DMI Bewahrungsdienst

Preservation Service Policy and Practice Statement

Inhaltsverzeichnis

1. Einleitung

1.1. Zweck

Das Deutsche Mikrofilm Institut (DMI) erbringt durch die R. Schmelter GmbH & Co.KG den DMI-Bewahrungsdienst für signierte, gesiegelte Dokumentationen sowie sonstige Daten (kurz DMI-Bewahrungsdienst) für seine Kunden. Der DMI-Bewahrungsdienst ist ein Dienst zur Langzeit-Aufbewahrung und nach der Verordnung (EU) Nr. 910/2014 [1] (eIDAS-Verordnung) des Europäischen Parlaments qualifiziert.

Das vorliegende Dokument dient der Beschreibung des DMI-Bewahrungsdienstes, der Nennung der Richtlinien, deren Anforderungen er genügt, und legt dar, wie DMI als Trust Service Provider / Preservation Service Provider deren Erfüllung sicherstellt. Die Anforderungen der Richtlinie ETSI TS 119 511 [2] an das Preservation Service Practice Statement und die Preservation Service Policy und damit auch die Anforderungen der Richtlinie ETSI EN 319 401 [3] an ein generelles Trust Service Practice Statement werden erfüllt.

1.2. Verweise

Sind Dokumente mit Veröffentlichungsdatum, Ausgabenummer oder Versionsnummer angegeben, gilt nur die spezifizierte Version, andernfalls gilt die jeweils aktuelle Version des genannten Dokuments.

1.2.1. Mitgeltende Dokumente

Die Regelungen der folgenden Dokumente gelten für das vorliegende Dokument und den darin beschriebenen DMI-Bewahrungsdienst:

[1] 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 (kurz eIDAS-Verordnung)

[2] ETSI TS 119 511 – Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques

[3] ETSI EN 319 401 – General Policy Requirements for Trust Service Providers

[4] ETSI TS 119 512 – Protocols for trust service providers providing long-term data preservation services

[5] BSI TR-ESOR - 03125 – BSI Technische Richtline 03125 - Beweiswerterhaltung kryptographisch signierter Dokumente, Version 1.2.2

[6] BSI TR-ESOR-F – Formate, Version 1.2.2

[7] BSI-TR-ESOR-v1.2.2-S4-v1.0-Profile.xml

[8] Vertrauensdienstegesetz (VDG)

[9] Verordnung zu Vertrauensdiensten (Vertrauensdiensteverordnung - VDV)

1.2.2. Sonstige Dokumente

[10] Preservation Evidence Policy

[11] ISO/IEC 27001 Hauptzertifikat

[12] Allgemeine Geschäftsbedingungen (AGB)

1.3. DMI-Bewahrungsdienst-Teilnehmer

1.3.1. timeproof GmbH

Die timeproof GmbH liefert die BSI TR-ESOR - 03125 [5] zertifizierten eArchive Suite Appliances, die DMI für den DMI-Bewahrungsdienst betreibt, und leistet Wartung und Support gemäß vertraglicher Vereinbarung.

1.3.2. Aussteller qualifizierter Zeitstempel

Timeproof bringt unter Verwendung der TSA Utimaco qualifizierte Zeitstempel auf, die das Datum und die Uhrzeit einer Transaktion des DMI-Bewahrungsdienstes bescheinigen. Der Zeitstempeldienst (TSA) der Utimaco ist nach eIDAS-Verordnung [1] qualifiziert und die Nutzung durch DMI vertraglich geregelt.

1.3.3. Qualifizierter Validierungsdienstleister

Die nach eIDAS-Verordnung [1] qualifizierte Validierung der verwahrten qualifizierten Signaturen und Siegel erfolgt durch den Digital Signature Service (DSS).

1.3.4. Vertragspartner

Vertragspartner sind DMI-Kunden, welche im Rahmen einer Auftragsverarbeitung DMI DPaaS qT, Produktname für den DMI-Bewahrungsdienst, basierend auf dem DMI qualified Trust Repository (qTR) nutzen. Diese Kunden sind Stand heute juristische Personen, in der Regel Krankenhäuser und Kliniken. Die Rechte und Pflichten der Vertragspartner ergeben sich aus deren individuellen Verträgen und den anerkannten AGB [12].

1.4. Abkürzungen

AGB..... Allgemeine Geschäftsbedingungen
AUG ..... Augmentation goal
BSI ..... Bundesamt für Sicherheit in der Informationstechnik, Bundesamt für Sicherheit in der Informationstechnik
DMI..... Deutsches Mikrofilm Institut
eIDAS..... electronic IDentification, Authentication and Trust Services
ETSI ..... European Telecommunications Standards Institute
ETSI EN .... ETSI European Standard
ETSI TS..... ETSI Technical Specification
EU ..... Europäische Union
IEC ..... International Electrotechnical Commission
ISMS ..... Information Security Management System
ISO..... International Organization for Standardization
PDS..... Preservation of Digital Signatures
PGD ..... Preservation of General Data
QESeal..... Qualified Electronic Seal
QESig..... Qualified Electronic Signature
QPres ..... Qualified Preservation Service
TR-ESOR .. BSI Technische Richtlinie 03125 - Beweiswerterhaltung kryptographisch signierter Dokumente
TSA ..... Time-Stamping Authority
VDG ..... Vertrauensdienstegesetz
VDV..... Verordnung zu Vertrauensdiensten / Vertrauensdiensteverordnung
WOS..... Without Storage
WST ..... With Storage
WTS ..... With Temporary Storage
XML..... Extensible Markup Language

2. Dokumentenverwaltung, Publikation und Repositorium

2.1. Verantwortliche Organisation

Dieses Dokument und das Repositorium für den DMI-Bewahrungsdienst werden von der

DMI Deutsches Mikrofilm Institut f. med. Dokumentation
R. Schmelter GmbH & Co.KG
Otto-Hahn-Straße 11-13
48161 Münster

Tel: 02534 8005-0
Fax: 02534 8005-20
E-Mail: info@dmi.de

verwaltet und verantwortet. Das **Repositorium** enthält unter anderem die in den Kapiteln 1.2.1 und 1.2.2 referenzierten Dokumente und ist der Öffentlichkeit zugänglich unter:

https://www.dmi.de/qtsp.html

2.2. Freigabeprozess

Das Preservation Service Policy and Practice Statement wird vom für den DMI-Bewahrungsdienst verantwortlichen Service Manager geprüft, freigegeben und beteiligten sowie interessierten Personen und Parteien mit allen anderen erforderlichen Dokumenten im Repositorium zur Verfügung gestellt.

Die Unternehmensführung des DMI erklärt mit der Veröffentlichung dieses Dokuments am oben genannten Ort, dass die im folgenden beschriebenen Prozesse und Verfahren zur Erfüllung der benannten Richtlinien und Vorgaben für einen nach der eIDAS-Verordnung [1] qualifizierten Bewahrungsdienst durch ihre Organisation etabliert und angewandt werden.

Die vorliegende Version des Dokuments ersetzt alle vorangegangenen Versionen. Alle 12 Monate oder bei Änderungsbedarf veranlasst der Service Manager des DMI-Bewahrungsdienstes die Überprüfung und gegebenenfalls Aktualisierung des Preservation Service Policy and Practice Statement, kontrolliert diese, gibt sie frei, veröffentlicht sie, nötigenfalls nach Voranmeldung und angemessener Vorlaufzeit, und informiert die beteiligten Personen und Parteien umgehend über das Inkrafttreten der Änderungen.

3. DMI-Bewahrungsdienst

Der DMI-Bewahrungsdienst ist ein gemäß eIDAS-Verordnung [1] Art. 34 nach ETSI TS 119 511 [2] qualifizierter Vertrauensdienst zur Bewahrung des Beweiswertes von qualifizierten elektronischen Signaturen und Siegeln, Dokumentationen, die mit diesen versehen sind, sowie sonstigen Daten (File-Objekten).

Der qualifizierte DMI-Bewahrungsdienst dient der eIDAS Art. 34 und 40 gemäßen Beweiswerterhaltung und Bewahrung obiger Fileobjekte. Die DMI-Fachapplikationen, z.B. die Clinical Document and Data Services (CDDS) basierend auf dem qTR, kommunizieren mit dem DMI-Bewahrungsdienst über dessen XML-Schnittstelle (DPaaS qT Dienst). Über diese stellt DPaaS qT folgende Funktionen zur Verfügung:

- Ablage von File-Objekten (ArchiveSubmission)
- Versionierte Änderung archivierter File-Objekte (ArchiveUpdate)
- Abfrage archivierter File-Objekte (ArchiveRetrieval)
- Löschen von File-Objekten (ArchiveDeletion)
- Rückgabe technischer Beweisdaten (ArchiveEvidence)
- Prüfen technischer Beweisdaten (Verify) – (im zertifizierten TR-ESOR Produkt nicht implementiert – Nutzung des BSI publizierten Verify Frameworks)
- Abruf des Bewahrungsprofils (PreservationProfile)
- Abruf von Protokoll-Daten

Die Archivierung auf dem Speicher des qTR ist nicht Gegenstand des qualifizierten DMI-Bewahrungsdienstes DPaaS qT.

