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·signtest Zertifikate für Testzwecke

Version: 1.0

Datum: 05.09.2002

Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH.
A-1030 Wien, Landstraßer Hauptstraße 5

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·signtest 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•signtest 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•signtest Zertifikate für Testzwecke
Version:	1.0/05.09.2002
Object Identifier:	**1.2.040.0.17** (A-Trust)**.1** (Policy)**.4** (a•signtest)**.1.0** (Version) vorliegende Version

Der A-Trust OID 1.2.040.0.17 ist bei ÖNORM registriert.

1.3 Anwendungsbereich

Die a•signtest 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.

Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH.
A-1030 Wien, Landstraßer Hauptstraße 5

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•signtest Zertifikate mit einer eigenen CA auszustellen, die nicht zur Ausstellung echter Zertifikate verwendet werden darf.

a•signtest 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•signtest Testzertifikate.

2.2 Verpflichtungen des Signators

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

2.3 Verpflichtungen des Überprüfers von Zertifikaten

Ein Empfänger einer mit einem a•signtest 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•signtest 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 trust|sign 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 trust|sign 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 trust|sign.

3.3 Lebenszyklus des Zertifikats

3.3.1 Abläufe

Die folgenden Abläufe entsprechen den Vorgangsweisen des Dienstes trust|sign und sind im Certification Practice Statement bzw. in der Certificate Policy von trust|sign 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•signtest Zertifikats und der CRL entsprechen denen des trust|sign Dienstes. Alle Informationen dazu sind in der Certificate Policy (siehe [Policy]) und im CPS (siehe [CPS]) von trust|sign 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 trust|sign Zertifikate für sichere Signaturen, http://www.a-trust.at/docs/cps/TrustSign/TrustSign_CPS.pdf
[Policy]	Certificate Policy für qualifizierte trust|sign Zertifikate für sichere Signaturen, http://www.a-trust.at/docs/cp/TrustSign/TrustSign_CP.pdf