



Zentrum für sichere Informationstechnologie – Austria Secure Information Technology Center – Austria

A-1030 Wien, Seidlgasse 22 / 9
Tel.: (+43 1) 503 19 63-0
Fax: (+43 1) 503 19 63-66

A-8010 Graz, Inffeldgasse 16a
Tel.: (+43 316) 873-5514
Fax: (+43 316) 873-5520

<http://www.a-sit.at>
E-Mail: office@a-sit.at
ZVR: 948166612

DVR: 1035461

UID: ATU60778947

A-SIT Bestätigungsstelle
Tel.: (+43 1) 503 19 63-0
E-Mail: office@a-sit.at

Merkblatt : Bescheinigungen der Bestätigungsstelle
gemäß § 18 Abs. 5 Signaturgesetz (SigG)

Tätigkeiten der Bestätigungsstelle

A-SIT führt als Bestätigungsstelle (laut § 19 SigG¹) Bescheinigungsverfahren gemäß § 18 Abs. 5 SigG durch. Dies beinhaltet die Durchführung von Prüfungen der sicherheitstechnischen Eignung von Komponenten und Verfahren gemäß § 18 Abs. 5 SigG bzw. gemäß Art. 3 Abs. 4 der EU-Signaturrechtlinie².

Zweck des Merkblatts

Zum Erlangen einer Bescheinigung sind der Bestätigungsstelle im Regelfall technische Dokumente vorzulegen, die sowohl formale als auch inhaltliche Anforderungen erfüllen müssen (siehe (C)).

Das Merkblatt soll den Bescheinigungswerbern die Vorbereitung dieser Dokumente und damit eine zügige Abwicklung des Bescheinigungsverfahrens erleichtern. Dieses Merkblatt enthält generelle Hinweise; die tatsächlichen Erfordernisse hängen vom konkreten Einzelfall ab.

(A) Warum Bescheinigung einer Bestätigungsstelle gemäß § 18 Abs. 5 SigG?

Für die besonders sicherheitsrelevanten Elemente der qualifizierten elektronischen Signatur (sichere Signaturerstellungseinheiten) ist im österreichischen Signaturgesetz (SigG) entsprechend den inhaltlichen Vorgaben der EU-Signaturrechtlinie die Verwendung besonders geprüfter und in ihrer Sicherheit bescheinigter Komponenten und Verfahren vorgesehen.

§ 18 Abs. 5 SigG: Die technischen Komponenten und Verfahren für die Erstellung qualifizierter elektronischer Signaturen müssen nach dem Stand der Technik hinreichend und laufend geprüft sein. Die Erfüllung der Sicherheitsanforderungen an sichere Signaturerstellungseinheiten nach diesem Bundesgesetz und den auf seiner Grundlage ergangenen Verordnungen muss von einer Bestätigungsstelle (§ 19) bescheinigt sein. Bescheinigungen von Stellen, die von anderen Mitgliedstaaten der Europäischen Union oder von anderen Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum zur Beurteilung der Sicherheitsanforderungen für sichere Signaturerstellungseinheiten nach Art. 3 Abs. 4 der Signaturrechtlinie namhaft gemacht wurden, sind den Bescheinigungen einer Bestätigungsstelle gleich zu halten.

¹ Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG, BGBl I Nr. 190/1999 vom 19. August 1999) in der Fassung des Bundesgesetzes BGBl. I Nr. 75/2010 vom 18. August 2010.

² Richtlinie 1999/93/EG des Europäischen Parlaments und des Rates vom 13. Dezember 1999 über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen

Diese Bescheinigungen werden von einer Bestätigungsstelle nach Signaturgesetz ausgestellt und **sind der Meldung der Aufnahme oder Änderung eines Zertifizierungsdienstes bei der Aufsichtsstelle beizubringen.**

(B) Welche Komponenten, Verfahren und Geräte sind der Prozedur der Bescheinigung zu unterziehen?

§ 2 Z. 5 SigG: sichere Signaturerstellungseinheit: eine konfigurierte Software oder Hardware, die zur Verarbeitung der Signaturerstellungsdaten verwendet wird und die den Sicherheitsanforderungen dieses Bundesgesetzes sowie der auf seiner Grundlage erlassenen Verordnungen entspricht;

Die Erfüllung der "Technischen Sicherheitserfordernisse für **Signaturerstellungsdaten** und **-einheiten** bei qualifizierten Signaturen" (vgl. § 3 SigV³) ist durch eine Bescheinigung nachzuweisen. Konkret ist dies für technische Komponenten und Verfahren zur

- a) Erzeugung von Signaturerstellungsdaten,
- b) Speicherung von Signaturerstellungsdaten,
- c) Verarbeitung der Signaturerstellungsdaten

notwendig.

