Bundesamt
für Sicherheit in der
Informationstechnik

BSI Technische Richtlinie 03138 Ersetzendes Scannen

Bezeichnung:	Ersetzendes Scannen(RESISCAN) Häufig gestellte Fragen
Kürzel:	BSI TR 03138-F
Version:	1.2
Datum:	15.06.2018

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: resiscan@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

1 Vorbemerkung

Dieses Dokument enthält Antworten auf häufig gestellte Fragen im Umfeld der BSI TR-03138 (RESISCAN).

Weitere Fragen zu dieser Richtlinie oder Hinweise zu diesem Dokument sollten Sie bitte an das E-Mail-Postfach resiscan@bsi.bund.de senden.

2 Generelle Fragen zur BSI TR-03138

2.1 Was ist Gegenstand der BSI TR-03138?

Die Technische Richtlinie (TR) 03138 „Ersetzendes Scannen“ des BSI bietet einen Handlungsleitfaden zur möglichst rechtssicheren Gestaltung der Prozesse und Systeme für das ersetzende Scannen. Dies umfasst die Phasen „Dokumentenvorbereitung“, „Scannen“, „Nachverarbeitung“ und „Integritätssicherung“ des „generischen Scanprozesses“ (vgl. [BSI TR-03138], Abschnitt 2.1).

2.2 Was regelt die BSI TR-03138 nicht?

Die BSI TR-03138 regelt insbesondere nicht die Zulässigkeit des ersetzenden Scannens als solches. Die Zulässigkeit des ersetzenden Scannens ist von jedem Anwender in seinem Anwendungs- und Verantwortungsbereich auf der Grundlage der für diesen einschlägigen Rechtsvorschriften zu prüfen. Rechtliche Betrachtungen hierzu finden sich beispielsweise in [BSI TR-03138-R].
Außerdem ist die beweiskräftige Aufbewahrung nicht Gegenstand der BSI TR-03138. Der Beweiswerterhalt kryptographisch signierter Dokumente ist in [BSI TR-03125] geregelt.

2.3 Wer kann die BSI TR-03138 anwenden?

Die BSI TR-03138 richtet sich an Betreiber von Scansystemen (Endanwender und Scandienstleister) und kann in den verschiedensten Branchen, wie z.B. Justiz, Verwaltung, Wirtschaft und Gesundheitswesen angewandt werden.

3 Fragen zur Zertifizierung

3.1 Ist eine Zertifizierung verpflichtend?

Die Zertifizierung gemäß BSI TR-03138 ist freiwillig, aber grundsätzlich empfehlenswert. Im Rahmen der Zertifizierung wird die Erfüllung der Anforderungen von einer unabhängigen Stelle (Auditor) geprüft und von der Zertifizierungsstelle des BSI bestätigt.

Hierdurch kann nachgewiesen werden, dass der Scanprozess mit Sicherheitsmaßnahmen nach dem Stand der Technik geschützt wird und Scanprodukte mit den Papierdokumenten bildlich und inhaltlich übereinstimmen, wenn sie lesbar gemacht werden (vgl. § 7 [EGovG]). Ein solcher Nachweis belegt die Qualität des implementierten Scanprozesses gegenüber potenziellen Kunden und Aufsichtsorganen und kann sich im Streitfall vor Gericht als besonders bedeutsam erweisen.

3.2 Genügt eine „Eigenerklärung“ für die Konformität zur TR?

Durch eine Zertifizierung gemäß BSI TR-03138 kann der qualifizierte Nachweis erbracht werden, dass ein Scanprozess konform zur TR implementiert wurde. Wie in Abschnitt 3.1 erläutert, ist die Zertifizierung freiwillig und ein Scanprozess kann selbstverständlich auch ohne ein formales Zertifizierungsverfahren konform zur TR gestaltet und betrieben werden.

Es spricht grundsätzlich auch nichts dagegen, dass die Prüfspezifikation [BSI TR-03138-P] unabhängig von einem formalen Zertifizierungsverfahren vom Verantwortlichen für den Scanprozess genutzt wird, um die Erfüllung der Anforderungen der TR systematisch zu überprüfen und zu dokumentieren. Da eine vom Verantwortlichen ausgefüllte Prüfspezifikation auch die Grundlage der Zertifizierung bildet, ist sie in jedem Fall empfehlenswert.

