Bugzilla ID: 531237
Bugzilla Summary: Scientific Trust operated by FernUniversitaet in Hagen -G1

CAs wishing to have their certificates included in Mozilla products must comply with the requirements of the Mozilla CA certificate policy (http://www.mozilla.org/projects/security/certs/policy/) and must supply the information necessary to determine whether or not the policy's requirements have been satisfied, as per http://wiki.mozilla.org/CA:Information_checklist.

CA's are also encouraged to review the Recommended Practices at https://wiki.mozilla.org/CA:Recommended_Practices.

General Information	**Data**
CA Name	Scientific Trust operated by FernUniversitaet in Hagen
Website URL	http://www.scientific-trust.de (German) http://www.scientific-trust.de/index_en.php (English)
Organizational type	Academic institution
Primary market / customer base	Scientific Trust is a division of the University of Hagen and has its own Root Certificate. Scientific Trust has passed a Webtrust audit and offers Intermediate Certificates to other universities and companies. The University of Hagen (FernUniversität in Hagen) is the only state-maintained distance teaching university in German-speaking countries. Our 67000 Students benefit from our modern distance education system. The primary market is the German speaking area (Austria, Germany, Switzerland).
CA Contact Information	CA Email Alias: caadmin@FernUni-Hagen.de An email alias is being requested so that more than one person in your organization will receive notifications in case the primary contact is out of the office or leaves the organization. CA Phone Number: *+49 (23 31) 9 87 - 28 29* A main phone number from which Mozilla can reach the organization responsible for root certificates for the CA. Title / Department: *Scientific Trust: Certification Authority (CA)* If Mozilla needed to call your main phone number, what Title/Department should the Mozilla representative ask for?

For Each Root CA whose certificate is to be included in Mozilla (or whose metadata is to be modified)

Info Needed	**Data**
Certificate Name	Scientific Trust operated by FernUniversitaet in Hagen – G1
Cert summary / comments	This Root has one internally-operated subordinate CA issuing client and server certificates. In future there will be more subordinate CAs, issuing client and server certificates.
Root certificate URL	http://www.scientific-trust.de/scientific-trust.crt
SHA-1 fingerprint	8A:A3:F5:A6:44:D1:B4:23:97:CF:82:67:5D:1F:D8:35:D0:BA:31:46

Valid from	2009-08-24
Valid to	2037-12-25
Cert Version	3
Modulus length / key length	4096
Test Website	https://www.scientific-trust.de
CRL URL	ARL: http://cdp1.scientific-trust.de/g1/crl/root.crl CRL for end-entity certs: http://ca.fernuni-hagen.de/certserver/certs/crl2009.crl (NextUpdate: 30 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 EV-enablement): "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.
OCSP Responder URL	None CP Section 4.4.11: Conforming CAs may support on-line revocation/status checking. Bearing in mind that this CP requires conforming CAs to issue CRL, it isn't mandatory to implement on-line revocation/status checking procedures.
CA Hierarchy	Diagram: https://bugzilla.mozilla.org/attachment.cgi?id=414700 At this time Scientific Trust has one internally-operated subordinate CA, but eight commitments of other companies that they want to become a subordinate CA.
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

