

Sicherheits- und Zertifizierungskonzept
der
Trosoft Entwicklungs u. Vertriebs GmbH
für den Zertifizierungs- und Zeitstempeldienst
Trodat Seal

Version 2.1, 10. Oktober 2005

Dieses Sicherheits- und Zertifizierungskonzept richtet sich an Kunden des Dienstes „Trodat Seal“ (Signatoren) und Personen, welche die Echtheit der mit „Trodat Seal“ versiegelten Dokumente prüfen wollen. Es beschreibt die mit „Trodat Seal“ erzeugten Siegel und die Dienstleistung der Trosoft Entwicklungs u. Vertriebs GmbH im Zusammenhang mit „Trodat Seal“. In rechtlicher Hinsicht sind neben diesem Dokument auch die Lizenzbedingungen von „Trodat Seal“ und die Allgemeinen Geschäftsbedingungen der Trosoft Entwicklungs u. Vertriebs GmbH sowie allfällige Allgemeine Geschäftsbedingungen der gewählten Registrierungsstelle relevant.



Inhaltsverzeichnis

Änderungen gegenüber früheren Versionen.....	4
Änderungen zwischen Version 2.0 und Version 2.1	4
Änderungen zwischen Version 1.0 und Version 2.0	4
1. Einführung	6
1.1 Kontaktinformationen.....	6
1.2 Dokumentation	6
1.3 Unterstützte Datenformate.....	6
1.4 Zeitstempel	7
1.5 Genauigkeit der Zeitangabe	7
1.6 Beschränkungen der Anwendbarkeit des Zeitstempeldienstes	7
1.7 Verpflichtungen des Signators, der ein Siegel erstellt	8
1.8 Verpflichtungen der Personen, die Siegel prüfen	9
1.9 Informationen zur Prüfung eines Siegels.....	9
1.10 Dauer der Archivierung und der Prüfbarkeit der Siegel	9
1.11 Anwendbares Recht	10
1.12 Haftungsbeschränkungen.....	10
1.13 Beschwerden und Konfliktlösung.....	11
1.14 Konformitätserklärung	11
2. Schlüsselmanagement	12
2.1 Schlüsselerzeugung	12
2.2 Speicherung, Backup und Wiederherstellung privater Schlüssel.....	12
2.3 Veröffentlichung der öffentlichen Schlüssel.....	12
2.4 Schlüssel hinterlegung	12
2.5 Verwendung der Schlüssel.....	13
2.6 Schlüsselwechsel	13
2.7 Ende des Lebenszyklus eines Schlüsselpaars	13
2.8 Lebenszyklus der „Trodat Seal Server“	13
3. Signatur- und Zeitstempeldienst	14
3.1 Zeitstempel	14
3.2 Zeitsynchronisierung	14
3.3 Registrierung der Signatoren.....	15
3.4 Zuordnung der Siegel zu den Signatoren	17
3.5 Widerruf	19
3.6 Prüfung der Echtheit von Siegeln	20
4. Physikalische, organisatorische und personelle Sicherheitsmaßnahmen.....	24
4.1 Sicherheitsmanagement.....	24
4.2 Risikoanalyse	24
4.3 Personelle Sicherheit.....	24
4.4 Physikalische Sicherheit.....	26
4.5 Organisatorische Sicherheitsmaßnahmen.....	27
4.6 Zugriffsrechte und Schutz vor unbefugtem Zugriff.....	27
4.7 Vertrauenswürdige Systeme.....	28
4.8 Kompromittierung	29
4.9 Einstellung des Betriebs	29
4.10 Übereinstimmung mit rechtlichen Anforderungen.....	30
4.11 Dokumentation und Archivierung.....	30
5. Organisatorisches.....	34
6. Administration dieses Sicherheits- und Zertifizierungskonzepts	35



7. Glossar 36



Änderungen gegenüber früheren Versionen

Änderungen zwischen Version 2.0 und Version 2.1

Version 2.1 des Dienstes „Trodat Seal“ wurde gegenüber Version 2.0 nur in Details geändert:

Als Hashverfahren wird SHA-256 *und* SHA-1 verwendet.

Das Rechenzentrum verfügt über eine 24x7x365 Zugangskontrolle mit biometrischer Überprüfung, Löschgasanlagen, ausfallsichere Stromversorgung mit USV und Backup-Generatoren, redundante Klimakontroll- und Kühlsysteme und redundante GBit-Internetanbindungen an mehrere Carrier. In Version 2.1 ist gegenüber Version 2.0 der garantierte Schutz vor Naturkatastrophen wie Wassereinbruch und Erdbeben nicht mehr enthalten.

Der Absatz "Die Auslastung der Systeme, insbesondere der „Trodat Seal Server“ wird von einem Security Officer überwacht und zukünftige Kapazitätserweiterungen werden geplant, um entsprechende Rechenleistung und ausreichenden Speicherplatz gewährleisten zu können" wurde aus Punkt 4.5 (Organisatorische Sicherheitsmaßnahmen) gestrichen.

In Version 2.1 ist der Systemadministrator und nicht mehr das Personal des beauftragten Rechenzentrums für die laufenden Backups verantwortlich.

In Version 2.1 wird der öffentliche Schlüssel des Signators (wobei es sich um den Einmalschlüssel eines nur für dieses Siegel generierten Schlüsselpaares handelt) bei der Prüfung des Siegels nicht angezeigt (siehe Punkt 3.4).

Die Website der Trosoft GmbH wird in Zukunft unter der URL <http://seal.trodat.net> erreichbar sein. Die bisherige Adresse <http://www.trosoft.net> wird bis mindestens Ende 2005 weiter existieren.

Änderungen zwischen Version 1.0 und Version 2.0

Version 2.0 des Dienstes „Trodat Seal“ wurde gegenüber Version 1.0 grundlegend geändert. Bei der neuen Version 2.0 wird ein Zertifizierungs- und Zeitstempeldienst mit zwei verschiedenen Sicherheitsstufen (fortgeschrittene elektronische Signatur und einfache elektronische Signatur) angeboten, die jeweils in einer Online-Variante mit einem von Trosoft erstellten Zeitstempel und einer Offline-Variante ohne Zeitstempel betrieben werden können. In Version 1.0 wurde nur eine dieser Varianten (Erstellung einfacher elektronischer Signaturen mit Zeitstempel von Trosoft) angeboten.

Trosoft bietet nun die Dienstleistung an, die Identität der Signatoren zu überprüfen (siehe 3.3) und in den mit „Trodat Seal“ erzeugten Siegeln zu bescheinigen (siehe 3.4). Wenn die Identität des Signators geprüft wurde, liegt eine fortgeschrittene



elektronische Signatur im Sinne der EU-Signaturrechtlinie vor, die insbesondere auch für die Signatur elektronischer Rechnungen eingesetzt werden kann.

Die Identität des Signators und die Sicherheitsstufe wird jeweils bei der Prüfung der Echtheit von Siegeln durch einen „Trodat Seal Server“ ausgewiesen (siehe 3.6). Dabei wird jeweils auch angegeben, ob es sich um eine fortgeschrittene elektronische Signatur oder eine einfache elektronische Signatur handelt und ob das Siegel von Trosoft mit einem Zeitstempel versehen wurde.

In der nun angebotenen Version 2.0 sichert Trosoft eine höhere Zuverlässigkeit des Zeitstempeldienstes (siehe 3.1 und 3.2) als in Version 1.0 zu, erhebt aber noch nicht den Anspruch, alle Anforderungen an sogenannte „sichere Zeitstempeldienste“ (§ 10 Satz 2 SigG) zu erfüllen.



1. Einführung

1.1 Kontaktinformationen

Der Dienst „Trodat Seal“ wird erbracht von der

Trosoft Entwicklungs u. Vertriebs GmbH
Linzer Straße 156
A-4600 Wels

Weitere Informationen zum Unternehmen und Informationen über die jeweiligen Möglichkeiten der Kontaktaufnahme mittels Telefon, Fax und E-Mail werden auf der Website <http://www.trosoft.net/> veröffentlicht.

1.2 Dokumentation

Die verschiedenen Fassungen dieses Sicherheits- und Zertifizierungskonzepts werden auf der Website <http://www.trosoft.net/> veröffentlicht. Dort ist jeweils auch ersichtlich, in welchem Zeitraum welche Fassung des Sicherheits- und Zertifizierungskonzepts zur Anwendung kam.

Bei der Überprüfung eines mit „Trodat Seal“ erzeugten Siegels (siehe 3.6) wird die Echtheit des Dokumentes und die jeweilige Sicherheitsstufe entsprechend dem zum Zeitpunkt der Erstellung des Siegels gültigen Sicherheits- und Zertifizierungskonzept geprüft und angezeigt.

1.3 Unterstützte Datenformate

Mit „Trodat Seal“ können ausschließlich Dokumente im Datenformat PDF versiegelt werden. PDF (Adobe Portable Document Format) wurde von Adobe Systems Incorporated spezifiziert. Die Spezifikation des Formates („PDF Reference“) ist allgemein verfügbar. „Trodat Seal“ unterstützt PDF ab Version 1.3 bis zur aktuellen Version 1.6 (spezifiziert in der PDF Reference, Second Edition bis Fifth Edition, vgl. http://partners.adobe.com/public/developer/pdf/index_reference.html).

Für die Erstellung der Siegel stellt Trosoft den Signatoren die Software „Trodat Seal for Windows“ zur Verfügung. Diese Software stellt (soweit erforderlich) die Verbindung zu dem von Trosoft betriebenen Zeitstempeldienst her und bringt das Siegel am PDF-Dokument an.

Ein mit „Trodat Seal“ erzeugtes Siegel enthält jedenfalls ein vom Signator wählbares Siegellogo, eine Sicherheitsgrafik (zweidimensionaler Barcode) und einen Prüf-Link („Click to Verify“). Optional wird im Siegel auch der Name des Signators und der Zeitpunkt der Versiegelung sichtbar dargestellt. (Bei der in 3.6 beschriebenen Prüfung der Echtheit des Siegels wird angegeben, ob die Identität des Signators von Trosoft geprüft wurde und ob die angegebene Zeitangabe durch den Zeitstempeldienst von Trosoft bestätigt wurde.) Weiters kann das Siegel optional auch eine biometrisch erfasste Unterschrift des Signators oder einer anderen Person enthalten, welche unabhängig von den anderen Sicherheitsfunktionen von „Trodat Seal“ als zusätzliches Beweismittel verwendet werden kann (siehe 3.6). Das Siegel



wird im PDF-Dokument so angebracht, dass es sowohl in elektronischer Form als auch beim Ausdruck des Dokuments sichtbar ist.

Die Sicherheitsgrafik enthält in einem von Trosoft entwickelten Datenformat unter anderem den Hashwert des Dokuments, den Zeitpunkt der Versiegelung und die verschlüsselte Accountkennung (Lizenznummer) des Signators. Optional kann die Sicherheitsgrafik auch charakteristische Daten des Dokuments (z. B. den Betreff eines Protokolls oder die Rechnungsnummer) enthalten. Da die Daten in der Sicherheitsgrafik teilweise verschlüsselt sind, ist zur Prüfung der Echtheit des Siegels eine Verbindung zu einem „Trodat Seal Server“ erforderlich, welcher die Daten entschlüsseln kann.

1.4 Zeitstempel

Wird „Trodat Seal“ in der Online-Variante betrieben, dann enthält das erzeugte Siegel auch die elektronische Signatur der Trosoft Entwicklungs u. Vertriebs GmbH, die von einem der von Trosoft betriebenen „Trodat Seal Server“ erzeugt wird. Diese Signatur umfasst den Inhalt des PDF-Dokumentes samt dem Siegel-Logo und den optionalen Angaben zum Signator und verknüpft somit den Inhalt des Dokumentes untrennbar mit dem Siegel. Die Signatur des „Trodat Seal Server“ umfasst auch den Zeitpunkt der Versiegelung und bringt somit einen Zeitstempel am Dokument an. Mit dem Siegel bescheinigt Trosoft daher, dass das versiegelte Dokument zum genannten Zeitpunkt in dieser Form vorgelegen ist. Spätere Änderungen des Dokumentes werden bei der Prüfung der Echtheit des Siegels erkannt.

Als Hashverfahren wird SHA-256 verwendet. Als Signaturverfahren wird RSA mit einer Schlüssellänge von mindestens 1024 Bit verwendet.

1.5 Genauigkeit der Zeitangabe

Trosoft gewährleistet eine Genauigkeit von maximal einer Minute (60 Sekunden) Abweichung zur tatsächlichen Zeit.

Die von den „Trodat Seal Servern“ verwendete Zeitangabe entspricht der Coordinated Universal Time (UTC). Diese Zeitzone wird in Siegeln und Prüfzertifikaten der Siegel auch jeweils ersichtlich gemacht.

Die getroffenen Maßnahmen zur Sicherstellung der Genauigkeit der Zeitangabe werden unter Punkt 3.2 beschrieben.

1.6 Beschränkungen der Anwendbarkeit des Zeitstempeldienstes

Der Zertifizierungs- und Zeitstempeldienst „Trodat Seal“ unterliegt in der derzeit angebotenen Form folgenden Beschränkungen:

- a) Als Datenformat wird ausschließlich PDF in den Versionen 1.3 bis 1.6 unterstützt.
- b) Zur Erstellung der Siegel kann ausschließlich die von Trosoft angebotene Software „Trodat Seal for Windows“ verwendet werden.



c) Zur Überprüfung der Echtheit der Siegel ist ein Verbindungsaufbau zu einem der von Trosoft betriebenen „Trodat Seal Server“ erforderlich.

d) Obwohl die „Trodat Seal Server“ von Trosoft grundsätzlich rund um die Uhr verfügbar sind und Trosoft den Dienst langfristig über mindestens sieben Jahre (siehe 1.10) betreiben wird, gewährleistet Trosoft bei der derzeit angebotenen Form des Dienstes keine bestimmte zeitliche Verfügbarkeit. Trosoft wird sich bemühen, Unterbrechungen des Dienstes so kurz wie möglich zu halten und Wartungsarbeiten zu Tageszeiten vorzunehmen, in denen der Dienst wenig genutzt wird.