Die Prozesse des BSI sehen jedoch bislang keine „Eigenerklärung“ vor, mit der die Konformität zur TR allein auf Basis einer ausgefüllten Prüfspezifikation „behauptet“ werden könnte.

Für Scandienstleister wird die formale Zertifizierung gemäß BSI TR-03138 besonders nachdrücklich empfohlen.

3.3 Wie läuft das Zertifizierungsverfahren ab?

Beim Zertifizierungsverfahren gemäß BSI TR-03138 handelt es sich um eine so genannte „Zertifizierung nach Technischen Richtlinien“.

Der generelle Ablauf einer solchen Zertifizierung ist auf der Webseite des BSI unter „Themen“ / „Zertifizierung und Anerkennung“ / „Zertifizierung von Produkten“ / „Zertifizierung nach TR“ / „Allgemeine Informationen zur Zertifizierung nach Technischen Richtlinien“ beschrieben.

3.4 Wo finde ich das Antragsformular für die Zertifizierung?

Das zur Eröffnung eines Zertifizierungsverfahrens gemäß BSI TR-03138 notwendige Antragsformular findet sich unter „Themen“ / „Zertifizierung und Anerkennung“ / „Zertifizierung von Produkten“ / „Zertifizierung nach TR“ / „Antragsformulare & Kontaktdaten zur Zertifizierung nach Technischen Richtlinien“.

3.5 Welche Kosten sind mit der Zertifizierung verbunden?

Für eine Zertifizierung gemäß BSI TR-03138 fallen Kosten für anerkannte Auditoren und zusätzlich eine Verwaltungsgebühr (derzeit 2.600 €) beim BSI für die Durchführung des Verfahrens an.

4 Fragen zur Verfahrensdokumentation

4.1 Was muss bzw. soll die Verfahrensdokumentation enthalten?

Die Mindestanforderungen für die Verfahrensdokumentation sind in Anforderung A.G.1 (siehe [BSI TR-03138], Abschnitt 4.2.1.1) definiert.

4.2 Gibt es formale Vorgaben für die Verfahrensdokumentation?

Nein. Es gibt keine formalen Vorgaben für die Erstellung und Pflege der Verfahrensdokumentation.

Eine generische Vorlage für eine Verfahrensanweisung, die regelmäßig Bestandteil der Verfahrensdokumentation ist, findet sich in [BSI TR-03138-V].

5 Fragen zum Scannen

5.1 Welche Auflösung ist beim Scannen ausreichend?

Welche Auflösung beim Scannen notwendig ist, hängt letztlich von der Charakteristik der im Scanprozess verarbeiteten Dokumente ab. Für „typische Dokumente“ ist im Regelfall eine Auflösung von 300dpi ausreichend.

5.2 Gibt es Vorgaben bzgl. der Stichprobenquote für die Qualitätssicherung der Scanprodukte?

Durch die Qualitätssicherung gemäß A.SC.8 (siehe [BSI TR-03138], Abschnitt 4.2.6.8) soll letztlich sichergestellt werden, dass *alle* im Scanprozess entstehenden elektronischen Dokumente (Scanprodukte), wenn sie lesbar gemacht werden, bildlich und inhaltlich mit den Papierdokumenten übereinstimmen.

Deshalb muss die Stichprobenquote so dimensioniert werden, dass eine fehlerhafte Erfassung im implementierten Scanprozess mit großer Wahrscheinlichkeit entdeckt wird.

A.SC.8 empfiehlt, dass sich die Stichprobenquote am Scan-Durchsatz, dem Schutzbedarf und nicht zuletzt der Zuverlässigkeit des Scansystems orientieren sollte.

Hierbei kann die Bandbreite von einer vollständigen Überprüfung der Scanprodukte, die unter Umständen im Rahmen der inhaltlichen Sachbearbeitung erfolgen kann, bis hin zu einer vergleichsweise geringen Stichprobe von 2 % der eingescannten Dokumente reichen.

