

Unterrichtung gemäß Artikel 24 Abs 2 lit d eIDAS-Verordnung

Informationen über die Bedingungen für die Nutzung der qualifizierten Zertifikate a.sign premium seal von A-Trust, Version 2.0

1 Vertragsbestandteile a sign premium seal

Die siegelerstellende Person schließt einen Vertrag mit dem qualifizierten Vertrauensdiensteanbieter A-Trust GmbH („A-Trust“). Die Registrierung für das Produkt a.sign premium seal erfolgt durch A-Trust in deren Räumlichkeiten. Das Vertragsverhältnis zwischen der siegelerstellende Person und A-Trust besteht ausschließlich aus folgenden Vertragsdokumenten in ihrer jeweils gültigen Version:

- Der Antrag/Siegelvertrag,
- die Allgemeinen Geschäftsbedingungen (AGB) der A-Trust Gesellschaft für Sicherheitssysteme im elektronischen Datenverkehr GmbH für qualifizierte und fortgeschrittene Zertifikate,
- die A-Trust Zertifizierungsrichtlinie (Certificate Practice Statement) für qualifizierte Zertifikate a.sign premium,
- die A-Trust Anwendungsvorgabe (Certificate Policy) für qualifizierte Zertifikate a.sign premium seal,
- die A-Trust Entgeltbestimmungen,
- die A-Trust Liste der empfohlenen Komponenten und Verfahren,
- dieser Unterrichtung.

Alle Vertragsdokumente wurden von der staatlichen Aufsichtsstelle geprüft und abgenommen. Der Umgang mit ihren persönlichen Daten ist im Datenschutzgesetz 2000, dem SVG und der eIDAS-Verordnung geregelt. A-Trust verwendet Ihre Daten nur insoweit, als im Rahmen ihrer Leistungserbringung erforderlich.

A-Trust haftet gem. Artikel 13 eIDAS-Verordnung für alle natürlichen oder juristischen Personen vorsätzlich oder fahrlässig zugefügten Schäden, die auf eine Verletzung der in dieser Verordnung festgelegten Pflichten zurückzuführen sind.

2 Der Siegelvertrag

Mit dem Siegelvertrag wird die Ausstellung eines qualifiziertes Zertifikat a.sign premium seal beantragt und dessen Inhalt festgelegt. Im Siegelvertrag wird die Geltung der übrigen Vertragsbestandteile vereinbart.

3 Die Zertifizierungsrichtlinie (Certification Practice Statement, CPS) zu a.sign premium seal

Die Zertifizierungsrichtlinie ist die allgemein verständliche Zusammenfassung des Sicherheits- und Zertifizierungskonzepts von A-Trust. In der Zertifizierungsrichtlinie werden die technischen und organisatorischen Bedingungen der Erstellung des qualifizierten Zertifikats durch A-Trust, sowie Details zu Registrierung und Aktivierung für die siegelerstellende Person bekannt gegeben. Damit kann sich jeder, auch die potentiellen Empfänger:innen bzw. Prüfer:innen der Siegel, ein Bild von der Gesamtsicherheit von a.sign premium seal machen.

4 Die Anwendungsvorgaben (CP: Certificate Policy) zu a.sign premium seal

Die Anwendungsvorgaben beschreiben den Inhalt und die Bedingungen der sicheren Verwendung des Zertifikats durch den die siegelerstellende Person. Anhand der Anwendungsvorgaben kann die Person, die ein Siegel empfängt eruieren, ob es sich um ein qualifiziertes Siegel handelt und ob das ihr zu Grunde liegende Zertifikat ein qualifiziertes Zertifikat ist. Neben den Rechten und Pflichten der

Kontakt E-Mail: office@a-trust.at, Telefon: +43 1 713 21 51 0
Konto Oberbank, BIC: OBKLAT2L, IBAN: AT17 1515 0005 0116 4396
Firmenbuch UID: ATU50272100, DVR: 1065181, FN: 195738a, HG Wien

siegelerstellenden Person sind dort auch jene des qualifizierten Vertrauensdiensteanbieters dargestellt. Auf die Anwendungsvorgaben stützt sich somit die Vertrauenswürdigkeit eines Zertifikats.