3.1. EU Trusted List

Die R. Schmelter GmbH & Co.KG wird als Trust Service Provider mit dem qualifiziertem Preservation Service (QPres for QESig & QPres for QESeal) "DMI-Bewahrungsdienst" in der Trusted List des eIDAS Dashboards

https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls/tl/DE

unter

https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls/tl/DE/tsp/30

geführt mit der ID:

Subject Name:
CN=Dt. Mikrofilminstitut f. med. Doku. R. Schmelter GmbH & Co. KG,L=Münster,SERIALNUMBER=SIG54FA24686F9D93564,2.5.4.97=DT:DE-0093033323,OU=Bewahrungsdienst,O=Dt. Mikrofilminstitut f. med. Doku. R. Schmelter GmbH & Co. KG,C=DE

Subject Key Identifier:
84F20F5EBE4E1409FD923874146881019889A7E4

3.2. Bewahrungsschema und Bewahrungsprofil

Zur Erbringung des DMI-Bewahrungsdienstes wird ein nach BSI TR-ESOR – 03125 Version 1.2.2 [5] zertifiziertes Produkt eingesetzt, das die XML-Schema-Definition in Kapitel 6 der Anlage BSI TR-ESOR-F [6] nutzt. Der DMI-Bewahrungsdienst nutzt ausschließlich das Bewahrungsprofil BSI-TR-ESOR-v1.2.2-S4-v1.0-Profile.xml [7]. Näheres ist der Preservation Evidence Policy [10] zu entnehmen.

3.3. Bewahrungsziele

Beim DMI-Bewahrungsdienst handelt es sich um einen qualifizierten Bewahrungsdienst mit Speicher **[WST]**, mit folgenden Bewahrungszielen:

- **[PDS+PGD]:** Bewahrung von kryptographisch signierten Dokumenten
  (combined preservation of digital signatures and general data)
- **[AUG]:** Beweiswerterhaltung der Archivdaten
  (augmentation of submitted preservation evidence)

4. Bewahrungsdienst-Richtlinien

Als qualifizierter Vertrauensdienstanbieter erfüllt die DMI Deutsches Mikrofilm Institut f. med. Dokumentation R. Schmelter GmbH & Co.KG die "General Policy Requirements for Trust Service Providers" der **ETSI EN 319 401 [3]** und als Anbieter des qualifizierten DMI-Bewahrungsdienstes die "Policy and security requirements for trust service providers providing long-term preservation of digital signatures or general data using digital signature techniques" der **ETSI TS 119 511 [2]**, sofern sie auf Bewahrungsdienste mit Speicher **[WST]** und die Bewahrungsziele **[PDS+PGD]** und **[AUG]** anzuwenden sind. Die vollständige Liste der anwendbaren Anforderungen befindet sich in Anhang A.

Die Verwendung der technischen "Protocols for trust service providers providing long-term data preservation services" der **ETSI TS 119 512 [4]** wird durch den Einsatz der nach der technischen Richtlinie **BSI TR-ESOR – 03125 V1.2.2 [5]** zertifizierten eArchive Suite der timeproof GmbH sichergestellt.

Im Folgenden stellt DMI dar, wie es diese Anforderungen an qualifizierte Trust Service Provider / Preservation Service Provider erfüllt.

5. Risikoeinschätzung und -behandlung

Das Management und der Betrieb des DMI-Bewahrungsdienstes gehört zum Geltungs- und Anwendungsbereich des nach ISO/IEC 27001 zertifizierten Informationssicherheitsmanagementsystems (ISMS) der DMI Deutsches Mikrofilm Institut f. med. Dokumentation R. Schmelter GmbH & Co.KG (siehe ISO/IEC 27001 Hauptzertifikat [11]).

In diesem Rahmen identifiziert DMI regelmäßig die Informationssicherheitsrisiken für den DMI-Bewahrungsdienst. Auf Basis der Analyse und Bewertung der identifizierten Risiken nach technischen und geschäftlichen Gesichtspunkten, werden angemessene organisatorische oder technisch Maßnahmen zur Risikobehandlung vorgeschlagen. Nach Freigabe durch das DMI-Management werden die beschlossenen Maßnahmen in den Risikobehandlungsplan integriert und danach umgesetzt. Die Umsetzung wird durch regelmäßig durchgeführte IMS-Audits und Managementreviews nachverfolgt und sichergestellt. Eine Risikoakzeptanz von Risiken, die den Zertifizierungsvorgaben zuwiderlaufen und / oder Risiken für den einwandfreien Betrieb des Dienstes darstellen, ist nicht zulässig.

6. Richtlinien und Verfahren

6.1. Preservation Service Policy and Practice Statement

Das vorliegende Dokument steht den Nutzern sowie anderen betroffenen oder interessierten Parteien im Repositorium der DMI in seiner aktuellen Fassung zur Verfügung gestellt.

6.2. Allgemeine Geschäftsbedingungen

Mit der vertraglichen Vereinbarung der Nutzung des DMI-Bewahrungsdienstes werden die im Repositorium (https://www.dmi.de/qtsp.html) veröffentlichten, allgemeinen Geschäftsbedingungen [12] akzeptiert. Aus ihnen gehen alle mit der Nutzung verbundenen Rechte und Pflichten hervor, sowie gegebenenfalls existierende (Haftungs-) Einschränkungen.

6.3. Informationssicherheitsrichtlinie

Die die von der Geschäftsführung freigegebene Richtlinie Informationssicherheit von DMI legt deren Sicherheitspolitik fest und ist allen Mitarbeitenden im Geltungs- und Anwendungsbereich des ISMS bekannt- und zugänglichgemacht. Die an der Erbringung des DMI-Bewahrungsdienstes beteiligten, externen Parteien sind in den Informationssicherheitsmanagementprozess eingebunden und DMI kontrolliert als Gesamtverantwortlicher für die Sicherheit der Dienstleistung die Umsetzung der geplanten Sicherheitsmaßnahmen.

Die qTSP spezifischen Assets werden mindestens einmal jährlich bezogen auf die wesentlichen Änderungen geprüft, um die weitere Eignung, Stabilität und Leistungsfähigkeit sicherzustellen, siehe hierzu auch die dbzgl. Regelungen in der IMS-Richtlinie.

6.4. Bewahrungsprofil

Der DMI-Bewahrungsdienst nutzt ausschließlich das Bewahrungsprofil BSI-TR-ESOR-v1.2.2-S4-v1.0-Profile.xml [7]. Es ist im Repositorium (https://www.dmi.de/qtsp.html) einsehbar.

6.5. Preservation Evidence Policy

Die Preservation Evidence Policy [10] beschreibt, mit welchen kryptographischen Algorithmen und in welchem Format die Bewahrungsnachweise erzeugt und gültig gehalten werden, sowie diese validiert werden können. Sie ist im Repositorium (https://www.dmi.de/qtsp.html) einsehbar.

6.6. Signature Validation Policy

Die Signature Validation Policy ist Bestandteil der Preservation Evidence Policy [10].

6.7. Nutzungsvertrag

Mit dem Nutzungsvertrag werden die Allgemeinen Geschäftsbedingungen [12] akzeptiert und festgelegt, welche Zugriffsrechte auf Nachweise und Protokolle eingeräumt werden.

7. DMI-Management und Betrieb

7.1. Interne Organisation

Als führender IT-Dienstleister rund um die digitale Patientenakte erfüllt DMI die Anforderungen seiner Kunden im Gesundheitswesen seit 50 Jahren zuverlässig. Eine diskriminierungsfreie Arbeitsumgebung ist selbstverständlich. DMI legt mit seinem nach ISO/IEC 27001 zertifizierten Rechenzentrumsbetrieb Wert auf eine normen- und regelkonforme Informationssicherheit. DMI reduziert die Möglichkeiten zu unbefugter oder unbeabsichtigter Änderung oder zum Missbrauch der (Informations-)Werte, indem es miteinander in Konflikt stehende Aufgaben und Verantwortlichkeitsbereiche trennt.

7.2. Personal

Das Personal von DMI und seiner Auftragnehmer wird sorgfältig unter Berücksichtigung fachlicher und Sicherheitskriterien ausgewählt, verstehen ihre Verantwortung und kennen die Konsequenzen von Sicherheitsvorfällen. Es wird regelmäßig für Sicherheitsaspekte sensibilisiert und in relevanten Themen unterwiesen.

7.3. Verwaltung der Werte

(Informations-)Werte im Zusammenhang mit der Erbringung des DMI-Bewahrungsdienstes sind inventarisiert und klassifiziert, Zuständigen zugeordnet, Regeln für den Umgang mit ihnen aufgestellt und deren Einhaltung kontrolliert. Die unerlaubte Offenlegung, Veränderung, Entfernung oder Zerstörung von Informationen, die vom DMI-Bewahrungsdienst verarbeitet werden, wird unterbunden.