6 Fragen zur Nachbearbeitung

6.1 Ist eine Umsetzung des Vier-Augen-Prinzips auch im nachgelagerten Bearbeitungsprozess möglich?

Beim „Vier-Augen-Prinzip“ gemäß A.AM.IN.SH.1 ([BSI TR-03138], Abschnitt 4.3.3.1) wird gefordert, dass die Erstellung und Qualitätssicherung von unterschiedlichen Personen durchgeführt wird.

Diese Anforderung kann auf vielfältige Weise umgesetzt werden. Eine mögliche Umsetzung ist, dass die Qualitätssicherung im Rahmen der dem Erfassungsprozess nachgelagerten Sachbearbeitung erfolgt und das Scannen und die Sachbearbeitung von unterschiedlichen Personen durchgeführt wird. Allerdings ist in diesem Fall zu beachten, dass bildliche und inhaltliche Übereinstimmung erst im Rahmen der spät erfolgenden Qualitätssicherung festgestellt und erst dann im Transfervermerk dokumentiert werden kann.

6.2 Welche Änderungen am Digitalisat (Leerseitenentfernung, Seitenausrichtung, Kontrastverstärkung etc.) sind zulässig?

Rechtlich maßgeblich ist häufig (vgl. § 7 [EGovG]) die bildliche und inhaltliche Übereinstimmung zwischen Scanprodukt und Papierdokument. Insofern sind Änderungen am Digitalisat nur dann zulässig, sofern die Lesbarkeit erhöht wird und die bildliche und inhaltliche Übereinstimmung gewährleistet bleibt. Sofern eine Nachbearbeitung erfolgt, sind die Anforderungen A.NB.1 ([BSI TR-03138], Abschnitt 4.2.7.1) und A.NB.2 ([BSI TR-03138], Abschnitt 4.2.7.2) zu beachten.

6.3 Ist die oftmals im Transfervermerk bestätigte bildliche Übereinstimmung auch beim Schwarz-Weiß-Scannen gewährleistet?

Nein. Sofern die einschlägigen rechtlichen Rahmenbedingungen neben der inhaltlichen auch die bildliche Übereinstimmung zwischen Scanprodukt und Papierdokument fordern, muss die Erfassung in Farbe erfolgen.

Sofern vom Gesetzgeber lediglich die inhaltliche Übereinstimmung gefordert wäre, so könnte die Erfassung in schwarz-weiß bzw. Graustufen erfolgen, sofern den Farben im Papierdokument keine inhaltliche Bedeutung zukommt. Siehe auch [RFJW08] und [RoJa08].

6.4 Welche Mindestangaben sind im Transfervermerk erforderlich?

Die Angaben, die der Transfervermerk mindestens enthalten soll, sind in A.NB.4 (siehe [BSI TR-03138], Abschnitt 4.2.7.4) dokumentiert.

6.5 Bezieht sich der Transfervermerk bei der Stapelverarbeitung auf ein einzelnes Dokument oder auf einen Stapel?

Sofern regelmäßig eine Stapelverarbeitung erfolgt, kann der Transfervermerk für einen verarbeiteten Stapel erstellt und mit den einzelnen Dokumenten logisch verknüpft werden.

6.6 Muss der Transfervermerk jeweils zusammen mit dem Dokument abgelegt oder in diesen integriert werden?

A.NB.4 (siehe [BSI TR-03138], Abschnitt 4.2.7.4) fordert, dass der Transfervermerk „mit dem Scanprodukt logisch verknüpft oder in das Scanprodukt integriert werden“ muss.

7 Fragen zur Integritätssicherung

7.1 Welchen Sinn und Zweck haben Signaturen, Siegel und Zeitstempel im Scanprozess?

Die im Scanprozess erstellten Signaturen, Siegel und Zeitstempel dienen dem Integritätsschutz der Scanprodukte und der zugehörigen Transfervermerke. Mit Zeitstempeln kann zudem Nachweis der Existenz der entsprechenden Daten zu einem bestimmten Zeitpunkt erbracht werden. Durch die im Scanprozess erstellten Signaturen und Siegel kann im Regelfall nicht die Authentizität des ursprünglichen Papierdokumentes, sondern lediglich die Authentizität des daraus abgeleiteten Scanproduktes und des Transfervermerkes nachgewiesen werden. Insofern kommt beim Einsatz qualifizierter elektronischer Signaturen, wie in [BSI TR-03138-R] (Abschnitt R.2.7.2) näher erläutert, nur der Transfervermerk, aber nicht eine möglicherweise im ursprünglichen Papierdokument verfasste Erklärung, in den Genuss der Beweisregel des § 371a ZPO.

