CRL URL	CRL for end-entity certs: http://ca.fernuni-hagen.de/certserver/certs/crl2009.crl (NextUpdate: 30 days)	*We reduced the "NextUpdate" period from 30 to 7 days.*
CRL Issuing Frequency for end-entity certs	CP Section 2.6.2. Frequency of publication Certificates must be published as soon as they are issued. CRLs must be published as soon as they are issued and always when needed (e.g. in case of revoking a certificate). There is no need to create CRLs periodically when no cause is given. Changes to this CP and to CPS shall be published as soon as they are updated. EV guidlines http://www.cabforum.org/EV_Certificate_Guidelines_V11.pdf (Recommended even if not applying for EVenablement): "CRLs MUST be updated and reissued at least every seven days, and **the nextUpdate field value SHALL NOT be more ten days;**" Note: I have not ever seen a CA get approved for inclusion whose nextUpdate for end-entity cert CRLs was greater than 10 days. Such limitation needs to be specified in the CP for all sub-CAs.	*Updated CP Section 2.6.2: CRLs have to be published at least every 7 days.*
Sub-CAs operated by 3rd parties	It looks like the sub-CAs will be able to serve as certificate service providers. Please see https://wiki.mozilla.org/CA:SubordinateCA_checklist, and provide the requested information. Note: We pay particular attention to how the CA enforces verification procedures (such as domain and email ownership) and regular auditing of the sub-CAs. Best solution is that the sub-CAs be included in the regular audit of the root. We also experience problems when sub-CAs don't properly support OCSP (don't regularly test with a Firefox browser with OCSP enforced), and when CRLs don't import correctly into Firefox. CP Section 1.3.3: Conforming CAs provide certificates for: • employees and students of Universities; • persons involved in research or administrative activities in collaboration with employees of Universities; • digital processing entities, capable of performing cryptographic operations, property of Universities or used for activities in which Universities are involved. • Business community • general public	*1. At this time there is only one sub-CA which is operated by ourselves, the FernUniversitaet in Hagen.* *2. CPS FernUniversitaet in Hagen and CP Scientific Trust* *3. The CA can only issue certs in their domain namespace *.fernuni-hagen.de and they can create their own sub-CAs (this has not happened yet).* *4. See CPS FernUniversitaet in Hagen Section 3.2.1 and 3.2.2* *5. See CP Scientific Trust Section* *The root CA audit does not includes the sub-CAs* *CP Section 2.7.2:* *Audits will be done by an independent external auditor for the Scientific Trust and by Scientific Trusts staff or persons assigned by the Scientific Trusts staff for intermediate CAs.* *CP Section 2.7.1:* *Audits will be done before initial approval as an authorized CA, and thereafter in an annual cycle for Scientific Trusts and intermediate CAs either.* *CPS Scientific Trust Section 2.3.1:* *The CA issues intermediate certificates for companies or universities. These companies and universities have to pass an audit, which is conducted by Scientific Trust CA*
Cross-Signing	Have any other root CAs issued cross-signing certificates for this root CA?	*No*
SSL Validation Type DV, OV, and/or EV	OV for the FernUniversitaet in Hagen sub-CA (Server certs are only issued to employees.) Requirements not clear for any future sub-CA.	*Any future sub-CA will be OV.*
Domain Name Ownership / Control	section 7 of http://www.mozilla.org/projects/security/certs/policy/: We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: • for a certificate to be used for SSL-enabled servers, the CA takes reasonable measures to verify that the entity submitting the certificate signing request has registered the domain(s) referenced in the certificate *or* has been authorized by the domain registrant to act on the registrant's behalf; Not found in CP – The requirement to verify the ownership/control of the domain name must be documented for all sub-CAs, and must be part of the regular audit. Not found in CPS Scientific Trust.	*Updated CP Section 3.5* *Scientific Trust does not issue server certs, so there is no information in the CPS.*
Email Address Ownership / Control	section 7 of http://www.mozilla.org/projects/security/certs/policy/: We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: • for a certificate to be used for digitally signing and/or encrypting	*Updated CP Section 3.6* *Scientific Trust does not issue client certs, so there is no information in the CPS.*

	email messages, the CA takes reasonable measures to verify that the entity submitting the request controls the email account associated with the email address referenced in the certificate *or* has been authorized by the email account holder to act on the account holder's behalf; Not found in CP –The requirement to verify the ownership/control of the email address must be documented for all sub-CAs, and must be part of the regular audit. Not found in CPS Scientific Trust. CPS FernUniversitaet in Hagen section 3.2.1: Step 1: Applicant Enroles at the university and has to accept the enrollment rules, The applicant is legally bound to indicate his proper email adress and retieve at least every 14 days the email box. Step 2: University Identifies the applicants address. Step 3: University Stores address, e-mail, registration number and network ID in central database. Step 4: Applicant Submits his registration number by filling out the web form https://account.fernunihagen.de/password.php in order to apply for a password. Step 5: CA Generates and stores password in combination with first name, second name, e-mail, network ID in certificate database. Step 6: CA Sends password by postal services to address located in central database. Step 7: Applicant Submits his registration number and password by filling out web form https://ca.fernunihagen.de/certserver/, follows the instructions displayed and requests a certificate. Step 8: CA Receives and reviews the request automatically. Step 9: CA Issues the requested certificate and offers it for download. Step 10: CA Stores the certificate in certificate database and publishes it (https://ca.fernuni-hagen.de/certserver/). Step 11: Applicant Downloads and installs certificate. Step 12: Applicant Ensures certificate usage in conformity with CP and this CPS. Who verifies that the applicant owns/controls the email address, and how?	