7.4. Zugangssteuerung

Der Zugang zu den Informationen und informationsverarbeitenden Einrichtungen des DMI-Bewahrungsdienstes ist eingeschränkt. DMI stellt durch seine Betriebsprozesse sicher, dass nur befugte Benutzer Zugriff haben und unbefugter Zugriff nicht möglich ist. Die Benutzer sind verpflichtet, ihre Authentisierungsinformationen geheim zu halten und ihre Aktivitäten in den Systemen werden protokolliert. Die dbzgl. Umsetzung ist in der ISP / im Betriebshandbuch behandelt.

7.5. Kryptographische Sicherheitsmaßnahmen

Die Verwaltung und der Schutz kryptographischer Schlüssel und Einrichtungen erfolgt über deren Lebenszyklus gemäß der DMI "Richtlinie zum Gebrauch, zum Schutz und zur Lebensdauer von kryptographischen Schlüsseln".

7.6. Physische Sicherheit und Umgebungsschutz

Die Einrichtungen des DMI-Bewahrungsdienstes werden in einer Sicherheitszone betrieben, die durch eine Alarmanlage gegen Einbruch geschützt ist. Der Zutritt zur Sicherheitszone sowie der Aufenthalt dort werden in den Richtlinien "Sicherheitszonen und Zutrittskontrolle DMI" sowie "Aufenthalt RZ" geregelt.

7.7. Betriebssicherheit

Der Einsatz vertrauenswürdiger Systeme und Produkte im DMI wird durch die Einhaltung der DMI-Richtlinien "Softwareentwicklung" und "IT-Sicherheit" sowie der Verfahrensbeschreibung "Beschaffung und Lieferantenauswahl" sichergestellt.

Zum Schutz der eingesetzten Systeme und Produkte vor Manipulation und zur Sicherstellung der Zuverlässigkeit der durch sie unterstützten Prozesse, erfolgt der Betrieb anhand des DMI "IT-Betriebshandbuch", Änderung werden nach den Vorgaben des DMI "Changemanagement" nachverfolgt.

Nach dem DMI "IT-Sicherheitskonzept" sind Erkennungs-, Vorbeugungs- und Wiederherstellungsmaßnahmen zum Schutz vor Schadsoftware umgesetzt. Rollen und Berechtigungen der Administratoren werden nach der "Richtlinie IMS“ und "Richtlinie Berechtigungsmanagement“ verwaltet.

7.8. Netzwerksicherheit

DMI segmentiert sein Netzwerk nach risikobasierten Kriterien, kontrolliert die Übergänge zwischen den Netzsegmenten und externen Netzen gemäß DMI "IT-Sicherheitskonzept" und führt quartalsweise Schwachstellenscans der Systeme des DMI-Bewahrungsdienstes durch. Der Speicher des DMI-Bewahrungsdienstes kann ausschließlich durch diesen geändert werden. Die Umsetzung ist im IT-Sicherheitskonzept behandelt.

7.9. Vorfalls-Management

Die Verfahren zur Meldung und Behandlung von Informationssicherheitsvorfällen und neu auftretenden Schwachstellen sind im "DMI Incidentmanagement-Prozess“ und im Dokument "IT-Sicherheitskonzept“ festgelegt.

7.10. Beweissicherung

DMI stellt die Aufbewahrung der Nachweise ihrer Geschäftsvorfälle gemäß Kunden-Vereinbarungen in Einklang mit den geltenden rechtlichen Vorgaben sicher.

Darüber hinaus werden alle Ereignisse der Systeme des DMI-Bewahrungsdienstes so protokolliert, gespeichert und gesichert, dass sie für spätere Nachweise der Zuverlässigkeit des Bewahrungsdienstes zur Verfügung stehen.

7.11. Business Continuity Management

DMI hat ein integriertes Notfall- und Business Continuity Management etabliert, das in Katastrophenfällen auszuführende Pläne vorhält. Auch für den Fall, dass private Schlüssel oder Zugangsdaten kompromittiert wurden, kann der Betrieb mit Wiederanlaufplänen in absehbarer Zeit wiederaufgenommen werden.

7.12. Beendigung des TSP/PSP, Vertragsende

DMI hat Regelungen und Vorkehrungen für den Fall getroffen, dass der DMI-Bewahrungsdienst dauerhaft eingestellt wird, der auch die Szenarien des Entzugs der Zertifizierung oder der Insolvenz bei gleichzeitiger Beendigung des Dienstes berücksichtigt.

Die Planung stellt sicher, dass Nutzer und Behörden rechtzeitig informiert werden, die Bewahrungsobjekte der Nutzer an andere Dienstleister transferiert werden, die den Dienst für die Kunden übernehmen, die Verpflichtung zum Erhalt aller Informationen in Bezug auf die Tätigkeit als Bewahrungsdienst eine vertrauenswürdige dritte Partei übergeben wird und Schlüssel, Speicher, System und Daten ordnungsgemäß unbrauchbar gemacht, gelöscht und entsorgt werden. Die Kosten für die Beendigung des Dienstes sind durch Rücklagen gedeckt.

Die Planung für die dauerhafte Beendigung des Dienstes sind regelmäßig überprüft und angepasst. Die Dauer der Preservation Period richtet sich nach den individualvertraglichen Vereinbarungen des übergeordneten Services (qTR) oder bis der Auftraggeber eine abweichende Weisung bzgl. der Aufbewahrung/Löschung erteilt.

Details sind im Beendigungsplan geregelt.

7.13. Compliance

Die nach ISO 9001 und ISO/IEC 27001 zertifizierter Abläufe des DMI dienen der Zuverlässigkeit des DMI-Bewahrungsdienstes, dem Schutz der damit verarbeiteten Bewahrungsobjekte, der Erfüllung der Anforderung an den nach eIDAS-Verordnung [1] qualifizierten DMI-Bewahrungsdienst (siehe Kapitel 4 und Anhang A), der Erfüllung der vertraglichen Verpflichtungen gegenüber den Nutzern des Dienstes und der Einhaltung der geltenden gesetzlichen Regelungen (z.B. VDG [8] und VDV [9]).

Es besteht beim Vertrauensdiensteanbieter die zur Erfüllung der Normanforderungen notwendige finanzielle Stabilität und die gemäß §10 Vertrauensdienstegesetz für haftungsauslösende Ereignisse geforderte Deckungsvorsorge für Vertrauensdiensteanbieter ist zusätzlich über eine Vermögensschadenhaftpflichtversicherung abgedeckt.

In Bezug auf den Vertrauensdienst ergeben sich noch über die ISO 27001 hinausgehenden Anforderungen, die wie folgt realisiert worden (EN 319 401: REQ 6.3-02):

- Änderungen RL ISMS werden auch extern kommuniziert, der jeweilige Adressatenkreis wird im Änderungszyklus festgelegt.
- Änderungen ISP werden auch extern kommuniziert, der jeweilige Adressatenkreis beinhaltet mindestens Bewertungsstellen, Aufsichts- oder andere Regulierungsbehörden, Partner, Kunden und Lieferanten
- Die Schulung der Mitarbeitenden ist im Schulungskonzept geregelt. Die qTSP-spezifischen Schulungen sind zu planen, durchzuführen und zu dokumentieren.
- Die Appliances werden im Rechenzentrum Leisnig in einem separaten Raum betrieben. (REQ 6.3-05)

- Der Zugang zu diesem Raum ist auch externen Mitarbeiterinnen und Mitarbeitern (in Begleitung eines internen Mitarbeiters) möglich, es gilt die Richtlinie zum Aufenthalt im RZ. REQ 6.3-06
- Es erfolgte eine Erweiterung der Prüfprozesse der Appliances für Änderungen, die gegen die Sicherheitsrichtlinien gehen, insbesondere Bewahrungsdienst spezifische, unter Einbeziehung von timeproof. Es werden nur abgestimmte Wartungen und Changes durchgeführt.
- Die qTSP spezifischen Assets werden mindestens einmal jährlich bezogen auf die wesentlichen Änderungen geprüft, um die weitere Eignung, Stabilität und Leistungsfähigkeit sicherzustellen

7.14. Kryptographische Überwachung

Die anforderungsgemäße Überwachung der Stärke der Verschlüsselungsalgorithmen wird durch den Einsatz der nach BSI TR-ESOR – 03125 V1.2.2 [5] zertifizierten eArchive Suite der timeproof GmbH sichergestellt.

7.15. Augmentation von Preservation Evidences

Die nach BSI TR-ESOR – 03125 V1.2.2 [5] zertifizierten eArchive Suite der timeproof GmbH stellt sicher, dass der Beweiswert der Bewahrungsobjekte über den Bewahrungszeitraum erhalten bleibt.

7.16. Export-Import Pakete

Die Anforderungen an das Format von Export-Import Paketen, die Schnittstellen, über die sie ausgetauscht werden, und die Protokollierung des Austauschs werden von der nach BSI TR-ESOR – 03125 V1.2.2 [5] zertifizierten eArchive Suite der timeproof GmbH erfüllt.

8. Operational and Notification Protocols

8.1. Preservation Protocol

Dass die Implementierung des Preservation Protocols anforderungsgemäß ist, wird durch die Zertifizierung der eArchive Suite der timeproof GmbH nach BSI TR-ESOR – 03125 V1.2.2 [5] nachgewiesen. Näheres zum Preservation Protocol kann der Preservation Evidence Policy [10] entnommen werden.