1.7 Verpflichtungen des Signators, der ein Siegel erstellt

Um mit „Trodat Seal“ Siegel erstellen zu können, ist der Kauf einer Lizenz erforderlich. Lizenzen sind unter anderem im Webshop <http://www.trosoft.net/> oder bei Vertriebspartnern erhältlich. Signatoren erhalten von Trosoft die für die Erstellung der Siegel erforderliche Software „Trodat Seal for Windows“. Für das Rechtsverhältnis zwischen dem Signator und Trosoft gelten neben diesem Sicherheits- und Zertifizierungskonzept die Lizenzbedingungen und die auf der Website <http://www.trosoft.net/> veröffentlichten Allgemeinen Geschäftsbedingungen von Trosoft sowie allfällige Allgemeine Geschäftsbedingungen der gewählten Registrierungsstelle.

Die Signatoren sind verpflichtet, die Siegel ausschließlich mit der Software „Trodat Seal for Windows“ zu erzeugen.

Alle mit „Trodat Seal“ erzeugten Siegel sind über die im Siegel in verschlüsselter Form gespeicherte Accountkennung (Lizenznummer) einem bestimmten Signator zugeordnet. Um eine missbräuchliche Erstellung von Siegeln durch andere Personen als den Signator auszuschließen, muss der Signator vor der Erstellung eines Siegels entweder sein Windows-Passwort eingeben (wenn seine Identität noch nicht geprüft wurde und eine einfache Signatur erstellt wird) oder er muss sich mit einem persönlichen PIN-Code identifizieren (wenn seine Identität bereits geprüft wurde und er eine fortgeschrittene Signatur erstellt). Die Signatoren sind verpflichtet, die Lizenznummer und das Passwort bzw. den PIN-Code sorgfältig zu verwahren, unbefugte Zugriffe darauf zu verhindern und die Weitergabe zu unterlassen. Weiters sind die Signatoren verpflichtet, einen Widerruf (siehe 3.5) zu veranlassen, wenn Anhaltspunkte für eine Kompromittierung (z. B. einen Zugriff eines Unbefugten auf Passwort oder PIN-Code) bestehen.

Trosoft sieht optional vor, dass Signatoren ihre Identität anhand eines amtlichen Lichtbildausweises überprüfen lassen können (siehe 3.3). Der Signator ist verpflichtet, bei der Registrierung wahre Angaben insbesondere über seine Identität zu machen und die in 3.3 genannten Unterlagen (insbesondere einen amtlichen Lichtbildausweis) vorzulegen. Im Zuge dieser Registrierung wählt der Signator auch einen persönlichen PIN-Code. Die nach einer solchen Registrierung erstellten Siegel sind fortgeschrittene elektronische Signaturen im Sinne der EU-Signaturrechtlinie und beispielsweise für die Erstellung elektronischer Rechnungen geeignet. Ob es sich bei einem mit „Trodat Seal“ erzeugten Siegel um eine fortgeschrittene elektronische Signatur handelt, wird bei der Prüfung des Siegels (siehe 3.6) dargestellt. Die Signatoren sind verpflichtet, bei Änderungen ihres Namens einen Widerruf (siehe



3.5) zu veranlassen. Für den neuen Namen kann ein neuer Account angelegt werden, bei dem nach neuerlicher Registrierung (siehe 3.3) wiederum fortgeschrittene elektronische Signaturen erstellt werden können. Bei der Registrierung kann optional auch die Zugehörigkeit des Signators zu einer juristischen Person überprüft werden. In diesem Fall sind sowohl der Signator als auch die juristische Person verpflichtet, einen Widerruf zu veranlassen, wenn diese Zugehörigkeit nicht mehr besteht.

„Trodat Seal“ kann auch in einer massensignaturfähigen Variante genutzt werden, d. h. dass der Signator seinen persönlichen PIN-Code nicht vor der Erstellung jedes einzelnen Siegels eingeben muss. Damit ist z. B. die automatisierte Massensignatur von elektronischen Rechnungen möglich. Ein Signator, der „Trodat Seal“ in dieser Variante nutzt, ist verpflichtet, durch angemessene technische und organisatorische Maßnahmen sicherzustellen, dass er die alleinige Kontrolle über den persönlichen PIN-Code ausübt.

1.8 Verpflichtungen der Personen, die Siegel prüfen

Die Echtheit eines mit „Trodat Seal“ erzeugten Siegel kann nur mit den unter 3.6 beschriebenen Methoden von einem „Trodat Seal Server“ überprüft werden. Trosoft übernimmt keine Haftung für Siegel, deren Echtheit nicht von einem „Trodat Seal Server“ überprüft wurde.

1.9 Informationen zur Prüfung eines Siegels

Zur Überprüfung der Echtheit eines Siegels bietet Trosoft verschiedene Methoden an, die laufend weiterentwickelt werden. Gemeinsam ist diesen Methoden, dass eine Verbindung zu einem „Trodat Seal Server“ aufgebaut wird. Der „Trodat Seal Server“ gibt dann ein signiertes Prüfzertifikat aus, welches vom Prüfenden zur weiteren Verwendung abgespeichert werden kann. Das Prüfzertifikat enthält unter anderem Angaben zur Identität des Signators und es informiert darüber, ob eine Identitätsprüfung vorgenommen wurde und somit eine fortgeschrittene elektronische Signatur vorliegt und ob der Zeitpunkt der Erzeugung des Siegels durch einen Zeitstempel von Trosoft bestätigt wurde. In 3.6 sind die verschiedenen Methoden der Prüfung und die Inhalte des Prüfzertifikates näher beschrieben.

1.10 Dauer der Archivierung und der Prüfbarkeit der Siegel

Welche Daten Trosoft wie lange archiviert, ist in 4.11 beschrieben.

Jedes mit Trodat Seal erstellte Siegel kann auf Grund der archivierten Informationen über einen Zeitraum von mindestens sieben Jahren überprüft werden. Auch im Fall der Einstellung des Dienstes „Trodat Seal“ werden die „Trodat Seal Server“ noch für einen Zeitraum von mindestens sieben Jahren betrieben werden, um die Prüfbarkeit der Siegel zu gewährleisten.



1.11 Anwendbares Recht

Die Trosoft Entwicklungs u. Vertriebs GmbH hat ihren Sitz in Österreich. Die Erbringung des Dienstes „Trodat Seal“ unterliegt dem österreichischen Signaturgesetz, welches der europäischen Signaturrechtlinie 1999/93/EG entspricht.

Auf die Rechtsverhältnisse zwischen der Trosoft Entwicklungs u. Vertriebs GmbH, den Signatoren und den Personen, welche die Echtheit eines mit „Trodat Seal“ erzeugten Siegels prüfen, ist österreichisches Recht anzuwenden und sie unterliegen der österreichischen Gerichtsbarkeit (Gerichtsstand ist Wels), soweit dem keine zwingenden rechtlichen Bestimmungen (z. B. § 14 KSchG) entgegenstehen.

1.12 Haftungsbeschränkungen

In der derzeit angebotenen Form des Dienstes „Trodat Seal“ ist die Haftung folgendermaßen beschränkt:

Die Echtheit des Siegels muss entsprechend der in 3.6 beschriebenen Methode überprüft werden. Trosoft übernimmt keine Haftung für Dokumente, welche nicht in dieser Form geprüft wurden, auch wenn sie den oberflächlichen Eindruck erwecken, sie würden ein mit „Trodat Seal“ erzeugtes Siegel enthalten. Wenn die Echtheit des Siegels nicht erfolgreich überprüft werden kann, dann wurde das Dokument entweder nicht mit „Trodat Seal“ versiegelt oder es wurde seit der Versiegelung verändert.

Ob die Identität des Signators anhand eines amtlichen Lichtbildausweises geprüft wurde, wird bei der in 3.6 beschriebenen Prüfung der Siegel ausgegeben. Wenn ein Siegel mit einer Lizenz erzeugt wurde, bei der keine Identitätsprüfung vorgenommen wurde, kann das Dokument nicht in zuverlässiger Weise einem bestimmten Signator zugeordnet werden. Trosoft haftet nur bei solchen Siegeln für die Feststellbarkeit der Identität des Signators, bei denen bei der Prüfung des Siegels angezeigt wird, dass eine Identitätsprüfung vorgenommen wurde.

„Trodat Seal“ bestätigt nicht die Richtigkeit des Inhalts eines bestimmten Dokumentes, sondern nur, dass es einem bestimmten Signator zugeordnet werden kann (wenn eine Identitätsprüfung vorgenommen wurde) bzw. dass es zu einem bestimmten Zeitpunkt einen bestimmten Inhalt hatte (wenn es mit einem Zeitstempel versehen wurde). Aus dem Inhalt des Dokumentes können daher keine Ansprüche an Trosoft abgeleitet werden. Für den Inhalt des Dokumentes ist der Signator verantwortlich.

Es ist unüblich, aber möglich, dass PDF-Dokumente dynamische Elemente enthalten, die z. B. zu unterschiedlichen Zeitpunkten unterschiedlich dargestellt werden. In der derzeit angebotenen Form des Dienstes verhindert „Trodat Seal“ nicht, dass der Ersteller eines PDF-Dokumentes solche dynamischen Elemente verwendet. Das Siegel verhindert aber, dass der binäre Inhalt der PDF-Datei unerkannt geändert wird; im Streitfall wäre eine allfällige Manipulation durch den Ersteller des Dokumentes daher beweisbar. Wird das PDF-Dokument mit dem Trodat Seal Printer erzeugt (mit dem aus beliebigen Windows-Anwendungen



versiegelte PDF-Dokumente erzeugt werden können), dann enthält das versiegelte Dokument keine dynamischen Elemente.

Mit Trodat Seal versiegelte Dokumente sind für einen Transaktionswert bis zu 2500 Euro bestimmt. Höhere Transaktionslimits können mit dem Signator vereinbart werden und werden in diesem Fall als Teil des Prüfzertifikates (siehe 3.6) ausgegeben. Trosoft haftet keinesfalls für Schäden, die sich aus einer Überschreitung des Transaktionslimits ergeben könnten. Weiters schließt Trosoft die Haftung für leichte Fahrlässigkeit (ausgenommen Personenschäden) aus.

1.13 Beschwerden und Konfliktlösung

Trosoft wird sich bemühen, Probleme und Beschwerden zur Zufriedenheit seiner Kunden zu lösen. Auf der Website <http://www.trosoft.net/> werden Supportinformationen, Softwareupdates und Kontaktmöglichkeiten veröffentlicht.

Gemäß § 15 Abs. 4 SigG können Kunden und Interessenvertretungen Streit- oder Beschwerdefälle, die mit Trosoft nicht befriedigend gelöst worden sind, (unbeschadet der Zuständigkeit der ordentlichen Gerichte) der Rundfunk und Telekom Regulierungs-GmbH (<http://www.rtr.at/>) zur Streitschlichtung vorlegen. Gemäß dieser gesetzlichen Bestimmung hat sich die RTR-GmbH zu bemühen, innerhalb angemessener Frist eine einvernehmliche Lösung herbeizuführen. Trosoft ist verpflichtet, entsprechend den von der RTR-GmbH erlassenen Verfahrensrichtlinien für die Streitschlichtung am Streitschlichtungsverfahren mitzuwirken.

1.14 Konformitätserklärung

Der Dienst „Trodat Seal“ kombiniert Funktionen eines Zeitstempeldienstes (Bescheinigung dass ein bestimmtes Dokument zu einem bestimmten Zeitpunkt vorgelegen ist) mit Funktionen eines Signatur- und Zertifizierungsdienstes (Zuordnung von Dokumenten zu bestimmten Signatoren).

Dieses Sicherheits- und Zertifizierungskonzept wurde daher entsprechend den Anforderungen und der Gliederung der Standards ETSI TS 102 023 V 1.2.1 (2003-01) „Policy requirements for time-stamping authorities“ (= RFC 3628) und ETSI TS 102 042 V 1.1.1 (2002-04) „Policy requirements for certification authorities issuing public key certificates“ erstellt. Auf Grund der besonderen Konstruktion von „Trodat Seal“ kann Trosoft für den Dienst „Trodat Seal“ aber nicht behaupten, dass alle in diesen Standards genannten Anforderungen erfüllt werden.

Trosoft unterliegt der laufenden Aufsicht der Telekom-Control-Kommission als österreichischer Aufsichtsstelle für elektronische Signaturen. Diese Aufsicht bezieht sich gemäß § 13 Abs.2 Z 1 SigG insbesondere darauf, dass Trosoft alle Zusicherungen dieses Sicherheits- und Zertifizierungskonzepts umsetzt.



2. Schlüsselmanagement

2.1 Schlüsselerzeugung

Die vom Trodat Seal Server für die Signatur von Siegeln und von Ergebnissen der Überprüfung von Siegeln verwendeten Schlüssel werden in kontrollierter Umgebung erzeugt.

Die Schlüssel werden in einer physikalisch gesicherten Umgebung (vgl. 4.4) erzeugt. An der Schlüsselerzeugung müssen zur Wahrung des Vier-Augen-Prinzips zwei Personen beteiligt sein, welche von der Geschäftsführung der Trosoft mit den Aufgaben eines „Security Officer“ betraut wurden (vgl. 4.3). Mit diesen Aufgaben wird nur eine begrenzte Anzahl vertrauenswürdiger und technisch kompetenter Personen betraut.

Die privaten Schlüssel werden auf dem „Trodat Seal Server“ in verschlüsselter Form gespeichert und durch dem Stand der Technik entsprechende Sicherheitsmaßnahmen gegen unbefugten Zugriff geschützt. Ein Hardware Security Modul wird derzeit nicht eingesetzt.

Als Algorithmus wird RSA verwendet, als Schlüssellänge mindestens 1024 Bit.

2.2 Speicherung, Backup und Wiederherstellung privater Schlüssel

Die privaten Schlüssel werden in verschlüsselter Form gespeichert und durch dem Stand der Technik entsprechende Sicherheitsmaßnahmen gegen unbefugten Zugriff geschützt. Ein Hardware Security Modul wird derzeit nicht eingesetzt.

Von den privaten Schlüsseln werden unter Wahrung des Vier-Augen-Prinzips von zwei Personen, welche von der Geschäftsführung der Trosoft mit den Aufgaben eines „Security Officer“ betraut wurden (vgl. 4.3) zwei Backups erstellt, die jeweils auf Diskette gespeichert und in einem versiegelten Kuvert aufbewahrt werden. Ein Backup wird in einem Safe in den Räumlichkeiten von Trosoft versperrt, welcher nur von einem Geschäftsführer und zwei Security Officers gemeinsam geöffnet werden darf. Das andere Backup wird bei einem Notar hinterlegt und darf nur einem Geschäftsführer und zwei Security Officers gemeinsam ausgefolgt werden.

