Zertifikatswerber-Vertrag

1) Gültigkeitsdauer des Zertifikatswerber-Vertrages

Der vorliegende Zertifikatswerber-Vertrag erlangt Gültigkeit an dem Tag, an dem Sie den Zertifikatswerber-Vertrag unterschrieben haben und gilt für maximal 3 Jahre.

Das ausgestellte a-sign User-Zertifikat Premium ist ab dem Ausstellungszeitpunkt (ist im Zertifikat enthalten) ein Jahr gültig. Dieses Zertifikat kann zweimal jeweils für die Dauer eines Jahres verlängert werden. Für die Verlängerung des ausgestellten Zertifikates wird keine neuerliche Identitätsüberprüfung gefordert. Die Verlängerung kann nur auf Basis eines gültigen a-sign Zertifikates Premium und einer gültigen Signatur vorgenommen werden. Eine Verlängerung eines bereits abgelaufenen qualifizierten Zertifikates ist nicht möglich.

2) Rechtliche Grundlagen des Zertifikatswerber-Vertrages

Der Zertifikatswerber-Vertrag basiert auf dem Österreichischen Signaturgesetz in der jeweils gültigen Fassung und der auf dessen Grundlage ergangenen Verordnungen.

2.1 Rechtswirkungen der elektronischen Signatur

Gemäß dem Österreichischen Signaturgesetz (SigG) können im Rechts- und Geschäftsverkehr Signaturverfahren mit unterschiedlichen Sicherheitsstufen und unterschiedlichen Zertifikatsklassen verwendet werden.

Das a-sign Zertifikat Premium (höchste Klasse, höchste Sicherheitsstufe) entspricht den Anforderungen des Österreichischen Signaturgesetzes an ein qualifiziertes Zertifikat und ermöglicht unter Einhaltung der unter Punkt 2.2. angeführten Bedingungen die Anfertigung einer „sicheren elektronischen Signatur" (gem. § 4 SigG). Eine "sichere elektronische Signatur" basiert demzufolge auf einem qualifizierten Zertifikat (=a-sign User-Zertifikat Premium) und wird entsprechend den Anordnungen unter Punkt 2.2. erstellt.

Rechtswirkungen der sicheren elektronischen Signatur
Die sichere elektronische Signatur entfaltet die Rechtswirkungen der eigenhändigen Unterschrift (=Schriftlichkeit) im Sinne des § 886 ABGB. Es besteht somit rechtlich kein Unterschied zwischen dieser elektronischen Signatur und der „händischen" Unterschrift (mit Kugelschreiber) auf Papier, mit Ausnahme nachfolgend angeführter sensibler Bereiche:

- Rechtsgeschäfte des Familien oder Erbrechts, die an die Schriftform oder eine strengere Form gebunden sind (z.B. Testament)
- Willenserklärungen oder Rechtsgeschäfte, die öffentlich beglaubigt oder beurkundet werden müssen oder die an einen Notariatsakt gebunden sind (z.B. Schenkung unter Ehegatten)
- Willenserklärungen, Rechtsgeschäfte oder Eingaben, die, um in das Grundbuch, Firmenbuch oder ein anderes öffentliches Register eingetragen werden zu können, öffentlich beglaubigt, gerichtlich oder notariell beurkundet werden müssen oder eines Notariatsaktes bedürfen sowie (z.B. Liegenschaftskauf)
- Bürgschaftserklärungen gem. § 1346 (2) ABGB

Weitere rechtliche Grundlagen und Informationen finden Sie auch in unserem Informationsdienst unter http://a-sign.datakom.at

2.2. Erstellung und Überprüfung einer sicheren elektronischen Signatur - empfohlene Signaturprodukte

Der Zertifizierungsdiensteanbieter Datakom empfiehlt zur Erstellung und Überprüfung sicherer elektronischer Signaturen entsprechende Signaturprodukte. Eine Liste der empfohlenen Signaturprodukte wird im Informationsdienst unter http://a-sign.datakom.at veröffentlicht. Nachfolgend angeführte Punkte sind zu beachten:

- Sicher elektronisch signiert werden dürfen ausschließlich Dokumentenformate, die vom Zertifizierungsdienstanbieter Datakom empfohlen werden. Eine Liste und Spezifikation der erlaubten Dokumentenformate finden Sie im Informationsdienst unter http://a-sign.datakom.at.
- Vor Auslösung des Signaturvorganges (d.i. vor Eingabe des 8-stelligen Autorisierungscodes) muss der Signator die Möglichkeit haben, dass ihm das zu signierende Dokument im empfohlenen Dokumentenformat angezeigt wird (=Secure Viewer Funktion).