8.2. Notification Protocol

Der DMI-Bewahrungsdienst verwendet kein Notification Protocol.

9. Preservation Process

9.1. Storage of Preserved Data and Evidence

Die Anforderungen dieses Kapitels betreffen nur Bewahrungsdienste ohne Speicher [WOS] oder mit temporärem Speicher [WTS], also nicht den DMI-Bewahrungsdienst, der mit Speicher [WST] ist.

9.2. Preservation Evidences

Mit der Zertifizierung der für den DMI-Bewahrungsdienst eingesetzten eArchive Suite nach BSI TR-ESOR – 03125 V1.2.2 [5] ist sichergestellt, dass die verwendeten Zeitstempel den Anforderungen genügen.

9.3. Preservation of Digital Signatures

Der DMI-Bewahrungsdienst belegt sowohl die Existenz der verwahrten Signaturen und der zu ihrer Validierung erforderlichen Daten als auch der signierten Daten.

10. Gemäß eIDAS-Verordnung Art. 34 qualifizierter Bewahrungsdienst für QES

Der DMI-Bewahrungsdienst verwahrt alle nicht öffentlich zugänglichen Informationen, die zur Überprüfung des Qualifizierungsstatus der elektronischen Signaturen oder Siegels erforderlich sind, bis zum Ende des Aufbewahrungszeitraums. Zeitstempel werden von einer qualifizierten Time-Stamping Authority (TSA) bezogen.

Der DMI-Bewahrungsdienst ist mit Service Digital Identifier unter

https://eidas.ec.europa.eu/efda/trust-services/browse/eidas/tls/tl/DE

aufgeführt.

Anhang A Anwendbare Anforderungen der einschlägigen Richtlinien

Richtlinie	Referenz	Thema	Anforderung (normativ)
ETSI EN 319 401	REQ-5-01	Risk Assessment	The TSP shall carry out a risk assessment to identify, analyse and evaluate trust service risks taking into account business and technical issues.
ETSI EN 319 401	REQ-5-02	Risk Assessment	The TSP shall select the appropriate risk treatment measures, taking account of the risk assessment results. The risk treatment measures shall ensure that the level of security is commensurate to the degree of risk.
ETSI EN 319 401	REQ-5-03	Risk Assessment	The TSP shall determine all security requirements and operational procedures that are necessary to implement the risk treatment measures chosen, as documented in the information security policy and the trust service practice statement (see clause 6).
ETSI EN 319 401	REQ-5-04	Risk Assessment	The risk assessment shall be regularly reviewed and revised.
ETSI EN 319 401	REQ-5-05	Risk Assessment	The TSP's management shall approve the risk assessment and accept the residual risk identified.
ETSI EN 319 401	REQ-6.1-01	Trust Service Practice Statement	The TSP shall specify the set of policies and practices appropriate for the trust services it is providing.
ETSI EN 319 401	REQ-6.1-02	Trust Service Practice Statement	The set of policies and practices shall be approved by management, published and communicated to employees and external parties as relevant. In particular
ETSI EN 319 401	REQ-6.1-03	Trust Service Practice Statement	The TSP shall have a statement of the practices and procedures used to address all the requirements identified for the applicable TSP's policy.
ETSI EN 319 401	REQ-6.1-04	Trust Service Practice Statement	The TSP's trust service practice statement shall identify the obligations of all external organizations supporting the TSP's services including the applicable policies and practices.
ETSI EN 319 401	REQ-6.1-05	Trust Service Practice Statement	The TSP shall make available to subscribers and relying parties its practice statement, and other relevant documentation, as necessary to assess conformance to the service policy.
ETSI EN 319 401	REQ-6.1-06	Trust Service Practice Statement	The TSP shall have a management body with overall responsibility for the TSP with final authority for approving the TSP's practice statement.
ETSI EN 319 401	REQ-6.1-07	Trust Service Practice Statement	The TSP's management shall implement the practices.
ETSI EN 319 401	REQ-6.1-08	Trust Service Practice Statement	The TSP shall define a review process for the practices including responsibilities for maintaining the TSP's practice statement.
ETSI EN 319 401	REQ-6.1-09	Trust Service Practice Statement	The TSP shall notify notice of changes it intends to make in its practice statement.
ETSI EN 319 401	REQ-6.1-10	Trust Service Practice Statement	The TSP shall, following approval as in REQ-6.1-06 above, make the revised TSP's practice statement immediately available as required under REQ-6.1-05 above.

Richtlinie	Referenz	Thema	Anforderung (normativ)
ETSI EN 319 401	REQ-6.1-11	Trust Service Practice Statement	The TSP shall state in its practices the provisions made for termination of service (see clause 7.12).
ETSI EN 319 401	REQ-6.2-01	Terms and Conditions	The TSP shall make the terms and conditions regarding its services available to all subscribers and relying parties.
ETSI EN 319 401	REQ-6.2-02	Terms and Conditions	The terms and conditions shall at least specify for each trust service policy supported by the TSP the following:
ETSI EN 319 401	REQ-6.2-02, a)	Terms and Conditions	the trust service policy being applied;
ETSI EN 319 401	REQ-6.2-02, b)	Terms and Conditions	any limitations on the use of the service provided including the limitation for damages arising from the use of services exceeding such limitations;
ETSI EN 319 401	REQ-6.2-02, c)	Terms and Conditions	the subscriber's obligations, if any;
ETSI EN 319 401	REQ-6.2-02, d)	Terms and Conditions	information for parties relying on the trust service;
ETSI EN 319 401	REQ-6.2-02, e)	Terms and Conditions	the period of time during which TSP's event logs are retained;
ETSI EN 319 401	REQ-6.2-02, f)	Terms and Conditions	limitations of liability;
ETSI EN 319 401	REQ-6.2-02, g)	Terms and Conditions	the applicable legal system;
ETSI EN 319 401	REQ-6.2-02, h)	Terms and Conditions	procedures for complaints and dispute settlement;
ETSI EN 319 401	REQ-6.2-02, i)	Terms and Conditions	whether the TSP's trust service has been assessed to be conformant with the trust service policy, and if so through which conformity assessment scheme;
ETSI EN 319 401	REQ-6.2-02, j)	Terms and Conditions	the TSP's contact information; and
ETSI EN 319 401	REQ-6.2-02, k)	Terms and Conditions	any undertaking regarding availability.
ETSI EN 319 401	REQ-6.2-03	Terms and Conditions	Subscribers and parties relying on the trust service shall be informed of precise terms and conditions, including the items listed above, before entering into a contractual relationship.
ETSI EN 319 401	REQ-6.2-04	Terms and Conditions	Terms and conditions shall be made available through a durable means of communication.
ETSI EN 319 401	REQ-6.2-05	Terms and Conditions	Terms and conditions shall be available in a readily understandable language.
ETSI EN 319 401	REQ-6.2-06	Terms and Conditions	Terms and conditions may be transmitted electronically.
ETSI EN 319 401	REQ-6.3-01	Information Security Policy	The TSP shall define an information security policy which is approved by management and which sets out the organization's approach to managing its information security.
ETSI EN 319 401	REQ-6.3-02	Information Security Policy	Changes to the information security policy shall be communicated to third parties, where applicable. This includes subscribers, relying parties, assessment bodies, supervisory or other regulatory bodies. I n particular:
ETSI EN 319 401	REQ-6.3-03	Information Security Policy	A TSP's information security policy shall be documented, implemented and maintained including the security controls and operating procedures for TSP's facilities, systems and information assets providing the services.

Richtlinie	Referenz	Thema	Anforderung (normativ)
ETSI EN 319 401	REQ-6.3-04	Information Security Policy	The TSP shall publish and communicate the information security policy to all employees who are impacted by it.
ETSI EN 319 401	REQ-6.3-05	Information Security Policy	The TSP shall retain overall responsibility for conformance with the procedures prescribed in its information security policy, even when the TSP's functionality is undertaken by outsourcers.
ETSI EN 319 401	REQ-6.3-06	Information Security Policy	TSP shall define the outsourcers' liability and ensure that outsourcer are bound to implement any controls required by the TSP.
ETSI EN 319 401	REQ-6.3-07	Information Security Policy	The TSP's information security policy and inventory of assets for information security (see clause 7.3) shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
ETSI EN 319 401	REQ-6.3-08	Information Security Policy	Any changes that will impact on the level of security provided shall be approved by the management body referred to in REQ-6.1-07.
ETSI EN 319 401	REQ-6.3-09	Information Security Policy	The configuration of the TSPs systems shall be regularly checked for changes which violate the TSPs security policies.
ETSI EN 319 401	REQ-6.3-10	Information Security Policy	The maximum interval between two checks shall be documented in the trust service practice statement.
ETSI EN 319 401	REQ-7.1.1-01	Organization reliability	The TSP organization shall be reliable. In particular:
ETSI EN 319 401	REQ-7.1.1-02	Organization reliability	Trust service practices under which the TSP operates shall be non-discriminatory.
ETSI EN 319 401	REQ-7.1.1-03	Organization reliability	The TSP should make its services accessible to all applicants whose activities fall within its declared field of operation and that agree to abide by their obligations as specified in the TSP's terms and conditions.
ETSI EN 319 401	REQ-7.1.1-04	Organization reliability	The TSP shall maintain sufficient financial resources and/or obtain appropriate liability insurance, in accordance with applicable law, to cover liabilities arising from its operations and/or activities.
ETSI EN 319 401	REQ-7.1.1-05	Organization reliability	The TSP shall have the financial stability and resources required to operate in conformity with this policy.
ETSI EN 319 401	REQ-7.1.1-06	Organization reliability	The TSP shall have policies and procedures for the resolution of complaints and disputes received from customers or other relying parties about the provisioning of the services or any other related matters.
ETSI EN 319 401	REQ-7.1.1-07	Organization reliability	The TSP shall have a documented agreement and contractual relationship in place where the provisioning of services involves subcontracting, outsourcing or other third party arrangements.
ETSI EN 319 401	REQ-7.1.2-01	Segregation of duties	Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the TSP's assets.

