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-inhouse Zertifikate

Version: 1.0.2

Datum: 09.11.2005

Inhaltsverzeichnis

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-inhouse Certificate Policy gilt für einfache a-sign-inhouse Zertifikate, die ausschließlich zum Zweck interner Verwendung ausgestellt werden.

1.2 Identifikation

Name der Policy:	a.trust Certificate Policy für a-sign-inhouse Zertifikate für interne Anwendungen
Version:	1.0.2/09.11.2005
Object Identifier:	**1.2.040.0.17** (a.trust)**.1** (Policy)**.19** (a-sign-inhouse)**.1.0.2** (Version) vorliegende Version

Der a.trust OID 1.2.040.0.17 ist bei ÖNORM registriert.

1.3 Anwendungsbereich

Die a-sign-inhouse Certificate Policy gilt nur für Zertifikate, die für interne Zwecke ausgestellt werden.

a-sign-inhouse Zertifikate sind nicht qualifizierte Zertifikate.

Eine Signatur mit diesen Zertifikaten entfaltet ihre rechtliche Wirksamkeit nur in dem Rahmen der Projekte und nur im Datenaustausch zwischen jenen Projektpartnern, für die die Zertifikate ausgestellt werden.

1.4 Übereinstimmung mit der Policy

a.trust verwendet den Object Identifier aus Kapitel 1.2 nur für die Erstellung von einfachen Zertifikaten, anlässlich deren Ausgabe die Regelungen der gegenständlichen Policy für a-sign-inhouse Zertifikate Beachtung finden.

2 Verpflichtungen und Haftungsbestimmungen

2.1 Verpflichtungen von a.trust

a.trust ist verpflichtet die a-sign-inhouse Zertifikate mit einer eigenen Zwischeninstanz-CA auszustellen, die nicht zur Ausstellung anderer Zertifikate verwendet wird.

a-sign-inhouse Zertifikate werden eindeutig als Zertifikate für interne Verwendung gekennzeichnet, so dass keine Verwechslung mit anderen Produkten von a.trust möglich ist.

Darüber hinaus erwachsen a.trust keinerlei Verpflichtungen aus der Ausstellung der a-sign-inhouse Zertifikate.

2.2 Verpflichtungen des Signators

Ein Signator, der über ein a-sign-inhouse Zertifikat verfügt, darf dieses nur für interne Zwecke im Rahmen definierter Anwendungen benützen.

2.3 Verpflichtungen des Überprüfers von Zertifikaten

Ein Empfänger einer mit einem a-sign-inhouse Zertifikat erstellten Signatur muss diese als Signatur behandeln, die ihre Rechtswirksamkeit nur in einem eingeschränkten, internen Rahmen entfaltet.

2.4 Haftung

a.trust übernimmt als Aussteller von a-sign-inhouse Zertifikaten keine Haftung für missbräuchliche Verwendung der Zertifikate.

3 Anforderung an die Erbringung von a-sign-inhouse Zertifizierungsdiensten

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

3.1 Certification Practice Statement

Ein Certification Practice Statement (CPS) für a-sign-inhouse Dienste existiert nicht. Die verwendete Infrastruktur und die 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-sign-inhouse Schlüssel erfolgt in gleicher Weise wie die Verwaltung der Schlüssel anderer nicht qualifizierter Dienste.

a-sign-inhouse CA-Schlüssel werden in einem Hardware Security Modul generiert und aufbewahrt, dessen private Schlüssel zum Zweck der Ausfallsicherheit exportierbar sind.

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.

- Veröffentlichung des Zertifikats im Verzeichnisdienst
- Sperre und Sperraufhebung
- Widerruf
- Ausstellung der Widerrufsliste (CRL)
- Maßnahmen in technischen und organisatorischen Belangen

3.3.2 Zertifikats- und CRL-Inhalt

Die Inhalte (Profil) des a-sign-inhouse 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.

Projektspezifische Erweiterungen können hinzukommen.

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