Bitte beachten Sie:

- Das a-sign User-Zertifikat Premium ermöglicht ausschließlich das elektronische Signieren von Dokumenten. Es darf nicht zur Verschlüsselung vertraulicher Daten herangezogen werden.
- Konkrete Anleitungen zur Erstellung und Überprüfung sicherer elektronischer Signaturen mit den empfohlenen Signaturprodukten werden im a-sign Informationsdienst unter http://a-sign.datakom.at veröffentlicht.

3) Antrag auf Ausstellung des a-sign User-Zertifikates Premium

Der Antrag auf Ausstellung des a-sign User-Zertifikates Premium wird vom Zertifikatswerber persönlich in der lokalen Registrierungsstelle gestellt. Eine Liste der für den a-sign Zertifizierungsdienst tätigen lokalen Registrierungsstellen erhalten Sie unter nachfolgend angeführten Adressen: support@a-sign.datakom.at; Tel.Nr.: 0800/501 555 sowie im a-sign Web unter http://a-sign.datakom.at. Zur Antragstellung ist ein amtlicher Lichtbildausweis (zugelassen sind Reisepass, Führerschein oder Personalausweis) zwecks Überprüfung der Identität mitzubringen.

Der Antrag auf Ausstellung des a-sign Zertifikates Premium hat insbesondere zu enthalten: Namen, Datum und Ort der Geburt sowie Adresse des Zertifikatswerbers, Datum der Ausstellung und Nummer des vorgelegten Lichtbildausweises sowie die Behörde, die diesen ausgestellt hat. Nach Erhalt des Zertifikatsantrages erfolgt die Identitätsüberprüfung des Zertifikatswerbers anhand des amtlichen Lichtbildausweises entsprechend dem a-sign Sicherheits- und Zertifizierungskonzept.

4) Überprüfung der Identität des Zertifikatswerbers

Es erfolgt die Sichtkontrolle (Vergleich des im amtlichen Lichtbildausweises angebrachten Lichtbildes mit dem Erscheinungsbild des Zertifikatswerbers) und ein Vergleich der Daten im Zertifikatsantrag anhand des amtlichen Lichtbildausweises. Nur wenn die Überprüfung ein positives Ergebnis liefert, wird dem Antrag auf Ausstellung eines qualifizierten Zertifikates stattgegeben.

Die Datakom Austria behält es sich vor, weitere Daten im Zertifikatsantrag auf deren Gültigkeit hin zu überprüfen. Die dem Zertifikatsantrag zugrundeliegenden Daten werden, soweit Sie nicht ins Zertifikat aufgenommen werden, streng vertraulich behandelt. Datakom ist berechtigt, die Daten zum bestimmungsgemäßen Gebrauch zu verarbeiten und zu übermitteln.

5) Ausstellung des a-sign User-Zertifikates Premium

a-sign User Zertifikate Premium werden ausschließlich in Verbindung mit einer Chipkarte ausgegeben. Eine Liste der eingesetzten Chipkarten wird im Informationsdienst unter http://a-sign.datakom.at veröffentlicht. Wenn die Identität des Zertifikatswerbers ein positives Ergebnis liefert, erfolgt die Personalisierung der Chipkarte (=der private Schlüssel wird auf dem Chip generiert und verlässt diesen nicht)

Schlüsselgenerierung (Erzeugung der Signaturerstellungsdaten des Signators)

Schritt 1: Der Local Registration Authority-Operator (=LRA-Operator) gibt eine Smartcard in den Smartcard Reader.