2.3 Veröffentlichung der öffentlichen Schlüssel

Für den öffentlichen Schlüssel jedes „Trodat Seal Server“ werden X.509-Zertifikate ausgestellt, wobei Trosoft entweder ein selbst signiertes Zertifikat ausstellt oder bei einem anderen Zertifizierungsdiensteanbieter ein Serverzertifikat ausstellen lässt. Die Zertifikate der einzelnen „Trodat Seal Server“ werden auf der Website veröffentlicht.

2.4 Schlüsselhinterlegung

Bei Trosoft werden keine privaten kryptographischen Schlüssel der Signatoren hinterlegt.



2.5 Verwendung der Schlüssel

Die in diesem Kapitel 2 beschriebenen kryptographischen Schlüssel von Trosoft werden ausschließlich in der beschriebenen Weise für den Dienst „Trodat Seal“ verwendet.

Die Schlüssel werden ausschließlich in gesicherter Umgebung verwendet.

2.6 Schlüsselwechsel

Die für „Trodat Seal“ eingesetzten Schlüssel können jederzeit gewechselt werden. Jedenfalls wechselt Trosoft die Schlüssel, wenn der verwendete Algorithmus oder die verwendete Schlüssellänge nach österreichischem Recht nicht mehr als ausreichend sicher im Sinne des §3 Abs.2 bzw. des Anhangs der Signaturverordnung angesehen werden.

2.7 Ende des Lebenszyklus eines Schlüsselpaars

Trosoft stellt sicher, dass die privaten Schlüssel nach dem Ende ihres Lebenszyklus nicht mehr verwendet werden.

Läuft das Zertifikat eines „Trodat Seal Server“ ab oder ist ein Schlüssel entsprechend 2.6 zu wechseln, dann wird entsprechend 2.1 ein neues Schlüsselpaar erzeugt und eine neue Instanz des „Trodat Seal Server“ in Betrieb genommen.

Da der private Schlüssel aufgrund der eingesetzten Technik auch zur Prüfung der (teilweise verschlüsselten) Siegel benötigt wird, wird er nicht zerstört, sondern für sieben Jahre weiter aufbewahrt. Sieben Jahre nachdem ein Schlüsselpaar außer Betrieb genommen wurde, werden der private Schlüssel und seine Backups zerstört.

Durch entsprechende Konfiguration der Software des „Trodat Seal Server“ wird gewährleistet, dass der Schlüssel nicht mehr zur Erstellung von Siegeln, sondern nur zur Prüfung der verschlüsselten Inhalte der Siegel verwendet wird.

2.8 Lebenszyklus der „Trodat Seal Server“

Die „Trodat Seal Server“ sind keine Hardware Security Module.

Ein „Trodat Seal Server“ wird während der gesamten Lebensdauer unter der Kontrolle von Trosoft betrieben. Der Server wird durch dem Stand der Technik entsprechende Maßnahmen (siehe Kapitel 4) gegen unbefugten Zugriff geschützt. Die Schlüsselpaare werden unter Beachtung des Vier-Augen-Prinzips erzeugt. Wird ein „Trodat Seal Server“ oder werden Hardwareteile (insbesondere Festplatten) außer Betrieb genommen, dann wird sichergestellt, dass sich darauf keine Schlüssel mehr befinden.



3. Signatur- und Zeitstempeldienst

3.1 Zeitstempel

„Trodat Seal“ kann in einer Online-Variante und einer Offline-Variante betrieben werden. Wird es in der Online-Variante betrieben, dann wird bei der Erstellung eines Siegels eine Verbindung zu einem „Trodat Seal Server“ aufgebaut. Dieser versieht das Siegel mit einem Zeitstempel.

Die in den Siegeln angegebene Zeit wird von Trosoft mit einer Abweichung von maximal 60 Sekunden mit der Coordinated Universal Time UTC synchronisiert. Im Datenformat des Siegels wird die Zeitangabe als UTC ausgewiesen. Im sichtbar dargestellten Teil des Siegels und in den Prüfzertifikaten wird die Zeitzone UTC neben den Zeitangaben ausgewiesen.

Wenn Trosoft feststellt, dass die interne Uhr eines „Trodat Seal Server“ mehr als 60 Sekunden von UTC abweicht oder wenn die Synchronisierung mit den verwendeten Zeitservern so lange ausfällt, dass die Genauigkeit von 60 Sekunden nicht mehr gewährleistet werden kann, dann werden von diesem „Trodat Seal Server“ keine Siegel erstellt, bis die Störung behoben wurde (siehe 3.2).

Jedes Siegel wird von einem „Trodat Seal Server“ mit einem Schlüssel signiert, der ausschließlich für „Trodat Seal“ eingesetzt wird (siehe 2.2)

Das Datenformat des Siegels wurde von Trosoft spezifiziert. Es entspricht nicht dem in RFC 3161 spezifizierten Format, enthält aber Angaben, die auch in RFC 3161 vorgesehen sind, unter anderem eine eindeutige Kennzeichnung jedes erzeugten Zeitstempels, die Zeitangabe (in UTC), einen Hashwert des zeitgestempelten Inhalts des Dokuments und eine Identifikation des Servers, der das Siegel erstellt hat. Weiters ist das Zertifikat des „Trodat Seal Server“ Teil des Siegels. Aus dem Zertifikat geht unter anderem der Name des Zertifizierungsdiensteanbieters und der Sitz seiner Niederlassung hervor.

3.2 Zeitsynchronisierung

Trosoft stellt sicher, dass die interne Uhr der „Trodat Seal Server“ nicht mehr als 60 Sekunden von der Coordinated Universal Time UTC abweicht.

Bei der Auswahl der Hardware der „Trodat Seal Server“ wird darauf geachtet, dass diese über eine interne Uhr verfügen, die nicht mehr als eine Sekunde pro Tag abweicht.

Die „Trodat Seal Server“ werden mit dem Simple Network Time Protocol (SNTP) mit im Internet verfügbaren Zeitservern koordiniert. Zur Sicherstellung der Genauigkeit der Zeitangaben werden die in (S)NTP vorgesehenen Prüfmechanismen verwendet. Bei der Auswahl der Zeitserver, mit denen Trosoft die Uhren der „Trodat Seal Server“ synchronisiert, wird darauf geachtet, dass die Zeit jedes Zeitserverns direkt oder indirekt von zumindest einem der UTC(k) laboratories des Bureau International des Poids et Mesures (BIPM) abgeleitet ist.



Durch die in Kapitel 4 beschriebenen organisatorischen und technischen Sicherheitsmaßnahmen werden die „Trodat Seal Server“ unter anderem auch gegen Angriffe geschützt, welche die Genauigkeit der Zeitangaben beeinträchtigen würden.

Fehlermeldungen der „Trodat Seal Server“, insbesondere betreffend die Synchronisierung der internen Uhr mit den Zeitservern, einen Ausfall der Synchronisierung oder unplausible Zeitsprünge werden von den Systemadministratoren laufend überwacht und entsprechend behandelt. Wenn nicht mehr sichergestellt werden kann, dass die gewährleistete Genauigkeit eingehalten wird, wird der betreffende „Trodat Seal Server“ abgeschaltet. Wenn der Verdacht besteht, dass ein „Trodat Seal Server“ kompromittiert wurde und Siegel erstellt hat, deren Zeit um mehr als 60 Sekunden von der tatsächlichen Zeit abweicht, wird eine entsprechende Information veröffentlicht (siehe 4.8).

Die von Trosoft verwendeten Systeme und Programme können die Einfügung oder Streichung von Schaltsekunden berücksichtigen. Diese Ereignisse werden aber nicht protokolliert, da Trosoft nur eine maximale Abweichung von 60 Sekunden zur tatsächlichen Zeit zusichert.

3.3 Registrierung der Signatoren

Jedes mit „Trodat Seal“ erzeugte Siegel enthält eine Zuordnung zum Account (Lizenznummer) eines Signators. Ein Signator ist eine natürliche Person, d. h. jedes „Trodat Seal“ ist einer natürlichen Person zuordenbar. Trosoft nimmt nicht in allen Fällen eine Identitätsprüfung anhand eines amtlichen Lichtbildausweises vor. In jenen Fällen, in denen eine Identitätsprüfung vorgenommen wird, sind die mit „Trodat Seal“ erzeugten Siegel fortgeschrittene elektronische Signaturen im Sinne der EU-Signaturrichtlinie. Ob eine Identitätsprüfung vorgenommen wurde, wird bei der Prüfung der Siegel (siehe 3.6) ersichtlich gemacht.

Beim Erwerb einer Lizenz im Webshop oder über einen Vertriebspartner erhält der Kunde für jede erworbene Lizenz einen Registrierungscode. Der Registrierungscode wird entweder per E-Mail an die angegebene E-Mail-Adresse übersandt oder vom Vertriebspartner in einem verschlossenen Kuvert übergeben. Mit dem Registrierungscode kann vom Signator über die Software „Trodat Seal for Windows“ ein persönlicher Account auf den „Trodat Seal Servern“ angelegt werden. Der Signator hat auch die Möglichkeit, seinen Registrierungscode auf mehreren verschiedenen Rechnern, auf denen die Software „Trodat Seal for Windows“ installiert ist, zu nutzen, um auf jedem dieser Rechner Siegel erstellen zu können. Der Registrierungscode muss dabei jeweils nur bei der ersten Benutzung der Software durch den jeweiligen Signator eingegeben werden. Die Software kann mehrere verschiedene Accounts verwalten, sodass mehrere Signatoren den selben Rechner verwenden können oder ein Signator mehrere verschiedene Accounts verwenden kann.

Beim erstmaligen Anlegen des Accounts werden zwar Daten zur Identität des Signators erfasst, es wird aber zunächst keine Identitätsprüfung vorgenommen. Will der Signator fortgeschrittene elektronische Signaturen erstellen, dann muss er sich bei Trosoft oder einer Registrierungsstelle registrieren und dabei seine Identität überprüfen lassen. An welche Registrierungsstelle sich der Signator dazu wenden



soll, kann er, wenn bereits ein Account angelegt ist, über die Shopfinder-Funktion im Webshop feststellen. Dort sind auch die Kontaktdaten, Entgelte und AGB der Registrierungsstelle abrufbar, sowie Informationen, welche Lichtbildausweise die Registrierungsstelle akzeptiert, in welchen Sprachen die Registrierung angeboten wird und ob die Registrierungsstelle auch die Möglichkeit anbietet, die Zugehörigkeit eines Signators zu einer juristischen Person zu überprüfen. Ein Signator, der noch keine Lizenz für „Trodat Seal“ erworben und noch keinen Account angelegt hat, kann sich auch direkt an eine Registrierungsstelle von Trosoft wenden und dort gleichzeitig die Lizenz (samt einem im verschlossenen Kuvert übergebenen Registrierungscode) erwerben und eine Identitätsprüfung vornehmen zu lassen.

Für die im Zuge der Registrierung durchgeführte Identitätsprüfung werden die folgenden Möglichkeiten angeboten:

1. persönliche Identitätsprüfung bei Trosoft oder einer Registrierungsstelle von Trosoft: Dazu ist das persönliche Erscheinen des Signators erforderlich. Der Signator muss sich mit einem amtlichen Lichtbildausweis ausweisen. Welche Arten von Lichtbildausweisen akzeptiert werden, wird von Trosoft festgelegt und von Trosoft bzw. den Registrierungsstellen veröffentlicht. Das Registrierungspersonal überprüft die Übereinstimmung des Lichtbilds mit dem Gesicht des Signators.

2. Übermittlung eines amtlichen Lichtbildausweises mittels Fax und Kontrollanruf: Das Registrierungspersonal von Trosoft oder einer Registrierungsstelle von Trosoft prüft die Lesbarkeit des übermittelten Dokumentes und fordert bei schlechter Lesbarkeit ein neues Fax oder eine per Brief übersandte Kopie an. Wenn das Dokument lesbar vorliegt, überprüft das Registrierungspersonal durch einen Kontrollanruf beim Signator, dass die Unterlagen von ihm stammen.

Im Zuge der Registrierung muss der Signator auch eine Erklärung übergeben, mit der er sich zur Einhaltung der in 1.7 genannten Sicherheitsmaßnahmen verpflichtet.

Für jeden Signator werden bei der Registrierung die folgenden Daten erfasst: Name (Nachname und Vorname(n) in der Schreibweise des vorgelegten Lichtbildausweises.), Datum und Ort der Geburt, postalische Adresse, E-Mail-Adresse. Vom vorgelegten Lichtbildausweis werden die Art des Ausweises, das Datum der Ausstellung, die Nummer des Ausweises und die ausstellende Behörde erfasst.

Optional kann der Signator bei der Registrierung auch ein Pseudonym wählen. Das Pseudonym kann frei gewählt werden, darf aber weder anstößig noch offensichtlich zur Verwechslung mit Namen oder Kennzeichen geeignet sein. Wählt der Signator ein Pseudonym, dann wird die Identität des Signators bei der Prüfung der Echtheit von Siegeln (3.6) nicht offengelegt. Trosoft legt die Identität aber auf Anfrage eines Gerichts oder einer Behörde offen oder gegenüber Personen, die ein rechtliches Interesse an der Offenlegung glaubhaft machen.

Wenn zusätzlich zur Identität des Signators auch dessen Zugehörigkeit zu einer juristischen Person erfasst werden soll, müssen vom Signator zusätzlich die folgenden Unterlagen vorgelegt werden: Kopie eines Registerauszugs, mit dem die juristische Person amtlich registriert wurde und aus dem organisatorisch



verantwortliche Personen hervorgehen (z. B. Auszug aus dem Firmenbuch, dem Vereinsregister oder dem Gewerbeverzeichnis), Kopie des amtlichen Lichtbildausweises einer in diesem Auszug genannten organisatorisch verantwortlichen Person (z. B. Geschäftsführer, Prokurist, Vereinsobmann, gewerberechtlicher Geschäftsführer, ...) sowie eine von dieser organisatorisch verantwortlichen Person unterschriebene Erklärung, dass der Signator berechtigt ist, für die genannte juristische Person mit „Trodat Seal“ Siegel zu erstellen. Bei der Prüfung der Echtheit von Siegeln (siehe 3.6) wird die juristische Person und die Zugehörigkeit des Signators zur juristischen Person angegeben.

