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

A-SIT

Seidlgasse 22 / 9, 1030 Wien
Tel.: +43 1 503 19 63–0
Fax: +43 1 503 19 63–66

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

http://www.a-sit.at
E-Mail: office@a-sit.at

DVR: 1035461
ZVR: 948166612
UID: ATU60778947

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

Merkblatt: Bescheinigungen der Bestätigungsstelle gemäß § 7 Abs. 1 SVG iVm Art. 30 Abs. 3 lit. b eIDAS-VO

Tätigkeiten der Bestätigungsstelle

A-SIT führt als Bestätigungsstelle (laut § 3 Abs. 1 Z 4 SVG[1]) Bescheinigungsverfahren gemäß Art. 30 eIDAS-VO[2] durch. In einem Bescheinigungsverfahren wird die Konformität qualifizierter elektronischer Signatur- und Siegelerstellungseinheiten (QSEE) mit den Anforderungen des Anhangs II der eIDAS-VO geprüft und zertifiziert. Wenn keine Normen für die Sicherheitsbewertung vorliegen, die durch die Kommission im Wege von Durchführungsrechtsakten festgelegt wurden, wird das Verfahren gemäß Art. 30 Abs. 3 lit. b eIDAS-VO durchgeführt und die Gleichwertigkeit des Sicherheitsniveaus wird von der Bestätigungsstelle nach dem Stand der Technik beurteilt.

Zweck des Merkblatts

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

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

(A) Warum Bescheinigung einer Bestätigungsstelle?

Für die Erstellung qualifizierter elektronischer Signaturen sowie qualifizierter elektronischer Siegel ist in der eIDAS-VO die Verwendung besonders geprüfter und in ihrer Sicherheit bescheinigter (zertifizierter) Komponenten und Verfahren (qualifizierte elektronische Signaturerstellungseinheiten bzw. qualifizierte elektronische Siegelerstellungseinheiten) vorgesehen. Die Konformität qualifizierter elektronischer Signaturerstellungseinheiten mit den Anforderungen des Anhangs II der eIDAS-VO wird dabei laut Art. 30 Abs. 1 der eIDAS-VO von geeigneten, von den Mitgliedstaaten benannten öffentlichen oder privaten Stellen (Bestätigungsstellen) bescheinigt bzw. zertifiziert. Die Anforderungen des Art. 30 der eIDAS-VO gelten

[1] Bundesgesetz über elektronische Signaturen und Vertrauensdienste für elektronische Transaktionen (Signatur- und Vertrauensdienstegesetz – SVG, BGBl. I Nr. 50/2016 vom 08.Juli 2016).
[2] Verordnung (EU) Nr. 910/2014 des europäischen Parlaments und des Rates vom 23. Juli 2014 über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt und zur Aufhebung der Richtlinie 1999/93/EG

sinngemäß nach Art. 39 Abs. 2 der eIDAS-VO auch für die Bescheinigung qualifizierter elektronischer Siegelerstellungseinheiten (jeweils als „QSEE“ bzw. „QSEE-Bescheinigung“ bezeichnet).

§ 7 Abs. 1 SVG: Die Konformität qualifizierter elektronischer Signatur- und Siegelerstellungseinheiten mit den Anforderungen des Anhangs II der eIDAS-VO wird durch eine Bestätigungsstelle oder eine in einem anderen Mitgliedstaat der Europäischen Union gemäß Art. 30 Abs. 1 eIDAS-VO benannte Stelle zertifiziert. Sofern eine Zertifizierung gemäß Art. 30 Abs. 3 lit. b eIDAS-VO vorgenommen wird, ist die Gleichwertigkeit des Sicherheitsniveaus von der Bestätigungsstelle oder benannten Stelle nach dem Stand der Technik zu beurteilen. […]

Art. 30 Abs. 3 lit. b eIDAS-VO: Die Zertifizierung nach Absatz 1 beruht auf einem der folgenden Verfahren:

a) […]

b) einem anderen als dem unter Buchstabe a genannten Verfahren, sofern dabei gleichwertige Sicherheitsniveaus angewendet werden und die öffentliche oder private Stelle gemäß Absatz 1 der Kommission dieses Verfahren mitteilt. Dieses Verfahren darf nur angewendet werden, wenn Normen im Sinne des Buchstaben a nicht vorliegen oder ein Sicherheitsbewertungsverfahren im Sinne des Buchstaben a im Gange ist.