Schritt 2: Der Zertifikatswerber vergibt persönlich eine achtstellige PIN (siehe dazu Punkt 7) mittels eines externen Tastaturblocks. Die PIN-Eingabe erfolgt zweimal mit Verifikation. Die Eingabe der PIN wird aus Sicherheitsgründen nicht angezeigt.

Schritt 3: Es erfolgt die Generierung des asymmetrischen Schlüsselpaares (privater und öffentlicher Schlüssel) gem. RSA, Schlüssellänge 1024bit; Hashwert SHA1

Schritt 4: Der Zertifikatsantrag wird vom LRA-Operator freigegeben und im Rahmen der SSLv2-Verbindung an den Zertifizierungsdienst Premium übermittelt.

Schritt 5: Generierung des a-sign Zertifikates Premium im Format X.509v3, Signatur des Zertifizierungsdiensteanbieters Datakom mittels Verschlüsselungsalgorithmus RSA/Schlüssellänge 1024 bit, Hashverfahren SHA1; Import auf die a-sign Smartcard

Schritt 6: Unterrichtung des Zertifikatswerbers im Sinne des Österreichischen Signaturgesetzes anhand Informationsmaterial

Schritt 7: Unterfertigung des Zertifikatswerber-Vertrages und Übergabe der Smartcard

6) Haftungsbestimmungen

Datakom haftet dafür, dass

a) alle Angaben im qualifizierten Zertifikat im Zeitpunkt seiner Ausstellung richtig sind,

b) der im qualifizierten Zertifikat angegebene Signator im Zeitpunkt der Ausstellung des Zertifikats im Besitz jener Signaturerstellungsdaten ist, die den im Zertifikat angegebenen Signaturprüfdaten entsprechen,

c) die Signaturerstellungsdaten und die ihnen zugeordneten Signaturprüfdaten einander bei Verwendung der von Datakom Austria bereitgestellten oder als geeignet bezeichneten Produkte und Verfahren in komplementärer Weise entsprechen,

d) das Zertifikat bei Vorliegen der Voraussetzungen unverzüglich widerrufen wird und die Widerrufsdienste verfügbar sind sowie

e) die Anforderungen des § 7 SigG erfüllt und für die Erzeugung und Speicherung von Signaturerstellungsdaten technische Komponenten und Verfahren nach § 18 SigG verwendet werden.

Für darüber hinausgehende Schäden haftet die Datakom entsprechend ihren AGB. http://www.datakom.at/unternehmen/agb.shtml.

Transaktionslimit

Das Transaktionslimit beträgt Euro 4.000,--/ATS 55.041,20 (im Zertifikat gekennzeichnet mit EUR,4,3). Dies bedeutet, dass die Haftung der Datakom Austria für von ihr verursachte Schäden (gleich welcher Art) mit diesem Betrag je Transaktion begrenzt ist. Ein Überschreiten des Transaktionslimits ändert jedoch nichts an der Gültigkeit der elektronischen Signatur. Signieren Sie also ein elektronisches Dokument / einen Vertrag, der das Transaktionslimit überschreitet, so erfüllt die elektronische Signatur dennoch das Erfordernis der Schriftlichkeit. Sie können sich beim Überschreiten des Transaktionslimits also nicht darauf berufen, dass der Vertrag nicht unterzeichnet (gültig) ist.
Bei Verwendung des Zertifikats erkennt der Empfänger der von ihnen elektronisch signierten elektronischen Nachricht das Transaktionslimit.

