Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Technische Richtlinie TR-03171

Optisch verifizierbarer kryptographischer Schutz von Verwaltungsdokumenten (Digitale Siegel)

Version 0.7

Änderungshistorie

Tabelle 1: Versionierung

Version	*Datum*	*Name*	*Beschreibung*
0.7	25.05.2021	BSI	Erstveröffentlichung

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: referat-di15@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhalt

1 Einleitung

Zahlreiche Verwaltungsprozesse in Deutschland resultieren in der Erstellung von Bescheiden, Zertifikaten oder sonstigen Dokumenten. Damit solche Dokumente als Nachweis gegenüber Dritten verwendet werden können, wurden sie traditionell mit Dienstsiegeln und/oder Unterschriften der Bearbeitenden versehen. Die handschriftliche Unterschrift kann in vielen Bereichen schon seit langem durch eine qualifizierte elektronische Signatur ersetzt werden, und die mit der eIDAS-Verordnung (eIDAS-VO) EU-weit eingeführten qualifizierten Siegel, die einen elektronischen Herkunftsnachweis darstellen, verfügen über dieselben mathematischen Eigenschaften.

Mit fortgeschrittenen oder qualifizierten elektronischen Signaturen oder Siegeln lässt sich die Authentizität und Integrität elektronischer Dokumente jederzeit überprüfen, solange sie in der ursprünglichen Form elektronisch vorliegen. Sofern die Dokumente jedoch nur in Papierform vorliegen oder z. B. auf einem mobilen Endgerät präsentiert werden, sind diese Integritätssicherungen nicht mehr prüfbar. Hierfür wurden optisch verifizierbare digitale Siegel entwickelt, die die wesentlichen Daten eines Nachweises in strukturierter Form und kryptographisch gesichert enthalten. Durch das Scannen eines digitalen Siegels (in Form eines Barcodes) wird ein elektronisches Dokument erzeugt, in das die mit einer Integritätssicherung versehenen Daten eingebunden sind. Sofern bei der Erstellung ein entsprechendes Zertifikat verwendet wurde, handelt es sich bei dem geschützten Datensatz um ein mit einer qualifizierten elektronischen Signatur bzw. einem qualifizierten elektronischen Siegel versehenes Dokument.

Auf diese Weise lässt sich die Authentizität und Integrität eines Verwaltungsdokuments feststellen, etwa im Rahmen der Prüfung einer Genehmigung durch Mitarbeitende einer Ordnungsbehörde, ohne dass dazu ein Zugriff auf in einem Hintergrundsystem gespeicherte Informationen zum Vorgang notwendig wäre.

Das vorliegende Dokument beschreibt einen auf (TR-03137-1) basierenden Standard zur Erzeugung digitaler Siegel auf Verwaltungsdokumenten.

2 Organisatorische Grundlagen

Sofern eine Stelle lediglich Nachweise prüfen möchte, die sie selbst erstellt und signiert hat, kann sie die dafür erforderlichen Formate und Konventionen selbst festlegen. Soll es jedoch ermöglicht werden, dass ein Verwaltungsdokument von unterschiedlichen Stellen (z. B. anderen Kommunen) validiert wird, so ist die Einhaltung einheitlicher Konventionen erforderlich. Zudem benötigt die prüfende Stelle Zugriff auf die Dokumentformate (Profile im Sinne der (TR-03137-1)) sowie auf die zur Erstellung der elektronischen Signatur / des elektronischen Siegels verwendeten Zertifikate samt zugehöriger Zertifikatskette und Rückrufinformationen.

2.1 Profilverwaltung

Damit eine Anwendung die Inhalte aller Verwaltungsdokumente strukturiert anzeigen kann, die von einer öffentlichen Stelle ausgegeben und mit einem optisch verifizierbaren digitalen Siegel versehen wurden, ist es notwendig, dass sie Zugriff auf alle zugrundeliegenden Dokumentenprofile hat. Hierzu ist eine zentrale Profilverwaltung der öffentlichen Verwaltung einzurichten, die von jeder öffentlichen Stelle Profile entgegennimmt und zusammen mit jeweils einer eindeutigen Kennung in Form einer Dokumentenprofilnummer auf einem öffentlich zugänglichen Server zur Verfügung stellt. Die benötigten Profile können dann bei Bedarf online abgerufen oder durch entsprechende Anwendungen bereits im Vorfeld für offline-Prüfungen heruntergeladen werden.