Die QSEE-Bescheinigungen sind im Zuge einer Konformitätsbewertung nach Artikel 20 der eIDAS-VO vorzuweisen bzw. der Meldung der Aufnahme oder Änderung eines Vertrauensdienstes bei der Aufsichtsstelle beizubringen.

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

Art. 3 Z 22 eIDAS-VO: „Elektronische Signaturerstellungseinheit“ ist eine konfigurierte Software oder Hardware, die zum Erstellen einer elektronischen Signatur verwendet wird.

Art. 3 Z 23 eIDAS-VO: „Qualifizierte elektronische Signaturerstellungseinheit“ ist eine elektronische Signaturerstellungseinheit, die die Anforderungen des Anhangs II erfüllt.

Art. 3 Z 31 eIDAS-VO: „Elektronische Siegelerstellungseinheit“ ist eine konfigurierte Software oder Hardware, die zum Erstellen eines elektronischen Siegels verwendet wird.

Art. 3 Z 32 eIDAS-VO: „Qualifizierte elektronische Siegelerstellungseinheit“ ist eine elektronische Siegelerstellungseinheit, die die Anforderungen des Anhangs II sinngemäß erfüllt.

Die Erfüllung der (1) "Anforderungen an qualifizierte elektronische Signaturerstellungseinheiten" (vgl. Art. 29 eIDAS-VO) und (2) „Anforderungen an qualifizierte elektronische Siegelerstellungseinheiten“ (vgl. Art. 39 Abs. 1 eIDAS-VO) im Einklang mit den im Anhang des Durchführungsbeschlusses (EU) 2016/650[3] angeführten Normen ist durch eine Bescheinigung nachzuweisen. Konkret ist dies für technische Komponenten und Verfahren zur

a) Erzeugung von Signatur- bzw. Siegelerstellungsdaten,

b) Speicherung von Signatur- bzw. Siegelerstellungsdaten,

c) Verarbeitung der Signatur- bzw. Siegelerstellungsdaten

notwendig.

Die elektronischen Signatur- bzw. Siegelerstellungsdaten können sich dabei (1) vollständig, aber nicht notwendigerweise ausschließlich in der Umgebung des Nutzers (Signator bzw. Siegelersteller) befinden (vgl. Durchführungsbeschluss 2016/650 Art. 1 Abs. 1) oder (2) durch einen qualifizierten Vertrauensdienste-anbieter (qualifizierter VDA) im Namen des Nutzers (Signator bzw. Siegelersteller) verwaltet werden (vgl. Durchführungsbeschluss 2016/650 Art. 1 Abs. 2). Im ersten Fall ist die Bescheinigung bzw. Zertifizierung nach den im Anhang des Durchführungsbeschlusses 2016/650 genannten Normen durchzuführen im zweiten Fall erfolgt die Bescheinigung bzw. Zertifizierung gemäß Artikel 30 Abs. 3 lit. b der eIDAS-VO, und

[3] Durchführungsbeschluss (EU) 2016/650 der Kommission vom 25. April 2016 zur Festlegung von Normen für die Sicherheitsbewertung qualifizierter Signatur- und Siegelerstellungseinheiten gemäß Artikel 30 Absatz 3 und Artikel 39 Absatz 2 der Verordnung (EU) Nr. 910/2014 des Europäischen Parlaments und des Rates über elektronische Identifizierung und Vertrauensdienste für elektronische Transaktionen im Binnenmarkt

es werden durch die Bestätigungsstelle gleichwertige Sicherheitsniveaus gemäß Artikel 30 Abs. 3 lit. a angewendet.

Ein Nachweis der Erfüllung von Anforderungen an die **Systemumgebung** ist nicht vorgesehen[4] (vgl. Erwägungsgrund 56 der eIDAS-VO).

Dies gilt beispielsweise für Komponenten und Verfahren

- zur Darstellung der zu signierenden bzw. zu besiegelnden Daten,
- zur Autorisierung des Signators bzw. Siegelerstellers gegenüber der qualifizierten elektronischen Signatur- bzw. Siegelerstellungseinheit,
- zum Erzeugen des Hashwertes aus den zu signierenden bzw. zu besiegelnden Daten, sowie für
- Chipkartenleser und sonstige Hardware.

