

Time-Stamp Policy und TSA Practice Statement der Zertifizierungsstelle der Bundesnotarkammer

Version: 1.0.
Datum: 20. Juni 2017

Dokumenthistorie

Version	Anmerkung	Datum
1.0	Erstellung des Dokuments im Rahmen der Prüfung der Einhaltung der Vorgaben der Verordnung (EU) Nr. 910/2014 des europäischen Parlamentes 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 (eIDAS-VO) durch eine akkreditierte Konformitätsbewertungsstelle	20.06.2017

Inhalt

1.	Einleitung.....	5
1.1.	Über dieses Dokument	5
1.2.	Identifizierung	5
2.	Definitionen und Abkürzungen	5
3.	Überblick	6
3.1.	Zeitstempeldienste.....	6
3.2.	Zeitstempelanbieter (Time Stamping Authority – TSA)	6
3.3.	Nutzer des Zeitstempeldienstes (Subscriber)	6
4.	Richtlinien und Verfahren	7
4.1.	Risikoanalyse.....	7
4.2.	Trust Service Practice Statement	7
4.2.1.	Format des Zeitstempels.....	7
4.2.2.	Genauigkeit der Zeit	7
4.2.3.	Beschränkungen der Nutzung des Zeitstempeldienstes	7
4.2.4.	Pflichten der Nutzer	7
4.2.5.	Verifikation des Zeitstempels	8
4.2.6.	Anwendbares Recht	8
4.2.7.	Verfügbarkeit des Zeitstempeldienstes	8
4.3.	Allgemeine Geschäftsbedingungen.....	8
4.4.	Informationssicherheitsrichtlinie.....	8
4.5.	Pflichten des Zeitstempelanbieters	8
4.6.	Informationen für Vertrauende Dritte.....	9
5.	Verwaltung und Nutzung des Zeitstempeldienstes.....	9
5.1.	Interne Organisation	9
5.2.	Personalkonzept.....	9
5.3.	Asset Management.....	9
5.4.	Zugriffskontrolle.....	10
5.5.	Kryptographische Kontrolle	10
5.5.1.	Schlüsselgenerierung	10
5.5.2.	Schutz des privaten Schlüssels.....	10

5.5.3.	Schlüssellängen.....	10
5.5.4.	Schlüsselparameter und Qualitätskontrolle der Parameter.....	11
5.5.5.	Schlüsselverwendung.....	11
5.5.6.	Gültigkeitsdauer von Schlüssel und Zertifikaten	11
5.6.	Nicht-technische Sicherheitsmaßnahmen	11
5.7.	Technische Sicherheitsmaßnahmen.....	11
5.8.	Netzwerksicherheit.....	11
5.9.	Notfallkonzept	12
5.10.	Archivierung von Unterlagen	12
5.10.1.	TSU Schlüsselverwaltung.....	12
5.10.2.	Synchronisation der Uhrzeit.....	12
5.11.	Business Continuity Management.....	12
5.12.	Beendigungsplan.....	12
5.13.	Konformität	12

1. Einleitung

1.1. Über dieses Dokument

Die Bundesnotarkammer ist akkreditierter Zertifizierungsdiensteanbieter i.S.d. § 15 SigG sowie qualifizierter Vertrauensdiensteanbieter i.S.d. Art. 21 Abs. 2 der VO (EU) Nr. 910/2014. Angebotene Dienste sind die Ausgabe von qualifizierten Zertifikaten und qualifizierten Zeitstempeln.

Dieses Dokument beschreibt die Vertrauensdiensterrichtlinie der Zertifizierungsstelle der Bundesnotarkammer (auch Vertrauensdiensteanbieter Bundesnotarkammer – kurz **VDA BNotK**) für qualifizierte elektronische Zeitstempel. Es stellt in Form einer Time-Stamp Policy sowie eines TSA Practice Statements dar, wie der VDA BNotK die Anforderungen und Vorgaben für die Erbringung der Zeitstempeldienste erfüllt.

Dieses Dokument nimmt Bezug auf die Zertifikatsrichtlinie der Zertifizierungsstelle der Bundesnotarkammer mit der OID 1.3.6.1.4.1.41460.5.1.1.1.1.1.0 sowie die ETSI Normen EN 319 401, EN 319 411-2 und EN 319 421.

