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 CA Phone Number: +49 (23 31) 9 87 - 28 29 Title / Department: Scientific Trust: Certification Authority (CA)

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 externally-operated 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: 6 days)

CRL Issuing Frequency for end-entity certs	CP Section 2.6.2: CRLs must be published as soon as they are issued and always when needed (e.g. in case of revoking a certificate). CRLs must be published at least every 7 days.
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	There are currently no externally-operated subordinate CAs. However, there will be in the future. CP Section 1.3.1: 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. However, an Intermediate CA can issue an Intermediate CA certificate for internal use only (e.g. an intermediate CA for activedirectory). It is not permitted that an Intermediate CA of Scientific Trust issues Intermediate CA certificates outside the Intermediate's 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. CP section 2.1.1: Conforming CAs will operate a certification authority service in accordance with all provisions of this CP and associated CPS. CP section 2.7: An annual audit is performed by an independent external auditor to assess the adequacy of the Scientific Trusts business practices disclosure and the effectiveness of the CA's controls over its CA operations (WebTrust Principles). Before initial approval, the CA must submit to a compliance audit. This audit's purpose is to verify • the quality of the services provided by the CA, • that the CA complies with all of the requirements of this CP, and • that the intermediate CAs CPS is consistent with the requirements of this CP. 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. 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 and their RAs. If an intermediate CA wants to provide certificates for the general public, the intermediate CA has to be audited anually by an independent external auditor (Webtrust Principles). CP section 2.7.4: The audit will verify the quality of the services provided by the CA, that the CA complies with all of the

	requirements of this CP and its CPS, and the CPS is consistent with the requirements of this CP. The Scientific Trusts audit will be done in compliance to the requirements defined by WebTrust principals. CP Section 6.3.2: The lifetime of the Scientific Trust signing key pair is twenty-eight years. The maximum lifetime of the intermediate CA signing key pair is fourteen years. The maximum lifetime of End Users signing key pair is three years.
Cross-Signing	None. None planned.
Requested Trust Bits	Websites (SSL/TLS) Email (S/MIME) Code Signing
SSL Validation Type DV, OV, and/or EV	OV
EV policy OID(s)	Not EV
CP/CPS	Certificate Policy (English): http://www.scientific-trust.de/download/cp.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 (English): http://www.scientific-trust.de/download/cps_st.pdf CPS FernUniversitaet in Hagen (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 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>
For the FernUniversitaet in Hagen sub-CA server certs are only issued to employees.
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>
CP section 3.5: Conforming CAs must verify that the entity requesting a server certificate has registered the domain(s) referenced in the certificate or is authorized to request a server certificate for this domain.

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.
</td>
</tr>
</table>

	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	CP section 3.6: Conforming CAs must verify that the entity requesting a client certificate controls the email account referenced in the certificate or is authorized to request a client certificate with this email address. 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. 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.

	(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	CP section 3.7: Conforming CAs must verify the identity information in the certificate to be that of the certificate subscriber. 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	http://wiki.mozilla.org/CA:Problematic_Practices • Long-lived DV certificates o SSL certs are OV. o For FernUniversitaet in Hagen sub-CA, server certs can have a validity of up to 2 years. o CP Section 6.3.2: The maximum lifetime of End Users signing key pair is three years. • Wildcard DV SSL certificates o Not found. • Delegation of Domain / Email validation to third parties o 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. Intermediate CAs and their RAs are audited by Scientific Trust staff. o 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 and their RAs. • Issuing end entity certificates directly from roots o Not applicable. End-entity certs are only issued from sub-CAs. • Allowing external entities to operate unconstrained subordinate CAs o CP Section 1.3.1: These Intermediate CAs may use as many Intermediate CAs below them as they required or either issue Certificates to End Entities. However, an Intermediate CA can issue an Intermediate CA certificate for internal use only (e.g. an intermediate CA for activedirectory). It is not permitted that an Intermediate CA of Scientific Trust issues Intermediate CA certificates outside the Intermediate's domain. However, the path length must not exceed the number of five.

	○ CP Section 2.7.2: If an intermediate CA wants to provide certificates for the general public, the intermediate CA has to be audited anually by an independent external auditor (Webtrust Principles). • Distributing generated private keys in PKCS#12 files ○ Not applicable • Certificates referencing hostnames or private IP addresses ○ Not applicable • Issuing SSL Certificates for Internal Domains ○ Not applicable • OCSP Responses signed by a certificate under a different root ○ OCSP not currently provided • CRL with critical CIDP Extension ○ CRLs import into Firefox browser without error. • Generic names for CAs ○ Root cert name is not generic.