Richtlinie	Referenz	Thema	Anforderung (normativ)
ETSI EN 319 401	REQ-7.2-01	Human resources	The TSP shall ensure that employees and contractors support the trustworthiness of the TSP's operations. In particular:
ETSI EN 319 401	REQ-7.2-02	Human resources	The TSP shall employ staff and, if applicable, subcontractors, who possess the necessary expertise, reliability, experience, and qualifications and who have received training regarding security and personal data protection rules as appropriate for the offered services and the job function.
ETSI EN 319 401	REQ-7.2-03	Human resources	TSP personnel should be able to fulfil the requirement of "expert knowledge, experience and qualifications" through formal training and credentials, or actual experience, or a combination of the two.
ETSI EN 319 401	REQ-7.2-04	Human resources	This should include regular (at least every 12 months) updates on new threats and current security practices.
ETSI EN 319 401	REQ-7.2-05	Human resources	Appropriate disciplinary sanctions shall be applied to personnel violating TSP's policies or procedures.
ETSI EN 319 401	REQ-7.2-06	Human resources	Security roles and responsibilities, as specified in the TSP's information security policy, shall be documented in job descriptions or in documents available to all concerned personnel.
ETSI EN 319 401	REQ-7.2-07	Human resources	Trusted roles, on which the security of the TSP's operation is dependent, shall be clearly identified.
ETSI EN 319 401	REQ-7.2-08	Human resources	Trusted roles shall be named by the management.
ETSI EN 319 401	REQ-7.2-09	Human resources	Trusted roles shall be accepted by the management and the person to fulfil the role.
ETSI EN 319 401	REQ-7.2-10	Human resources	TSP's personnel (both temporary and permanent) shall have job descriptions defined from the view point of roles fulfilled with segregation of duties and least privilege (see clause 7.1.2), determining position sensitivity based on the duties and access levels, background screening and employee training and awareness.
ETSI EN 319 401	REQ-7.2-11	Human resources	Where appropriate, job descriptions shall differentiate between general functions and TSP's specific functions. These should include skills and experience requirements.
ETSI EN 319 401	REQ-7.2-12	Human resources	Personnel shall exercise administrative and management procedures and processes that are in line with the TSP's information security management procedures.
ETSI EN 319 401	REQ-7.2-13	Human resources	Managerial personnel shall possess experience or training with respect to the trust service that is provided, familiarity with security procedures for personnel with security responsibilities and experience with information security and risk assessment sufficient to carry out management functions.

Richtlinie	Referenz	Thema	Anforderung (normativ)
ETSI EN 319 401	REQ-7.2-14	Human resources	All TSP's personnel in trusted roles shall be free from conflict of interest that might prejudice the impartiality of the TSP's operations.
ETSI EN 319 401	REQ-7.2-15	Human resources	Trusted roles shall include roles that involve the following responsibilities: a) Security Officers: Overall responsibility for administering the implementation of the security practices. b) System Administrators: Authorized to install, configure and maintain the TSP's trustworthy systems for service management. c) System Operators: Responsible for operating the TSP's trustworthy systems on a day-to-day basis. Authorized to perform system backup. d) System Auditors: Authorized to view archives and audit logs of the TSP's trustworthy systems.
ETSI EN 319 401	REQ-7.2-16	Human resources	TSP's personnel shall be formally appointed to trusted roles by senior management responsible for security requiring the principle of "least privilege" when accessing or when configuring access privileges.
ETSI EN 319 401	REQ-7.2-17	Human resources	Personnel shall not have access to the trusted functions until the necessary checks are completed.
ETSI EN 319 401	REQ-7.3.1-01	General requirements	The TSP shall ensure an appropriate level of protection of its assets including information assets. In particular:
ETSI EN 319 401	REQ-7.3.1-02	General requirements	The TSP shall maintain an inventory of all information assets and shall assign a classification consistent with the risk assessment.
ETSI EN 319 401	REQ-7.3.2-01	Media handling	All media shall be handled securely in accordance with requirements of the information classification scheme. Media containing sensitive data shall be securely disposed of when no longer required.
ETSI EN 319 401	REQ-7.4-01	Access control	The TSP's system access shall be limited to authorized individuals. In particular:
ETSI EN 319 401	REQ-7.4-02	Access control	Controls (e.g. firewalls) shall protect the TSP's internal network domains from unauthorized access including access by subscribers and third parties.
ETSI EN 319 401	REQ-7.4-03	Access control	Firewalls should also be configured to prevent all protocols and accesses not required for the operation of the TSP.
ETSI EN 319 401	REQ-7.4-04	Access control	The TSP shall administer user access of operators, administrators and system auditors.
ETSI EN 319 401	REQ-7.4-05	Access control	The administration shall include user account management and timely modification or removal of access.
ETSI EN 319 401	REQ-7.4-06	Access control	Access to information and application system functions shall be restricted in accordance with the access control policy.
ETSI EN 319 401	REQ-7.4-07	Access control	The TSP's system shall provide sufficient computer security controls for the separation of trusted roles identified in TSP's practices, including the separation

Richtlinie	Referenz	Thema	Anforderung (normativ)
			of security administration and operation functions. Particularly, use of system utility programs shall be restricted and controlled.
ETSI EN 319 401	REQ-7.4-08	Access control	TSP's personnel shall be identified and authenticated before using critical applications related to the service.
ETSI EN 319 401	REQ-7.4-09	Access control	TSP's personnel shall be accountable for their activities.
ETSI EN 319 401	REQ-7.4-10	Access control	Sensitive data shall be protected against being revealed through re-used storage objects (e.g. deleted files) being accessible to unauthorized users.
ETSI EN 319 401	REQ-7.5-01	Cryptographic controls	Appropriate security controls shall be in place for the management of any cryptographic keys and any cryptographic devices throughout their lifecycle.
ETSI EN 319 401	REQ-7.6-01	Physical and environmental security	The TSP shall control physical access to components of the TSP's system whose security is critical to the provision of its trust services and minimize risks related to physical security. In particular:
ETSI EN 319 401	REQ-7.6-02	Physical and environmental security	Physical access to components of the TSP's system whose security is critical to the provision of its trust services shall be limited to authorized individuals.
ETSI EN 319 401	REQ-7.6-03	Physical and environmental security	Controls shall be implemented to avoid loss, damage or compromise of assets and interruption to business activities.
ETSI EN 319 401	REQ-7.6-04	Physical and environmental security	Controls shall be implemented to avoid compromise or theft of information and information processing facilities.
ETSI EN 319 401	REQ-7.6-05	Physical and environmental security	Components that are critical for the secure operation of the trust service shall be located in a protected security perimeter with physical protection against intrusion, controls on access through the security perimeter and alarms to detect intrusion.
ETSI EN 319 401	REQ-7.7-01	Operation security	The TSP shall use trustworthy systems and products that are protected against modification and ensure the technical security and reliability of the processes supported by them. In particular:
ETSI EN 319 401	REQ-7.7-02	Operation security	An analysis of security requirements shall be carried out at the design and requirements specification stage of any systems development project undertaken by the TSP or on behalf of the TSP to ensure that security is built into IT systems.
ETSI EN 319 401	REQ-7.7-03	Operation security	Change control procedures shall be applied for releases, modifications and emergency software fixes of any operational software and changes to the configuration which applies the TSP's security policy.
ETSI EN 319 401	REQ-7.7-04	Operation security	The procedures shall include documentation of the changes.
ETSI EN 319 401	REQ-7.7-05	Operation security	The integrity of TSP's systems and information shall be protected against viruses, malicious and unauthorized software.