Die Gliederung des Dokuments basiert auf der Norm ETSI EN 319 421, um einen Vergleich mit entsprechenden Richtlinien anderer Vertrauensdiensteanbieter zu erleichtern.

Maßgeblich ist allein die deutsche Fassung dieser Richtlinie. Bei Abweichungen zwischen der deutschen und der englischen Fassung dieses Dokuments, gilt daher ausschließlich die deutsche Fassung.

Diese Richtlinie ist nicht rechtsverbindlich. Für das Verhältnis zwischen VDA BNotK und dem Nutzer des Zeitstempeldienstes bzw. dem Vertrauenden Dritten sind vielmehr ausschließlich die vertraglichen oder, bei Fehlen eines Vertragsverhältnisses, die gesetzlichen Bestimmungen maßgeblich. Soweit nicht ausdrücklich anders vermerkt, beinhaltet diese Richtlinie keine Zusicherungen, Garantien oder Gewährleistungen.

1.2. Identifizierung

Dokumentenname: TSA Policy und Practice Statement der Zertifizierungsstelle der Bundesnotarkammer

Kennzeichnung (OID): 1.3.6.1.4.1.41460.5.4.1.1.2.1.0

Version: 1.0

2. Definitionen und Abkürzungen

Begriff	Beschreibung
TSA	Siehe Zeitstempelanbieter
Zeitstempelanbieter	Vertrauensdiensteanbieter, der (qualifizierte) elektronische Zeitstempel anbietet.

Siehe ferner Abschnitt 2.4 der Zertifikatsrichtlinie (CP) der Zertifizierungsstelle der Bundesnotarkammer.

3. Überblick

3.1. Zeitstempeldienste

Der VDA BNotK erstellt nur qualifizierte elektronische Zeitstempel.

Die angebotenen Zeitstempeldienste werden in dieser Richtlinie in zwei Bestandteile unterteilt:

► **Bereitstellung von Zeitstempeln**

Die Erstellung von Zeitstempeln.

► **Verwaltung von Zeitstempeln**

Die Überwachung und Kontrolle des Betriebs der Zeitstempeldienste, um sicherzustellen, dass die Dienste wie in dieser Richtlinie vorgegeben bereitgestellt werden. Dieser Dienst ist sowohl für die Implementierung als auch für Änderungen oder Einstellungen der Zeitstempeldienste zuständig.

Diese Unterteilung erfolgt nur für die Zwecke dieser Richtlinie und stellt keine Beschränkung der (internen) Organisation des Zeitstempeldienstes durch den VDA BNotK dar.

3.2. Zeitstempelanbieter (Time Stamping Authority – TSA)

Der VDA BNotK (nachfolgend auch als **Zeitstempelanbieter** bezeichnet) ist in seiner Eigenschaft als Zeitstempelanbieter für die Bereitstellung der in Abschnitt 3.1 genannten Dienste zuständig.

Der VDA BNotK kann Aufgaben auf Dritte übertragen. Auch bei der Übertragung von Aufgaben auf Dritte verbleibt die Gesamtverantwortung für den Betrieb des Vertrauensdienstes in der Hand des VDA BNotK. Vgl. zur Übertragung von Aufgaben auf Dritte Abschnitt 1.7. der Zertifikatsrichtlinie der Zertifizierungsstelle der Bundesnotarkammer.

3.3. Nutzer des Zeitstempeldienstes (Subscriber)

Der VDA BNotK stellt qualifizierte elektronische Zeitstempel nicht unmittelbar an Endnutzer zur Verfügung. In ausgewählten Einzelfällen werden qualifizierte elektronische Zeitstempel bzw. Zeitstempeldienste Dritten zur Verfügung gestellt, die diese ggf. Endnutzern zur Verfügung stellen. In diesem Fall ist der Dritte für die Information der Endnutzer verantwortlich sowie dafür, dass die Endnutzer ihren Pflichten nachkommen.

4. Richtlinien und Verfahren

4.1. Risikoanalyse

Der VDA BNotK führt eine regelmäßige Risikoanalyse durch, um die Risiken für die angebotenen Vertrauensdienste zu identifizieren, zu analysieren und zu bewerten. Einzelheiten sind im Sicherheitskonzept des VDA BNotK niedergelegt. Vgl. dazu Abschnitt 8. der Zertifikatsrichtlinie der Zertifizierungsstelle der Bundesnotarkammer.