	Each conforming CA must detail the (End-) Entities it will certify in its CPS. Conforming CAs may provide certificates to parties not affiliated with the University / business, as long as those parties have a bonafide need to possess a certificate issued by the CA. In this case a suitable procedure to ascertain the identity of the requestors has to be established.
Cross-Signing	Have any other root CAs issued cross-signing certificates for this root CA?
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing
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.
EV policy OID(s)	http://www.cabforum.org/EV_Certificate_Guidelines_V11.pdf
CP/CPS	Certificate Policy URL (English): http://www.scientific-trust.de/download/cp_V1.2.pdf More detailed information about the practices, which conforming CAs employ in their operations in issuing certificates, can be found in the Certificate Authorities Certification Practise Statements (CPS). Every of the above mentioned CAs must issue its own CPS in order to provide information to potential clients of the CA about the underlying technical, operational and legal foundations which are not specified in this Certification Policy (CP). CPS Scientific Trust URL (English): http://www.scientific-trust.de/download/cps_st_V1.0.pdf CPS FernUniversitaet in Hagen URL (English): http://www.scientific-trust.de/download/cps_feu_V1.0.pdf
AUDIT	Audit Type (WebTrust, ETSI etc.): WebTrust Auditor: KPMG Auditor Website: www.kpmg.de Audit Document URL(s): https://cert.webtrust.org/ViewSeal?id=974 (2009.06.30)
Organization Identity Verification	CP Section 3.1.9 Procedures differ if the subject is a person, an organizational unit or a Digital Processing Entity. Authentication of persons: Identification can be done by personal contact. Subscribers present a suitable document[2] to prove their identity (identity card, passport, driver's license, government badge etc.). User-authentication may also be done using a postal address which can be verified with suitable measures. This postal address must not be anonymous (e.g. post restante, post-office boxes...). Authentication of working groups: A person with a proper affiliation of the working group has to be authenticated according to the rules for authentication of persons. Authentication of Digital Processing Entities: The person in charge has to present a suitable document to prove their identity (identity card, passport, driver's license, government badge etc.).

<table>
<tr><td></td><td>
CPS FernUniversitaet in Hagen section 3.2.2:
The server certificate is intended for server and code signing purposes.
Employee applicants for a server Certificate must physically identify themselves. Applicants will be authenticated by CAs security officers in the computing centers location with their identity card or passport.
No other documents will be accepted.
Authentication level is personal.
Server certificates will not be issued for universities students or guests.

CPS FernUniversitaet in Hagen section 4.2:
The following table highlights certain differences between the validation requirements for each certificate class. The CA shall have the right to update these validation requirements to improve the validation process.
<table>
<tr><th></th><th>client certificate</th><th>server certificate</th></tr>
<tr><td>personal authentication</td><td>not applicable</td><td>mandatory</td></tr>
<tr><td>web authentication</td><td>mandatory</td><td>mandatory</td></tr>
<tr><td>authentication code</td><td>mandatory</td><td>mandatory</td></tr>
<tr><td>identity card validation</td><td>not applicable</td><td>mandatory</td></tr>
</table>

The following table describes, who is allowed to apply for which type of certificate
<table>
<tr><th></th><th>client certificate</th><th>server certificate</th></tr>
<tr><td>students</td><td>yes</td><td>no</td></tr>
<tr><td>employees</td><td>yes</td><td>yes</td></tr>
<tr><td>guests</td><td>yes</td><td>no</td></tr>
</table>
</td></tr>
<tr><td>Domain Name Ownership / Control</td><td>
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.
</td></tr>
</table>

	Not found in CPS Scientific Trust. CPS FernUniversitaet in Hagen section 3.2.2: Step 1: Applicant Takes employment at University Step 2: University Stores office address, network ID in central database and assigns the applicant an e-mail address Step 3: Applicant Submits his network ID by filling out the web form https://account.fernuni-hagen.de/password.php in order to apply for a password. Step 4: CA Stores password in combination with first name, second name, e-mail, network ID in certificate database. Step 5: CA Sends password by postal services to address located in central database. Step 6: Applicant Submits his network ID and password by filling out the web form https://ca.fernuni-hagen.de/certserver/, follows the instructions displayed and requests a certificate. Step 7: CA Receives and reviews the request manually. Step 8: CA Identifies the applicant with applicants identity card. Step 9: CA Verifies the domain ownership by asking the dns administrator of the university. The administrator knows the link between person and domain ownership. Step 10: CA Issues the requested certificate. Step 11: CA Hands out certificate to applicant. Step 12: CA Stores the certificate in certificate database and publishes it (https://ca.fernuni-hagen.de/certserver/). Step 13: Applicant Ensures certificate usage in conformity with CP and this 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 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.fernuni-hagen.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.fernuni-hagen.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?
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.
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 o • 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 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 o • Allowing external entities to operate unconstrained subordinate CAs o • 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 o • Issuing SSL Certificates for Internal Domains o • OCSP Responses signed by a certificate under a different root o • CRL with critical CIDP Extension o • Generic names for CAs o Root cert name is not generic.