Richtlinie	Referenz	Thema	Anforderung (normativ)
ETSI EN 319 401	REQ-7.7-06	Operation security	Media used within the TSP's systems shall be securely handled to protect media from damage, theft, unauthorized access and obsolescence.
ETSI EN 319 401	REQ-7.7-07	Operation security	Media management procedures shall protect against obsolescence and deterioration of media within the period of time that records are required to be retained.
ETSI EN 319 401	REQ-7.7-08	Operation security	Procedures shall be established and implemented for all trusted and administrative roles that impact on the provision of services.
ETSI EN 319 401	REQ-7.7-09	Operation security	The TSP shall specify and apply procedures for ensuring that: a) security patches are applied within a reasonable time after they come available; b) security patches are not applied if they introduce additional vulnerabilities or instabilities that outweigh the benefits of applying them; and c) the reasons for not applying any security patches are documented.
ETSI EN 319 401	REQ-7.8-01	Network security	The TSP shall protect its network and systems from attack. In particular:
ETSI EN 319 401	REQ-7.8-02	Network security	The TSP shall segment its systems into networks or zones based on risk assessment considering functional, logical, and physical (including location) relationship between trustworthy systems and services.
ETSI EN 319 401	REQ-7.8-03	Network security	The TSP shall apply the same security controls to all systems co-located in the same zone.
ETSI EN 319 401	REQ-7.8-04	Network security	The TSP shall restrict access and communications between zones to those necessary for the operation of the TSP.
ETSI EN 319 401	REQ-7.8-05	Network security	The TSP shall explicitly forbid or deactivate not needed connections and services.
ETSI EN 319 401	REQ-7.8-06	Network security	The TSP shall review the established rule set on a regular basis.
ETSI EN 319 401	REQ-7.8-07	Network security	The TSP shall keep all systems that are critical to the TSP's operation in one or more secured zone(s) (e.g. Root CA systems see ETSI EN 319 411-1 [i.9]).
ETSI EN 319 401	REQ-7.8-08	Network security	The TSP shall separate dedicated network for administration of IT systems and TSP's operational network.
ETSI EN 319 401	REQ-7.8-09	Network security	The TSP shall not use systems used for administration of the security policy implementation for other purposes.
ETSI EN 319 401	REQ-7.8-10	Network security	The TSP shall separate the production systems for the TSP's services from systems used in development and testing (e.g. development, test and staging systems).
ETSI EN 319 401	REQ-7.8-11	Network security	The TSP shall establish communication between distinct trustworthy systems only through trusted channels that are logically distinct from other communication channels and provide assured identification of its end points and protection of the channel data from modification or disclosure.

Richtlinie	Referenz	Thema	Anforderung (normativ)
ETSI EN 319 401	REQ-7.8-12	Network security	If a high level of availability of external access to the trust service is required, the external network connection shall be redundant to ensure availability of the services in case of a single failure.
ETSI EN 319 401	REQ-7.8-13	Network security	The TSP shall undergo or perform a regular vulnerability scan on public and private IP addresses identified by the TSP and record evidence that each vulnerability scan was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.
ETSI EN 319 401	REQ-7.8-14	Network security	The TSP shall undergo a penetration test on the TSP's systems at set up and after infrastructure or application upgrades or modifications that the TSP determines are significant.
ETSI EN 319 401	REQ-7.8-15	Network security	The TSP shall record evidence that each penetration test was performed by a person or entity with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable report.
ETSI EN 319 401	REQ-7.9-01	Incident management	System activities concerning access to IT systems, use of IT systems, and service requests shall be monitored. In particular:
ETSI EN 319 401	REQ-7.9-02	Incident management	Monitoring activities should take account of the sensitivity of any information collected or analysed.
ETSI EN 319 401	REQ-7.9-03	Incident management	Abnormal system activities that indicate a potential security violation, including intrusion into the TSP's network, shall be detected and reported as alarms.
ETSI EN 319 401	REQ-7.9-04	Incident management	The TSP IT systems shall monitor the following events: a) start-up and shutdown of the logging functions; and b) availability and utilization of needed services with the TSP's network.
ETSI EN 319 401	REQ-7.9-05	Incident management	The TSP shall act in a timely and co-ordinated manner in order to respond quickly to incidents and to limit the impact of breaches of security.
ETSI EN 319 401	REQ-7.9-06	Incident management	The TSP shall appoint trusted role personnel to follow up on alerts of potentially critical security events and ensure that relevant incidents are reported in line with the TSP's procedures.
ETSI EN 319 401	REQ-7.9-07	Incident management	The TSP shall establish procedures to notify the appropriate parties in line with the applicable regulatory rules of any breach of security or loss of integrity that has a significant impact on the trust service provided and on the personal data maintained therein within 24 hours of the breach being identified.
ETSI EN 319 401	REQ-7.9-08	Incident management	Where the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, the TSP shall also notify the natural or legal person of the breach of security or loss of integrity without undue delay.

Richtlinie	Referenz	Thema	Anforderung (normativ)
ETSI EN 319 401	REQ-7.9-09	Incident management	The TSP's systems shall be monitored including the monitoring or regular review of audit logs to identify evidence of malicious activity implementing automatic mechanisms to process the audit logs and alert personnel of possible critical security events.
ETSI EN 319 401	REQ-7.9-10	Incident management	The TSP shall address any critical vulnerability not previously addressed by the TSP, within a period of 48 hours after its discovery.
ETSI EN 319 401	REQ-7.9-11	Incident management	For any vulnerability, given the potential impact, the TSP shall [CHOICE]: - create and implement a plan to mitigate the vulnerability; or - document the factual basis for the TSP's determination that the vulnerability does not require remediation.
ETSI EN 319 401	REQ-7.9-12	Incident management	Incident reporting and response procedures shall be employed in such a way that damage from security incidents and malfunctions are minimized.
ETSI EN 319 401	REQ-7.10-01	Collection of evidence	The TSP shall record and keep accessible for an appropriate period of time, including after the activities of the TSP have ceased, all relevant information concerning data issued and received by the TSP, in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service. In particular:
ETSI EN 319 401	REQ-7.10-02	Collection of evidence	The confidentiality and integrity of current and archived records concerning operation of services shall be maintained.
ETSI EN 319 401	REQ-7.10-03	Collection of evidence	Records concerning the operation of services shall be completely and confidentially archived in accordance with disclosed business practices.
ETSI EN 319 401	REQ-7.10-04	Collection of evidence	Records concerning the operation of services shall be made available if required for the purposes of providing evidence of the correct operation of the services for the purpose of legal proceedings.
ETSI EN 319 401	REQ-7.10-05	Collection of evidence	The precise time of significant TSP's environmental, key management, access, clock synchronization events shall be recorded.
ETSI EN 319 401	REQ-7.10-06	Collection of evidence	The time used to record events as required in the audit log shall be synchronized with UTC at least once a day
ETSI EN 319 401	REQ-7.10-07	Collection of evidence	Records concerning services shall be held for a period of time as appropriate for providing necessary legal evidence and as notified in the TSP's terms and conditions (see clause 6.3).
ETSI EN 319 401	REQ-7.10-08	Collection of evidence	The events shall be logged in a way that they cannot be easily deleted or destroyed (except if reliably transferred to long-term media) within the period of time that they are required to be held.
ETSI EN 319 401	REQ-7.11-01	Business continuity management	The TSP shall define and maintain a continuity plan to enact in case of a disaster.

Richtlinie	Referenz	Thema	Anforderung (normativ)
ETSI EN 319 401	REQ-7.11-02	Business continuity management	In the event of a disaster, including compromise of a private signing key or compromise of some other credential of the TSP, operations shall be restored within the delay established in the continuity plan, having addressed any cause for the disaster which may recur (e.g. a security vulnerability) with appropriate remediation measures.
ETSI EN 319 401	REQ-7.12-01	TSP termination and termination plans	Potential disruptions to subscribers and relying parties shall be minimized as a result of the cessation of the TSP's services, and in particular continued maintenance of information required to verify the correctness of trust services shall be provided. In particular:
ETSI EN 319 401	REQ-7.12-02	TSP termination and termination plans	The TSP shall have an up-to-date termination plan. Before the TSP terminates its services at least the following procedures apply:
ETSI EN 319 401	REQ-7.12-03	TSP termination and termination plans	Before the TSP terminates its services, the TSP shall inform the following of the termination: all subscribers and other entities with which the TSP has agreements or other form of established relations, among which relying parties, TSPs and relevant authorities such as supervisory bodies.
ETSI EN 319 401	REQ-7.12-04	TSP termination and termination plans	Before the TSP terminates its services, the TSP shall make the information of the termination available to other relying parties.
ETSI EN 319 401	REQ-7.12-05	TSP termination and termination plans	Before the TSP terminates its services, the TSP shall terminate authorization of all subcontractors to act on behalf of the TSP in carrying out any functions relating to the process of issuing trust service tokens.
ETSI EN 319 401	REQ-7.12-06	TSP termination and termination plans	Before the TSP terminates its services, the TSP shall transfer obligations to a reliable party for maintaining all information necessary to provide evidence of the operation of the TSP for a reasonable period, unless it can be demonstrated that the TSP does not hold any such information.
ETSI EN 319 401	REQ-7.12-07	TSP termination and termination plans	Before the TSP terminates its services, the TSP's private keys, including backup copies, shall be destroyed, or withdrawn from use, in a manner such that the private keys cannot be retrieved.
ETSI EN 319 401	REQ-7.12-08	TSP termination and termination plans	Before the TSP terminates its services, where possible TSP should make arrangements to transfer provision of trust services for its existing customers to another TSP.
ETSI EN 319 401	REQ-7.12-09	TSP termination and termination plans	The TSP shall have an arrangement to cover the costs to fulfil these minimum requirements in case the TSP becomes bankrupt or for other reasons is unable to cover the costs by itself, as far as possible within the constraints of applicable legislation regarding bankruptcy.
ETSI EN 319 401	REQ-7.12-10	TSP termination and termination plans	The TSP shall state in its practices the provisions made for termination of service. This shall include: a) notification of affected entities; and b) transferring the TSP's obligations to other parties.