4.2. Trust Service Practice Statement

4.2.1. Format des Zeitstempels

Der eingesetzte Zeitstempeldienst ist nach dem Signaturgesetz bestätigt, konform zu RFC 3161 unter Beachtung der ETSI EN 319 422 und unterstützt ausschließlich RSA Verschlüsselung mit 2048 bit und dem SHA256 Hash Algorithmus.

4.2.2. Genauigkeit der Zeit

Als verlässliche Zeitquelle werden Zeitserver mit einem DFC77-Epfänger genutzt, um die die gesetzlich gültige Zeit von der Physikalisch Technischen Bundesanstalt zu empfangen. Bei temporärem Signalverlust übernimmt ein hochgenauer Oszillator die Aufgabe des Zeitgebers für den NTP-Server. Als zusätzliche Referenzquelle sind weitere NTP-Server der Physikalisch Technischen Bundesanstalt eingebunden. Die durchschnittliche maximale Abweichung der Zeit liegt bei +/- 100 ms und ist in keinem Fall größer als eine Sekunde. Die Einhaltung der genauen Uhrzeit, sowie Änderungen und Manipulationsversuche an der Uhrzeit werden fortlaufend überwacht. Bei Überschreitung der maximal erlaubten Abweichung wird der Zeitstempeldienst automatisch deaktiviert. Schaltsekunden werden berücksichtigt, korrekt verarbeitet und protokolliert.

Vgl. Abschnitte 5.7. bis 5.9. zu den technischen und nicht-technischen Sicherheitsmaßnahmen gegen Angriffe und Manipulationsversuche der Uhrzeit.

4.2.3. Beschränkungen der Nutzung des Zeitstempeldienstes

Es gelten die gesetzlichen Bestimmungen, insbesondere etwaige Vorgaben der eIDAS-VO, des Signaturgesetzes und der Signaturverordnung..

4.2.4. Pflichten der Nutzer

Es gelten die gesetzlichen Bestimmungen, insbesondere etwaige Vorgaben der eIDAS-VO, des Signaturgesetzes und der Signaturverordnung.

Bitte beachten Sie, dass der VDA BNotK grundsätzlich keine Zeitstempeldienste unmittelbar an Endanwender zur Verfügung stellt.

4.2.5. Verifikation des Zeitstempels

Die Überprüfung des Zeitstempels erfordert die folgenden Schritte:

- ▶ **1. Verifikation des Ausstellers des Zeitstempels**
Zur Prüfung des Ausstellers wird der öffentliche Schlüssel der signierenden CA benötigt. Dieser kann auf der TSL und der Webseite heruntergeladen werden.
- ▶ **2. Verifikation des Status des Zeitstempels**
Die Prüfung des Zertifikatsstatus der signierenden CA erfolgt über einen OCSP-Responder. Die Adresse des OCSP-Responders ist Teil des Zertifikats.
- ▶ **3. Verifikation der Integrität des Zeitstempels**
Die Integrität des Zeitstempels lässt sich mit jeder RFC 3161 konformen Software prüfen.

4.2.6. Anwendbares Recht

Der VDA BNotK erfüllt die Voraussetzungen für die Erbringung eines Zeitstempeldienstes nach deutschem Recht.

4.2.7. Verfügbarkeit des Zeitstempeldienstes

Der Zeitstempeldienst wird auf hochverfügbaren IT-Systemen in einem hochverfügbaren Rechenzentrum betrieben, um eine jederzeitige Verfügbarkeit des Zeitstempeldienstes zu erreichen. Es gilt die mit dem VDA BNotK geschlossene einzelvertragliche Vereinbarung zur garantierten Verfügbarkeit.

4.3. Allgemeine Geschäftsbedingungen

Es gilt die mit dem VDA BNotK geschlossene einzelvertragliche Vereinbarung.

4.4. Informationssicherheitsrichtlinie

Siehe dazu Abschnitt 5.1. der Zertifikatsrichtlinie der Zertifizierungsstelle der Bundesnotarkammer.

