> A Server cert can have a maximum lifetime of 2 years (for all sub-CAs).

See FernUniversitaet in Hagen CPS document Section 5.3. We want to add this information to the CP as well.

> Future externally-operated Sub-CAs

Based on CP section 1.3.1, it looks like any business may operate a sub-CA, and

those sub-CAs may issue their own sub-CAs, up to a path length of 5. There does

not seem to be any restriction on the types of businesses that may operate

sub-CAs, or who they can issue sub-CAs to.

If Mozilla accepts and includes the “Scientific Trust operated by

FernUniversitaet in Hagen – G1” root, then we have to assume that we also

accept any of your future sub-CAs and their sub-CAs. Therefore, the selection

criteria for your sub-CAs and their sub-CAs will be a critical decision factor.

Please point me to the parts of the CP that clearly explain who can apply to

operate a sub-CA (at any level), the selection/approval process for sub-CAs and

their sub-CAs, the verification procedures applied to sub-CAs and their

sub-CAs, what restrictions (legal and technical) are placed on all sub-CAs (eg

constraints to issuing certs within certain domains).

We will update our CP Section 1.3.1 to specify the information:

Scientific Trust issues Certificates to the CAs Staff or Business or Universities operating as Intermediate CAs. These Intermediate CAs may use as many Intermediate CAs below them as they required or either issue Certificates to End Entities. But an Intermediate CA can only issue an Intermediate CA certificate for internal use only (e.g. an intermediate CA for their active directory). It is not permitted that an Intermediate CA of Scientific Trust issues an Intermediate CA certificate outside the Intermediate domain. However, the path length must not exceed the number of five.

Scientific Trust may also operate an Intermediate CA, which issues Certificates for the general public.

Intermediate CAs must sign an agreement with the issuing CA, stating the obligation to adhere to the agreed procedures.

*Selection / approval / verification process of Intermediate CAs*

If Scientific Trust wants to issue an Intermediate CA certificate see Section 3.1.1 of Scientific Trust CPS document.

If an Intermediate CA wants to issue an Intermediate CA certificate, we want to add the following to the Scientific Trust CPS document:

For intermediate certificates authentication level is personal. Actor's actions are as defined below:

|  |  |  |
| --- | --- | --- |
| Actor | Number | Action |
| Applicant | 1. | Wants to have an intermediate certificate |
| Intermediate CA | 2. | Requests more informationen over the applicant and wants a CPS document. |
| Applicant | 3. | Submits his CPS document to the CA |
| Intermediate CA | 4. | Checks the CPS document. |
| Scientific Trust | 5. | CA performs an audit at the applicant. |
| Intermediate CA | 6. | Issues the requested certificate. |
| Intermediate CA | 7. | Hands out certificate to applicant. |
| Applicant | 8. | Ensures certificate usage in conformity with CP and this CPS. |