Alle Vertragsdokumente sind zum Download verfügbar: <http://www.a-trust.at/downloads>

5 Rechtswirkungen von qualifizierten elektronischen Siegeln

Gemäß Artikel 35 Abs. 2 eIDAS-Verordnung hat ein qualifiziertes elektronisches Siegel folgende Rechtswirkungen:

- Einem elektronischen Siegel darf die Rechtswirkung und die Zulässigkeit als Beweismittel in Gerichtsverfahren nicht allein deshalb abgesprochen werden, weil es in einer elektronischen Form vorliegt oder nicht die Anforderungen an qualifizierte elektronische Siegel erfüllt.
- Für ein qualifiziertes elektronisches Siegel gilt die Vermutung der Unversehrtheit der Daten und der Richtigkeit der Herkunftsangabe der Daten, mit denen das qualifizierte elektronische Siegel verbunden ist.
- Ein qualifiziertes elektronisches Siegel, das auf einem in einem Mitgliedstaat ausgestellten qualifizierten Zertifikat beruht, wird in allen anderen Mitgliedstaaten als qualifiziertes elektronisches Siegel anerkannt.

6 Technische Komponenten (Signatur- bzw. Siegelprodukte), Formate und Verfahren

Die von a.trust empfohlenen Komponenten, Formate und Verfahren für qualifizierte Signaturen und Siegel behandeln eine qualitätsgesicherte Arbeitsumgebung des Zertifikatsinhabers, der mit einer von A-Trust ausgestellten Karte eine sichere digitale Signatur oder ein sicheres digitales Siegel erstellt. Das Hauptaugenmerk dieser Empfehlung wird auf die folgenden Aspekte gelegt:

- Schutz des privaten Schlüssels und der Signatur-PIN: Der private Schlüssel ist auf der Karte sicher gespeichert. Der Signatur- bzw. Siegelschlüssel kann und darf nur mit der geheimen Signatur- bzw. Siegel-PIN genutzt werden. Auf der A-Trust-Homepage finden Sie die jeweils von A-Trust geprüften und als für den PIN-Schutz geeignet empfohlenen Chipkartenleser. Die Änderung dieser PIN geschieht mit dem kostenlos von der Homepage herunter ladbaren Software a.sign client.
- Erstellung der qualifizierten Signatur bzw. des Siegels: Damit die siegelerstellende Person selbst und auch die empfangende Person wirklich sicher sein können, dass das übermittelte Dokument unverfälscht ankommt, soll die siegelerstellende Person als Signatur- bzw. Siegelformate keine Dateiformate verwenden, die etwa dynamische Datumsfelder beinhalten oder Weiß-auf-Weiß-Darstellungen zulassen.
- Sichere Überprüfung: Die Person, die ein qualifiziertes Zertifikat prüft oder eine darauf beruhende Signatur bzw. ein darauf beruhendes Siegel wird von A-Trust eine geeignete Infrastruktur bereitgestellt. Detaillierte Angaben darüber und über den Zertifikatsdatenbank mit der aktuellen Widerrufs- und Sperrliste zur Zertifikats- und Signatur- bzw. Siegelprüfung finden Sie auf der Homepage der A-Trust. Die Inanspruchnahme der Verzeichnisdienste erfolgt unentgeltlich und anonym.

A-Trust haftet im Fehlerfall nur insoweit als Vertrauensdiensteanbieter, als ausschließlich die von ihr empfohlenen Komponenten, Formate und Verfahren eingesetzt wurden. (Siehe www.a-trust.at/docs/verfahren)

7 Pflichten der siegelerstellenden Person

Der Umgang der siegelerstellenden Person mit der a.sign premium seal Karte ist ein wesentlicher Aspekt der Gesamtsicherheit des qualifizierten Siegels. Prämisse beim Umgang mit der Siegelstellungseinheit und beim Einsatz der empfohlenen Signatur- bzw. Siegelprodukte und Verfahren ist der Schutz und die Geheimhaltung der Siegelerstellungsdaten mit zugehöriger Siegel-PIN.

Pflichten für die siegelerstellende Person ergeben sich aus den Vertragsdokumenten, der eIDAS-Verordnung und dem Signatur- und Vertrauensdienstegesetz. Insbesondere haben siegelerstellende Personen a.sign premium seal Zertifikate auf der Karte sorgfältig zu verwahren und soweit zumutbar Zugriffe von Dritten auf ihre elektronischen Siegelerstellungsdaten zu verhindern und deren Weitergabe an Dritte zu unterlassen. Die Weitergabe von elektronischen Siegelerstellungsdaten an autorisierte Personen ist zulässig. Siegelerstellende Person haben den Widerruf des qualifizierten Zertifikats zu verlangen, wenn die elektronischen Siegelerstellungsdaten abhandengekommen, wenn Anhaltspunkte für deren Kompromittierung bestehen oder wenn sich die im qualifizierten Zertifikat bescheinigten Umstände geändert haben.

