



A-Trust Gesellschaft für Sicherheitssysteme im elektronischen
Zahlungsverkehr GmbH.
Landstraßer Hauptstraße 5
Tel.: +43 (1) 713 21 51 – 0
Fax: +43 (1) 713 21 51 – 350
office@a-trust.at
www.a-trust.at

a.trust

**Certificate Policy für a-sign^{test}
Zertifikate
für Testzwecke**

Version: 1.0.1

Datum: 23.09.2005

Inhaltsverzeichnis

1	Einführung	3
1.1	Überblick.....	3
1.2	Identifikation.....	3
1.3	Anwendungsbereich	3
1.4	Übereinstimmung mit der Policy	4
2	Verpflichtungen und Haftungsbestimmungen	5
2.1	Verpflichtungen von a.trust	5
2.2	Verpflichtungen des Signators	5
2.3	Verpflichtungen des Überprüfers von Zertifikaten	5
2.4	Haftung	5
3	Anforderung an die Erbringung von a-sign test Zertifizierungsdiensten	6
3.1	Certification Practice Statement.....	6
3.2	Verwaltung der Schlüssel zur Erbringung von Zertifizierungsdiensten	6
3.2.1	Erzeugung der a.trust Schlüssel	6
3.2.2	Erzeugung der Schlüssel für die Signatoren.....	6
3.3	Lebenszyklus des Zertifikats	7
3.3.1	Abläufe.....	7
3.3.2	Zertifikats- und CRL-Inhalt	7
4	Anhang	8

1 Einführung

1.1 Überblick

Eine Certificate Policy enthält ein Regelwerk, das den Einsatzbereich eines Zertifikats für eine bestimmte Benutzergruppe und/oder Anwendungsklasse mit gemeinsamen Sicherheitsanforderungen definiert.

Die a•sign**test** Certificate Policy gilt für Testzertifikate, die ausschließlich zu Testzwecken an Projektpartner und Entwickler, die mit a.trust Produkten arbeiten wollen, ausgestellt werden.

1.2 Identifikation

Name der Policy: a.trust Certificate Policy für a•sign**test** Zertifikate für Testzwecke
Version: 1.0.1/23.09.2005
Object Identifier: **1.2.040.0.17** (a.trust).1 (Policy).4 (a•sign**test**).1.0.1 (Version)
vorliegende Version

Der a.trust OID 1.2.040.0.17 ist bei ÖNORM registriert.

1.3 Anwendungsbereich

Die a•sign**test** Certificate Policy gilt nur für Testzertifikate, die zum Testen von Applikationen ausgestellt werden.

Eine Signatur mit diesen Zertifikaten hat keinerlei rechtliche Wirksamkeit, d. h. diese Zertifikate sind nicht zum Erstellen einer gültigen digitalen Signatur geeignet.

1.4 Übereinstimmung mit der Policy

a.trust verwendet den Object Identifier aus Kapitel 1.2 nur für die Erstellung von Zertifikaten, anlässlich deren Ausgabe die Regelungen der gegenständlichen Policy für Testzertifikate Beachtung fanden.

2 Verpflichtungen und Haftungsbestimmungen

2.1 Verpflichtungen von a.trust

a.trust ist verpflichtet die a•sign**test** Zertifikate mit einer eigenen CA auszustellen, die nicht zur Ausstellung echter Zertifikate verwendet werden darf.

a•sign**test** Zertifikate werden eindeutig als Testzertifikate gekennzeichnet, so dass keine Verwechslung mit gültigen Produkten von a.trust möglich ist.

Darüber hinaus erwachsen a.trust keinerlei Verpflichtungen aus der Ausstellung der a•sign**test** Testzertifikate.

2.2 Verpflichtungen des Signators

Ein Signator, der über ein a•sign**test** Zertifikat verfügt, darf dieses nur für Tests von Applikationen verwenden.

2.3 Verpflichtungen des Überprüfers von Zertifikaten

Ein Empfänger einer mit einem a•sign**test** Zertifikat erstellten Signatur muss diese als rechtlich unwirksame Signatur behandeln, welche nur zu Testzwecken erstellt wurde.

2.4 Haftung

a.trust übernimmt als Aussteller von a•sign**test** Zertifikaten keine Haftung für missbräuchliche Verwendung der Zertifikate.

3 Anforderung an die Erbringung von a•signtest Zertifizierungsdiensten

Diese Policy ist auf die Erbringung von a•signtest Zertifizierungsdiensten für Testzertifikate ausgerichtet. Dies umfasst die Bereitstellung von Registrierungsdiensten, Schlüssel- und Zertifikatsgenerierung, Zertifikatsausgabe und Widerrufsdiensten und Abfragediensten über den Zertifikatsstatus.

3.1 Certification Practice Statement

Ein Certification Practice Statement (CPS) für a•signtest Dienste existiert nicht. Die verwendete Infrastruktur und die organisatorischen, personellen und technischen Abläufe und Maßnahmen entsprechen grundsätzlich jenen, die bei a.sign Premium angewandt werden.

3.2 Verwaltung der Schlüssel zur Erbringung von Zertifizierungsdiensten

3.2.1 Erzeugung der a.trust Schlüssel

Die Verwaltung der a•signtest Schlüssel erfolgt in gleicher Weise wie die Verwaltung der a.sign Premium Schlüssel mit der Ausnahme, dass a•signtest CA-Schlüssel nicht in einem Hardware Security Modul generiert und aufbewahrt werden, sondern mittels Software generiert und gespeichert werden.

3.2.2 Erzeugung der Schlüssel für die Signatoren

Die Generierung der Schlüssel der Signatoren entspricht der Vorgangsweise für a.sign Premium.

3.3 Lebenszyklus des Zertifikats

3.3.1 Abläufe

Die folgenden Abläufe entsprechen den Vorgangsweisen des Dienstes a.sign Premium und sind im Certification Practice Statement bzw. in der Certificate Policy von a.sign Premium nachzulesen.

- Kartenbestellung und -abholung
- Zertifikatserstellung
- Veröffentlichung des Zertifikats im Verzeichnisdienst
- Sperre und Sperraufhebung
- Widerruf
- Ausstellung der Widerrufsliste (CRL)
- a.trust Verwaltung
- Maßnahmen in personellen, technischen und organisatorischen Belangen

3.3.2 Zertifikats- und CRL-Inhalt

Die Inhalte (Profil) des a•sign**test** Zertifikats und der CRL entsprechen denen des a.sign Premium Dienstes. Alle Informationen dazu sind in der Certificate Policy (siehe [Policy]) und im CPS (siehe [CPS]) von a.sign Premium enthalten.

Was die Korrektheit der zertifizierten Daten betrifft, werden, da es sich um Testzertifikate handelt, keine Anforderungen gestellt. Somit muss bei der Registrierung keine Überprüfung der Daten auf Grund eines Ausweises erfolgen.

4 Anhang

A Referenzdokumente

- [CPS] a.trust Certification Practice Statement für qualifizierte a.sign
Premium Zertifikate für sichere Signaturen,
<http://www.a-trust.at/docs/cps/a-sign-premium/a-sign-premium.pdf>
- [Policy] Certificate Policy für qualifizierte a.sign Premium Zertifikate für
sichere Signaturen,
<http://www.a-trust.at/docs/cp/a-sign-premium/a-sign-premium.pdf>