Certificate Authority (CA)-Policy der RS Utility Service (English version: see below)

(siehe auch: http://certauth.rs-utilityservice.de/policy.pdf)

Die RS Utility Service betreibt eine Certificate Authority (im Folgenden CA genannt) und stellt private und Organisationszertifikate aus mit denen einfache und fortgeschrittene elektronische Signaturen/Siegel erzeugt werden können. Die Ausstellung von Zertifikaten erfolgt diskriminierungsfrei, insbesondere für Marktteilnehmer der deutschen Energiewirtschaft. Die ausgestellten Zertifikate sind mit dem Root-Zertifikat der CA signiert.

Die IT-Sicherheit des CA-Betriebs ist durch ein Audit/eine Zertifizierung in Anlehnung an BSI TR-03145, Secure Certification Authority operation, geprüft.

Die CA unterhält einen Rückrufservice, über den Zertifikate widerrufen werden können. Dazu führt sie eine Zertifikatsperrliste (certificate revocation list, CRL), welche öffentlich zugängig ist. Die Adresse zum automatisierten Abruf der Zertifikatsperrliste ist in den End-User-Zertifikaten eingetragen.

Darüber hinaus betreibt die CA einen OCSP-Server. Mittels des OCSP-Servers kann der Gültigkeitsstatus aller ausgegeben Zertifikate online, automatisiert und in Echtzeit abgefragt bzw. geprüft werden. Die Adresse des OCSP-Servers ist in den End-User-Zertifikaten eingetragen.

Der Registrierungsservice, einschließlich an Dienstleister (Registrare) ausgelagertem Service, erfolgt auf einem sehr hohen Sicherheitsniveau. Die Registrierung/ Identifizierung der Antragsteller erfolgt nach einheitlichen Richtlinien. Evtl. Dienstleister (Registrare) sowie eigene Mitarbeiter müssen an speziellen Schulungen teilnehmen und ihren Wissensstand nachweisen. Alternativ ist eine Registrierung /Identifizierung der Antragsteller mittels öffentlicher (notarieller) oder amtlicher Beglaubigung durch landesrechtlich hierzu ermächtigte Behörden (dazu zählt auch das Post-Ident-Verfahren) möglich. Für einfache Zertifikate werden elektronische/automatisierte Indentifizierungsverfahren verwendet.

Die Vertrauenswürdigkeit des Betreibers und des Betriebs, auch unter Berücksichtigung von Eingriffsrechten Dritter, ist durch langjährige berufliche Erfahrung, u.a. in TrustCentern und in der IT-Security, gegeben.

Die CA beachtet die gesetzlichen Anforderungen zur Geheimhaltung von vertraulichen Daten, insbesondere das Bundesdatenschutzgesetz sowie weitere Datenschutzvorschriften. Als vertraulich gelten alle personenbezogenen Daten, die nicht Bestandteil eines Zertifikats oder einer CRL(Sperrliste) sind. Alle im Zertifikat enthaltenen Informationen gelten als nicht vertraulich.

Die CA behandelt alle Daten des Zertifikatsinhabers, soweit sie in personenbezogener Form vorliegen, unter Einhaltung der einschlägigen Bestimmungen der Datenschutzvorschriften. Die Daten werden ausschließlich zum Zweck der Zertifikatserstellung verarbeitet.

Personenbezogenen Daten werden ausschließlich zum Zweck der Zertifizierungsdienstleistung verarbeitet und gespeichert.

Die CA haftet nur im Rahmen der zur Verfügung stehenden Prüfungsmöglichkeiten sowie nur bei vorsätzlich verursachten Schäden. Insbesondere wird jede Haftung für Schäden jeglicher Art, die durch die nicht bestimmungsgemäße Verwendung der Zertifikate verursacht werden, ausgeschlossen. Dies gilt ebenso für unmittelbare oder mittelbare Folgeschäden, Datenverlust, entgangenen Gewinn, System- oder Produktionsausfälle. Für die Geheimhaltung des privaten Schlüssels und dessen ordnungsgemäßen Gebrauch ist der Antragsteller bzw. die im Zertifikat eingetragene natürliche Person verantwortlich.

Der Rechtsstand, insbesondere in Bezug auf das geltende Haftungs- und Datenschutzrecht ist Deutschland. Es gilt deutsches Recht.

Certificate Authority (CA) Policy of RS Utility Service

(see also: http://certauth.rs-utilityservice.de/policy.pdf)

RS Utility run a Certificate Authority (hereinafter referred to as CA) and issue private and organization certificates that can be applied to generate simple and advanced electronic signatures/seal. The certificates are issued non-discriminatory, in particular for market players of the German energy branch. The issued certificates are signed by the root certificate of the CA.

The IT security of the CA operation has been reviewed by an audit/a certification based on BSI TR-03145, Secure Certification Authority operation.

The CA maintains a call-back service that can be used to revoke certificates. For this purpose it keeps a certificate revocation list, which is accessible to the public. The address for the automated call of the certificate revocation list is stated in the end-user certificates.

In addition, the CA operates an OSCP server. The OSCP server can be used online, automated and in real time to query and/or check the validity status of the issued certificates. The address of the OSCP server is stated in the end-user certificates.

The registration service, including an outsourced service (registrars), is provided on a very high security level. The registration/identification of the applicants are rendered according to uniform guidelines. Possible service providers (registrars) and our own employees have to attend specific training courses and give evidence of their level of knowledge. Alternatively, the registration/identification of the applicants can be made by a public (notarial) or official certification by authorities accordingly empowered by state law (this also includes the post-ident procedure). Electronic/automated identification procedures are applied for simple certificates.

The trustworthiness of the operator and of the operation, also considering intervention rights of third parties, is ensured by professional experience over many years, e.g. in trust centers and in the IT security.

The CA complies with the legal requirements concerning the non-disclosure of confidential data, in particular the Federal Data Protection Act and other data protection regulations. All personal data that are no part of a certificate or a CRL (certificate revocation list) are considered to be confidential.

The CA deals with all data of the certificate holder, as far as they are available in person-related form, by complying with the associated stipulations of the data protection regulations. The data are exclusively processed for certificate issuance purposes.

Personal data are exclusively processed and stored for purposes of the certificate service.

The CA is only liable within the available review options and only for cases of deliberately caused damages. In particular, any liability for damages of any kind caused by the use of the certificates for other than the intended purposes is excluded. This also applies to direct or indirect consequential damages, loss of data, lost profit, system or production failures. The applicant or the natural person named in the certificate is responsible for the non-disclosure of the private code and its proper use.

The place of jurisdiction, in particular concerning the applicable liability and data-protection law, is Germany. German law shall apply.