

TR-03186 Empfehlungen zu Siegeldiensten

Berlin, 21.01.2025

Ausgangssituation



- Die eIDAS-VO (Verordnung (EU) Nr. 910/2014) ist die rechtliche Grundlage für elektronische Signaturen und Siegel:

„Elektronische Siegel sollten als Nachweis dafür dienen, dass ein elektronisches Dokument von einer juristischen Person ausgestellt wurde, und sollten den Ursprung und die Unversehrtheit des Dokuments belegen.“

- Die qualifizierte elektronische Signatur und das qualifizierte elektronische Siegel sind grundsätzlich bekannt in der öffentlichen Verwaltung
- Qualifizierte Vertrauensdienste sind in DE und EU verfügbar

Motivation

Ausgangssituation



BSI

Veröffentlichte Richtlinien

BSI TR-01201 De-Mail

BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen

BSI TR-02103 X.509-Zertifikate und Zertifizierungspfadvalidierung

BSI TR-03104 Produktionsdatenerfassung, -qualität und -sicherheit

BSI TR-03105 Conformity Assessment

BSI TR-03106 eHealth

BSI TR-03107 Elektronische Identifizierung

BSI TR-03108 Sicherer E-Mail

BSI TR-03109 Technische Verfahren

BSI TR-03110 Advanced Security

BSI TR-03111 Elliptische-Kurven

BSI TR-03112 Das eCard-API-Format

BSI TR-03114 Stapelsignatur mit

BSI TR-03115 Komfortsignatur mit

Bundesnetzagentur

Grundlagen

Leitfäden der Agentur der Europäischen Union für Cybersicherheit (ENISA)

Die Agentur der Europäischen Union für Cybersicherheit ([European Network and Information Security Agency](#))

Die Richtlinien sind bei [European Network and Information Security Agency](#)

Wir weisen insbesondere auf folgende Richtlinien hin:

- Guidelines on Initiation of Qualified Trust Services
- Guidelines on Supervision of Qualified Trust Services
- Guidelines on Termination of Qualified Trust Services

(EN) und Europäische Normen (EN), ETSI

ETSI Electronic Signatures and Trust Infrastructures Activities

Test specifications

- TR 119 124-1: CAAdES digital signatures Testing; Part 1: Overview
- TS 119 124-2: CAAdES digital signatures Testing; Part 2: Test suites for test
- TS 119 124-3: CAAdES digital signatures Testing; Part 3: Test suites for
- TS 119 124-4: CAAdES digital signatures Testing; Part 4: Test
- TS 119 124-5: CAAdES digital signatures Testing; Part 5: Test
- TR 119 134-1: XAdES digital signatures Testing; Part 1: Overview
- TS 119 134-2: XAdES digital signatures Testing; Part 2: Test suites for
- TS 119 134-3: XAdES digital signatures Testing; Part 3: Test suites for
- TS 119 134-4: XAdES digital signatures Testing; Part 4: Test
- TS 119 134-5: XAdES digital signatures Testing; Part 5: Test
- TR 119 144-1: PAdES digital signatures Testing; Part 1: Overview
- TS 119 144-2: PAdES digital signatures Testing; Part 2: Test suites for
- TS 119 144-3: PAdES digital signatures Testing; Part 3: Test suites for
- TS 119 144-4: PAdES digital signatures Testing; Part 4: Test
- TR 119 144-5: PAdES digital signatures Testing; Part 5: Test

BSI TR-03125 TR-ESOR

13 Quellenverzeichnis

[1999/93/EC] *Directive 1999/93/EC of the European Parliament and of the Council on a legal framework for electronic signatures*, <http://data.europa.eu/eli/dir/1999/93/EC>, No longer in force, Date of end of validity: 30/06/2016; Repealed by [32002/L0013](#)

[2012/0146/COD] *European Commission. Procedure 2012/0146/COD, Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on electronic trust services for electronic transactions in the internal market*, http://eur-lex.europa.eu/procedure/EN/2012_146, June 2012.