2.2 Zertifikatsverwaltung

Während fortgeschrittene und qualifizierte Signaturen und Siegel meistens das Zertifikat enthalten, mit dem sie erstellt wurden, enthalten digitale Siegel aufgrund der begrenzten Speicherkapazität nur eine Referenz auf ein Zertifikat, das an anderer Stelle vorliegt. Damit eine Anwendung die Integrität aller Verwaltungsdokumente prüfen kann, die von einer öffentlichen Stelle ausgegeben und mit einem digitalen Siegel versehen wurden, ist es notwendig, dass sie Zugriff auf alle verwendeten Zertifikate hat. Hierzu ist eine zentrale Zertifikatsverwaltung der öffentlichen Verwaltung einzurichten, die von jeder öffentlichen Stelle Zertifikate entgegennimmt und zusammen mit jeweils einer eindeutigen Kennung bestehend aus *Signer Identifier* („DEZV“) und *Certificate Reference* (<Zertifikatsnummer>) auf einem öffentlich zugänglichen Server zur Verfügung stellt. Die benötigten Zertifikate und Zertifikatsketten können dann bei Bedarf online geprüft oder durch entsprechende Anwendungen bereits im Vorfeld für offline-Prüfungen heruntergeladen werden. Dabei ist zu beachten, dass Zertifikate bei offline-Verwendung gerade nicht in Echtzeit auf Gültigkeit bzw. Rückruf geprüft werden können und eine solche Prüfung daher je nach Anwendungsszenario mit den für eine offline-Prüfung heruntergeladenen Zertifikaten regelmäßig online durchzuführen ist.

3 Format digitaler Siegel auf Verwaltungsdokumenten

Das Format digitaler Siegel auf Verwaltungsdokument folgt grundsätzlich den Vorgaben der (TR-03137-1). Zulässige Ausprägungen sowie notwendige Abweichungen werden im Folgenden beschrieben.

3.1 Header

Die vorliegende Technische Richtlinie unterstützt ausschließlich Header der Version 4 gemäß (TR-03137-1). Die Header sind gemäß (TR-03137-1) zu befüllen; ausgewählte Header werden im Folgenden erläutert und vorgeschriebene Belegungen in Anführungszeichen angegeben.

Als Dokumentenkategorie wird die Nummer `200` für Verwaltungsdokumente vergeben. Aufgrund der zu erwartenden Vielzahl an zu siegelnden Verwaltungsdokumenten wird die jeweilige Ausprägung des Verwaltungsdokuments nicht im für Ausprägungen vorgesehenen Header-Feld *Document Feature Definition Reference*, der nur 256 verschiedene Werte zulässt, sondern in einem eigenen Feld als Dokumentenprofilnummer in der Message Zone (s. Abschnitt 3.2) codiert.

Tabelle 2: Header gemäß TR-03137-1

Position gem. (TR-03137-1)	*Inhalt*	*Wert*
`0x01`	*Version*	„`0x03`“
`0x02`	*Issuing Country*	„`D<<`“
`0x04`	*Signer Identifier and Certificate Reference*	von der Zertifikatsverwaltung ausgegebene Kennung
`0x0A+v`	*Document Feature Definition Reference*	„`01`“ für Konformität mit Abschnitt 3.2 (die eigentliche Feature Definition der Inhaltsdaten wird im ersten Feld der Message Zone gesetzt)
`0x0B+v`	*Document Type Category*	„`200`“ (Verwaltungsdokument)
`0x01`	*Version*	„`0x03`“
`0x02`	*Issuing Country*	„`D<<`“