Richtlinie	Referenz	Thema	Anforderung (normativ)
ETSI EN 319 401	REQ-7.12-11	TSP termination and termination plans	The TSP shall maintain or transfer to a reliable party its obligations to make available its public key or its trust service tokens to relying parties for a reasonable period.
ETSI EN 319 401	REQ-7.13-01	Compliance	The TSP shall ensure that it operates in a legal and trustworthy manner. In particular:
ETSI EN 319 401	REQ-7.13-02	Compliance	The TSP shall provide evidence on how it meets the applicable legal requirements.
ETSI EN 319 401	REQ-7.13-03	Compliance	Trust services provided and end user products used in the provision of those services shall be made accessible for persons with disabilities, where feasible.
ETSI EN 319 401	REQ-7.13-04	Compliance	Applicable standards on accessibility such as ETSI EN 301 549 [i.10] should be taken into account.
ETSI EN 319 401	REQ-7.13-05	Compliance	Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.
ETSI TS 119 511	OVR-6.1-02	Preservation Service Practice Statement	The preservation service provider (PSP) should list or make reference to (e.g. through OIDs), and briefly describe the supported preservation service policies in its preservation service practice statement
ETSI TS 119 511	OVR-6.1-03	Preservation Service Practice Statement	The PSP shall list in its preservation service practice statement the supported preservation profiles.
ETSI TS 119 511	OVR-6.1-04	Preservation Service Practice Statement	The PSP shall state in its preservation service practice statement how the preservation goals are achieved.
ETSI TS 119 511	OVR-6.1-05	Preservation Service Practice Statement	The PSP shall define in its preservation service practice statement how the availability of the submitted data objects (SubDO) and the associated preservation evidences is achieved.
ETSI TS 119 511	OVR-6.1-06	Preservation Service Practice Statement	The PSP shall identify in its preservation service practice statement the obligations of all external organisations supporting the preservation service services including the applicable policies and practices.
ETSI TS 119 511	OVR-6.1-07	Preservation Service Practice Statement	[WST] The PSP shall state in its preservation service practice statement the details on the process of requesting export-import package(s).
ETSI TS 119 511	OVR-6.1-08	Preservation Service Practice Statement	[WST] The PSP shall specify in its preservation service practice statement the production methods of the export-import package(s), see clause 7.16.
ETSI TS 119 511	OVR-6.1-09	Preservation Service Practice Statement	[WST] The PSP shall specify in its preservation service practice statement what happens to the data at the end of the preservation period.
ETSI TS 119 511	OVR-6.2-02	Terms and Conditions	The PSP shall list in the terms and conditions all the preservation service policies it supports.
ETSI TS 119 511	OVR-6.2-03	Terms and Conditions	The PSP shall state where to find information on the supported preservation profiles.

Richtlinie	Referenz	Thema	Anforderung (normativ)
ETSI TS 119 511	OVR-6.2-05	Terms and Conditions	[WST] The PSP shall state in its terms and conditions how the request for an export-import package can be done.
ETSI TS 119 511	OVR-6.4-01	Preservation profiles	A preservation service shall support at least one preservation profile.
ETSI TS 119 511	OVR-6.4-02	Preservation profiles	A preservation service may support more than one preservation profile.
ETSI TS 119 511	OVR-6.4-03	Preservation profiles	A preservation profile shall be uniquely identified.
ETSI TS 119 511	OVR-6.4-04	Preservation profiles	A preservation profile:
ETSI TS 119 511	OVR-6.4-04 a)	Preservation profiles	Shall contain the identifier which uniquely identifies the preservation profile.
ETSI TS 119 511	OVR-6.4-04 b)	Preservation profiles	Shall contain the supported operations of the preservation protocol. For each operation it: Shall contain the supported input formats. [CONDITIONAL] Shall contain additional output formats, in case other output is supported that is different from the supported input format and preservation evidence format.
ETSI TS 119 511	OVR-6.4-04 c)	Preservation profiles	Shall contain a set of applicable technical policies. The set of policies Shall contain the reference to the preservation evidence policy as defined in clause 6.5. [PDS][PDS+PGD] [CONDITIONAL] Shall contain the reference to the signature validation policy as defined in clause 6.6, in case the client does not provide the validation data.
ETSI TS 119 511	OVR-6.4-04 d)	Preservation profiles	Shall contain the validity period of the profile. The validity period: Shall contain the point in time from which on the preservation profile has become or will become active. May contain a point in time until which the preservation profile is active.
ETSI TS 119 511	OVR-6.4-04 e)	Preservation profiles	Shall contain the preservation storage model (WST, WTS or WOS).
ETSI TS 119 511	OVR-6.4-04 f)	Preservation profiles	Shall contain the preservation goals (PDS, PGD, AUG or a combination of them).
ETSI TS 119 511	OVR-6.4-04 g)	Preservation profiles	Shall contain all supported evidence formats.
ETSI TS 119 511	OVR-6.4-04 h)	Preservation profiles	May contain a specification which can be used to refer to a publicly available specification in which the preservation profile is described.
ETSI TS 119 511	OVR-6.4-04 j)	Preservation profiles	May contain an identifier which can be used to refer to a publicly available specification in which the preservation scheme related to the profile is described.
ETSI TS 119 511	OVR-6.4-09	Preservation profiles	The supported preservation profiles shall be available online.
ETSI TS 119 511	OVR-6.4-10	Preservation profiles	A preservation service shall make publicly available all the preservation profiles it supports or that it has supported.
ETSI TS 119 511	OVR-6.4-11	Preservation profiles	[WST] The same preservation profile shall apply during the whole preservation period.

Richtlinie	Referenz	Thema	Anforderung (normativ)
ETSI TS 119 511	OVR-6.4-13	Preservation profiles	The preservation profile should not change over time, thus all dynamic aspects should be specified outside the preservation profile (e.g. the preservation evidence policy or signature validation policy).
ETSI TS 119 511	OVR-6.4-14	Preservation profiles	The preservation evidence policies or signature validation policies referenced by the preservation profile may change over time. However, all versions related to a specific preservation profile shall be publicly available, and it shall be clear which version applied at which time.
ETSI TS 119 511	OVR-6.5-01	Preservation evidence policy	The preservation evidence policy which is referenced by the preservation profile (see OVR-6.4-04) may be in human readable form.
ETSI TS 119 511	OVR-6.5-03	Preservation evidence policy	The preservation evidence policy shall contain the description of how the preservation evidence is created including and which cryptographic algorithms are used.
ETSI TS 119 511	OVR-6.5-04	Preservation evidence policy	The cryptographic algorithms used should be chosen according to TS 119 312 [i.5].
ETSI TS 119 511	OVR-6.5-05	Preservation evidence policy	The preservation evidence policy shall contain the description of which trust service providers (e.g. digital signature creation service or time stamping authorities, certificate status authorities) may be used by the preservation service.
ETSI TS 119 511	OVR-6.5-06	Preservation evidence policy	The preservation evidence policy shall contain how the preservation evidence can be validated, including Which trust anchors can be used to validate digital signatures within the preservation evidence. Which trust anchors can be used to validate time-stamps within the preservation evidence.
ETSI TS 119 511	OVR-6.5-07	Preservation evidence policy	[WST][WTS] The preservation service evidence policy shall state how evidence is augmented.
ETSI TS 119 511	OVR-6.5-08	Preservation evidence policy	The preservation evidence policy shall describe the format of the preservation evidence.
ETSI TS 119 511	OVR-6.5-09	Preservation evidence policy	The preservation evidence policy shall state if and, in this case, how the evidence contains explicit information of the applicable Preservation service, Preservation evidence policy, or Preservation profile.
ETSI TS 119 511	OVR-6.6-01	Signature validation policy	The signature validation policy contained in the preservation profile (see OVR-6.4-04) may be in human readable form.
ETSI TS 119 511	OVR-6.6-03	Signature validation policy	[CONDITIONAL] If present in the preservation profile, the signature validation policy shall state the strategy to how the validation material is selected, e.g. trust anchors, validation model (chain/shell), etc.