7.2 Welche Daten sollen Signaturen, Siegel und Zeitstempel umfassen?

Grundsätzlich soll sich die Integritätssicherung auf die Verfahrensdokumentation und alle im Scanprozess entstehenden Daten beziehen, die später unter Umständen für Beweiszwecke herangezogen werden sollen. Dies umfasst insbesondere die Scanprodukte und Transfervermerke sowie möglicherweise auch die Index- und Metadaten sowie Protokolldaten.

7.3 Welche Formate sollen für Signaturen, Siegel, Zeitstempel etc. genutzt werden?

In A.AM.IN.H.1 ([BSI TR-03138], Abschnitt 4.3.2.1) und beispielsweise auch [BSI TR-03125-F] (Abschnitt 5.1) wird hierfür der Einsatz von standardisierten Formaten, wie z.B. [CAdES], [PAdES], [XAdES], [ASiC], [RFC3161], [RFC4998] und [RFC6283], empfohlen.

7.4 Ist ein Scanprozess mit fortgeschrittener oder qualifizierter elektronischer Signatur bzw. Siegel in einem separaten Netz möglich?

Für die Validierung von fortgeschrittenen oder qualifizierten elektronischen Signaturen und Siegeln wird regelmäßig das Online Certificate Status Protocol (OCSP) gemäß [RFC6960] genutzt, das im Regelfall eine ausgehende Verbindung über http (Port 80) oder https (Port 443) voraussetzt. In ähnlicher Form wird bei der Fernsignatur im Regelfall eine ausgehende https-Verbindung (Port 443) benötigt. Sofern diese Kommunikationsanforderungen in der Netzwerk- und Firewallkonfiguration entsprechend berücksichtigt werden, können fortgeschrittene oder qualifizierte elektronische Signaturen und Siegel auch in einem separaten Netz erstellt und validiert werden.

7.5 In welchen Fällen müssen bzw. sollen qualifizierte elektronische Signaturen, Siegel und Zeitstempel eingesetzt werden?

Wie in A.AM.IN.SH.2 ([BSI TR-03138], Abschnitt 4.3.3.2) spezifiziert, sollen für die Integritätssicherung des Scanproduktes bzw. des Transfervermerkes qualifizierte elektronische Signaturen oder qualifizierte elektronische Siegel und qualifizierte Zeitstempel eingesetzt werden, sofern Datenobjekte

a) mit einem Schutzbedarf von „sehr hoch“ bezüglich der Integrität verarbeitet werden,

b) die Verkehrsfähigkeit gefordert ist und

c) die im Rahmen des Scanprozesses entstandenen Datenobjekte (Scanprodukt, Transfervermerk, Index- und Metadaten, Protokolldaten) voraussichtlich als Beweismittel genutzt werden.

Ob der Einsatz qualifizierter elektronischer Signaturen, Siegel und/oder Zeitstempel auch in anderen Fällen sinnvoll ist, hängt häufig nicht zuletzt von wirtschaftlichen Aspekten ab.

7.6 Können elektronische Siegel statt elektronischer Signaturen eingesetzt werden?

Wie in Abschnitt 7.1 erläutert, dienen elektronische Signaturen, Siegel und Zeitstempel im Scanprozess vor allem der Integritätssicherung. Sofern – z.B. anhand des Transfervermerk gemäß A.NB.4 (siehe [BSI TR-03138], Abschnitt 4.2.7.4) – ermittelt werden kann, welche natürliche Person den Scanprozess verantwortet und das Scanprodukt erzeugt hat, können statt elektronischer Signaturen, die unmittelbar einer natürlichen Person zugeordnet sind, auch elektronische Siegel eingesetzt werden, die einer juristischen Person zugeordnet sind.

7.7 Wie viele elektronische Signaturen, Siegel und/oder Zeitstempel sollen beim Scannen einer elektronischen Akte angebracht werden?