(C) Was ist zum Erlangen einer QSEE-Bescheinigung erforderlich?

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

Um eine QSEE-Bescheinigung zu beantragen, sollte der Antragsteller das entsprechende **Antragsformular** ausfüllen und an A-SIT übermitteln. Es ist notwendig, die Typenbezeichnungen aller HW- und SW-Komponenten aufzulisten, da die QSEE-Bescheinigung nur für die vorgelegte Konfiguration gültig ist.

Weiters sollten folgende **Unterlagen** eingereicht werden:

(1) Funktionstüchtiges **Referenzmuster** (bzw. Zugang zu einer Referenzinstallation) und dazugehörige Benutzer- bzw. Installations- und Administrator-**Handbücher.**

(2) **Beschreibung der Produktion und des Lebenszyklus** von der Produktion bis zur Auslieferung an den qualifizierten VDA oder Signator/Siegelersteller (falls anwendbar der Personalisierung und der Verwendung im Betrieb bis zur Entsorgung). Falls anwendbar[5], müssen auch alle Anwendungen beschrieben werden, die neben den Signatur- und Siegelerstellungsapplikationen 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 Authentifizierungs-information erforderlich? Wer hat Zugang zu diesen Authentifizierungsinformationen?

(3) **Sicherheitsvorgaben**, die von einer Bestätigungsstelle (§ 3 Abs. 1 Z. 4 SVG) als geeignet anerkannt werden.

Insbesondere können Sicherheitsvorgaben nach Common Criteria oder ISO/IEC 18045 (vgl. Durchführungsbeschluss (EU) 2016/650) als geeignet anerkannt werden.

Die Vorlage von Zertifizierungsberichten der Komponenten zur Erzeugung, Speicherung und Verarbeitung von Signatur- bzw. Siegelerstellungsdaten ist nicht Bedingung zur Erlangung einer QSEE-Bescheinigung, beschleunigt aber das Verfahren zur zwingend notwendigen Bewertung der Gleichwertigkeit des Sicherheitsniveaus zu den nach eIDAS-VO Artikel 30 Abs. 3 lit a. festgelegten Standards. Ebenso vereinfacht ein Ausrichten der Sicherheitsvorgaben an die nach eIDAS-VO Artikel 30 Abs. 3 lit a. festgelegten Standards diese Bewertung, ist aber im Sinne eIDAS-VO Artikel 30 Abs. 3 lit b. nicht Bedingung.

(4) Relevante **Nachweise laut Anhang**

[4] Er kann jedoch optional durch ein Gutachten erbracht werden.
[5] d.h., falls die Anwendungen zum Zeitpunkt der Bescheinigung bekannt sind, ansonsten müssen sie im Sicherheitskonzept des Vertrauensdiensteanbieters spezifiziert werden

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[6] 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 QSEE-Bescheinigung beeinflussen könnten.

(D) Was beinhaltet die Bescheinigung?

Bei positivem Abschluss des Verfahrens wird gemäß § 7 Abs. 1 SVG iVm Art. 30 Abs. 3 lit. b eIDAS-VO eine QSEE-Bescheinigung mit folgendem Inhalt ausgestellt:

1. Erfüllung der Anforderungen der eIDAS-VO und des SVG durch die bescheinigten Komponenten und Verfahren und Auflistung der bescheinigten Kategorien[7] (Anwendungen, für welche die Bescheinigung gilt).
2. Gültigkeitsdauer der Bescheinigung,

   In der Regel werden die QSEE-Bescheinigungen bis auf Widerruf ausgestellt. A-SIT führt nach Ausstellung einer QSEE-Bescheinigung eine laufende Evidenthaltung von Bescheinigungen und ein Monitoring hinsichtlich der Sicherheit der eingesetzten Produkte und Verfahren sowie der kryptografischen Algorithmen und Parameter durch. Sofern sich aus den Erkenntnissen der Technologiebeobachtung Umstände ergeben, die ein Ablaufen der QSEE-Bescheinigung erzwingen, wird die Bescheinigung durch A-SIT widerrufen. Mit der erstmaligen Ausstellung einer QSEE-Bescheinigung ist ein Monitoring für zwei Jahre verbunden und im Entgelt enthalten. Für ein über diesen Zeitraum hinausgehendes Monitoring ist eine weitere Beauftragung erforderlich, ansonsten wird die Bescheinigung von A-SIT zurückgezogen.
3. Einsatzbedingungen,
4. Algorithmen und zugehörige Parameter und
5. Prüfstufe und Mechanismenstärke.