Richtlinie	Referenz	Thema	Anforderung (normativ)
ETSI TS 119 511	OVR-6.7-01	Subscriber agreement	The PSP shall provide a subscriber agreement, which shall include an acceptance of the terms and conditions.
ETSI TS 119 511	OVR-6.7-04	Subscriber agreement	[WTS][WST] The PSP shall state in the subscriber agreement who has the right to access to POs including the SubDOs and preservation evidences.
ETSI TS 119 511	OVR-6.7-05	Subscriber agreement	[WTS][WST] The PSP shall state in the subscriber agreement who has the right to request traces on the actions related to the POs.
ETSI TS 119 511	OVR-7.5-02	Cryptographic controls	The PSP shall insure that the time-stamps used in preservation process come from a TSA that follows state-of-the-art practices for policy and security requirements for trust service providers issuing time-stamps. In particular the TSA should conform to ETSI EN 319 421 [i.11].
ETSI TS 119 511	OVR-7.5-03	Cryptographic controls	The PSP should only use in preservation process time-stamps that are verifiable using CRLs or OCSP responses which include a 'reason code' in case of the revocation of a public key certificate.
ETSI TS 119 511	OVR-7.5-05 a)	Cryptographic controls	Is a trustworthy system which is assured to EAL 4 or higher in accordance with ISO/IEC 15408 [3], or equivalent national or internationally recognized evaluation criteria for IT security. This shall be to a security target or protection profile which meets the requirements of the present document, based on a risk analysis and taking into account physical and other non-technical security measures; or
ETSI TS 119 511	OVR-7.5-05 b)	Cryptographic controls	Meets the requirements identified in ISO/IEC 19790 [4] or FIPS PUB 140-2 [5], level 3.
ETSI TS 119 511	OVR-7.8-02	Network security	[WST] The preservation service shall be integrated in the IT environment implemented in such a way that all storage access by the preservation client changing the content of the storage cannot bypass the preservation service.
ETSI TS 119 511	OVR-7.10-02	Collection of evidence	The preservation service shall implement event logs to establish information needed for later proofs.
ETSI TS 119 511	OVR-7.12-02	TSP termination and termination plans	[WST] The termination plan shall include what happens with the stored POs at the termination of the preservation service.
ETSI TS 119 511	OVR-7.14-01	Cryptographic monitoring	For every supported active preservation profile, the TSP shall monitor the strength of every cryptographic algorithm that was used in connection with this profile. In case, one of the used algorithms or parameters is thought to become less secure or the validity of a relevant certificate is going to expire, it shall either update the related preservation evidence policy or create a new preservation profile to handle newly submitted POs.

Richtlinie	Referenz	Thema	Anforderung (normativ)
ETSI TS 119 511	OVR-7.14-02	Cryptographic monitoring	[WST] [CONDITIONAL] If one of the algorithms or parameters which were used in a preservation evidence, is thought to become less secure or the validity of a relevant certificate is going to expire, the preservation evidence shall be augmented by the preservation service according to a new version of the preservation evidence policy during the preservation period.
ETSI TS 119 511	OVR-7.14-03	Cryptographic monitoring	For the evaluation of the cryptographic algorithms in OVR-7.14.01 and OVR-7.14.02, ETSI TS 119 312 [i.5] should be considered.
ETSI TS 119 511	OVR-7.15-01	Augmentation of preservation evidences	[WST] During the preservation period, the preservation service shall make sure that the preservation evidence can be used to achieve the corresponding preservation goal.
ETSI TS 119 511	OVR-7.15-03	Augmentation of preservation evidences	[WST] [WTS] The preservation service shall augment the preservation evidences before they cannot be used anymore to achieve the corresponding preservation goal, to make sure that OVR-7.15-01 or OVR-7.15-02 is fulfilled.
ETSI TS 119 511	OVR-7.16-01	Export-Import package	[WST] The PSP shall allow the preservation client or another authorized preservation service to request the export-import package(s), containing the preserved data, the evidences and all information needed to validate the evidences.
ETSI TS 119 511	OVR-7.16-02	Export-Import package	[WST] The PSP should use standardised format for the export-import package(s).
ETSI TS 119 511	OVR-7.16-03	Export-Import package	[WST] The export-import package shall only be delivered to an authorized legal or natural person or preservation client.
ETSI TS 119 511	OVR-7.16-04	Export-Import package	[WST] The PSP shall keep records of all released export-import packages including:
ETSI TS 119 511	OVR-7.16-04 1)	Export-Import package	the date of the event
ETSI TS 119 511	OVR-7.16-04 2)	Export-Import package	the criteria that has been used to select the set of preservation objects to be included in the export-import package
ETSI TS 119 511	PRP-8.1-01	Preservation protocol	The communication channel between the preservation client and the PSP shall be secured, i.e. the PSP shall offer a way to be authenticated by the client and the confidentiality of the data shall be ensured.
ETSI TS 119 511	PRP-8.1-02	Preservation protocol	The preservation protocol as defined in ETSI TS 119 512 [i.13] should be used.
ETSI TS 119 511	PRP-8.1-03	Preservation protocol	The protocols shall be protected against unauthorised usage.
ETSI TS 119 511	PRP-8.1-04	Preservation protocol	A preservation service shall allow to retrieve information about the currently and previously supported preservation profiles.
ETSI TS 119 511	PRP-8.1-05	Preservation protocol	A preservation service shall allow one or more submission data objects (SubDO) to be preserved under a specific preservation profile, and to receive back either a preservation object identifier or to receive back immediately a preservation evidence (synchronous mode).

Richtlinie	Referenz	Thema	Anforderung (normativ)
ETSI TS 119 511	PRP-8.1-06	Preservation protocol	A preservation service may allow to get the traces of all operations related to a specific preservation object identifier.
ETSI TS 119 511	PRP-8.1-07	Preservation protocol	A preservation service may allow to search for specific preservation objects and retrieve a set of preservation object identifiers, which can be used in other operations, like for example PRP-8.1-05.
ETSI TS 119 511	PRP-8.1-08	Preservation protocol	A preservation service may allow to submit to the preservation service a preservation evidence and a sequence of POs to which the evidence corresponds, in order to validate the evidence and to receive back a preservation evidence validation report.
ETSI TS 119 511	PRP-8.1-10	Preservation protocol	[WST] A preservation service with storage shall allow to retrieve evidences and/or preservation objects (POs).
ETSI TS 119 511	PRP-8.1-11	Preservation protocol	[WST] A preservation service with storage shall allow to delete stored POs. In case the deletion of the preservation evidence the corresponding SubDO shall be deleted as well. The preservation service shall assure that stored POs can only be deleted before expiry of the preservation period when the delete request will be submitted together with a justification. The preservation service shall log any DeletePO requests and the accompanying justifications.
ETSI TS 119 511	PRP-8.1-12	Preservation protocol	[WST] The preservation service shall assure that stored POs can only be deleted before the end of the preservation period when the delete request will be submitted together with a justification. Any submitted justification shall be logged together with the information of the deletion request.
ETSI TS 119 511	PRP-8.1-13	Preservation protocol	[WST] A preservation service with storage should allow to request a set of preservation object identifiers, which can be used to retrieve or delete POs as in PRP-8.1-05 and PRP-8.1-06.
ETSI TS 119 511	PRP-8.1-14	Preservation protocol	[WST] A preservation service with storage may allow to provide a new version of an already submitted POC. The newly provided version may be specified only by the difference to the previous version.
ETSI TS 119 511	OVR-9.2-01	Preservation evidences	[CONDITIONAL] If the preservation service uses a time-stamp token it shall conform to IETF RFC3161 [i.23] and updated by RFC 5816 [i.18].
ETSI TS 119 511	OVR-9.2-02	Preservation evidences	[CONDITIONAL] If the preservation service uses a time-stamp token it should conform to the time-stamping protocol and time-stamp token profiles as defined ETSI EN 319 422 [i.11].
ETSI TS 119 511	OVR-9.2-03	Preservation evidences	[CONDITIONAL] If the preservation service uses an evidence record it shall conform to IETF RFC 4998 [i.25] or IETF RFC 6283 [i.27].
ETSI TS 119 511	OVR-9.3-01	Preservation of digital signatures	[PDS][PDS+PGD] [CONDITIONAL] If the validation data is not submitted by the preservation client, the preservation service shall make its best efforts to collect and verify the validation data according to the signature validation policy supported by the preservation profile (see clause 6.6).

Richtlinie	Referenz	Thema	Anforderung (normativ)
ETSI TS 119 511	OVR-9.3-04	Preservation of digital signatures	[PDS+PGD] To extend the ability to validate a digital signature and to maintain its validity status, the preservation service shall, on one side, provide a proof of existence of the signature and of the validation data needed to validate the signature and on the other side a proof of existence of the signed data.
ETSI TS 119 511	OVR-A-01	Assessment criteria for Annex A (normative): Qualified preservation service for QES as defined by article 34 the Regulation (EU) No 910/2014	[PDS] [PDS+PGD] All requirements from clause 5 to 9 shall apply. In addition:
ETSI TS 119 511	OVR-A-02	Assessment criteria for Annex A (normative): Qualified preservation service for QES as defined by article 34 the Regulation (EU) No 910/2014	[PDS] [PDS+PGD] The preservation service shall preserve all information needed to check the qualification status of the electronic signature or seal that would not be publicly available until the end of the preservation period.
ETSI TS 119 511	OVR-A-03	Assessment criteria for Annex A (normative): Qualified preservation service for QES as defined by article 34 the Regulation (EU) No 910/2014	[PDS] [PDS+PGD] Time-stamps used within the preservation evidence should be provided by a qualified TSA.
ETSI TS 119 511	OVR-A-04	Assessment criteria for Annex A (normative): Qualified preservation service for QES as defined by article 34 the Regulation (EU) No 910/2014	The preservation service shall have one service digital identifier as defined in 5.5.3 of ETSI TS 119 612 [2] which allows to uniquely and unambiguously identify the service within an EUMS trusted list.