Zur Sicherheit der siegelerstellenden Person empfiehlt A-Trust:

- das Siegelpasswort nur auf Seiten anzugeben, auf denen in der Adresszeile des Browsers die URL <https://www.a-trust.at/> oder <https://www.handy-signatur.at> zu sehen ist;
- in der Verifikations-Nachricht, welche die TAN enthält, ist ein Vergleichswert enthalten, der auch auf der Webseite angezeigt wird. Es obliegt der siegelerstellenden Person, diese beiden Vergleichswerte auf Übereinstimmung zu prüfen, sodass sichergestellt wird, dass das richtige Dokument signiert wird;
- sämtliche Browserfunktionen, die ein Speichern der Feldeingaben (Handynummer sowie Siegelpasswort) zum Ziel haben, für die Benutzung der Vertrauensdienstleistungen zu deaktivieren (z.B. Auto Vervollständigung, Speichern von Passwörtern);
- den Einsatz aktueller Sicherheits-Software (Viruschutz, Firewall), um das Ausspähen des Siegelpasswortes durch Schadsoftware zu verhindern;
- die Sicherheitsmechanismen des Betriebssystems des Mobiltelefons nicht durch Roots bzw. Jailbreaks zu umgehen;

- in Verbindung mit Vertrauensdienstleitungen eingesetzte Apps nur aus offiziellen App-Stores der jeweiligen Anbieter zu beziehen: iTunes Appstore, Google Play Store, Windows App Store etc.);
- den privaten Schlüssel nach erfolgtem Widerruf des Handy-Signatur Zertifikates löschen zu lassen. Online – Durchführung sowie Informationen unter <http://www.a-trust.at/widerruf>;
- die zusätzlichen Informationen unter <https://www.a-trust.at/app-security> zu beachten.

8 Widerrufsdienst

A-Trust stellt mit dem Widerrufsdienst sicher, dass bei Bedenken hinsichtlich der Sicherheit eines Zertifikats jederzeit, schnell und einfach der Widerruf bzw. die Aussetzung des Zertifikats möglich ist. Dies und die allfällige Aufhebung einer Aussetzung sind die einzigen, aber sehr wichtigen Aufgaben des Widerrufsdienstes.

Die Gründe für einen Widerruf können sein:

Karte wurde verloren, gestohlen, abgenommen, oder ist defekt

- PIN wurde vergessen oder ist einer anderen Person bekannt geworden (auch bei Verdacht)
- Zertifikatsdaten haben sich geändert

A-Trust hat ein qualifiziertes Zertifikat auszusetzen, wenn:

- Die siegelerstellende Person oder eine sonstige dazu berechnigte Person dies verlangt,
- die Aufsichtsstelle die Aussetzung des Zertifikats verlangt,
- A-Trust Kenntnis vom Ableben der siegelerstellenden Person oder sonst von der Änderung der im Zertifikat bescheinigten Umstände erlangt,
- das Zertifikat auf Grund unrichtiger Umstände erlangt wurde, oder
- die Gefahr einer missbräuchlichen Verwendung des Zertifikats besteht.

Die Aufhebung einer Aussetzung kann innerhalb der Sperrfrist von 10 Tagen unter Verwendung des Widerrufspasswortes bzw. des Aussetzungspasswortes erfolgen, welches Sie für diesen Zweck bei der telefonischen Beantragung der Aussetzung vom Widerrufsdienst erhalten.

Die Zertifikatsnummern widerrufener oder ausgesetzter Zertifikate werden durch A-Trust in die so genannte Sperrliste (CRL: Certificate Revocation List) eingetragen. Diese von A-Trust signierte Sperrliste wird laufend aktualisiert, somit kann jederzeit der Status eines Zertifikats geprüft werden – dies geschieht in der Regel automatisch durch die verwendeten Softwareprodukte.

Nähere Erklärungen zu Widerruf und Aussetzung, sowie Erreichbarkeit des Widerrufsdienstes finden Sie unter www.a-trust.at/widerruf

9 Call Center

Im Falle von technischen Probleme beim Einsatz von a.sign premium seal, steht die kostenpflichtige Hotline (1,09 EUR/Min.) der A-Trust zur Verfügung. (siehe: www.a-trust.at/callcenter)

10 Unterrichtung laut eIDAS-Verordnung: Informationen zur Sicherheit der siegelerstellende Person

Die siegelerstellende Person bestätigt mit der Anerkennung des Siegelvertrages, dass vor Abschluss des

Vertrags über folgende Punkte ausführliche Informationen zur Verfügung standen und ich diese akzeptiert wurden:

Den Leistungen von A-Trust liegen Zertifizierungsrichtlinie (CPS) und Anwendungsvorgaben (CP) für qualifizierte Zertifikate zu Grunde. Diese Dokumente sind von der Homepage der A-Trust abrufbar und liegen in der Registrierungsstelle frei verfügbar auf. Die maximale Gültigkeitsdauer eines Zertifikats beträgt 5 Jahre. Danach muss die Gültigkeit des Zertifikats verlängert (Zertifikatserneuerung) oder allenfalls ein neues Zertifikat aktiviert werden. A-Trust hat sich bei der staatlichen Aufsichtsstelle, der Telekom-Control-Kommission (TKK) akkreditieren lassen und wird von der TKK entsprechend überprüft.