Ergebnis des Bescheinigungsverfahrens ist die schriftliche QSEE-Bescheinigung sowie ein Bescheinigungsbericht, der die detaillierten Prüfungsergebnisse enthält.

Der Bescheinigungsbericht geht auf vorgenannte Punkte (1. Erfüllung der Anforderungen der eIDAS-VO bis 5. Prüfstufe und Mechanismenstärke) detailliert ein. Insbesondere werden die Anforderungen aus eIDAS-VO Anhang II einzeln behandelt (vgl. auch Anhang zu erforderlichen Nachweisen).

Hinweise:

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

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

In jedem Fall werden neu ausgestellte und zurückgezogene QSEE-Bescheinigungen gemäß Artikel 31 Abs. 1 eIDAS-VO an die Europäische Kommission gemeldet, die für die Aufstellung, Veröffentlichung und

[6] Anmerkung: Dabei handelt es sich beispielsweise um die exakte Angabe (Mindestlängen kryptografischer Schlüssel etc.) der verwendeten kryptografischen Mechanismen (insbesondere an Hand von „SOG-IS Crypto Evaluation Scheme – Agreed Cryptographic Mechanisms, https://www.sogis.org)

[7] siehe auch (B) Lit. a - c

Führung einer Liste zertifizierter qualifizierter elektronischer Signatur- und Siegelerstellungseinheiten sorgt. Die Notifizierung erfolgt durch die Aufsichtsstelle.

(E) Geheimhaltung durch A-SIT

A-SIT verfolgt eine strenge Politik der Vertraulichkeit.

Das Non-Disclosure Statement (NDS) ist auf der Webseite von A-SIT verfügbar (https://www.a-sit.at/pdfs/nds_asit.pdf).

Um den Anforderungen seitens der betroffenen Anbieter gerecht zu sein, wird seitens A-SIT auf Wunsch eine unterfertigte Fassung des NDS ausgehändigt. 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, Oktober 2017

A-SIT Zentrum für sichere Informationstechnologie – Austria

SIGNATURINFORMATIONEN	**Unterzeichner**	Reinhard Posch
	Datum/Zeit-UTC	2017-10-24T23:41:37+02:00
	Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at
Hinweis	Dieses mit einer qualifizierten elektronischen Signatur versehene Dokument hat gemäß Art. 25 Abs. 2 der Verordnung (EU) Nr. 910/2014 vom 23. Juli 2014 ("eIDAS-VO") die gleiche Rechtswirkung wie ein handschriftlich unterschriebenes Dokument.	

Anhang: Erforderliche Nachweise gem. eIDAS-VO

für Komponenten und Verfahren zur Erzeugung, Speicherung und Verarbeitung von Signatur- oder Siegelerstellungsdaten (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.

Sicherheitsanforderungen, die bei elektronischen Signaturen bzw. elektronischen Siegeln, welche vollständig in der Umgebung des Nutzers erstellt werden, technisch sichergestellt werden müssen, können bei elektronischen Fernsignaturdiensten in der kontrollierten Umgebung eines qualifizierten Vertrauensdiensteanbieters auch organisatorisch oder technisch-organisatorisch sichergestellt werden (vgl. Erwägungsgrund 52 der eIDAS-VO). 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 bzw. qualifizierte elektronische Siegel nur solche Algorithmen und Parameter eingesetzt werden, die im Einklang mit den Normen für die Sicherheitsbewertung, die gemäß Artikel 30 Abs. 3 lit. a eIDAS-VO gelten, stehen und dem Stand der Technik entsprechen.

