In Ergänzung zum Vertrag über die Teilnahme an der PKI-1-Verwaltung verpflichtet sich der Antragsteller

1. den ordnungsgemäßen Betrieb der Zertifizierungsstelle nach dem aktuellen Stand der Technik sicherzustellen,
2. den ordnungsgemäßen Betrieb der Zertifizierungsstelle mindestens für den Gültigkeitszeitraum der ausgestellten Endanwender-Zertifikate aufrechtzuerhalten,
3. das Einstellen des Betriebs der Wurzelzertifizierungsstelle rechtzeitig anzuzeigen und die damit verbundene Sperrung des eigenen Zertifizierungsstellen-Zertifikats zu beantragen,
4. das Sperren von Zertifikaten zuverlässig und unverzüglich durchzuführen,
5. den mit der Wurzelzertifizierungsstelle vereinbarten Namensraum einzuhalten,
6. die Konformität zu der MailTrust-Spezifikation (MTTv2), definiert durch die jeweils aktuellste Version des Dokuments SPHINX-Tailoring MTTv2 zu garantieren und, falls aus Gründen der Interoperabilität oder anderen wichtigen Gründen der Fortentwicklung erforderlich, die Migration zu weiteren Standards (z.B. ISIS-MTT) innerhalb einer angemessenen Frist vorzunehmen,
7. Zertifikate ausschließlich für die Realisierung von Ende-zu-Ende-Sicherheit bei E-Mails, zur Absicherung von Internet-Verbindungen mit SSL oder als Gruppenzertifikate gemäß dem in den aktuell geltenden Sicherheitsleitlinien der Wurzelzertifizierungsstelle der Verwaltung bestimmten Zweck auszustellen,
8. die eigenen Sicherheitsleitlinien nach anerkannten Standards (z. B. RFC 2527) der Allgemeinheit in verständlicher Form zugänglich zu machen,
9. die für den operativen Betrieb erforderlichen Standardsicherheitsmaßnahmen nach IT-Grundschutzhandbuch umzusetzen und in einem Sicherheitskonzept zu dokumentieren,
10. kryptografische Verfahren einzusetzen, die nach dem derzeitigem Stand der Technik die Abhörsicherheit der elektronischen Kommunikation hinreichend gewährleisten,
11. alle Antragsteller eines Zertifikates zuverlässig und persönlich zu identifizieren,
12. im Falle juristischer Personen die Vertretungsvollmacht der sie vertretenden natürlichen Person zuverlässig zu überprüfen,
13. sicherzustellen, dass Zertifikate nur auf den Namen des Antragstellers bzw. auf ein von diesem gewähltes Pseudonym bzw. bei nicht personenbezogenen Zertifikaten (z.B. Gruppenzertifikate) jeweils gemäß dem aktuell geltenden Namenskonzept ausgestellt werden,
14. zu gewährleisten, dass sich der Zertifikatsinhaber im Besitz des korrespondierenden privaten Schlüssels befindet,
15. auf ein Pseudonym ausgestellte und nicht personenbezogene Zertifikate als solche kenntlich zu machen,
16. den Zertifikatsinhaber über den Anwendungsbereich und die mit dem Einsatz verbundenen Risiken der ausgestellten Teilnehmerzertifikate sowie seine Grundpflichten angemessen zu unterrichten,
17. das Speichern privater Teilnehmerschlüssel – falls diese Leistung für Verschlüsselungszertifikate durch die Zertifizierungsstelle erbracht wird – nur und nach umfassender Information über die möglichen sicherheitsrelevanten Konsequenzen durchzuführen,
18. diese Selbsterklärung allgemein zugänglich zu veröffentlichen.

Der Unterzeichner ist sich bewusst, dass jede unrichtige Angabe in der Selbsterklärung das BSI zur sofortigen Zurückweisung des Antrags, zur Kündigung des Vertrags und zur Sperrung des Zertifizierungsstellen-Zertifikats berechtigt.

Stempel und rechtsverbindliche Unterschrift der Zertifizierungsstelle

Bonn, 4 .01.2006

BUNDESMINISTERIUM DER VERTEIDIGUNG 164

Bonn