Wie viele elektronische Signaturen, Siegel oder Zeitstempel beim Scannen einer elektronischen Akte angebracht werden sollen, hängt nicht nur vom Schutzbedarf der verarbeiteten Daten[1], sondern auch von der detaillierten technischen und organisatorischen Ausgestaltung des Scanprozesses ab, so dass es hierzu leider keine einfache und pauschal gültige Antwort gibt.

Wie in Abschnitt 7.8 erläutert, sollte die Integritätssicherung zu einem möglichst frühen Zeitpunkt erfolgen. Außerdem sollte zur Gewährleistung der Verkehrsfähigkeit die Integrität einzelner Datenobjekte prüfbar sein. Auf der anderen Seite wird man schon allein aus ökonomischen Gründen bestrebt sein, möglichst wenige Signaturen, Siegel oder Zeitstempel zu verwenden.

Um einen verkehrsfähigen Integritätsschutz mit wenigen Zeitstempeln zu erreichen, kann der Einsatz von Merkle-Hashbäumen gemäß [RFC4998] bzw. [RFC6283] sinnvoll sein.

Beim Einsatz von XML-basierten Signaturen können in ähnlicher Weise mehrere Datenobjekte und Dokumente mit entsprechenden `ds:Object`- (siehe [XML-DSig], Abschnitt 8) und `ds:Manifest`-Elementen (siehe [XML-DSig], Abschnitt 9.1) mit einer Signatur geschützt werden.

1 Vgl. A.IS.1 ([BSI TR-03138], Abschnitt 4.2.8), A.AM.IN.H.1 ([BSI TR-03138], Abschnitt 4.3.2.1) und A.AM.IN.SH.2 ([BSI TR-03138], Abschnitt 4.3.3.2)

7.8 Wann sollte die Integritätssicherung erfolgen?

Grundsätzlich sollte die Integrität der im Scanprozess entstehenden Datenobjekte (Scanprodukt, Index- und Metadaten, Transfervermerk, Protokolldaten etc.) jeweils möglichst umgehend nach ihrer Erzeugung gesichert werden, damit ab diesem möglichst frühen Zeitpunkt unentdeckte Manipulationen ausgeschlossen werden können.

Wie streng diese generelle Empfehlung ausgelegt werden sollte, hängt vom Schutzbedarf der verarbeiteten verarbeiteten Datenobjekte und den zum Schutz temporärer Zwischenspeicher implementierten Sicherheitsmaßnahmen ab.

8 Sonstige Fragen

8.1 Was ist der Unterschied zwischen A.AM.IN.H.6 und A.AM.IN.SH.3?

In A.AM.IN.H.6 ([BSI TR-03138], Abschnitt 4.3.2.6) wird gefordert, dass das für den Scanprozess relevante Netzwerksegment durch ein Sicherheitsgateway (Firewall) geschützt ist, das nur Kommunikationsverbindungen zulässt, die von innen aufgebaut werden. Sofern der Schutzbedarf lediglich „hoch“ ist, könnte es sich bei diesem Netzwerksegment um ein auch für andere Zwecke (z.B. Bürokommunikation) genutztes Netz handeln. Bei einem Schutzbedarf von „sehr hoch“ fordert A.AM.IN.SH.3 ([BSI TR-03138], Abschnitt 4.3.3.3) jedoch, dass sich das Scansystem in einem eigenständigen Netz befindet, in dem nur die für den Scanprozess benötigten System eingebunden sind.

Was bedeutet „zuverlässig gelöscht“ in A.AM.VT.H.3 und A.AM.VT.SH.2?
In A.AM.VT.H.3 ([BSI TR-03138], Abschnitt 4.3.4.3) und A.AM.VT.SH.2 ([BSI TR-03138], Abschnitt 4.3.5.2) wird gefordert, dass temporär abgespeicherte Zwischenergebnisse bzw. komplette Datenträger „zuverlässig gelöscht“ werden müssen. Was bedeutet das genau?
Eine Löschung ist dann zuverlässig, wenn ein „Angreifer“ mit einem dem Schutzbedarf entsprechenden Angriffspotenzial die gelöschten Daten nicht rekonstruieren kann. Welche Maßnahmen hierfür genau notwendig sind, hängt von der eingesetzten Speichertechnologie ab.
Die Maßnahme M 2.167 (Auswahl geeigneter Verfahren zur Löschung oder Vernichtung von Daten) geht näher auf das Löschen und Vernichten von Daten bei verschiedenen Speichertechnologien ein.