7) Sorgfaltspflichten des Signators

a) Autorisierungscode (im folgenden auch PIN Code genannt):
Der Autorisierungscode (die PIN) zum Auslösen des Signaturvorgangs ist nur dem Kunden bekannt (siehe Punkt 5). Wir empfehlen dringend im Sinne Ihrer Sicherheit keine PIN-Kombinationen wie z. B. Geburtsdatum, Sozialversicherungsnummer usw., die in Zusammenhang mit Ihrer Person von Dritten ausfindig gemacht werden können, zu verwenden. Beachten Sie bitte nachfolgend angeführte Informationen zum Autorisierungscode(=PIN)

- Zweck des Autorisierungscodes: Der Autorisierungscode ist für die Auslösung des Signaturvorganges notwendig. Die Auslösung des Signaturvorganges ohne Eingabe des Autorisierungscodes ist nicht möglich.
- Vergabe des Autorisierungscodes: Der Autorisierungscode besteht aus einer 8-stelligen PIN. Diese wird im Rahmen des Zertifikatsantrag in der lokalen Registrierungsstelle durch den Zertifikatswerber vor Auslösung der Schlüsselgenerierung, mittels eines externen Tastaturblocks generiert. Die Eingabe des Autorisierungscodes erfolgt zweimal mit Verifikation. Die Eingabe des Autorisierungscodes wird aus Sicherheitsgründen nicht angezeigt.
- Kenntnis des Autorisierungscodes: Der Autorisierungscode ist nur dem Signator bekannt. Die Weitergabe, das Kopieren, Speichern usw. des Autorisierungscodes ist untersagt.
- Eingabe des Autorisierungscodes: Der Autorisierungscode muss vor Auslösung des Signaturvorganges in voller Länge durch den Signator persönlich eingegeben werden. Die Speicherung oder eine Eingabeerleichterung (z.B. Abkürzungen, Aufschreiben, Weitergabe) sind untersagt.
- Sperre des Autorisierungscodes: Nach dreimaliger Falscheingabe des Autorisierungscodes wird der Chip automatisch gesperrt. Eine Entsperrung des Chips ist nicht möglich. Der Zugriff resp. die Auslösung des Signaturvorganges ist nicht mehr möglich. Das dazugehörige digitale Zertifikat muss widerrufen werden.
- Regelmäßiger Wechsel des Autorisierungscodes: Der Zertifikatsinhaber verpflichtet sich, seinen Autorisierungscode in regelmäßigen Abständen zu ändern.
- Signaturprodukte und Chipkartenlesegeräte: Der Signator verwendet zur Erstellung der sicheren elektronischen Signatur, basierend auf einem a-sign Zertifikat Premium, ausschließlich vom Zertifizierungsdiensteanbieter empfohlene Signaturprodukte und Chipkartenlesegeräte.

b) Chipkarte
Die Weitergabe der Chipkarte an Dritte ist untersagt. Der Kunde verpflichtet sich seine Chipkarte sorgsam zu verwahren und vor Zugriffen Dritter zu schützen. Wird die Chipkarte vom Signator – aus welchen Gründen auch immer – nicht mehr benötigt, so ist er verpflichtet – im Sinne der eigenen Sicherheit – den Zugriff auf die Chipkarte durch dreimalige Falscheingabe einer PIN zu sperren und diese in einer lokalen Registrierungsstelle zur ordnungsgemäßen Entsorgung abzugeben.

c) Änderung der im Zertifikat enthaltenen persönlichen Daten
Jede Änderung der im Zertifikatsantrag enthalten persönlichen Daten des Zertifikatswerbers (insbesondere Vorname, Nachname, Postanschrift etc.) ist dem Zertifizierungsdiensteanbieter Datakom umgehend bekannt zu geben.

d) Widerruf des a-sign Zertifikats Premium
Bei Verlust, Diebstahl, Verdacht der missbräuchlichen Verwendung seines Zertifikates, Änderung der im Zertifikat enthalten Daten oder automatischer Sperre des Chips nach dreimaliger falscher Eingabe des PIN Codes ist das Zertifikat umgehend zu widerrufen (http://a-sign.datakom.at/content/services/revoke.html):

- Telefonisch durch die Angabe persönlicher Daten (Vorname, Nachname, Geburtsort, Geburtsdatum, persönliches Revoke-Paßwort, telefonische Rückrufnummer) bei der Datakom Austria GmbH, Wiedner

Hauptstraße 73, 1040 Wien von Montag - Sonntag 00:00 bis 24:00 Uhr unter 01/50145-1354