Nach der Identitätsprüfung kann der Signator in seiner Software „Trodat Seal for Windows“ einen persönlichen PIN-Code auswählen, den er in weiterer Folge zur Erstellung der Siegel benutzt. Der PIN-Code muss vom Signator sorgfältig verwahrt und unter seiner alleinigen Kontrolle gehalten werden (siehe 1.7). Die Übertragung des PIN-Codes zu den „Trodat Seal Servern“ erfolgt in verschlüsselter Form, auf den „Trodat Seal Servern“ ist der PIN-Code selbst nicht gespeichert, es ist aber ein Hashwert des PIN-Codes gespeichert.

Solange keine Identitätsprüfung vorgenommen wurde, übernimmt Trosoft keine Haftung für die Identität des Signators. Ein solcher Account ist nicht geeignet, um damit fortgeschrittene elektronische Signaturen im Sinne der EU-Signaturrechtlinie zu erstellen. Ab dem Zeitpunkt, zu dem der gesamte Registrierungsvorgang inkl. Auswahl des PIN-Codes abgeschlossen wurde, können mit dem jeweiligen Account fortgeschrittene elektronische Signaturen im Sinne der EU-Signaturrechtlinie erstellt werden.

Vor dem Vertragsabschluss informiert Trosoft den Kunden über die Allgemeinen Geschäftsbedingungen, die Lizenzbedingungen und dieses Sicherheits- und Zertifizierungskonzept. Wenn der Signator und der Kunde nicht die selbe Person sind, wird auch der Signator über die ihn treffenden Verpflichtungen (siehe 1.7) informiert. Die genannten Informationen stehen auf der Website <http://www.trosoft.net/> als PDF-Dokumente zur Verfügung.

Die Registrierungsstellen archivieren im Auftrag von Trosoft Kopien aller entsprechend diesem Kapitel vorzulegenden Nachweise (Lichtbildausweise, Vertrag mit dem Kunden bzw. dem Signator, Registerauszug einer juristischen Person, Erklärung zur Zugehörigkeit des Signators zur juristischen Person). Trosoft archiviert die elektronisch erfassten Informationen (siehe 4.11) und im Fall, dass eine Registrierungsstelle ihre Tätigkeit einstellt, deren Archiv. Die genannten Nachweise werden bis mindestens sieben Jahre nach dem Ende der Vertragsbeziehung zwischen Trosoft und dem Kunden aufbewahrt (siehe 4.11).

3.4 Zuordnung der Siegel zu den Signatoren

Die bei „Trodat Seal“ verwendete Technologie unterscheidet sich folgendermaßen von den bei Public-Key-Infrastrukturen, die auf X.509 basieren, eingesetzten Technologien:

Ein Zertifikat im Sinne der EU-Signaturrechtlinie und § 2 Z 8 SigG ist eine elektronische Bescheinigung, mit der Signaturprüfdaten einer bestimmten Person



zugeordnet werden und deren Identität bestätigt wird. Bei Public-Key-Infrastrukturen, die auf X.509 basieren, wird ein solches Zertifikat in der Regel zu Beginn der Geschäftsbeziehung zwischen Signator und Zertifizierungsdiensteanbieter ausgestellt und in weiterer Folge vom Signator ohne Interaktion mit dem Zertifizierungsdiensteanbieter verwendet. Bei „Trodat Seal“ hingegen erfolgt die Ausstellung des Zertifikates, also die Zuordnung zu einer bestimmten Person bei den einzelnen Versiegelungsvorgängen. Um mit „Trodat Seal“ eine fortgeschrittene elektronische Signatur zu erzeugen, wird das Dokument zunächst mit Signaturerstellungsdaten signiert, die nur für diesen Versiegelungsvorgang erzeugt werden und nach der Versiegelung vernichtet werden, die der Signator also jedenfalls unter seiner alleinigen Kontrolle halten kann. Dann wird eine Verbindung zum „Trodat Seal Server“ aufgebaut und von diesem wird überprüft, ob der Signator sich mit seinem persönlichen PIN-Code (den er ebenfalls unter seiner alleinigen Kontrolle halten muss, siehe 1.7) ausgewiesen hat. Mit der vom „Trodat Seal Server“ erzeugten Signatur des Siegels bescheinigt Trosoft die Zuordnung zwischen den (in das Siegel eingebetteten) Signaturprüfdaten des Signators und der Person des Signators und bestätigt dessen Identität, erzeugt also ein Zertifikat im Sinne der EU-Signaturrechtlinie und des Signaturgesetzes.

„Trodat Seal“ kann auch in einer Offline-Variante betrieben werden, bei der zum Zeitpunkt der Erstellung des Siegels keine Verbindung zu einem „Trodat Seal Server“ aufgebaut wird. Auch in diesem Fall wird eine Signatur mit nur für diesen Versiegelungsvorgang erzeugten Signaturerstellungsdaten erstellt, die der Signator unter seiner alleinigen Kontrolle halten kann. Die Zuordnung zu einer bestimmten Person und die Bescheinigung dieser Zuordnung durch die Signatur eines „Trodat Seal Server“ erfolgt diesfalls aber erst bei der Prüfung der Echtheit des Siegels durch das bei dieser Prüfung ausgestellte und vom „Trodat Seal Server“ signierte Prüfzertifikat (siehe 3.6). Auch das Prüfzertifikat bescheinigt die Zuordnung zwischen den (in das Siegel eingebetteten) Signaturprüfdaten des Signators und der Person des Signators und bestätigt dessen Identität, ist also ein Zertifikat im Sinne der EU-Signaturrechtlinie und des Signaturgesetzes.

Die meisten Informationen, die bei X.509 im Zertifikat enthalten sind, werden bei „Trodat Seal“ bei der Prüfung der Siegel angezeigt, wobei jeweils die Daten angegeben werden, die zum Zeitpunkt der Erstellung des Siegels zugetroffen haben: Name des Zertifizierungsdiensteanbieters und Staat, in dem er seinen Sitz hat; Name des Signators (oder ein Pseudonym, welches als solches ersichtlich gemacht wird), allfällige Angaben zur Zuordnung des Signators zu einer juristischen Person. Anders als ein X.509-Zertifikat weist ein „Trodat Seal“ bzw. ein vom „Trodat Seal Server“ erzeugtes Prüfzertifikat aber keine Gültigkeitsdauer auf, sondern enthält stattdessen einen Zeitstempel.

Die erstellten Siegel sind jeweils einem Account zugeordnet. Die Sicherheit der Zuordnung beruht auf der Angabe der Lizenznummer und des persönlichen PIN-Codes. Der Signator ist verpflichtet (siehe 1.7), Lizenznummer und PIN-Code sorgsam zu verwahren.

Schon beim Anlegen des Accounts wird darauf geachtet, dass verschiedene Personen gleichen Namens unterschiedliche Kundennummern zugewiesen erhalten. Die Kundennummer wird auch in den Prüfzertifikaten angegeben (siehe 3.6), damit



bei der Prüfung der Siegel verschiedene Signatoren auch im Fall der Namensgleichheit unterschieden werden können.

Persönliche Daten, die der Kunde bzw. der Signator für Zwecke der Registrierung an Trosoft oder an Registrierungsstellen in elektronischer Form übermittelt, können großteils über den Webshop <http://www.trosoft.net/> eingegeben werden. Dabei wird die Vertraulichkeit der Daten durch HTTPS geschützt. Daten, die zwischen den Registrierungsstellen und Trosoft übertragen werden, werden ebenfalls verschlüsselt übertragen und es wird beim Verbindungsaufbau beiderseitige Authentifizierung sichergestellt.

3.5 Widerruf

Die Überprüfung der Echtheit eines Siegels kann nur von einem „Trodat Seal Server“ vorgenommen werden (siehe 3.6). Jedes Siegel enthält Angaben, mit denen es einem bestimmten Account in der Datenbank von „Trodat Seal“ zugeordnet ist. Ein „Account“ ist immer einem bestimmten Signator, also einer natürlichen Person zugeordnet.

An die Stelle des Widerrufs oder der Sperre eines Zertifikates tritt bei „Trodat Seal“ der Widerruf des Accounts. Bei der Prüfung eines Siegels (siehe 3.6) wird auch geprüft und als Teil des Prüfzertifikats ausgegeben, ob der Account zum Zeitpunkt der Erstellung des Siegels gültig oder widerrufen war. In der Online-Variante können nach dem Widerruf eines Accounts überhaupt keine Siegel mehr erstellt werden. Nach einem Widerruf muss, um neue gültige Siegel erstellen zu können, ein neuer Account eröffnet und allenfalls eine neue Registrierung (siehe 3.3) vorgenommen werden.

In den folgenden Fällen wird ein Widerruf eines Accounts vorgenommen:

1. auf Verlangen des Signators, des Kunden (wenn der Kunde vom Signator verschieden ist) oder einer juristischen Person, wenn bei der Registrierung die Zugehörigkeit des Signators zu dieser juristischen Person geprüft wurde,
2. wenn Trosoft Kenntnis vom Ableben des Signators, einer Namensänderung des Signators oder einer Änderung betreffend die Zugehörigkeit des Signators zu einer juristischen Person erlangt,
3. wenn vom Signator beim Anlegen des Accounts oder bei der Identitätsprüfung unrichtige Angaben gemacht wurden oder wenn sich herausstellt, dass ein vom Signator gewähltes Pseudonym in fremde Namens- oder Markenrechte eingreift,
4. wenn der Dienst „Trodat Seal“ eingestellt wird (siehe 4.9)
5. wenn die Telekom-Control-Kommission gemäß § 14 SigG die Sperre oder den Widerruf anordnet oder
6. wenn die Gefahr einer missbräuchlichen Verwendung des Accounts besteht (insbesondere weil der Signator die alleinige Kontrolle über seine Zugangsdaten verloren hat).



Trosoft verständigt den Signator (und auch den Kunden, wenn der Kunde vom Signator verschieden ist) von einem durchgeführten Widerruf. Die Auswirkungen des Widerrufs auf den Vertrag mit dem Signator bzw. dem Kunden werden in den Allgemeinen Geschäftsbedingungen geregelt.

Ein Signator hat die folgenden Möglichkeiten, den Widerruf seines Accounts zu veranlassen:

a) Elektronischer Widerruf: Wenn der Signator registriert wurde (siehe 3.3), hat er im Zuge der Registrierung einen eigenen PIN-Code ausgewählt. In diesem Fall kann er den Widerruf durch Eingabe des PIN-Codes in ein auf der Website <http://www.trosoft.net/> dafür zur Verfügung stehendes Formular veranlassen. Diese Möglichkeit steht im Rahmen der Verfügbarkeit der „Trodat Seal Server“ rund um die Uhr zur Verfügung und löst umgehend den Widerruf des Accounts aus.

b) Schriftlicher Widerruf: Wenn der Signator keinen PIN-Code hat oder diesen nicht mehr weiß, kann er den Widerruf in einem mittels Fax oder Brief übermittelten Schreiben verlangen. Das Registrierungspersonal nimmt dann einen Kontrollanruf beim Signator vor, um festzustellen, ob das Ersuchen von ihm stammt.

Verlangt der Kunde (falls der Kunde vom Signator verschieden ist) oder eine juristische Person (falls die Zugehörigkeit des Signators zur juristischen Person bei der Registrierung überprüft wurde, siehe 3.3) den Widerruf, dann steht nur die Möglichkeit des schriftlichen Widerrufs zur Verfügung. Das Registrierungspersonal nimmt dann einen Kontrollanruf beim Kunden bzw. bei einer organisatorisch verantwortlichen Person der juristischen Person vor.

Ein schriftliches Ersuchen um Widerruf ist grundsätzlich an jene Registrierungsstelle zu richten, welche die Registrierung (siehe 3.3) vorgenommen hat. Wurde keine Registrierung vorgenommen oder hat diese Registrierungsstelle ihre Tätigkeit eingestellt, dann kann über die Shopfinder-Funktion auf der Website <http://www.trosoft.net/> die für den jeweiligen Vertrag zuständige Registrierungsstelle herausgefunden werden. Ein Ersuchen um Widerruf kann auch direkt an Trosoft gerichtet werden, allerdings nur in deutscher oder englischer Sprache. Der Widerruf wird innerhalb der Geschäftszeiten der jeweiligen Registrierungsstelle binnen maximal eines Werktages bearbeitet. Trosoft verpflichtet die Registrierungsstellen zu Geschäftszeiten an jedem Werktag (ausgenommen Samstag, Sonntag und landesübliche Feiertage). Die Geschäftszeiten von Trosoft selbst sind: Montag bis Donnerstag: 9 bis 16 Uhr, Freitag: 9 bis 12 Uhr. An Samstagen, Sonntagen und österreichischen Feiertagen nimmt Trosoft keine schriftlichen Widerrufe vor.

3.6 Prüfung der Echtheit von Siegeln

Jedes Siegel enthält Angaben, mit denen es einem bestimmten Account in der Datenbank von „Trodat Seal“ zugeordnet ist. Ein „Account“ ist immer einem bestimmten Signator, also einer natürlichen Person zugeordnet. Ein Signator kann mehrere Accounts haben. Ein Account wird niemals von einem Signator auf einen anderen übertragen. Ändert sich die Person des Signators, dann wird ein neuer Account angelegt. Die Sicherheitsstufe der Zuordnung eines Accounts zu einem bestimmten Signator kann sich im Lauf der Zeit ändern. Beispielsweise ist möglich,



dass ein Account zunächst auf Grund der Kundendaten bei der Bestellung im Webshop ohne besondere Überprüfung der Identität des Signators angelegt wird, dass später eine Registrierung (Überprüfung der Identität durch eine Registrierungsstelle, siehe 3.3) erfolgt und dass in weiterer Folge ein Widerruf des Accounts (siehe 3.5) vorgenommen wird. Bei der Prüfung der Echtheit eines Siegels wird überprüft und als Teil des Prüfzertifikates ausgegeben, welche Sicherheitsstufe zum Zeitpunkt der Erstellung des Siegels vorlag.