Dies beinhaltet eine hinreichend detaillierte Angabe der Algorithmen und verwendeten Parameter (Mindestlängen kryptografischer Schlüssel etc.) sowie soweit zutreffend des Paddings. Die Bewertung des Stands der Technik erfolgt an Hand von anerkannten Kryptokatalogen (insbesondere „SOG-IS Crypto Evaluation Scheme – Agreed Cryptographic Mechanisms, https://www.sogis.org).

(A3) Nachweis, dass die Vertraulichkeit der Signatur- bzw. Siegelerstellungsdaten sichergestellt ist (siehe Anhang II Abs. 1 lit. a eIDAS-VO).

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

(A4) Nachweis, dass die Signatur- bzw. Siegelerstellungsdaten mit an Sicherheit grenzender Wahrscheinlichkeit nur einmal vorkommen (siehe Anhang II Abs. 1 lit. b eIDAS-VO).

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.

(A5) Nachweis, dass die Signatur- bzw. Siegelerstellungsdaten mit hinreichender Sicherheit nicht ableitbar sind (siehe Anhang II Abs. 1 lit. c eIDAS-VO).

Dies beinhaltet eine detaillierte Darstellung der Schlüsselorganisation.

(A6) Nachweis, dass die elektronische Signatur bzw. das elektronische Siegel bei Verwendung der jeweils verfügbaren Technik verlässlich gegen Fälschung geschützt ist (siehe Anhang II Abs. 1 lit. c eIDAS-VO).

Dies beinhaltet auch den Nachweis, dass die Fälschung von Signaturen bzw. Siegeln zuverlässig erkennbar gemacht werden und sicherheitstechnische Veränderungen an den Komponenten für den Signator bzw. Siegelersteller erkennbar werden (d.h. Veränderungen, nach denen die erforderliche Sicherheitsstufe nicht mehr gegeben sein würde).

(A7) Nachweis, dass die unbefugte Verwendung von Signatur- bzw. Siegelerstellungsdaten verlässlich verhindert wird (siehe Anhang II Abs. 1 lit. d eIDAS-VO).

Dies beinhaltet auch die allfällig vorhandenen technischen Sicherstellungen der ausschließlichen Anwendbarkeit der Signatur- bzw. Siegelerstellungsdaten durch den Signator bzw. Siegelersteller.

(A8) Nachweis, dass die zu unterzeichnenden Daten durch die qualifizierte elektronische Signatur- bzw. Siegelerstellungseinheit nicht verändert werden (Anhang II Abs. 2 eIDAS-VO)

Dies beinhaltet auch den Nachweis, dass die Verfälschung signierter bzw. besiegelter Daten zuverlässig erkennbar gemacht und sicherheitstechnische Veränderungen an den Komponenten für den Signator bzw. Siegelersteller erkennbar werden (d.h. Veränderungen, nach denen die erforderliche Sicherheitsstufe nicht mehr gegeben sein würde).

(A9) Nachweis, dass die qualifizierte elektronische Signatur- bzw. Siegelerstellungseinheit nicht verhindert, dass dem Signator bzw. Siegelersteller die zu unterzeichnenden Daten vor dem Unterzeichnen angezeigt werden (Anhang II Abs. 2 eIDAS-VO).

Dies beinhaltet eine Beschreibung der Anwendung der Signatur- bzw. Siegelerstellungseinheit (nachvollziehbare Darstellung des Signatur- bzw. Siegelprozesses).

Im Fall von elektronischen Fernsignaturdiensten:

(A10) Nachweis, dass das Erzeugen und Verwalten von elektronischen Signatur- bzw. Siegelerstellungsdaten im Namen eines Signators bzw. Siegelerstellers nur von einem qualifizierten Vertrauensdiensteanbieter durchgeführt wird (Anhang II Abs. 3 eIDAS-VO).

Dies beinhaltet eine detaillierte Beschreibung der vorgesehenen Einsatzumgebung der Signatur- bzw. Siegelerstellungseinheit.

(A11) Nachweis, dass elektronische Signatur- bzw. Siegelerstellungsdaten ausschließlich zu Sicherungszwecken kopiert werden und dies unter Einhaltung der Anforderungen nach eIDAS-VO Anhang II Abs. 4 lit. a und b erfolgt (Anhang II Abs. 4 eIDAS-VO).

Dies beinhaltet eine detaillierte Beschreibung der vorgesehen Backup und Redundanz-Mechanismen.