Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center - Austria

A-1040 Wien, Weyringergasse 35
Tel.: ++43 1 – 503 19 63 – 0
Fax: ++43 1 – 503 19 63 – 66

A-8010 Graz, Inffeldgasse 16a
Tel.: ++43 316 – 873 5514
Fax: ++43 316 – 873 5520

Homepage: www.a-sit.at
E-Mail: office@a-sit.at

Conformity assessment statement

for the
certificate policy for qualified certificates
issued by the
TOP Certification Service
provided by the
Rundfunk und Telekom Regulierungs-GmbH, Vienna, Austria
and specified in the
Certification Practice Statement Version 1.1

The RTR-GmbH[1] provides the TOP Certification Service[2] on behalf of the Austrian supervisory body for electronic signatures (i.e., the Telekom-Control Commission[3]). This certification service serves the purpose of fulfilling the requirements on the supervisory body from the Austrian Electronic Signature Act[4].

Hereby we confirm that the TOP Certification Service fulfills all relevant requirements[5] from ETSI TS 101.456 V1.2.1 (2002-04)[6], Section 8[7]. The corresponding certificate policy is specified in the Certification Practice Statement Version 1.1[8] (the corresponding CPS OID is 1.2.040.0.21.0.0.0.1.1)[9].

This statement is based on the expert report[10] issued by A-SIT Secure Information Technology Center – Austria on October 30, 2002, and on the examinations carried out as part of this conformity assessment procedure.

In Vienna, Austria, on July 10, 2003

A-SIT Secure Information Technology Center – Austria

o. Univ.-Prof. Dipl.-Ing. Dr. Reinhard Posch
Scientific Director

Manfred Holzbach
Managing Director

---

[1] Rundfunk und Telekom Regulierungs-GmbH, A-1060 Vienna, Mariahilferstrasse 77-79, Tel +43-1/580 58-0, Fax: +43-1/580 58-9191. email: signatur@signatur.rtr.at (the applicant)
[2] German name: "TOP-Zertifizierungsdienst"
[3] Contact information: see Rundfunk und Telekom Regulierungs-GmbH
[4] Electronic Signature Act: Bundesgesetz über elektronische Signaturen, BGBl. I Nr. 190/1999 amended by BGBl I Nr. 137/2000, BGBl I Nr. 32/2001, and BGBl I Nr. 152/2001.
[5] Exceptions: Requirements c) and d) from Section 7.2.2 c) and d) concerning the backup of the private signing key cannot be applied because the Austrian Electronic Signature Act does not allow either copying or cloning of the private signing keys. The requirements from Section 7.2.8 are not applicable because the RTR-GmbH does not generate any subject keys. The requirements from Section 7.2.9 and requirements e) and f) from Section 6.2 are not applicable because the RTR-GmbH does not require the use of a Secure Signature-Creation Device.
[6] "Policy requirements for certification authorities issuing qualified certificates"
[7] Framework for the definition of other qualified certificate policies (i.e., not `qcp-public` or `qcp-public-with-sscd`)
[8] Aufsichtsstelle für elektronische Signaturen, "Sicherheits- und Zertifizierungskonzept - Certification Practice Statement," Version 1.1, Aufsichtsstelle für elektronische Signaturen Telekom-Control-Kommission, July 14, 2003.
[9] The CPS is available at http://www.signatur.rtr.at/de/directory/cps.html (in German) and http://www.signatur.rtr.at/en/directory/cps.html (in English).
[10] The report states the conformity of the public key infrastructure of the Austrian supervisory body for electronic signatures, which is operated by the RTR-GmbH, to the requirements on the supervisory body from the Austrian Electronic Signature Act.