Zur Überprüfung der Echtheit eines Siegels bietet Trosoft verschiedene Methoden an, die laufend weiterentwickelt werden. Gemeinsam ist diesen Methoden, dass eine Verbindung zu einem „Trodat Seal Server“ aufgebaut wird und die sicherheitsrelevanten Daten (nicht notwendigerweise der Gesamthalt) des Dokumentes übertragen werden. Der „Trodat Seal Server“ gibt dann ein signiertes Prüfzertifikat aus, welches vom Prüfenden zur weiteren Verwendung abgespeichert werden kann.

Die Prüfung unterscheidet sich danach, ob das versiegelte Dokument in elektronischer oder in ausgedruckter Form vorliegt:

a) Bei einem in elektronischer Form vorliegenden versiegelten Dokument wird durch Anklicken des mit „Click to Verify“ bezeichneten Prüf-Links ein Plugin geladen, welches den Hashwert des Dokumentes berechnet und je nach eingesetzter Methode den Gesamthalt des Dokumentes oder nur die sicherheitsrelevanten Daten des Siegels an den „Trodat Seal Server“ überträgt. Der „Trodat Seal Server“ prüft dann die Echtheit des Dokumentes und gibt ein signiertes Prüfzertifikat zurück. Trosoft informiert auf der Website <http://www.trosoft.net/> darüber, mit welchen Betriebssystemen und welcher Software (Browser) die Überprüfung vorgenommen werden kann.

b) Ein ausgedrucktes Dokument kann eingescannt werden, wobei die im Siegel enthaltene Sicherheitsgrafik gelesen und automationsunterstützt ausgewertet werden kann. Trosoft wird verschiedene Methoden anbieten, die dies unterstützen. Aus den in der Sicherheitsgrafik enthaltenen Daten kann der „Trodat Seal Server“ die Echtheit des Siegels überprüfen. Wenn bei der Erzeugung des Siegels bestimmte charakteristische Daten des Dokumentes in das Siegel aufgenommen wurden (z. B. der Betreff eines Protokolls oder die Rechnungsnummer), kann auch die Unverfälschtheit dieser Angaben bestätigt werden. Die Echtheit des gesamten Dokumentes kann mit dieser Methode nicht geprüft werden, die eingesetzte Technologie unterstützt aber die Auffindung des elektronischen Originals im Dokumentenmanagement des Signators, sodass im Zweifelsfall das elektronische Original angefordert und dessen Echtheit geprüft werden kann.

Je nach der zum Zeitpunkt der Erstellung des Siegels vorliegenden Identitätsprüfung (siehe 3.3) wird als Teil des Prüfzertifikates auch angegeben, ob die Identität des Signators geprüft wurde. Hat der Signator bei der Registrierung ein Pseudonym gewählt, dann wird anstelle seines Namens das (als solches gekennzeichnete) Pseudonym als Teil des Prüfzertifikates ausgegeben. Die Identität des Signators wird auf Anfrage von Gerichten oder Behörden oder von Personen, die ein rechtliches Interesse daran glaubhaft machen, offen gelegt. Wurde bei der Registrierung auch die Zugehörigkeit des Signators zu einer juristischen Person geprüft, dann wird auch



dieser Umstand und der Name der juristischen Person als Teil des Prüfzertifikates ausgegeben.

Je nachdem, ob das Siegel mit der Online-Variante erstellt wurde (d. h. dass bei der Erstellung des Siegels eine Verbindung zu einem „Trodat Seal Server“ aufgebaut und von diesem ein Zeitstempel erstellt wurde) oder mit der Offline-Variante (d. h. das Siegel enthält keinen Zeitstempel) erstellt wurde, wird im Prüfzertifikat auch angegeben, ob ein Zeitstempel vorliegt, dessen Genauigkeit (maximal 60 Sekunden Abweichung von der tatsächlichen Zeit, siehe 3.1) von Trosoft gewährleistet wird.

Bei der Siegelerstellung können in das Siegel auch charakteristische Daten des Dokuments (z. B. der Betreff eines Protokolls oder die Rechnungsnummer) eingebettet worden sein. War dies der Fall, dann werden auch diese Daten in das Prüfzertifikat aufgenommen.

Insgesamt kann das Prüfzertifikat die folgenden Angaben enthalten:

- Umfang der Prüfung: Gesamthalt des Dokumentes / nur das Siegel selbst und die darin enthaltenen charakteristischen Daten des Dokumentes
- Angaben zur Authentifizierung des Signators bei der Signaturerstellung: keine Authentifizierung am Server (bloß Authentifizierung mittels Windows-Passwort am Client) oder Authentifizierung mittels persönlichem PIN-Code
- Angaben zur Identität des Signators: Name oder Pseudonym des Signators, evtl. auch die Zugehörigkeit zu einer juristischen Person, weiters die Kundennummer des Signators. Verschiedene Signatoren gleichen Namens können anhand ihrer Kundennummer unterschieden werden. (Es ist aber nicht ausgeschlossen, dass dieselbe Person mehrere Kundennummern hat.)
- Das Prüfzertifikat ist ein Zertifikat im Sinne des Signaturgesetzes. Es enthält auch den öffentlichen Schlüssel des Schlüsselpaars, das der Signator bei der Erstellung des Siegels verwendet hat. Mit der Ausstellung des Prüfzertifikates bescheinigt Trosoft die Zuordnung zwischen dem Signator und dem von ihm verwendeten Schlüsselpaar.
- Angaben dazu, ob es sich um eine fortgeschrittene elektronische Signatur handelt (die Identität des Signators und optional auch die Zugehörigkeit zu einer juristischen Person wurde von Trosoft geprüft) oder um eine einfache elektronische Signatur (die Identität des Signators wurde nicht geprüft). Wenn es sich um eine fortgeschrittene elektronische Signatur handelt, wird auch das Datum angegeben, an dem die Registrierung (Identitätsüberprüfung) durchgeführt wurde.
- Angaben dazu, ob das Siegel mit einem Zeitstempel von Trosoft versehen wurde. Siegel können mit der Online-Variante erstellt werden (d. h. der Zeitpunkt der Erstellung des Siegels wird durch den Zeitstempeldienst von Trosoft bestätigt) oder mit der Offline-Variante (d. h. die Zeitangabe des Sieges basiert auf der internen Uhr am Rechner des Signators und Trosoft kann die Genauigkeit nicht gewährleisten).



- Wenn zum Account des Signators ein höheres Transaktionslimit als das standardmäßig vorgesehene Transaktionslimit von 2.500 Euro vereinbart wurde, wird auch dies als Teil des Prüfzertifikats ausgegeben.
- Wenn charakteristische Daten in das Siegel eingebettet wurden, bilden diese einen Teil des Prüfzertifikates
- Wenn bei der Prüfung des Siegels ein Fehler festgestellt wurde (insbesondere, dass das Dokument oder das Siegel nachträglich verändert wurde), wird dieser im Prüfzertifikat ausgegeben

Optional können Siegel auch eine bei der Erstellung des Siegels biometrisch erfasste Unterschrift des Signators oder einer anderen Person enthalten. Dabei wird im Siegel ein Abbild der Unterschrift ausdrückbar dargestellt, weiters sind im Siegel die biometrisch erfassten Daten enthalten. In der derzeit angebotenen Fassung von „Trodat Seal“ wird diese biometrisch erfasste Unterschrift weder bei der Erstellung des Siegels noch bei der hier beschriebenen Prüfung und Ausstellung von Prüfzertifikaten mit einem Unterschriftenmuster des Signators verglichen. Die Sicherheit des Siegels, die Prüfung der Echtheit von Siegeln und die Zuordnung der Siegel zum jeweiligen Signator erfolgt auf der Grundlage der im Siegel eingebetteten verschlüsselten Lizenznummer, dem vom Signator verwendeten PIN-Code und den verwendeten kryptographischen Verfahren. Die biometrisch erfasste Unterschrift kann unabhängig davon als zusätzliches Beweismittel eingesetzt werden. In Streitfällen kann sie auf Grund der erfassten und in das Siegel eingebetteten Daten von einem Sachverständigen mit einem Unterschriftenmuster verglichen werden.



4. Physikalische, organisatorische und personelle Sicherheitsmaßnahmen

4.1 Sicherheitsmanagement

Trosoft stellt sicher, dass das Sicherheitsmanagement dem Stand der Technik entspricht.

Trosoft trägt die Letztverantwortung für die Gesamtheit des Zeitstempel- und Zertifizierungsdienstes Trodat Seal im Sinne dieses Sicherheits- und Zertifizierungskonzeptes, unabhängig davon, ob einzelne Tätigkeiten zu Dienstleistern ausgelagert werden. Die Verantwortung beauftragter Dienstleister wird durch Trosoft klar definiert und durch entsprechende vertragliche Vereinbarungen sichergestellt, dass die Dienstleister alle Maßnahmen implementieren, die von Trosoft verlangt werden.

Die Verantwortung für das Sicherheitsmanagement obliegt einem innerhalb von Trosoft eingerichteten Sicherheitsteam, das sich aus der Geschäftsführung von Trosoft und zwei Personen zusammensetzt, die mit der Rolle eines „Security Officer“ betraut wurden (siehe 4.3). Entscheidungen des Sicherheitsteams zu Fragen des Sicherheitsmanagements und alle Änderungen der Sicherheitsvorgaben werden allen betroffenen Mitarbeitern von Trosoft oder von beauftragten Dienstleistern mitgeteilt.

Sicherheitsmaßnahmen und Betriebsvorschriften betreffend den Dienst „Trodat Seal“ werden vom Sicherheitsteam dokumentiert, implementiert und gewartet (vgl. auch Kapitel 6).

4.2 Risikoanalyse

Trosoft hat eine Risikoanalyse durchgeführt, um die möglichen Bedrohungen für die Sicherheit von „Trodat Seal“ festzustellen und die dagegen nötigen Sicherheitsmaßnahmen zu ergreifen.

Die in diesem Kapitel 4 beschriebenen Sicherheitsmaßnahmen schützen die „Trodat Seal Server“ und die Firewall-Rechner, das Rechenzentrum, in dem diese Server untergebracht sind, die Geschäftsräumlichkeiten und das interne Netzwerk von Trosoft, die von Trosoft oder von Beauftragten vorgenommene Softwareentwicklung sowie alle verwendeten kryptographischen Schlüssel und ihre Backups. Weiters werden Sicherheitsmaßnahmen betreffend Registrierungsstellen und andere Dienstleister getroffen.

4.3 Personelle Sicherheit

Die mit dem Dienst „Trodat Seal“ beschäftigten Personen müssen – unabhängig davon, ob sie bei Trosoft oder anderen Unternehmen angestellt sind, und unabhängig davon, ob sie langfristig oder für einzelne Aufgaben kurzfristig mit dem Dienst befasst sind – das für die jeweiligen Aufgaben erforderliche Fachwissen sowie die nötige Erfahrung aufweisen.



Für die sicherheitsrelevanten Aufgaben werden die unten genannten Rollen definiert. Die Rollen werden den jeweiligen Personen von der Geschäftsführung zugewiesen und in der Stellenbeschreibung dokumentiert. Bei der Wahrnehmung der übertragenen Aufgaben sind die Entscheidungen der Geschäftsführung zum Sicherheitsmanagement zu beachten (vgl. 4.1).

Personen in leitenden Funktionen müssen über ausreichende Kenntnisse der Technologie der elektronischen Signatur und der Zeitstempel, der Zeitsynchronisierung, der IT-Sicherheit und der Risikoanalyse verfügen. Das technische Personal muss über ausreichendes Fachwissen in den in § 10 Abs. 5 SigV genannten Bereichen verfügen (allgemeine EDV-Ausbildung, Sicherheitstechnologie, Kryptographie, elektronische Signatur, PKI, technische Normen, Hard- und Software).

Als Rollen im Sinne dieses Kapitels werden die folgenden definiert:

Geschäftsführung: Der Geschäftsführung von Trosoft obliegt die Letztverantwortung für das gesamte Sicherheitsmanagement. Die Geschäftsführung trägt dafür Sorge, dass Entscheidungen betreffend das Sicherheitsmanagement allen betroffenen Mitarbeitern von Trosoft oder beauftragten Dienstleistern mitgeteilt werden (siehe 4.1). Die Geschäftsführung betraut Personen mit den in diesem Kapitel beschriebenen Rollen.

Security Officer: Einer Person, die mit dieser Rolle betraut wurde, kommt umfassende Verantwortung für die Umsetzung dieses Sicherheits- und Zertifizierungskonzepts zu. Security Officer sind insbesondere mit Aufgaben betreffend die von den „Trodat Seal Servern“ verwendeten kryptographischen Schlüssel betraut (vgl. Kapitel 2 und das dort vorgesehene Vier-Augen-Prinzip).

Systemadministrator: Eine Person, die mit dieser Rolle betraut wurde, ist dazu autorisiert, die vertrauenswürdigen Systeme (siehe 4.7), zu installieren, konfigurieren, laufende Backups zu erstellen und warten oder Wartungsarbeiten, welche von Dritten vorgenommen werden, zu beaufsichtigen. Ein Vier-Augen-Prinzip ist nicht vorgesehen. Die Systemadministratoren haben Zutritt zu den vertrauenswürdigen Systemen und kennen die Administratorpasswörter dieser Server.

Rechenzentrumspersonal: Das Personal des beauftragten Rechenzentrums ist für bestimmte Tätigkeiten der laufenden Betreuung der vertrauenswürdigen Systeme (siehe 4.7) verantwortlich, insbesondere für die Bereitstellung der unterbrechungsfreien Stromversorgung und der Netzverbindung. Das Rechenzentrumspersonal hat keinen physikalischen Zugriff auf die vertrauenswürdigen Systeme und kennt auch nicht die Administratorpasswörter. Ein Vier-Augen-Prinzip ist nicht vorgesehen. Die Rollenzuweisung erfolgt nicht durch die Geschäftsführung von Trosoft, sondern durch das beauftragte Rechenzentrum, welches die erforderliche Zuverlässigkeit und Fachkenntnisse sicherzustellen hat.