Derartige Komponenten und Verfahren sind bei den Signatoren und bei der Aufsichtsstelle nach den Bestimmungen des Gesetzes notwendig.

Hinweis: Werden solche Komponenten bei Zertifizierungsdiensteanbietern für die Erstellung von qualifizierten Zertifikaten, für die Speicherung von Signaturerstellungsdaten für qualifizierte Zertifikate oder für qualifizierte Zeitstempeldienste eingesetzt, so ist für diese Komponenten keine Bescheinigung nach § 18 Abs. 5 SigG notwendig. Die Bestätigungsstelle kann in diesen Fällen ein Gutachten über die Erfüllung der Sicherheitsanforderungen (nach SigV § 5 Abs. 1 bzw. § 11 Abs. 1) erstellen.

Ein Nachweis der Erfüllung der "Technischen Sicherheitserfordernisse für die **Systemumgebung** der Signaturerstellungseinheit bei qualifizierten Signaturen" (vgl. § 4 SigV) ist nicht vorgesehen⁴.

Dies gilt beispielsweise für Komponenten und Verfahren

- zur Darstellung der zu signierenden Daten,
- zur Autorisierung des Signators gegenüber der sicheren Signaturerstellungseinheit,
- zum Erzeugen des Hashwertes aus den zu signierenden Daten, sowie für
- Chipkartenleser und sonstige Hardware.

(C) Was ist zum Erlangen einer Bescheinigung nach § 18 Abs. 5 SigG erforderlich?

Mit den hier beschriebenen Unterlagen muss in formaler und inhaltlicher Hinsicht der Nachweis erbracht werden, dass die Bestimmungen des Signaturgesetzes und der Signaturverordnung von den vorgelegten Komponenten in der definierten Einsatzumgebung erfüllt werden. Sind die vorgelegten Materialien dazu nicht geeignet, so kann keine positive Bescheinigung ausgestellt werden. Daher werden hier wesentliche Anforderungen an die Art und Qualität der vorzulegenden Materialien dargestellt.

Um eine Bescheinigung zu beantragen, sollte der Antragsteller das entsprechende **Antragsformular** ausfüllen und an A-SIT übermitteln (das Formular ist im Internet in elektronischer Form erhältlich). Es ist notwendig, die Typenbezeichnungen aller HW- und SW-Komponenten aufzulisten, da die Bescheinigung nur für die vorgelegte Konfiguration gültig ist.

Weiters sollten folgende **Unterlagen** eingereicht werden:

³ Verordnung des Bundeskanzlers über elektronische Signaturen (Signaturverordnung 2008 – SigV 2008, BGBl. II Nr. 3/2008 vom 7. Jänner 2008) in der Fassung BGBl. II Nr. 401/2010 vom 9. Dezember 2010.

⁴ Er kann jedoch optional durch ein Gutachten erbracht werden.

- (1) Funktionstüchtiges **Referenzmuster** und dazugehörige Benutzer- bzw. Installations- bzw. Administrator-**Handbücher**.
- (2) **Beschreibung der Produktion und des Lebenszyklus** von der Produktion bis zur Auslieferung an den ZDA/Signator (falls anwendbar der Personalisierung und der Verwendung im Betrieb bis zur Entsorgung). Falls anwendbar⁵, müssen auch alle Anwendungen beschrieben werden, die neben den Signatur- und Zertifizierungsapplikationen auf den gleichen Geräten verarbeitet werden.

Komponenten sind z.B. HW, SW, Betriebssystem, Funktionsbibliotheken/APIs. Anwendungen sollten gesondert dargestellt werden, weil unterschiedliche Hersteller und Lebenszyklen möglich sind und damit andere Dokumente relevant sein könnten. Bei unterschiedlichen Lebenszyklen sollte in jedem Fall ein Konzept vorgelegt werden, welches die Zusammenhänge zwischen Komponenten und darauf laufenden Anwendungen vollständig beschreibt.

Weiters ist es notwendig zu klären, unter welchen Umständen sicherheitsrelevante Änderungen der bescheinigten Konfiguration möglich sind, z.B.: Kann ausführbarer Code nachgeladen werden? Ist dafür ein Schlüssel / eine andere Authentifizierungsinformation erforderlich? Wer hat Zugang zu diesen Authentifizierungsinformationen?

- (3) **Sicherheitsvorgaben**, die von einer Bestätigungsstelle (§ 19 SigG) als geeignet anerkannt werden.

Beispielsweise können Sicherheitsvorgaben nach Common Criteria oder ITSEC als geeignet anerkannt werden. Insbesondere werden durch die Bestätigungsstelle Referenznummern berücksichtigt, die im Amtsblatt der Europäischen Gemeinschaften nach Art. 3 Abs. 5 der Signaturrechtlinie 1999/93/EG veröffentlicht sind (vgl. § 6 Abs. 2) SigV)

- (4) Relevante **Nachweise laut Anhang**

Alle eingereichten Unterlagen sollen in einem **Deckblatt** zum Antrag kurz aber vollständig, mit Referenzen auf eingereichte Unterlagen oder andere relevante Dokumente (inkl. relevante Kapitel/Abschnitte falls angebracht) dargestellt werden.