*Extract of the official announcements of the FernUniversitaet in Hagen* *(1) The students are required to report immediately to the FernUniversitaet in Hagen:* *1. the change of name, address and e-mail address* *2. changing the account details for participation in the collection process,* *3.passed or failed exams, the results for the continuation of the study are significant,* *4. the loss of a student ID.* *Upon request, the evidence must lead.* *(2) The students, Applicants and Prospective Students are involved in the automated business processes and procedures of the FernUniversitaet in Hagen. Because of that they must have an Internet-enabled PC and a serviceable e-mail address. The FernUniversitaet in Hagen is entitled to assign students an e-mail address and explain their use for binding. E-Mails must be retrieved at least every 14 days under the enrollment or re-entered e-mail address.* *If a student subscribes with his personal data and his e-mail adress at the FernUniversitaet in Hagen, the student will get an automatic e-mail with information to his e-mail account.* *Employees:* *Employees get an e-mail address assigned by our identity management system. So the employee definitely controls this e-mail address.*
Identity of Code Signing Subscriber	section 7 of http://www.mozilla.org/projects/security/certs/policy/: We consider verification of certificate signing requests to be acceptable if it meets or exceeds the following requirements: • for certificates to be used for digitally signing code objects, the CA takes reasonable measures to verify that the entity submitting the certificate signing request is the same entity referenced in the certificate *or* has been authorized by the entity referenced in the certificate to act on that entity's behalf; Information about Code Signing certs not found in CP. In order to enable the Code Signing trust bit, there must be documented verification requirements for such certs for all sub-CAs. Information about Code Signing certs not found in CPS Scientific Trust. CPS FernUniversitaet in Hagen section 3.2.2: The server certificate is intended for server and code signing purposes. Server certs are only issued to employees.	*Updated CP Section 3.6* *Scientific Trust does not issue code signing certs, so there is no information in the CPS.*
Potentially Problematic Practices	Please review the list of Potentially Problematic Practices at http://wiki.mozilla.org/CA:Problematic_Practices. Identify the ones that are and are not applicable. For the ones that are applicable, please provide further information about the controls that are in place to address the related concerns. • Long-lived DV certificates o Not clear what validity periods are allowed for other sub-CAs. Could not find in CP. o For FernUniversitaet in Hagen sub-CA, server certs can have a validity of up to 2 years. • Wildcard DV SSL certificates • Delegation of Domain / Email validation to third parties o **Applicable**. CP Section 1.3.2: Each Intermediate CA may use one or more Registration Authorities (RAs). It may also act as a RA	Long-lived DV certificates: *A Server cert can have a maximum lifetime of 2 years (for all sub-CAs). After this time the server cert is not valid anymore and a server cert has to apply again.* Wildcard: *No Wildcard certificates* Delegation of Domain / Email validation to third parties: *The Intermediate CA **and** its RAs are audited by Scientific Trust Staff (Updated CP Section 2.7.2, 1.3.2).* Issuing end entity certificates directly from roots:

	itself. RAs must sign an agreement with its operating CA, stating the obligation to adhere to the agreed procedures as identified in the CAs CPS. RAs may act for one or more CAs. • Issuing end entity certificates directly from roots • Allowing external entities to operate unconstrained subordinate CAs • Distributing generated private keys in PKCS#12 files o **Applicable**. CP section 4.1: This CP permits two alternative procedures for certificate application: • Certification of entities done entirely by the CA/RA. The details about this procedure must be specified in the CPS. • An entity generates its own key pair and submits public key and other required data to the CA after being authenticated by the CA/RA. The details about this procedure must be specified in the CPS. • Certificates referencing hostnames or private IP addresses • Issuing SSL Certificates for Internal Domains • OCSP Responses signed by a certificate under a different root • CRL with critical CIDP Extension • Generic names for CAs	*No* Allowing external entities to operate unconstrained subordinate CAs: No Distributing generated private keys in PKCS#12 files: *We are not distributing private keys in PKCS#12 files, the entity generates its own key pair and no one else has access to the entities private key.* Certificates referencing hostnames or private IP addresses: *No* Issuing SSL Certificates for Internal Domains: *No* OCSP Responses signed by a certificate under a different root: *We don`t have OCSP* CRL with critical CIDP Extension: *No critical CIDP* Generic names for CAs: *Our Root cert name “Scientific Trust operated by FernUniversitaet in Hagen – G1” is not generic*