Personal der Registrierungsstellen: Das Personal der Registrierungsstellen ist für die Registrierung (siehe 3.3) und den Widerruf (siehe 3.5) und die Archivierung der jeweiligen Vorgänge verantwortlich. Jede mit dieser Rolle betraute Person hat einen



entsprechenden persönlichen Zugang zum Webshop von Trosoft und kann bei den von der jeweiligen Registrierungsstelle betreuten Accounts die bei der Registrierung aufgenommenen Daten eingeben, den Abschluss der Registrierung vermerken und einen Widerruf vornehmen. Ein Vier-Augen-Prinzip ist nicht erforderlich. Das Personal der Registrierungsstellen hat keinen Zutritt den Geschäftsräumlichkeiten von Trosoft oder zum Rechenzentrum und kennt keine (mit Ausnahme des persönlichen Passworts für den Zugang zum Webshop) keine Passwörter der vertrauenswürdigen Systeme, insbesondere keine Administrationspasswörter. Die Rollenzuweisung, Überwachung der Tätigkeit und allfällige Entziehung der Berechtigung erfolgt durch die Geschäftsführung der Trosoft oder durch den Registrierungsstellenbeauftragten. Trosoft kann mit Registrierungsstellen auch vertragliche Vereinbarungen treffen, in denen diese Registrierungsstellen im Auftrag von Trosoft selbst das Personal auswählen und für die jeweiligen Personen Zugänge zum Webshop von Trosoft einrichten können. In diesem Fall wird die Registrierungsstelle vertraglich dazu verpflichtet, bei der Personalauswahl die Vorgaben von Trosoft an Fachkenntnisse und Zuverlässigkeit einzuhalten, entsprechende Schulungen nach den Vorgaben von Trosoft vorzunehmen und Trosoft Einsicht in alle relevanten Unterlagen zu gewähren.

Registrierungsstellenbeauftragter: Eine oder mehrere Personen, die innerhalb von Trosoft für den Vertrieb zuständig sind, werden von der Geschäftsführung mit der Rolle eines „Registrierungsstellenbeauftragten“ betraut. Eine Person, die mit dieser Rolle betraut wurde, ist für die Berechtigungsverwaltung des Personals der Registrierungsstellen verantwortlich, also für die Vergabe von Berechtigungen für das Registrierungsstellenpersonal, die Änderung von Berechtigungen, wenn der Umfang der Tätigkeit der Registrierungsstelle ausgeweitet oder eingeschränkt wird, und den Entzug von Berechtigungen, wenn der Vertrag mit der Registrierungsstelle erlischt oder Personal die Registrierungsstelle verlässt. Die Person ist auch dafür verantwortlich, Beschwerden über die Tätigkeit der Registrierungsstellen nachzugehen, stichprobenartige Überprüfungen vorzunehmen, Logdateien auf Auffälligkeiten zu untersuchen und Anzeichen für die Unzuverlässigkeit einzelner Registrierungsstellen an die Geschäftsführung zu berichten.

Personen, die mit einer der oben genannten Rollen beauftragt werden, dürfen in keinem Interessenskonflikt stehen, der ihre Unvoreingenommenheit beeinträchtigt. Zwischen den einzelnen Rollen bestehen folgende Unvereinbarkeiten: Personen mit den Rollen „Rechenzentrumspersonal“ bzw. „Personal der Registrierungsstellen“ werden von den Rollen „Security Officer“, „Systemadministrator“ bzw. „Registrierungsstellenbeauftragter“ überwacht und können daher nicht gleichzeitig mit einer dieser Rollen betraut werden. Es bestehen keine Unvereinbarkeiten zwischen den Rollen „Geschäftsführung“, „Security Officer“ und „Systemadministrator“. Für manche Aufgaben der „Security Officer“, insbesondere im Zusammenhang mit den kryptographischen Schlüsseln (siehe Kapitel 2) ist ein Vier-Augen-Prinzip vorausgesetzt, für alle anderen Aufgaben nicht.

4.4 Physikalische Sicherheit

Die folgenden Räumlichkeiten werden durch physikalische Sicherheitsmaßnahmen geschützt: Die vertrauenswürdigen Systeme (siehe 4.7) befinden sich in einem versperrten Käfig in einem beauftragten Rechenzentrum. Weiters werden die



Geschäftsräumlichkeiten von Trosoft und der Registrierungsstellen sowie jene Stellen, an denen Backups der kryptographischen Schlüssel aufbewahrt werden, geschützt.

Der Zutritt zum beauftragten Rechenzentrum wird vom Rechenzentrumspersonal überwacht und protokolliert. Den Käfig, in dem sich die vertrauenswürdigen Systeme (siehe 4.7) befinden, können nur die Systemadministratoren öffnen. Andere Personen (z. B. Wartungspersonal) haben nur in Begleitung und unter Aufsicht eines Systemadministrators Zutritt. Das Rechenzentrum verfügt über eine 24x7x365 Zugangskontrolle mit biometrischer Überprüfung, Löschgasanlagen, ausfallsichere Stromversorgung mit USV und Backup-Generatoren, redundante Klimakontroll- und Kühlsysteme und redundante GBit-Internetanbindungen an mehrere Carrier.

Zu den Büroräumlichkeiten hat nur das Personal von Trosoft und von Trosoft beauftragter Dienstleister Zutritt. Andere Personen, die sich nicht in den ausdrücklich für Besucher vorgesehenen Räumen befinden, müssen vom Personal angemessen beaufsichtigt werden.

Die Safes, in denen die Backups der kryptographischen Schlüssel verwahrt werden (siehe 2.2), befinden sich in Räumen, zu denen nur befugtes Personal Zutritt hat.

Die Registrierungsstellen sind verpflichtet, ihre Räumlichkeiten und Hardware so zu schützen, dass die Computer, mit denen die Registrierungen und Widerrufe durchgeführt werden, vor unbefugten Veränderungen, und die archivierten Unterlagen zu Registrierungen und Widerrufen vor unbefugter Einsichtnahme, Diebstahl und Verlust geschützt sind.

4.5 Organisatorische Sicherheitsmaßnahmen

Alle Systeme von Trosoft, insbesondere die vertrauenswürdigen Systeme (siehe 4.7) und die Rechner der Softwareentwicklung, werden gegen unbefugten Zugriff (siehe oben 4.4) sowie gegen Viren und andere schädliche Software geschützt.

Alle sicherheitsrelevanten Vorfälle und Störungen sind umgehend einem Security Officer zu melden, soweit für den konkreten Vorfall keine besonderen Maßnahmen festgelegt wurden.

Alle Datenträger, die im Zusammenhang mit „Trodat Seal“ verwendet werden, werden gegen Beschädigung, Diebstahl und unbefugten Zugriff geschützt. Datenträger, die nicht mehr benötigt werden, werden auf sichere Weise vernichtet, wenn sie nicht mehr benötigt werden (vgl. 2.7 zur Vernichtung kryptographischer Schlüssel).

4.6 Zugriffsrechte und Schutz vor unbefugtem Zugriff

Trosoft stellt sicher, dass nur autorisierte Personen Zugriff auf die für „Trodat Seal“ verwendeten Systeme haben.

Die vertrauenswürdigen Systeme (siehe 4.7) und das interne Netzwerk in den Geschäftsräumlichkeiten von Trosoft werden durch Firewalls gegen unbefugten Zugriff (einschließlich unbefugten Zugriff von Kunden, Registrierungsstellen und



anderen Dienstleistern) geschützt. Die Firewalls werden so konfiguriert, dass alle Protokolle und Zugriffsmöglichkeiten gesperrt werden, die für die Tätigkeit von Trosoft nicht erforderlich sind.

Die Datenübertragung zwischen der Clientsoftware „Trodat Seal for Windows“ des Signators und den „Trodat Seal Servern“ wird mittels HTTPS verschlüsselt. Ebenso wird die Datenübertragung zwischen den Registrierungsstellen und den Servern von Trosoft verschlüsselt. Serverseitig erfolgt jeweils eine Authentifizierung mittels Serverzertifikat, clientseitig mittels User-ID und Passwort bzw. durch den in der Clientsoftware gespeicherten Registrierungscode (Lizenznummer) und den vom Signator gewählten PIN-Code (siehe 3.3).

Ein Security Officer beaufsichtigt die Vergabe von Zugriffsrechten auf die vertrauenswürdigen Systeme (siehe 4.7), insbesondere die Zugriffsrechte der Systemadministratoren und sorgt dafür, dass Zugriffsrechte entzogen bzw. Passwörter geändert werden, wenn eine Person ihrer Rolle enthoben wird. Ein Registrierungsstellenbeauftragter überwacht die Zugriffsrechte des Registrierungsstellenpersonals und sorgt dafür, dass Zugriffsrechte entzogen werden, wenn sich ein Vertrag mit einer Registrierungsstelle gekündigt wird, der Umfang der Tätigkeit der Registrierungsstelle eingestellt wird oder Personal die Registrierungsstelle verlässt.

Für den Zutritt und Zugriff auf alle vertrauenswürdigen Systeme (siehe 4.7) ist erforderlich, dass das Personal entsprechend authentifiziert ist (Zutrittskontrolle siehe 4.4, Schutz gegen unbefugten Zugriff mittels User-ID und Passwort).

Das Personal (siehe 4.3) ist für seine Tätigkeiten verantwortlich. Über sicherheitsrelevante Ereignisse werden Protokolle geführt (siehe 4.11).

4.7 Vertrauenswürdige Systeme

Folgende Systeme werden als besonders schutzwürdig angesehen: die Rechner, auf denen die Serversoftware zu „Trodat Seal“ betrieben wird („Trodat Seal Server“), die Rechner, auf denen die Software des Webshop betrieben wird, weiters die entsprechenden Firewall-Rechner und Netzwerkkomponenten (Router, Switches).

Die vertrauenswürdigen Systeme sind in einem Rechenzentrum untergebracht und durch einen versperrbaren Käfig vor unbefugtem Zugriff geschützt (siehe 4.4). Weiters werden die Systeme durch organisatorische Maßnahmen (siehe 4.5) und eingeschränkte Vergabe von Zugriffsrechten (siehe 4.6) geschützt. Zutrittsrechte und Zugriffsrechte zu den vertrauenswürdigen Systemen (dazu gehört insbesondere die Kenntnis der Administrationspasswörter) haben nur die Systemadministratoren (siehe 4.3).

Beim Design der Software für die „Trodat Seal Server“ und für den Webshop wird eine Analyse der erforderlichen Sicherheitsmaßnahmen vorgenommen. Die Installation neuer Versionen der Software, Konfigurationsänderungen und die Installation von Patches werden protokolliert.



Bei der derzeit angebotenen Form des Dienstes „Trodat Seal“ ist nicht vorgesehen, dass vertrauenswürdige Systeme nach Common Criteria oder ITSEC evaluiert werden oder dass Hardware Security Module eingesetzt werden.

4.8 Kompromittierung

Als Fälle der Kompromittierung der Sicherheit von „Trodat Seal“ werden insbesondere angesehen: der Verlust der Kontrolle über den privaten Schlüssel eines „Trodat Seal Servers“ oder der Verdacht, dass ein solcher Schlüssel von Unbefugten missbraucht werden konnte oder könnte; weiters der Verdacht, dass die Uhr eines „Trodat Seal Server“ um mehr als 60 Sekunden von der tatsächlichen Zeit abgewichen ist und ungenaue Zeitstempel erstellt wurden.

Im Fall der Kompromittierung wird Trosoft überprüfen, inwieweit der eingetretene Schaden und die betroffenen Siegel eingegrenzt werden können und wird eine dem Sicherheitsproblem entsprechende Veröffentlichung bzw. Verständigung vornehmen, um die auf die Sicherheit von „Trodat Seal“ Vertrauenden, die betroffenen Kunden bzw. Signatoren und die betroffenen anderen Vertragspartner (insbesondere Registrierungsstellen) zu informieren. Weiters werden im Fall der Kompromittierung die betroffenen „Trodat Seal Server“ abgeschaltet und keine neuen Siegel oder Prüfzertifikate erstellt, bis das Problem zuverlässig behoben ist.

4.9 Einstellung des Betriebs

Trosoft behält sich vor, den Betrieb von „Trodat Seal“ einzustellen. Die Einstellung des Betriebs bedeutet, dass ab diesem Zeitpunkt keine weiteren neuen Siegel mehr erstellt werden können. Alle Accounts werden widerrufen (siehe 3.5). Um die Überprüfung bereits erstellter Siegel zu gewährleisten, wird Trosoft (oder ein Rechtsnachfolger oder ein beauftragter Dienstleister) die „Trodat Seal Server“ nach der Einstellung noch mindestens sieben Jahre lang weiter betreiben. Erst dann wird die Tätigkeit völlig eingestellt.

Vor der Einstellung des Betriebs werden alle Signatoren, die laufende Verträge mit Trosoft haben, mittels E-Mail über den Umstand der Einstellung des Betriebs informiert. Weiters erfolgt eine Information auf der Website <http://www.trosoft.net/>. Die Auswirkungen der Einstellung auf die Verträge mit den Signatoren bzw. Kunden werden in den Allgemeinen Geschäftsbedingungen geregelt.

Die Verträge mit Registrierungsstellen und anderen Dienstleistern, die an der Erbringung des Dienstes beteiligt sind, werden gekündigt, soweit die Dienstleistung nicht für den Weiterbetrieb der „Trodat Seal Server“ benötigt wird.

Wenn der siebenjährige Weiterbetrieb der „Trodat Seal Server“ und die erforderliche Aufbewahrung der Dokumentation (siehe 4.11) sowie die Veröffentlichung der Zertifikate der „Trodat Seal Server“ nicht von Trosoft oder einem Rechtsnachfolger selbst wahrgenommen wird, wird Trosoft diese Aufgabe gemäß § 12 SigG an einen anderen Zertifizierungsdiensteanbieter übertragen.



Alle privaten Schlüssel und allfällige Backups werden zerstört, sobald sie nicht mehr benötigt werden. Dabei wird gewährleistet, dass die privaten Schlüssel nicht mehr wiederhergestellt werden können.

Ein Widerruf der Zertifikate der Schlüssel für die „Trodat Seal Server“ in Form einer Widerrufsliste ist nicht vorgesehen. Da die Überprüfung der Siegel durch Kontaktaufnahme mit einem „Trodat Seal Server“ (siehe 3.6) erfolgt, wird direkt in der Konfiguration der „Trodat Seal Server“ eingetragen, welche Schlüsselpaare nicht mehr gültig sind.

4.10 Übereinstimmung mit rechtlichen Anforderungen

Der Dienst „Trodat Seal“ wird in Übereinstimmung mit allen Anforderungen des österreichischen Rechts erbracht. Zu beachten sind insbesondere das Signaturgesetz und die Signaturverordnung (durch welche die Signaturrichtlinie 1999/93/EG umgesetzt wurde) und das Datenschutzgesetz 2000 (durch welches die Datenschutzrichtlinie 95/46/EG umgesetzt wurde).