4.5. Pflichten des Zeitstempelanbieters

Es gilt die mit dem VDA BNotK geschlossene einzelvertragliche Vereinbarung oder, bei Fehlen einer vertraglichen Vereinbarung, die gesetzlichen Bestimmungen.

Diese Richtlinie begründet keine zusätzlichen Pflichten des VA BNotK, insbesondere enthält dieses Dokument keine Zusicherungen, Garantien oder Gewährleistungen.

4.6. Informationen für Vertrauende Dritte

Dieses Dokument sowie die Zertifikatsrichtlinie der der Zertifizierungsstelle der Bundesnotarkammer werden Dritten durch Veröffentlichung auf der Website des VDA BNotK zugänglich gemacht.

Vertrauende Dritte dürfen nur dann auf einen Zeitstempel des VDA BNotK vertrauen, wenn zumindest folgende Voraussetzungen vorliegen:

- ▶ der Zeitstempel wurde ordnungsgemäß signiert und der zur Signierung des Zeitstempels verwendete private Schlüssel wurde bis zum Zeitpunkt der Verifikation des Zeitstempels nicht kompromittiert,
- ▶ eventuelle Einschränkungen der Nutzung wurden beachtet,
- ▶ alle weiteren Vereinbarungen und sonstigen Vorsichtsmaßnahmen wurden eingehalten,
- ▶ der Vertrauende Dritte hat die maßgebliche Vertrauensliste genutzt, um festzustellen, dass der Zeitstempel und die Zeitstempel Einheit (**TSU**) qualifiziert sind.

5. Verwaltung und Nutzung des Zeitstempeldienstes

5.1. Interne Organisation

Der VDA BNotK ist eine Körperschaft des öffentlichen Rechts nach deutschem Recht.

Der VDA BNotK verfügt über ein vertrauliches Sicherheitskonzept, in dem die betrieblichen Anforderungen unter anderem betreffend das Personal, die Zugriffskontrolle und die Risikobewertung niedergelegt sind.

Der VDA BNotK verfügt über zuverlässiges und qualifiziertes Personal in ausreichender Anzahl. Das eingesetzte Personal besitzt die für ihre Aufgaben notwendige Fachkunde, Erfahrungen und Qualifikationen und wird vor Übernahme einer Aufgabe und während der Tätigkeit geschult.

5.2. Personalkonzept

Im Personal- und Rollenkonzept des VDA BNotK sind zum einen die personellen Maßnahmen für den Betrieb von Zertifizierungsdiensten und zum anderen die Rollenverteilung innerhalb des VDA BNotK festgelegt. Es werden alle für den Zertifizierungsbetrieb erforderlichen Rollen identifiziert und festgelegt und ihre Aufgaben beschrieben.

Einzelheiten sind in Abschnitt 5.3 des Zertifizierungskonzepts der Zertifizierungsstelle der Bundesnotarkammer beschrieben.

5.3. Asset Management

Der VDA BNotK hat ein gesetzlichen Anforderungen entsprechendes Asset Management eingeführt.

Einzelheiten sind in Abschnitt 5.2. der Zertifikatsrichtlinie der Zertifizierungsstelle der Bundesnotarkammer beschrieben.

5.4. Zugriffskontrolle

Siehe dazu Abschnitte 5.1., 5.4. und 6.5. des Zertifizierungskonzepts der Zertifizierungsstelle der Bundesnotarkammer.

5.5. Kryptographische Kontrolle

Alle für qualifizierten Zeitstempel genutzten Schlüssel und die darauf basierenden Zertifikate sind auf zertifizierten SSEEs gespeichert. Die SSEEs werden in einem sicheren Umfeld gemäß der Einsatzumgebung der Zertifizierung der SSEEs betrieben.