Hinweise:

Handbücher von Herstellern sind nur dann verwendbar, wenn darin bzw. im Deckblatt nachvollziehbar dargestellt ist, welche Optionen/Parameter tatsächlich zum Einsatz kommen (mit den Referenzen auf die relevanten Abschnitte).

Zertifikate nach Evaluierungsnormen zu einzelnen Komponenten sind allein nicht ausreichend. Es muss der Nachweis erbracht werden, dass die sicherheitsrelevanten Eigenschaften erfüllt werden (z.B. Sicherheitsvorgaben, Zertifizierungsbericht, Evaluierungsunterlagen und -berichte).

Es sind alle weiteren Umstände zu erklären und zu belegen, welche die technisch begründete Entscheidung über die Gültigkeitsdauer der befristeten Bescheinigung beeinflussen könnten.

(D) Was beinhaltet die Bescheinigung?

Bei positivem Abschluss des Verfahrens wird gemäß § 18 Abs. 5 SigG eine Bescheinigung mit folgendem Inhalt ausgestellt:

1. Erfüllung der Anforderungen des SigG und der SigV durch die bescheinigten Komponenten und Verfahren und Auflistung der bescheinigten Kategorien⁶ (Anwendungen, für welche die Bescheinigung gilt).
2. Gültigkeitsdauer der Bescheinigung,

In der Regel ist die Gültigkeitsdauer einer Bescheinigung auf einen Zeitraum von max. 2 Jahren ab Datum der Ausstellung beschränkt. Sollen die Komponenten und Verfahren über diesen Zeitpunkt hinaus verwendet werden, ist eine Erneuerung der Bescheinigung zu erwirken. Sofern sich aus den Erkenntnissen der Technologiebeobachtung Umstände ergeben, die ein vorzeitiges Ablaufen der Bescheinigung erzwingen, kann eine Bescheinigung auch während der Gültigkeitsdauer widerrufen werden.
3. Einsatzbedingungen,
4. Algorithmen und zugehörige Parameter und
5. Prüfstufe und Mechanismenstärke.

⁵ d.h., falls die Anwendungen zum Zeitpunkt der Bescheinigung bekannt sind, ansonsten müssen sie im Sicherheitskonzept des Zertifizierungsdiensteanbieters spezifiziert werden

⁶ siehe auch (B) Lit. a - c

Ergebnis des Bescheinigungsverfahrens ist die schriftliche Bescheinigung sowie ein Bescheinigungsbericht, der an die Aufsichtsstelle ergeht.

Hinweise:

Sofern der Bescheinigungswerber dies nicht ausdrücklich untersagt, wird die positive Bescheinigung auf der Internetseite von A-SIT veröffentlicht.

Sofern eine ausgestellte Bescheinigung während ihrer Gültigkeitsdauer widerrufen wird, wird dies in jedem Fall auf der Internetseite von A-SIT veröffentlicht.

(E) Geheimhaltung durch A-SIT

A-SIT verfolgt eine strenge Politik der Vertraulichkeit.

Das Non-Disclosure Statement (NDS) ist auf der Internetseite von A-SIT verfügbar (http://www.asit.at/pdfs/nds_asit.pdf).

Um den Anforderungen seitens der betroffenen Anbieter gerecht zu sein, wird seitens A-SIT auf Wunsch eine unterfertigte Vertraulichkeitserklärung ausgehändigt, die in der aktuellen Version ebenfalls im Internet verfügbar ist. Andere Non-Disclosure Agreements (NDAs) werden seitens A-SIT nicht eingegangen. Vom Bescheinigungswerber oder seinen Lieferanten selbst erstellte Vertraulichkeitserklärungen bzw. NDAs werden daher nicht notwendig.

Wien, Jänner 2011

A-SIT Zentrum für sichere Informationstechnologie – Austria

Anhang: Erforderliche Nachweise gem. SigG/SigV

für Komponenten und Verfahren zur Erzeugung, Speicherung und Verarbeitung von Signaturerstellungsdaten (sofern anwendbar):

(A1) Nachweise, dass die technischen Komponenten und Verfahren erfolgreich nach den Sicherheitsvorgaben geprüft wurden.