Die im Zusammenhang mit „Trodat Seal“ verarbeiteten personenbezogenen Daten der Signatoren werden durch die in diesem Dokument beschriebenen Sicherheitsmaßnahmen vor unbefugtem Zugriff, Veränderung oder Verlust geschützt.

Angaben zur Identität des Signators und dazu, ob eine Registrierung (Identitätsprüfung) vorgenommen wurde, werden in den Prüfzertifikaten offengelegt (siehe 3.6). Das Prüfzertifikat kann jede Person abrufen, die Zugriff auf ein von diesem Signator versiegeltes Dokument hat. Darüber hinaus erfolgt die Übermittlung personenbezogener Daten nur in dem für die Erbringung des Dienstes erforderlichen Ausmaß (z. B. zur Verrechnung oder zur Geltendmachung rechtlicher Ansprüche Trosofts gegen den Signator).

4.11 Dokumentation und Archivierung

Trosoft archiviert Informationen über sicherheitsrelevante Ereignisse (z. B. zum Lebenszyklus der eingesetzten kryptographischen Schlüssel und der für diese Schlüssel ausgestellten Zertifikate, zu wichtigen Konfigurationsänderungen der „Trodat Seal Server“ und zu Störfällen) bis mindestens sieben Jahre nach Einstellung des Dienstes „Trodat Seal“. Soweit sich diese Informationen auf bestimmte „Trodat Seal Server“ beziehen, werden sie mindestens sieben Jahre nach Außerbetriebnahme des Servers aufbewahrt.

Die Kundendaten der Signatoren (insbesondere Informationen zur allfälligen Registrierung der Signatoren und zu einem allfälligen Widerruf) werden bis mindestens sieben Jahre nach Ende der Vertragsbeziehungen betreffend den jeweiligen Account aufbewahrt. Soweit die Daten nicht elektronisch erfasst wurden (siehe unten), werden sie von der jeweiligen Registrierungsstelle archiviert. Endet die Vertragsbeziehung zwischen Trosoft und einer Registrierungsstelle, dann sind die archivierten Informationen Dokumente an Trosoft oder eine von Trosoft bestimmte andere Registrierungsstelle zur weiteren Archivierung zu übergeben.



Die Echtheit eines mit „Trodat Seal“ erzeugten Siegels kann nur durch einen „Trodat Seal Server“ geprüft werden. Im Fall der Einstellung des Dienstes „Trodat Seal“ wird Trosoft (oder ein allfälliger Rechtsnachfolger oder ein von Trosoft beauftragtes Unternehmen) den Betrieb der „Trodat Seal Server“ und die Aufbewahrung der Dokumentation noch für einen Zeitraum von sieben Jahren aufrecht erhalten, um für diesen Zeitraum die Prüfbarkeit der mit „Trodat Seal“ erzeugten Siegel zu gewährleisten.

Personen, die an einer längeren Prüfbarkeit der Siegel interessiert sind, können die vom „Trodat Seal Server“ signierten Prüfzertifikate gemeinsam mit dem versiegelten Dokument über eine längere Frist aufbewahren und damit unabhängig von Trosoft als Beweismittel verwenden.

Trosoft und die Registrierungsstellen gewährleisten die Vertraulichkeit der archivierten Informationen. Diese werden Gerichten und Behörden auf Anfrage im Einzelfall zur Verfügung gestellt. Macht eine andere Person ein rechtliches Interesse an einem bestimmten Siegel geltend, dann prüft Trosoft anhand der vorliegenden Unterlagen, ob eine Identitätsprüfung bzw. ein Widerruf vorgenommen wurde, und gibt der Person entsprechend ihrem rechtlichen Interesse darüber Auskunft. Die Signatoren und Kunden haben nach dem Datenschutzrecht Anspruch auf Auskunft über die von Trosoft verarbeiteten, sie betreffenden personenbezogenen Daten.

In den automationsunterstützt erstellten Protokollen werden Zeitangaben verwendet, deren Genauigkeit der in 3.1 genannten Genauigkeit des Zeitstempeldienstes entspricht. Soweit Protokolle nicht von einem „Trodat Seal Server“ erstellt werden, wird die Uhr des jeweiligen Servers mit einem „Trodat Seal Server“ oder einer vergleichbar genauen Zeitquelle synchronisiert.

Die automationsunterstützt erstellten Protokolle und die elektronisch archivierten Daten werden so aufbewahrt, dass sie nicht auf einfache Weise verändert oder zerstört werden können.

Zu den von Trosoft automationsunterstützt erstellten Protokollen zählen:

- Protokolle zu jedem einzelnen mit der Online-Version erstellten „Trodat Seal“, unter anderem mit Angaben zum Account, zum Hashwert des Dokumentes, zum Zeitstempel und einer eindeutigen Identifikation des Siegels (Transaction ID).
- Protokolle zu jedem einzelnen von einem „Trodat Seal Server“ erstellten Prüfzertifikat, unter anderem mit Angaben zum Account, zum Hashwert des Dokumentes, zum Zeitpunkt der Erstellung des Prüfzertifikates und einer eindeutigen Identifikation des Prüfzertifikates.
- Protokolle zur durchgeführten Identitätsprüfung durch eine Registrierungsstelle (siehe 3.3): Name (Nachname und Vorname(n) in der Schreibweise des vorgelegten Lichtbildausweises, Datum und Ort der Geburt, postalische Adresse, E-Mail-Adresse, Daten zum Lichtbildausweis (Ausstellende Behörde, Ausstellungsdatum und Nummer), Angaben zu einem allfällig höheren Transaktionslimit, Angaben zu einem allfällig gewählten Pseudonym, Angaben zur allfälligen Zuordnung des Signators zu einer juristischen Person (Name bzw.



Firma der juristischen Person, Art und Nummer des vorgelegten Registerauszuges, Name und allenfalls Geburtsdatum der organisatorisch verantwortlichen Person, Daten zum Lichtbildausweis der organisatorisch verantwortlichen Person), Art der Identitätsprüfung (persönlich oder per Fax mit telefonischem Rückruf), Vermerke (insbesondere über den vorgenommenen Rückruf), Zeitpunkt der Registrierung, Protokoll zur Auswahl des PIN-Codes durch den Signator, Zeitpunkt des Abschlusses der Registrierung, Angaben zur Person, die die Registrierung vorgenommen hat.

- Protokolle zum Widerruf eines Accounts (siehe 3.5): Angaben dazu, auf welche Art (mit PIN-Code, schriftlich) und vom wem (Signator, Kunde, juristische Person) der Widerruf beantragt wurde, Vermerk über einen allfällig durchgeführten Rückruf zur Kontrolle, Zeitpunkt des Einlangens des Ersuchens um Widerruf und der Durchführung des Widerrufs, allfällige Vermerke (insbesondere über einen mangels Authentifizierung abgelehnten Widerrufs Antrag oder zu den Gründen eines allfällig verspätet vorgenommenen Widerrufs), Angaben zur Person, die den Widerruf vorgenommen hat.
- Protokolle zur Berechtigungsvergabe und -entziehung an das Registrierungsstellenpersonal, unter anderem mit dem eindeutigen Usernamen der Person, dem Namen und der Bezeichnung der Registrierungsstelle, den vergebenen bzw. entzogenen Berechtigungen und dem Zeitpunkt der Berechtigungsvergabe bzw. -entziehung, sowie mit einer Identifikation der Person, welche die Berechtigungsvergabe bzw. -entziehung vorgenommen hat.
- Logdateien zur Zeitsynchronisierung der „Trodat Seal Server“, insbesondere zu Ausfällen bei der Synchronisierung.

Folgende Unterlagen werden von Trosoft in Papierform oder elektronisch archiviert:

- Protokolle über sicherheitsrelevante Ereignisse, insbesondere zum Lebenszyklus der kryptographischen Schlüssel der „Trodat Seal Server“ und der dazu ausgestellten Zertifikate, zur Konfiguration der vertrauenswürdigen Systeme (siehe 4.7) und zu Konfigurationsänderungen, zu Störfällen und Ausfällen des Systems (siehe auch 4.8), insbesondere auch zu Ausfällen der Zeitsynchronisierung (siehe 3.2).
- Verträge mit Registrierungsstellen, dem Rechenzentrum und anderen Dienstleistern, Unterlagen zum Personal von Trosoft (Personalakten).

Folgende Unterlagen werden von den Registrierungsstellen in Papierform oder elektronisch archiviert:

- Unterlagen zur Registrierung: Kopie des Lichtbildausweises des Signators, Vertrag des Signators, allfällig vorgelegter Lichtbildausweis einer organisatorisch verantwortlichen Person der zum Signator erfassten juristischen Person, Einverständniserklärung der juristischen Person, Registerauszug der juristischen Person, allfällige weitere vorgelegte Unterlagen.
- Unterlagen zum Widerruf: Schriftliche Ersuchen um Widerruf und allfällig weitere dazu vorgelegte Unterlagen.



Das beauftragte Rechenzentrum protokolliert im Rahmen des mit dem Rechenzentrums geschlossenen Vertrages die Zutritte zum Rechenzentrum. Diese Protokolle werden von Trosoft nicht archiviert.



5. Organisatorisches

Durch folgende Maßnahmen stellt Trosoft die Zuverlässigkeit von Trosoft und von „Trodat Seal“ sicher:

Policies, Sicherheitskonzepte und organisatorische Maßnahmen für „Trodat Seal“ sind nicht diskriminierend.

Der Dienst „Trodat Seal“ steht allen Kunden zur Verfügung, die sich zu den Allgemeinen Geschäftsbedingungen und Lizenzbedingungen verpflichten (vgl. insbesondere auch die Pflichten des Signators bzw. Kunden in 1.7).

Die Trosoft Entwicklungs u. Vertriebs GmbH ist eine Kapitalgesellschaft mit eigener Rechtspersönlichkeit nach österreichischem Recht.

Trosoft betreibt ein internes Qualitätssicherheitssystem.

Trosoft ist angemessen versichert, um Haftungen aus dem Dienst „Trodat Seal“ entsprechen zu können.

Trosoft verfügt über ausreichende Finanzmittel, um in Übereinstimmung mit diesen Sicherheits- und Zertifizierungskonzept handeln zu können.

Trosoft beschäftigt ausreichend Personal mit entsprechender Ausbildung, Schulung, technischem Wissen und Erfahrung um „Trodat Seal“ entsprechend diesem Sicherheits- und Zertifizierungskonzept (vgl. 4.3) betreiben zu können.

Trosoft hat Maßnahmen implementiert, um Beschwerden im Zusammenhang mit der Erbringung von „Trodat Seal“ nachzugehen und Streitfälle zu lösen. Wenn Streitfälle mit Trosoft nicht zur Zufriedenheit der Kunden gelöst werden können, steht ein Streitschlichtungsverfahren zur Verfügung (siehe 1.13).

Wenn Tätigkeiten von Trosoft an Dienstleister ausgelagert werden, wird dies durch ordnungsgemäß dokumentierte Verträge geregelt.



6. Administration dieses Sicherheits- und Zertifizierungskonzepts

Das innerhalb von Trosoft eingerichtete Sicherheitsteam (siehe 4.1) hat die Aufgabe, dieses Sicherheits- und Zertifizierungskonzept laufend dahingehend zu überprüfen, ob Änderungen oder Ergänzungen erforderlich sind sowie mögliche Neuerungen und ihre Auswirkungen auf die Sicherheit zu beraten. Änderungen dieses Sicherheits- und Zertifizierungskonzeptes werden vom Sicherheitsteam beschlossen.

Mit jeder Änderung dieses Sicherheits- und Zertifizierungskonzepts ist eine Änderung der Versionsnummer und des Datums des Dokumentes verbunden. Bei Änderungen ist jeweils auch festzulegen, wann diese in Kraft treten. Der wesentliche Inhalt der Änderungen wird in der Versionsgeschichte am Beginn des Dokumentes dargestellt. Gemäß § 6 Abs. 2 SigG werden Änderungen der Telekom-Control-Kommission als Aufsichtsstelle für elektronische Signaturen angezeigt.

Die verschiedenen Fassungen dieses Sicherheits- und Zertifizierungskonzeptes werden auf der Website <http://www.trosoft.net/> veröffentlicht, wobei auch ersichtlich gemacht wird, welche Fassung in welchem Zeitraum zur Anwendung kam.