A-Trust haftet für die alle natürlichen oder juristischen Personen vorsätzlich oder fahrlässig zugefügten Schäden, die auf eine Verletzung der in der eIDAS-Verordnung, dem Signatur- und Vertrauensdienstegesetz oder der Signatur- und Vertrauensdiensteverordnung festgelegten Pflichten zurückzuführen sind. Sollte eine betragsmäßige Haftungsbeschränkung der A-Trust vorliegen, so wird diese explizit als Transaktionslimit im Zertifikat ausgewiesen.

Die siegelerstellende Person muss auf die sorgsame Verwahrung seiner Karte (Siegelerstellungseinheit) achten. Diese und die zugehörige Signatur-PIN dürfen niemandem außer vertraglichen oder gesetzlichen Vertretern der siegelerstellenden Person zugänglich sein. Die PIN muss so ausgewählt werden, dass sie andere nicht logisch ableiten können. Nur durch die Eingabe der Siegel-PIN wird das Siegel im Chip der Karte erstellt. Zum Schutz der Siegel-PIN muss darauf geachtet werden, welche Hard- und Software genutzt wird. Eine Liste von empfohlenen Hard- und Softwarekomponenten ist von der Homepage von A-Trust abrufbar.

Wenn der Schutz von Karte oder Siegel-PIN nicht gewährleistet ist, muss das Zertifikat beim Widerrufsdienst der A-Trust widerrufen werden. Dies gilt auch für den Fall, dass sich die im Zertifikat enthaltenen Angaben ändern, oder falsch sind. Der Widerruf des Zertifikats erfolgt telefonisch oder per Fax unter Nennung von Namen, Kartenummer und des gewählten Widerrufspassworts. A-Trust stellt ebenfalls die Möglichkeit einer vorübergehenden Aussetzung zur Verfügung, die mittels des Widerrufspassworts, oder einem vereinbarten Passwort für die Aufhebung der Aussetzung wieder rückgängig gemacht werden kann (Siehe www.a-trust.at/widerruf).

Die Haftung von A-Trust für das qualifizierte Siegel ist nur bei Verwendung von A-Trust empfohlenen technischen Komponenten und Verfahren gewährleistet. Die A-Trust Homepage verweist auf entsprechende Produkte und Dienstleistungen, bei welchen eine sichere Siegelumgebung vorausgesetzt werden kann. Weiters ist auf die von A-Trust empfohlenen Dateiformate Rücksicht zu nehmen. Die empfangende Person eines qualifizierten Siegels vertraut auf die Verwendung empfohlener Komponenten, da die Verwendung aus dem besiegelten elektronischen Inhalt und dem Siegel selbst nicht ableitbar ist. Die Empfehlungen der A-Trust stehen ihm ebenfalls zur Gänze und in gleicher Form zur Verfügung. Bei Verwendung anderer Verfahren und Formate als der von A-Trust empfohlenen hat die siegelerstellende Person die Pflicht, die Person, die das Siegel empfängt, des Siegels davon in Kenntnis zu setzen oder eine gesonderte Vereinbarung mit ihm zu treffen, um die Vertrauensbasis zur Akzeptanz des Siegels zu gewährleisten.

Informationen über die Zertifikatsdatenbank mit der aktuellen Widerrufs- und Sperrliste zur Zertifikatsprüfung befindet sich auf der Homepage von A-Trust. Die Inanspruchnahme der Zertifikatsdatenbank erfolgt nach Maßgabe der technischen Möglichkeiten unentgeltlich und anonym. Für die Siegelprüfung können dieselben Komponenten und Verfahren wie für die Siegelerstellung verwendet werden. Auf der Homepage der A-Trust werden Änderungen betreffend der relevanten Verfahren und Komponenten veröffentlicht. In diesem Zusammenhang sind den Erneuerungsempfehlungen der Hersteller, oder von A-Trust Folge zu leisten.

Manche Staaten beschränken den Import bzw. Export von Verschlüsselungstechnologien. Vor Reisen muss sich die siegelerstellende Person über die entsprechenden Rechtsvorschriften des jeweiligen Staates informieren.