5.5.1. Schlüsselgenerierung

Schlüssel für Zeitstempel werden in einer sicheren Umgebung nach Vorgaben des Herstellers und unter Einhaltung der zertifizierten Bedingungen auf einer nach dem Signaturgesetz zugelassenen SSEE, die gemäß den Common-Criteria-Vorgaben evaluiert wurde, den Bestimmungen des § 17 SigG entspricht und auf der EU-Liste der vertrauenswürdigen zertifizierten Komponenten steht, generiert. Aussteller der Root-CA ist die Bundesnetzagentur. Der Prozess und die Aktivierung des Schlüssels wird von Personen mit den entsprechenden Rollen laut Rollenkonzept (Vergleiche Abschnitt 5.2) im Vier-Augen-Prinzip in einer sicheren Umgebung durchgeführt. Die öffentlichen Zertifikate, die auf den Schlüsseln basieren, werden auf der Webseite des VDA BNotK unter der folgenden Adresse veröffentlicht: <https://zertifizierungsstelle.bnotk.de/veroeffentlichungen>. Darüber hinaus sind sie auch auf den Seiten der Bundesnetzagentur und auf der deutschen Trusted List veröffentlicht. Der Prozess zur Schlüsselgenerierung wird rechtzeitig vor Ablauf der Gültigkeit der Schlüssel wiederholt, um einen reibungslosen Übergang zu gewährleisten. Um sicherzustellen, dass dies rechtzeitig erfolgt, wird die Gültigkeit der Schlüssel durch ein Monitoring-System überwacht.

5.5.2. Schutz des privaten Schlüssels

Der private Schlüssel für Zeitstempel ist auf einer SSEE gespeichert und nicht extrahierbar. Es existieren keine Backups. Die SSEE werden in einer sicheren, zutrittsgeschützten Umgebung betrieben. Nur berechtigte Personen laut Rollenkonzept haben Zugriff auf die SSEE. Der Zugriff kann nur im Vier-Augen-Prinzip erfolgen.

5.5.3. Schlüssellängen

Für die Schlüssellänge gilt die jeweils gültige Vorgabe aus dem vorgeschriebenen Algorithmenkatalog der BNetzA. Die momentan verwendeten Schlüssel haben eine Länge von 2048 Bit.

5.5.4. Schlüsselparameter und Qualitätskontrolle der Parameter

Die Schlüsselparameter und die eingesetzten SSEE richten sich nach der jeweils gültigen Vorgabe aus dem vorgeschriebenen Algorithmenkatalog der BNetZA bzw. den Bestätigungsdokumenten der SSEE. Die Einhaltung der Vorgaben wird kontinuierlich von einer dafür verantwortlichen Person geprüft.

5.5.5. Schlüsselverwendung

Die Schlüssel werden ausschließlich zum Signieren von Zeitstempeln verwendet. Der Verwendungszweck ist im X.509 Zertifikat des Schlüssels hinterlegt.

5.5.6. Gültigkeitsdauer von Schlüssel und Zertifikaten

Die Gültigkeitsdauer der Schlüsselpaare und darauf basierenden Zertifikate entspricht maximal der erlaubten Gültigkeit für qualifizierte Zertifikate nach dem Algorithmenkatalog der BNetZA. Beim Auslaufen der Eignung eines eingesetzten Algorithmus oder der eingesetzten SSEE werden die Schlüssel vor Ablauf der Zertifikatsgültigkeit gesperrt. Nach Ablauf der Gültigkeit werden die SSEE zerstört.

Nach Ablauf der Gültigkeit des privaten Schlüssels ist ein Ausstellen von Zeitstempeln nicht mehr möglich,.

5.6. Nicht-technische Sicherheitsmaßnahmen

Der VDA BNotK hat den gesetzlichen Anforderungen entsprechende nicht-technische Sicherheitsmaßnahmen eingeführt.

Einzelheiten sind in Abschnitt 5. des Zertifizierungskonzepts der Zertifizierungsstelle der Bundesnotarkammer beschrieben.

5.7. Technische Sicherheitsmaßnahmen

Der VDA BNotK hat den gesetzlichen Anforderungen entsprechende technische Sicherheitsmaßnahmen eingeführt.

Einzelheiten sind in Abschnitt 6. des Zertifizierungskonzepts der Zertifizierungsstelle der Bundesnotarkammer beschrieben.

5.8. Netzwerksicherheit

Der VDA BNotK hat den gesetzlichen Anforderungen entsprechende Maßnahmen zur Netzwerksicherheit eingeführt.

Einzelheiten sind in Abschnitt 6.7. des Zertifizierungskonzepts der Zertifizierungsstelle der Bundesnotarkammer beschrieben.