Literaturverzeichnis

[ASiC] ETSI: Electronic Signatures and Infrastructures (ESI); Associated Signature Containers (ASiC); EN 319 162

[BSI TR-03125] Bundesamt für Sicherheit in der Informationstechnik (BSI): Beweiswerterhaltung kryptographisch signierter Dokumente (TR-ESOR), BSI TR-03125, Version 1.2.1, 2018

[BSI TR-03125-F] Bundesamt für Sicherheit in der Informationstechnik (BSI): Beweiswerterhaltung kryptographisch signierter Dokumente (TR-ESOR), Anlage F – Formate, BSI TR-03125-F, Version 1.2.1, 2018

[BSI TR-03138] Bundesamt für Sicherheit in der Informationstechnik (BSI): Ersetzendes Scannen, Technische Richtlinie (TR) des BSI Nr. 03138, Version 1.2, 2018

[BSI TR-03138-A] Bundesamt für Sicherheit in der Informationstechnik (BSI): Ersetzendes Scannen – Anwendungshinweis A: Ergebnis der Risikoanalyse, BSI TR- 03138-A, Version 1.2, 2018

[BSI TR-03138-P] Bundesamt für Sicherheit in der Informationstechnik (BSI): Ersetzendes Scannen – Anlage P: Prüfspezifikation, BSI TR-03138-P, Version 1.3, 2018

[BSI TR-03138-R] Bundesamt für Sicherheit in der Informationstechnik (BSI): Ersetzendes Scannen – Anwendungshinweis A: Unverbindliche rechtliche Hinweise, BSI TR-03138-R, Version 1.2, 2018

[BSI TR-03138-V] Bundesamt für Sicherheit in der Informationstechnik (BSI): Ersetzendes Scannen – Anwendungshinweis V: Exemplarischen Verfahrensanweisung, BSI TR-03138-V, Version 1.2, 2018

[CAdES] ETSI: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures, EN 319 122

[EGovG] Gesetz zur Förderung der elektronischen Verwaltung (E-Government-Gesetz - EGovG)

[eIDAS-VO] 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, http://data.europa.eu/eli/reg/2014/910/oj

[ETSI TS 119 312] ETSI TS 119 312: Electronic Signatures and Infrasctructures (ESI); Cryptographic Suites

[PAdES] ETSI: Electronic Signatures and Infrastructures (ESI), PAdES digital signatures; EN 319 142

[RFC3161] C. Adams, P. Cain, D. Pinkas, R. Zuccherato: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). IETF RFC 3161, http://www.ietf.org/rfc/rfc3161.txt

[RFC4998] T. Gondrom, R. Brandner, U. Pordesch: Evidence Record Syntax (ERS), IETF RFC 4998, http://www.ietf.org/rfc/rfc4998.txt

[RFC6283] A. J. Blazic, S. Saljic, T. Gondrom: Extensible Markup Language Evidence Record Syntax (XMLERS), IETF RFC 6283, http://www.ietf.org/rfc/rfc6283.txt

[RFC6960] S. Santesson, M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, IETF RFC 6960, http://www.ietf.org/rfc/rfc6960.txt

[RFJW08] A. Roßnagel, S. Fischer-Dieskau, S. Jandt, D. Wilke: *Scannen von Papierdokumenten – Anforderungen, Trends und Empfehlungen*, Band 18 der Reihe „Der elektronische Rechtsverkehr“, Nomos, 2008

[RoJa08] A. Roßnagel, S. Jandt: *Handlungsleitfaden zum Scannen von Papierdokumenten.* Herausgegeben im Auftrag des Bundesministeriums für Wirtschaft und Technologie, Nr. 571, Berlin April 2008

[XAdES] ETSI: Electronic Signatures and Infrastructures (ESI); XAdES digital signatures; EN 319 132

[XML-DSig] W3C: XML Signature Syntax and Processing, Version 2.0, W3C Working Group Note 23 July 2015, https://www.w3.org/TR/xmldsig-core2/