[2015/1506/EU] *COMMISSION IMPLEMENTING DECISION (EU) 2015/1506 of 8 September 2015 laying down specifications relating to formats of advanced electronic signatures to be recognized by public sector bodies pursuant to Articles 27(5) and 28(5) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market*

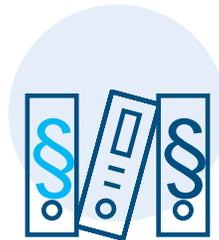
Rechtlicher Rahmen: VwVfG und EGovG

Verwaltungsverfahrensgesetz (VwVfG)

§ 3a Elektronische Kommunikation

(3) Die Schriftform kann auch ersetzt werden (...)

3. bei elektronischen Verwaltungsakten oder sonstigen elektronischen Dokumenten der Behörde,
 - a) indem diese mit dem **qualifizierten elektronischen Siegel der Behörde** versehen werden;



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

neu !!
ab Juli 2024

§ 2a Siegeldienst; Verordnungsermächtigung

(1) Das Bundesministerium des Innern und für Heimat wird ermächtigt, durch Rechtsverordnung, die nicht der Zustimmung des Bundesrates bedarf, eine öffentliche Stelle des Bundes zu bestimmen, die den Behörden des Bundes zur Unterstützung ihrer elektronischen Verwaltungstätigkeit einen **zentralen Siegeldienst** bereitstellt. Auf der Grundlage einer Verwaltungsvereinbarung mit dem Bundesministerium des Innern und für Heimat können Länder diesen Siegeldienst zur Unterstützung der elektronischen Verwaltungstätigkeit ihrer Behörden mitnutzen.

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

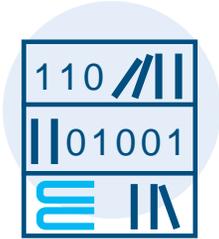
§ 2a Siegeldienst; Verordnungsermächtigung

(2) Der zentrale Siegeldienst erfüllt mindestens die folgenden Basisfunktionen:

1. **Erstellung** qualifizierter elektronischer Siegel,
2. **Validierung** qualifizierter elektronischer Siegel und Signaturen sowie
3. Erstellung digitaler Siegel zum **optisch verifizierbaren** kryptographischen Schutz von Verwaltungsdokumenten.

Technische Empfehlungen, Vorgaben und Standards

Kryptographie: TR-02102, TR-03116, TS 119 312



 Bundesamt für Sicherheit in der Informationstechnik

Deutschland
Digital•Sicher•BSI

BSI – Technische Richtlinie

Bezeichnung: Kryptographische Verfahren:
Empfehlungen und Schlüssellängen

Kürzel: BSI TR-02102-1

Version: 2024-01

Stand: 02. Februar 2024



 Bundesamt für Sicherheit in der Informationstechnik

Deutschland
Digital•Sicher•BSI

Technische Richtlinie BSI TR-03116
Kryptographische Vorgaben für Projekte der Bundesregierung

Teil 4: Kommunikationsverfahren in Anwendungen

Stand 2023
Datum: 7. März 2023



ETSI TS 119 312 v1.5.1 (2024-12)