7. Glossar

Account	Ein Account entspricht einer →Lizenz für →„Trodat Seal“. Jeder Account ist genau einem →Signator zugeordnet. Alle mit „Trodat Seal“ erstellten →Siegel enthalten die verschlüsselte →Lizenznummer und sind damit einem bestimmten Account und einem bestimmten Signator zugeordnet.
Biometrie	Biometrie bezeichnet die Vermessung biologischer Merkmale von Menschen als Mittel zur Authentifizierung. Bei →„Trodat Seal“ kann bei der Erstellung des →Siegels die eigenhändige Unterschrift des →Signators oder einer anderen Person mit einem Stifttablett biometrisch erfasst werden. Die erfassten Daten werden in das Siegel eingebettet und dienen als zusätzliches Beweismittel (siehe 3.6).
Certification Practice Statement (CPS)	Ein Teil des Sicherheits- und Zertifizierungskonzepts, in welchem der Zertifizierungsdiensteanbieter darlegt, wie er bei der Erbringung seiner Dienstleistungen vorgeht
Common Criteria	Eine internationale Vereinbarung, mit der zahlreiche Staaten „Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik“ festgelegt haben, siehe http://www.commoncriteriaportal.org/
digitale Tinte	Die Verrechnungseinheit für die Nutzung von →„Trodat Seal“. Bei der Erstellung von →SiegelIn wird digitale Tinte vom →Account des →Signators abgebucht. Digitale Tinte kann über den →Webshop nachgekauft werden.
einfache elektronische Signatur	Eine Form der elektronischen →Signatur, bei der keine besonderen Anforderungen an die Sicherheit der Signatur gewährleistet werden. Vgl. auch: →fortgeschrittene elektronische Signatur
Einmalschlüssel	Die Software „Trodat Seal for Windows“ erzeugt für jedes einzelne damit erstellte Siegel ein →Schlüsselpaar, das zur Erstellung der →Signatur verwendet und danach vernichtet wird.
EU-Signaturrichtlinie	Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, ABl. L 13 vom 19.1.2000, S. 12. Die Richtlinie gewährleistet die europaweite rechtliche Anerkennung elektronischer →Signaturen



fortgeschrittene elektronische Signatur	Eine Form der elektronischen →Signatur, bei der bestimmte, in der →EU-Signaturrechtlinie festgelegte Anforderungen gewährleistet werden. Fortgeschrittene elektronische Signaturen können insbesondere zur Signatur elektronischer Rechnungen verwendet werden. Vgl. auch: einfache elektronische Signatur
Hashverfahren	Ein →kryptographisches Verfahren, mit dem aus beliebigen Dokumenten eine eindeutige Zahl fester Länge (der Hashwert) errechnet werden kann. Hashverfahren sind so konstruiert, dass in der Praxis aus dem Hashwert das Dokument nicht errechnet werden kann und dass es in der Praxis nicht vorkommt, dass zwei verschiedene Dokumente den selben Hashwert haben. Bei →„Trodat Seal“ wird das Hashverfahren →SHA-256 verwendet.
ITSEC	Eine internationale Vereinbarung, mit der einige Staaten „Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik“ festgelegt haben. ITSEC wird zunehmend durch die →Common Criteria abgelöst.
Kryptographie	Ein Teilgebiet der Mathematik, das sich unter anderem mit der Verschlüsselung von Daten und der Erstellung elektronischer →Signaturen beschäftigt.
Kunde	Jemand, der eine Lizenz für →„Trodat Seal“ erworben hat. Ein Kunde kann eine natürliche oder eine juristische Person sein. Ein Kunde kann die Lizenz entweder selbst als →Signator nutzen (wenn er eine natürliche Person ist) oder für einen anderen →Signator erworben haben (z. B. wenn der Kunde ein Unternehmen ist).
Lichtbildausweis	Bei der Registrierung (siehe 3.3) muss der →Signator zum Nachweis seiner Identität einen amtlichen Lichtbildausweis vorlegen. Je nach Staat, in dem →„Trodat Seal“ angeboten wird, werden unterschiedliche Arten von Lichtbildausweisen (z. B. Reisepass, Personalausweis, ...) akzeptiert.
Lizenznummer	Jede Lizenz für →„Trodat Seal“ hat eine eindeutige Nummer. In jedem mit „Trodat Seal“ erzeugten Siegel ist die Lizenznummer in verschlüsselter Form enthalten. Dadurch kann bei der Prüfung der Echtheit von Siegeln (siehe 3.6) ein Bezug zum →Account und somit zum →Signator hergestellt werden. Vgl. auch →Registrierungscode.



Massensignatur	Eine Form der elektronischen →Signatur, bei der die Erstellung der Signatur nicht für jedes Dokument einzeln ausgelöst werden muss. →„Trodat Seal“ wird auch in einer massensignaturfähigen Variante angeboten. Der →Signator kann damit die Versiegelung von Dokumenten automatisieren.
Offline	→„Trodat Seal“ kann in einer Offline-Variante betrieben werden. Bei dieser Variante wird bei der Erstellung des →Siegels keine Verbindung zu einem „Trodat Seal Server“ aufgebaut. Das Siegel enthält in diesem Fall keinen →Zeitstempel, d. h. Trosoft gewährleistet nicht die Genauigkeit der Zeit der Erstellung.
Online	→„Trodat Seal“ kann in einer Online-Variante betrieben werden. Bei dieser Variante wird bei der Erstellung des →Siegels eine Verbindung zu einem „Trodat Seal Server“ aufgebaut. Das Siegel wird in diesem Fall mit einem →Zeitstempel versehen, d. h. Trosoft bescheinigt den Zeitpunkt der Erstellung des Siegels.
PDF	Portable Document Format. Ein von Adobe Inc. spezifiziertes Datenformat, mit dem druckfertig layoutierte Dokumente erstellt werden können.
PIN-Code	Zum Abschluss der →Registrierung muss der →Signator einen persönlichen PIN-Code wählen. In weiterer Folge muss dieser PIN-Code vor der Erstellung jedes →Siegels eingegeben werden. Der PIN-Code schützt dagegen, dass der →Account des Signators von Unbefugten missbraucht wird. Daher muss der PIN-Code vom Signator geheim gehalten werden. Bei Verlust des PIN-Codes muss der Account →widerrufen werden.
Prüfzertifikat	Die Echtheit eines →Siegels kann nur geprüft werden, indem eine Verbindung zu einem „Trodat Seal Server“ aufgebaut wird. Das Ergebnis der Prüfung wird vom „Trodat Seal Server“ in einem Prüfzertifikat bestätigt, das zum Nachweis der Echtheit des Siegels aufbewahrt werden kann. Der Prüfungsvorgang und die Inhalte des Prüfzertifikats sind in 3.6 beschrieben.



Public-Key-Infrastruktur	Ein technisches Umfeld, in dem mittels asymmetrischer →Kryptographie gesicherte Kommunikation möglich ist. Meist wird der Begriff im Zusammenhang mit →X.509-Technologien verwendet. →„Trodat Seal“ verwendet ähnliche Sicherheitstechniken, unterscheidet sich aber in manchen Punkten von Public-Key-Infrastrukturen, die auf X.509 basieren.
Registrierung	Der Vorgang, bei dem die Identität eines →Signators anhand eines →Lichtbildausweises geprüft wird (siehe 3.3). Nach der Registrierung können mit →„Trodat Seal“ →fortgeschrittene elektronische Signaturen erstellt werden.
Registrierungscode	Ein 20-stelliger, aus vier Gruppen zu je fünf Buchstaben oder Ziffern bestehender Code, der beim Erwerb einer Lizenz ausgefolgt wird. Mit dem Code kann der →Signator seinen persönlichen →Account am „Trodat Seal Server“ anlegen (siehe 3.3).
Registrierungsstelle	Eine Stelle, die →Registrierungen, also Überprüfungen der Identität von →Signatoren vornimmt. Registrierungsstellen können über den →Webshop http://www.trosoft.net/ gefunden werden.
RFC	Request for Comments. Ein Standardisierungsdokument für das Internet, siehe http://ietf.org/rfc.html
RSA	Ein asymmetrisches →kryptographisches Verfahren, welches zur Verschlüsselung und zur Erstellung von →Signaturen verwendet werden kann. Bei →„Trodat Seal“ wird RSA mit einer Schlüssellänge von mindestens 1024 Bit verwendet.
Schlüssel, öffentlicher	Jener Teil des →Schlüsselpaars eines asymmetrischen →kryptographischen Verfahrens, welcher veröffentlicht und zur Signaturprüfung verwendet wird. Vgl. auch →Signaturprüfdaten.
Schlüssel, privater	Jener Teil des →Schlüsselpaars eines asymmetrischen →kryptographischen Verfahrens, welcher geheim gehalten und z. B. zur Erstellung von →Signaturen verwendet wird. Bei →„Trodat Seal“ werden →Einmalschlüssel verwendet, d. h. der private Schlüssel des →Signators wird gleich nach der Erstellung des →Siegels vernichtet. Vgl. auch →Signaturerstellungsdaten



Schlüsselpaar	Bei asymmetrischen →kryptographischen Verfahren hat jeder Teilnehmer ein Schlüsselpaar, das aus einem öffentlichen und einem privaten →Schlüssel besteht. Der private Schlüssel wird geheimgehalten und z. B. für die Erstellung von →Signaturen verwendet. Der öffentliche Schlüssel dient der Signaturprüfung.
SHA-1	Ein bei →„Trodat Seal“ verwendete →Hashverfahren. Mit SHA-1 errechnete Hashwerte haben eine Länge von 160 Bit.
SHA-256	Ein bei →„Trodat Seal“ verwendete →Hashverfahren. Mit SHA-256 errechnete Hashwerte haben eine Länge von 256 Bit. Das Verfahren ist ein Nachfolger des auch verwendeten verbreiteten Verfahrens SHA-1.
Shopfinder	Eine Funktion im →Webshop http://www.trosoft.net/ , über die z. B. →Registrierungsstellen gefunden werden können.
Sicherheitsstufe	→„Trodat Seal“ wird in zwei Sicherheitsstufen angeboten. Solange der →Signator keine Identitätsprüfung (→Registrierung) vornehmen hat lassen, sind die mit „Trodat Seal“ erstellten →Siegel →einfache elektronische Signaturen. Nach der Registrierung sind es →fortgeschrittene elektronische Signaturen, die z. B. für elektronische Rechnungen verwendet werden können.
Siegel	Mit →„Trodat Seal“ können →PDF-Dokumente versiegelt werden, d. h. sie werden von einem →Signator mit einer elektronischen →Signatur versehen. Siegel können mit verschiedenen →Sicherheitsstufen erstellt werden. Siegel können in →online (dabei enthält das Siegel auch einen →Zeitstempel) oder →offline erstellt werden. Das Siegel ist sowohl in elektronischer als auch in ausgedruckter Form sichtbar. Z. B. durch Anklicken des Feldes „Click to Verify“ im Siegel kann die Echtheit des Siegels geprüft werden, das Prüfergebnis wird als →Prüfzertifikat ausgegeben (siehe 3.6).
SigG	Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG), BGBl. I Nr. 190/1999 in der geltenden Fassung.



Signator	Die Person, die elektronische →Signaturen, also z. B. →Siegel erstellt. Ein Signator ist immer eine natürliche Person. Bei →„Trodat Seal“ ist jedem Signator eine Lizenz und ein →Account zugeordnet. Alle mit „Trodat Seal“ erstellten Siegel sind einem bestimmten Account, also einem bestimmten Signator zugeordnet. Die Lizenz kann vom Signator selbst erworben werden oder ihm von einem anderen →Kunden (z. B. seinem Arbeitgeber) zur Verfügung gestellt werden.
Signatur	Elektronische Daten, die an ein Dokument angefügt oder mit diesem logisch verknüpft werden, und die der Feststellung der Identität des →Signators dienen. Bei →„Trodat Seal“ wird eine spezielle Form der elektronischen Signatur verwendet, die in →PDF-Dokumente eingebettet und als →Siegel bezeichnet wird. Es gibt verschiedene Sicherheitsstufen von elektronischen Signaturen, unter anderem die →einfache elektronische Signatur und die →fortgeschrittene elektronische Signatur.
Signaturerstellungsdaten	Der juristische Begriff für den →privaten Schlüssel. Der Begriff ist breiter und würde theoretisch auch andere Technologien als die asymmetrische →Kryptographie umfassen.
Signaturprüfdaten	Der juristische Begriff für den →öffentlichen Schlüssel. Der Begriff ist breiter und würde theoretisch auch andere Technologien als die asymmetrische →Kryptographie umfassen.
Signaturrechtlinie	Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen, ABl. L 13 vom 19.1.2000, S. 12. Die Richtlinie gewährleistet die europaweite rechtliche Anerkennung elektronischer →Signaturen
SigV	Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung – SigV), BGBl. II Nr. 30/2000 in der geltenden Fassung
SNTP	Simple Network Time Protocol. Ein Protokoll, mit dem Zeitserver im Internet untereinander synchronisiert werden. Das Protokoll ist in →RFC 2030 standardisiert, es ist eine vereinfachte Variante einer noch nicht standardisierten Version des Network Time Protocol (NTP).
Trodat	Trodat GmbH. →Trosoft, der Anbieter von →„Trodat Seal“, ist eine 100-%-Tochter der Trodat GmbH.



Trodat Seal	Der Markenname des Zertifizierungs- und Zeitstempeldienstes „Trodat Seal“, welcher in diesem Dokument beschrieben wird. „Trodat Seal“ wird von →Trosoft angeboten.
Trosoft	Trosoft Entwicklungs u. Vertriebs GmbH, der Anbieter von →„Trodat Seal“, siehe 1.1.
Webshop	Siehe http://www.trosoft.net/ . Über den Webshop können unter anderem →digitale Tinte und Logos für die Gestaltung der →Siegel erworben werden. Weiters ermöglicht die →Shopfinder-Funktion des Webshops, →Registrierungsstellen zu finden.
Widerruf	Wenn die Sicherheit eines →Accounts beeinträchtigt ist (z. B. weil der →PIN-Code des →Signators ausgespäht wurde) oder wenn sich Daten des Signators (z. B. der Name des Signators oder seine Zuordnung zu einem Unternehmen) geändert haben, dann muss der →Account widerrufen werden. Die Fälle, in denen ein Widerruf vorgenommen werden muss, und die Methoden für den Widerruf, sind in 1.7 und 3.5 beschrieben. Nach einem Widerruf können zu diesem →Account keine weiteren gültigen →Siegel mehr erstellt werden.
X.509	Ein Standard für die Codierung von Zertifikaten und Widerrufslisten (derzeit in →RFC 3280 standardisiert). Die „Trodat Seal Server“ haben X.509-Zertifikate. Die mit →„Trodat Seal“ erstellten →Siegel und →Prüfzertifikate werden nicht nach X.509, sondern nach einer von →Trosoft erstellten Spezifikation erstellt. Bei „Trodat Seal“ werden auch keine Widerrufslisten verwendet, sondern die in 3.6 beschriebene Methode zur Prüfung der Echtheit von Siegeln.
Zeitstempel	Eine elektronisch signierte Bescheinigung, dass bestimmte Daten zu einem bestimmten Zeitpunkt vorgelegen sind. Die in der →Online-Variante von →„Trodat Seal“ erstellten →Siegel enthalten einen von →Trosoft ausgestellten Zeitstempel, mit dem der Zeitpunkt der Erstellung des Siegels bestätigt wird.
Zeitstempeldienst	Eine Dienstleistung, bei der eine unabhängige Stelle →Zeitstempel ausstellt. →„Trodat Seal“ ist ein Zeitstempeldienst.



- Zertifikat** Eine elektronisch signierte Bescheinigung, mit der
→ Signaturprüfdaten einer bestimmten Person zugeordnet und deren Identität bestätigt wird. Bei → „Trodat Seal“ sind sowohl die in der → Online-Variante erstellten → Siegel als auch die → Prüfsertifikate Zertifikate im Sinne des → SigG und der → Signaturrechtlinie
- Zertifizierungsdienst** Eine Dienstleistung, bei der eine unabhängige Stelle
→ Zertifikate ausstellt. → „Trodat Seal“ ist ein Zertifizierungsdienst.