- Persönlich durch die Angabe persönlicher Daten (Vorname, Nachname, Geburtsort, Geburtsdatum, persönliches Revoke-Paßwort) und Dokumentation dieser Daten durch einen amtlichen Lichtbildausweis (Reisepass, Führerschein oder Personalausweis) bei der Datakom Austria GmbH, Wiedner Hauptstraße 73, 1040 Wien von Montag - Donnerstag (wenn Werktag): 09:00 – 15:00; Fr (wenn Werktag) : 09:00- 13:00

Zum Widerruf berechtigte Personen
Zum Widerruf berechtigt ist der Zertifikatsinhaber (ohne Angabe von Gründen). DATAKOM akzeptiert jeden, der die notwendigen Daten und das Passwort nennt, als bevollmächtigt.

Durchführung und Veröffentlichung des Widerrufs
Datakom Austria bemüht sich, eingegangene Zertifikatswiderrufe umgehend zu bearbeiten, diese nach positiver Authentisierung vorzunehmen und umgehend zu veröffentlichen. Der Widerruf wird jedenfalls während der im Österreichischen Signaturgesetz genannten Geschäftszeiten (Werktags 09:00-17:00; Samstag (wenn Werktag) 09:00 – 12:00) spätestens innerhalb von drei Stunden ab Bekanntwerden des Widerrufsgrundes erfolgen. Alle widerrufenen Zertifikate werden im a-sign Informationsdienst in eigens dafür vorgesehen Widerrufslisten (CRLv2) veröffentlicht.

Der Signator haftet bei Verletzung seiner Sorgfaltspflichten selbst für alle Ansprüche, die in der Folge gegen Datakom Austria bzw. ihn selbst erhoben werden. Der Signator wird die Datakom Austria bei Inanspruchnahme durch Dritte schad- und klaglos halten.

e) Aufbewahrung des Zertifikatswerber-Vertrages
Der Kunde hat die ihm überreichte Ausfertigung des Zertifikatswerber-Vertrages sicher zu verwahren. Der Zertifikatswerber-Vertrag enthält alle für den telefonischen Widerruf des Zertifikates notwendigen Informationen. Bei nicht entsprechender Verwahrung kann der Widerruf des ausgestellten Zertifikate jederzeit durch unbefugte Dritte durchgeführt werden.

8) Sorgfaltspflichten des Empfängers eines elektronisch signierten Dokuments auf Basis des a-sign Zertifikates Premium

Grundsätzlich kann der Anwender (=Empfänger) einer elektronischen Signatur nicht zur sicheren Signaturprüfung verpflichtet werden (analog zur eigenhändigen Unterschrift). Der Empfänger hat diesbezüglich Wahlfreiheit. Das bedeutet, dass der Empfänger entscheiden kann, ob er die Signatur sicher verifizieren will oder ausschließlich eine Plausibilitätskontrolle vorzunehmen. Will der Empfänger die sichere Signaturprüfung vornehmen, so hat er jedenfalls ein vom Zertifizierungsdiensteanbieter Datakom empfohlenes Signaturprodukt (siehe dazu Punkt 2.2.) zu verwenden sowie die Gültigkeit des Zertifikates durch Überprüfung im Verzeichnis- oder Widerrufsdienst vorzunehmen. Liefert die Überprüfung ein positives Ergebnis (=Vorliegen der sicheren elektronischen Signatur) so entfaltet die vorliegende sichere elektronische Signatur die Rechtswirkungen der eigenhändigen Unterschrift im Sinne des § 886 ABGB (siehe dazu Punkt 2.1.) Hat der Empfänger jedoch die Prüfung unterlassen, und war das Zertifikat zum Zeitpunkt, als er das signierte Dokument erhalten hat, nicht mehr gültig, entfaltet das Dokument nicht die Rechtswirkungen des § 886 ABGB. Die Datakom ist in diesem Fall von jeglicher Haftung befreit.