TECHNICAL SPECIFICATION

**Electronic Signatures and Trust Infrastructures (ESI);
Cryptographic Suites**

Zertifikat, qualifiziertes - nach eIDAS

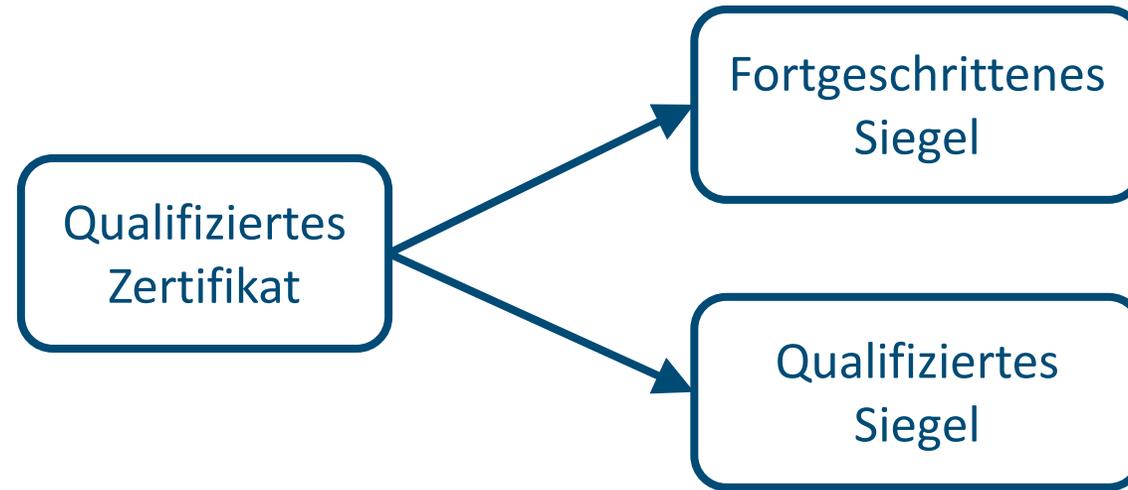
Artikel 3: „Qualifiziertes Zertifikat für elektronische Siegel“ ist ein von einem **qualifizierten Vertrauensdiensteanbieter** ausgestelltes Zertifikat für elektronische Siegel, das die Anforderungen des Anhangs III erfüllt.

Artikel 38: Qualifizierte Zertifikate für elektronische Siegel

- (1) Qualifizierte Zertifikate für elektronische Siegel müssen die Anforderungen des Anhangs III erfüllen.
- (2) Für qualifizierte Zertifikate für elektronische Siegel dürfen keine verbindlichen Anforderungen gelten, die über die in Anhang III festgelegten hinausgehen.

(...)

Zertifikat, qualifiziertes - für fortgeschrittene und für qualifizierte Siegel



Qualifiziertes Zertifikat:

- unterhalb der EU Vertrauensliste
- Validierbar in der ganzen EU



Elektronisches Siegel: Anwendungsfall digitales Zeugnis

Unterschriften

Alle prüfen

Revision 1: Unterschrieben von Ministerium für Schule und Bildung Land

Unterschrift ist ungültig:

- Dokument wurde nach dem Unterzeichnen verändert oder beschädigt.
- Die Identität des Unterzeichners ist unbekannt, weil sie sich nicht in der
- Die Uhrzeit der Signatur stammt von der Uhr des Computers vom Signie

Unterschriftsinformationen

Zertifikatdetails...

Zuletzt geprüft: 2023.11.03 16:44:03 +01'00'

Feld: Signature1 (Unsichtbare Unterschrift)

4. Seite des Zeugnisses der Allgemeinen Hochschulreife für die Schulaufstufung 1127/002/04

Fach	Leistungswert		GefR
	von	bis	
Englisch	5	13	B1
Französisch	5	13	B2
Spanisch	8	13	B1/B2

Fremdsprachennachweis:

Für die modernen Fremdsprachen schließt dieses Zeugnis Kompetenzen des Gemeinsamen europäischen Referenzrahmens für Sprachen (GeR) ein.
Dieses Zeugnis schließt das Lateinum und das Graecum gemäß "Verabbarung über das Lateinum und das Graecum" (Beschluss der Kultusministerkonferenz vom 22.09.2005) ein.
Dieses Zeugnis schließt das Hebraicum ein.

Bemerkungen:

Auf Wunsch der Schüler/der Schüler kann hier die Teilnahme an Arbeitsgemeinschaften in der Qualifikationsphase oder die erfolgreiche Teilnahme an Landes- oder Bundeswettbewerben vermerkt werden. Auch können hier gemäß § 49 Abs. 3 SchulG Aussagen zum außer- unterrichtlichen Engagement aufgenommen werden.

Frau Silke Eckstaedt_TESTPERSON
hat die Abiturprüfung bestanden und damit die Berechtigung zum Studium an einer Hochschule in der Bundesrepublik Deutschland erworben.
Die allgemeine Hochschulreife ist im Deutschen und Europäischen Qualifikationsrahmen dem Niveau 4 zugeordnet.