5.9. Notfallkonzept

Der VDA BNotK verfügt über ein Notfallkonzept.

Einzelheiten sind in Abschnitt 5.7. des Zertifizierungskonzepts der Zertifizierungsstelle der Bundesnotarkammer beschrieben.

5.10. Archivierung von Unterlagen

Der VDA BNotK archiviert Unterlagen gemäß der gesetzlichen Anforderungen. Einzelheiten sind in Abschnitt 5.5. des Zertifizierungskonzepts der Zertifizierungsstelle der Bundesnotarkammer beschrieben

Speziell für den Zeitstempeldienst gilt:

5.10.1. TSU Schlüsselverwaltung

Alle Ereignisse betreffend (i) den Lebenszyklus (life-cycle) des TSU-Schlüssels sowie (ii) des TSU-Zertifikats (falls erforderlich) werden protokolliert.

5.10.2. Synchronisation der Uhrzeit

Alle Ereignisse betreffend (i) die Synchronisation der Uhr des TSU und der UTC sowie (ii) die Erkennung von Synchronisierungsverluste werden protokolliert.

5.11. Business Continuity Management

Der VDA BNotK verfügt über ein Notfallkonzept. Im Fall einer Kompromittierung des Zeitstempeldienstes oder bei ausgestellten Zeitstempeln mit falscher Uhrzeit werden die betroffenen Kunden informiert und der Zeitstempeldienst bis zur Behebung der Ursache deaktiviert. Darüber hinaus werden Informationen zur Identifizierung der falsch ausgestellten Zeitstempel auf der Webseite des VDA BNotK zur Verfügung gestellt.

Weitere Einzelheiten sind in Abschnitt 5.7. des Zertifizierungskonzepts der Zertifizierungsstelle der Bundesnotarkammer beschrieben.

5.12. Beendigungsplan

Der VDA BNotK hat einen den gesetzlichen Anforderungen entsprechenden Beendigungsplan.

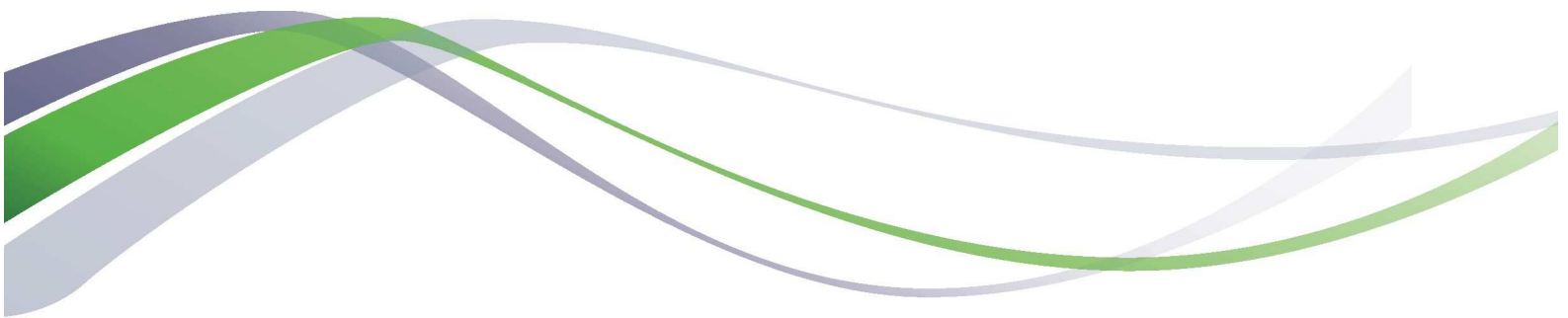
Einzelheiten sind in Abschnitt 4.11. des Zertifizierungskonzepts der Zertifizierungsstelle der Bundesnotarkammer beschrieben.

5.13. Konformität

Der VDA BNotK betreibt den Zeitstempeldienst im Einklang mit dem geltenden Recht.

Eine akkreditierte Konformitätsbewertungsstelle überprüft in regelmäßigen Abständen, dass der VDA BNotK die gesetzlichen Anforderungen erfüllt.

Einzelheiten sind in der Zertifikatsrichtlinie beschrieben.



<https://zertifizierungsstelle.bnotk.de/>