier attribute contains the register information (register ID and jurisdiction). The following attributes are redundant and therefore should be *optional* as well:
  - all JurisdictionOfIncorporation fields, i.e. JoiCountry, JoIStateOrProvince and JoILocality (These can be concluded from the value in the OrganizationIdentifer.)
  - serialNumber (the register ID is included in the OrganizationIdentifer as well)

OrganizationIdentifier: Structure & Examples

- Structure: <prefix><country code>-<id, conditional>
- E.g.
  - NTRCH-CHE-109.357.012 – National Trade Register
  - VATDE-123456789 - Tax id
  - GOVUS-NY - Government Entity
  - INTXG (International Organization)
  - LEIXG-UXIATLMNPCXXT5KR1S08 - Legal Entity Identifier (financial sector)
- Please note: OrganizationIdentifier is a SHALL for Organization Validated and Sponsor Validated (S/MIME BR) in addition to organizationName.

CABFOrganizationIdentifier

- OrganizationIdentifier is an *optional* SDN attribute (EVG, chapter 7.1.4.2.8)
- The CABFOrganizationIdentifier extension is mandatory if the OrganizationIdentifier is set (EVG chapter 7.1.2.2)
- Extension originally introduced to streamline with ETSI where OrganizationIdentifier stems from.
- However, this extension is not described in ETSI documents.
- Discussion on GitHub, see https://github.com/cabforum/servercert/issues/499
- Added value very limited
- *Suggestion: Make CABFOrganizationIdentifier optional*

SDN attributes: JoI fields & serialNumber

- JoI fields *currently*
  - JoICountry: Must
  - JoIState: Conditional (e.g. commercial registers on state level)
  - JoILocality: Conditional (German commercial registers and few others)
- serialNumber: Usually contains register ID as included in OrganizationIdentifier as well
- *Suggestion: Make these attributes optional if OrganzationIdentifier is included*

Example

Example SwissSign:

- **NTRCH-CHE-109.357.012** (worldwide unique within this context)

  vs.
- Subject Distinguished Name fields:
  - CN = swisssign.com
  - **serialNumber = CHE-109.357.012** (ID in national and cantonal/state trade register)
  - O = SwissSign AG
  - STREET = Sägereistrasse 25
  - postalCode = 8152
  - L = Glattbrugg
  - ST = ZH
  - C = CH
  - businessCategory = Private Organization (loose dependency/coupling with prefix)
  - **(jurisdictionLocality empty)**
  - **jurisdictionStateOrProvinceName = Zürich**
    (registered in commercial register of Zurich. Not in OrganizationIdentifier, but can be deduced and is redundant to State attribute)
  - **jurisdictionCountryName = CH**

Expected Benefits

- Reduced complexity
- clear requirements
- Less error prone

SwissSign

Data security specialist of

SwissSign

Data security specialist of