Testschule zu Demonstrationszwecken



Digitale Test-Zeugnisausfertigung zum ZEUGNIS DER ALLGEMEINEN HOCHSCHULREIFE

Frau Silke Eckstaedt_TESTPERSON

geboren am 30.01.1997 in Dresden

wohnhaft in Dortmund

hat sich nach dem Besuch der gymnasialen Oberstufe der Abiturprüfung unterzogen.

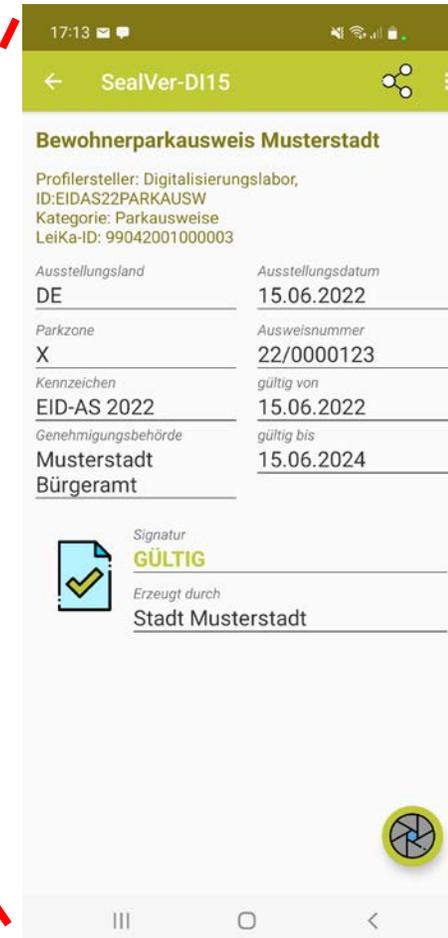
Dem Zeugnis liegen zugrunde:

- Verabbarung zur Gestaltung der gymnasialen Oberstufe und der Abiturprüfung (Beschluss der Kultusministerkonferenz vom 7. 7. 1972 in der jeweils gültigen Fassung)
- Bildungsstandards für die Allgemeine Hochschulreife und Vereinbarungen über die Einheitlichen Prüfungsanforderungen in der Abiturprüfung
- Verordnung über den Bildungsgang und die Abiturprüfung in der gymnasialen Oberstufe - APO OOS - vom 5. Oktober 1980 in der jeweils gültigen Fassung (BAGS 13-32 Nr. 17)

```
</xsc:schule>
<xsc:block-iii>
  <xsc:durchschnittsnote>
    <xbd:note>1,8</xbd:note>
    <xbd:wortbezeichnung>Zwei Komma Acht</xbd:w<sup>Abbildung vom</sup>
  </xsc:durchschnittsnote>
  <xsc:gesamtpunktzahl>
    <xbd:punkte>451</xbd:punkte>
    <xbd:bewertungsschemaPunkte>
      <xbd:schemaURI>
        <code>http://www.xbildung.de/def/xb<sup>Abbildung von</sup>
      </code>
    </xbd:schemaURI>
  </xsd:bewertungsschemaPunkte>
```

Optisch verifizierbares digitales Siegel: TR-03171

- Inhaltsdaten des jeweiligen Dokuments + Profil + Referenz auf elektronisches Siegel → zweidimensionaler Barcode
- Dokument mit zweidimensionalem Barcode kann ausgedruckt oder auf mobilem Endgerät vorgezeigt werden
- Verifikation und Prüfung des Integritätsschutzes durch eine App:
- Empfehlung: elektronische und optische Siegel kombinieren !



Coming Soon

Coming Soon

TR-03186 Siegeldienste



Deutschland
Digital•Sicher•BSI•

Technische Richtlinie TR-03186 Empfehlungen zu Siegeldiensten

Behördensiegel: Fortgeschrittene und qualifizierte elektronische Siegel und optisch verifizierbare digitale Siegel

Version: „0.7“ (*Entwurf – nicht final*)



Deutschland
Digital•Sicher•BSI•

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

Sascha Neinert

digitale-siegel@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 87
53175 Bonn
www.bsi.bund.de



Das BSI als die Cybersicherheitsbehörde des Bundes gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft.

Bild: ©Adobe Stock, Bee