9) Widerruf des a-sign Zertifikates durch den Zertifizierungsdiensteanbieter Datakom
Datakom ist berechtigt, bei Verdacht einer missbräuchlichen Verwendung des Zertifikats, bei Ableben des Signators oder einer sonstigen Änderung der im Zertifikat bescheinigten Umstände das Zertifikat zu widerrufen. Das Zertifikat kann auch dann widerrufen werden, wenn es auf Grund unrichtiger Angaben erwirkt wurde, wenn der Zertifizierungsanbieter seine Tätigkeit einstellt, auf Anordnung des Gerichts bzw. einer sonstigen Behörde oder sonstigen wichtigen Gründen. In diesen Fällen erfolgt kein wie immer gearteter Ersatz der Kosten des Zertifikates oder Schadenersatz.

10) Sicherheitswert elektronischer Signaturen
Die Parameter zur Erstellung einer sicheren elektronische Signatur, basierend auf dem a-sign Zertifikat Premium (Hashverfahren: SHA1; Verschlüsselungsalgorithmus RSA, 1024bit) entsprechen den Anforderungen des Österreichischen Signaturgesetzes und der auf dessen Grundlage ergangenen Verordnung und werden bis zum 31.12.2005 als sicher eingestuft (Signaturverordnung Anhang 1).

Elektronische Signaturen, die über den 31.12.2005 hinaus gültig und vor Manipulationen geschützt werden sollen (z.B. für Beweiswürdigung, Rechtsverbindlichkeit), müssen nachsigniert werden. Darunter versteht man das erneuerte Anbringen einer sicheren elektronischen Signatur vor Ablauf der oben angeführten Sicherheitsperiode (also vor dem 31.12.2005). Der Zeitpunkt des Nachsignierens muss mittels eines Zeitstempels dokumentiert werden. Das Nachsignieren ist daher nur bei gültigen sicheren elektronischen Signaturen zielführend. Eine gültige sichere elektronische Signatur liegt vor, wenn die Signatur auf Basis eines a-sign Zertifikates Premium erstellt und die Dokumentenvorgaben des Zertifizierungsdienstesanbieters eingehalten werden. Soll dem sicher elektronisch signierten Dokument nach dem 31.12.2005 dasselbe Sicherheitsniveau zugewiesen werden, muss es daher spätestens bis zum 31.12.2005 nachsigniert werden.

Das Nachsignieren eines sicher elektronisch signierten Dokumentes ist ein rein technischer Vorgang und muss nicht von einer bestimmten Person durchgeführt bzw. veranlasst werden. Das Nachsignieren kann somit auch von einer beliebig wählbaren vertrauenswürdigen Person vorgenommen werden. Veranlasst wird das Nachsignieren in der Regel von der Person, die an der Erhaltung des Sicherheitsniveaus der elektronischen Signatur interessiert ist. Wesentlich ist, dass der Sicherheitswert der sicheren elektronischen Signatur beibehalten wird und das Nachsignieren innerhalb der genannten Sicherheitsperiode durchgeführt wird.

11) Hinweis auf Streitbeilegungsverfahren
Unbeschadet der Zuständigkeit der ordentlichen Gerichte können Beschwerdefälle, die zuvor mit der Datakom nicht gelöst werden konnten, gem. § 15 (4) SigG der RTR vorgelegt werden.

12) Weitere rechtliche Informationen über digitale Zertifikate finden Sie unter folgender Web-Adresse: http://a-sign.datakom.at/content/hilfe_infos/recht_info/recht.html

13) Es gelten die AGB der Datakom Austria GmbH. Die AGB finden Sie unter folgender Web-Adresse: http://www.datakom.at/unternehmen/agb.shtml.

14) Die Policy Premium (Richtlinien bezüglich Zertifikaten der Klasse Premium) finden Sie unter folgender Web-Adresse: http://a-sign.datakom.at.

15) Das a-sign Sicherheits- und Zertifizierungskonzept finden Sie unter folgender Web-Adresse http://a-sign.datakom.at

16) Die Bestimmungen des Signaturgesetzes finden Sie unter: http://www.ris.bka.gv.at; http://a-sign.datakom.at)

17) Bei weiteren Fragen wenden Sie sich bitte an unseren Kundendienst:
e-mail: support@a-sign.datakom.at,
a-sign Hotline: 0800-501 555