Dies kann beispielsweise durch entsprechende Gutachten, Zertifizierungsberichte, Sicherheitszertifikate, Prüfberichte (Evaluation Technical Report) und ggf. Evaluationsunterlagen erfolgen. Die relevanten Einsatzbedingungen aus den entsprechenden Gutachten werden ggf. in die Bescheinigung aufgenommen. Eine spezifische Vorgabe, von wem Prüfungen der Komponenten und Verfahren durchzuführen sind, gibt es nicht. Auf Wunsch können die notwendigen Prüfungen auch durch die Bestätigungsstelle in Auftrag gegeben werden bzw. durch diese durchgeführt werden. Wird die Prüfung bei der Bestätigungsstelle in Auftrag gegeben, werden die Nachweise im Rahmen des Bescheinigungsverfahrens erbracht. Gemäß § 6 Abs. 3 SigV können Sicherheitsanforderungen, die nach § 6 Abs. 1 technisch sichergestellt werden müssen, in einer kontrollierten Umgebung auch organisatorisch oder technisch-organisatorisch sichergestellt werden. Das Vorliegen solcher Anforderungen ist nachvollziehbar darzulegen. Die Erfüllung dieser Anforderungen wird durch die Bestätigungsstelle geprüft, die zu erbringenden Nachweise werden im Einzelfall bekannt gegeben.

(A2) Nachweis, dass für qualifizierte elektronische Signaturen nur solche Algorithmen und Parameter eingesetzt werden, die die Anforderungen des Anhangs der SigV erfüllen (siehe § 3 Abs. 2 SigV⁷).

Dies beinhaltet eine hinreichend detaillierte Angabe der Algorithmen und verwendeten Parameter und soweit zutreffend des Paddings.

(A3) Nachweis, dass die Signaturerstellungsdaten mit an Sicherheit grenzender Wahrscheinlichkeit nur einmal vorkommen (siehe § 18 Abs. 2 SigG⁸).

Dies beinhaltet eine detaillierte und nachvollziehbare Darstellung der Methoden und Algorithmen für die Schlüsselerzeugung und des verwendeten Zufalls sowie eine genaue Darstellung des qualitätsvollen Zufalls und der Sicherung gegen alterungsbedingte Veränderungen.

(A4) Nachweis, dass die Signaturerstellungsdaten mit hinreichender Sicherheit nicht ableitbar sind (siehe § 18 Abs. 2 SigG⁹).

Dies beinhaltet eine detaillierte Darstellung der Schlüsselorganisation.

(A5) Nachweis, dass die unbefugte Verwendung von Signaturerstellungsdaten verlässlich verhindert wird (siehe § 18 Abs. 1 SigG¹⁰).

Dies beinhaltet auch die allfällig vorhandenen technischen Sicherstellungen der ausschließlichen Anwendbarkeit der Signaturerstellungsdaten durch den Signator.

(A6) Nachweis, dass die Geheimhaltung der Signaturerstellungsdaten sichergestellt ist (siehe § 18 Abs. 2 SigG¹¹).

Dies beinhaltet auch den Nachweis, dass sicherheitstechnische Veränderungen an den Komponenten für den Signator erkennbar sind (d.h. Veränderungen, nach denen die erforderliche Sicherheitsstufe nicht mehr gegeben sein würde).

(A7) Nachweis, dass die Fälschung von Signaturen sowie die Verfälschung signierter Daten zuverlässig erkennbar gemacht werden (siehe § 18 Abs. 1 SigG¹²).

Dies beinhaltet auch den Nachweis, dass sicherheitstechnische Veränderungen an den Komponenten für den Signator erkennbar werden (d.h. Veränderungen, nach denen die erforderliche Sicherheitsstufe nicht mehr gegeben sein würde).

⁷ Es dürfen nur jene Algorithmen und Parameter eingesetzt werden, die die Anforderungen des Anhangs erfüllen. Die Rahmenbedingungen für die technische Sicherheit sind so zu wählen, dass sie dem jeweiligen Stand der Technik entsprechen.

⁸ (...) Die Signaturerstellungsdaten dürfen mit an Sicherheit grenzender Wahrscheinlichkeit nur einmal vorkommen (...).

⁹ (...) Die Signaturerstellungsdaten (...) dürfen weiters mit hinreichender Sicherheit nicht ableitbar sein; (...).

¹⁰ Für die Erzeugung und Speicherung von Signaturerstellungsdaten sowie für die Erstellung qualifizierter Signaturen sind solche technische Komponenten und Verfahren einzusetzen, (...) die die unbefugte Verwendung von Signaturerstellungsdaten verlässlich verhindern.

¹¹ (...) Die Signaturerstellungsdaten (...); ihre Geheimhaltung muss sichergestellt sein.

¹² Für die Erzeugung und Speicherung von Signaturerstellungsdaten sowie für die Erstellung qualifizierter Signaturen sind solche technische Komponenten und Verfahren einzusetzen, die die Fälschung von Signaturen sowie die Verfälschung signierter Daten zuverlässig erkennbar machen (...).