3.2 Message Zone

Die Message Zone ist wie in (TR-03137-1) definiert zu befüllen. Dabei ist unter Tag `0x00` die Dokumentenprofilnummer zu hinterlegen, und zwar in der folgenden Form:

Tabelle 3: Angabe der Dokumentenprofilnummer in der Message Zone

Eigenschaft	*Wert*
tag	„`0x00`“
length	Länge der C40-Darstellung des nachfolgenden Werts
value	Dokumentenprofilnummer wie von der Profilverwaltung übermittelt (in C40-Codierung)

Die Tags `0x01` bis `0x03` werden für eine spätere Verwendung reserviert. Für Inhaltsdaten stehen die Tags `0x04` bis `0xfe` zur Verfügung.

3.3 Verwendete Zertifikate

Für die Erstellung fortgeschrittener oder qualifizierter Signaturen oder Siegel können verschiedenartige Zertifikate zum Einsatz kommen:

- Fortgeschrittene Signaturen und Siegel können mit Zertifikaten aus der Verwaltungs-PKI erzeugt werden.
- Zur Erstellung qualifizierter Signaturen und Siegel werden qualifizierte Zertifikate eines (kommerziellen) qualifizierten Vertrauensdiensteanbieters benötigt.

Um keine zusätzlichen Einschränkungen an die zu verwendenden Zertifikate zu machen, gelten im Anwendungsbereich des vorliegenden TR-Teils die Vorgaben aus Abschnitt 4.3 der (TR-SEAL) nicht. Bei Verifizierung eines digitalen Siegels wird das benötigte Zertifikate nicht über die darin enthaltenen Zertifikatsdetails, sondern ausschließlich über die von der Zertifikatsverwaltung vergebene und im digitalen Siegel codierte eindeutige Zertifikatsnummer identifiziert.

4 Dokumentenprofile

Zur korrekten Codierung und Darstellung der Daten im digitalen Siegel muss ein Profil folgende Daten enthalten:

- Dokumentenprofilnummer wie von der Profilverwaltung übermittelt
- Profilname
- Ersteller des Profils (zuständige Stelle)
- Kategorie des Profils (Freitext; optional)
- Schlüssel der relevanten Verwaltungsleistung (LeiKa-ID[1]; optional, auch mehrfach)
- Liste der enthaltenen Datenfelder (TLV-Objekte) mit folgenden Angaben:
  - Tag (Position)
  - optional?
  - Name des Datenfeldes
  - Beschreibungstext
  - maximale Länge (zu ignorieren beim Datentyp `date`)
  - Datentyp

Es werden nur Datenfelder nach den in Abschnitt 3.2 genannten obligatorischen Feldern beschrieben. Es sind daher nur Tags von 4 bis 254 (`0x04` bis `0xfe`) zu verwenden.

Als Datentypen stehen zur Verfügung:

- `alphanum`
  Datentyp für die effiziente Kodierung ausschließlich von Großbuchstaben ‚A'-‚Z', Ziffern ‚0'-‚9', Leerzeichen und dem Symbol ‚<', insbesondere für maschinenlesbare Zonen auf Ausweisdokumenten.
- `string`
  Zeichenkette.
- `multistring`
  Wie `string`, jedoch mehrzeilige Eingabe/Darstellung möglich.
- `date`
  Datum (Tag, Monat, Jahr).
- `binary`
  Binärdaten. Darstellung erfolgt, soweit nicht anders definiert, wie bei Zeichenketten, und sollte daher nicht benutzt werden.

Die Datentypen werden wie in (TR-SEAL) angegeben codiert, wobei die hier zur Vereinfachung der Eingabe und Darstellung neu eingeführten `string` und `multistring` als `binary` behandelt werden. Sämtliche Zeichenketten sind dazu im Format `UTF-8` auszulesen bzw. zu codieren. Dadurch wird insbesondere die Verarbeitung und Darstellung aller lateinischen Zeichen gemäß Vorgaben der KoSIT[2] ermöglicht.

Das Profil ist in Form eines XML-Datensatzes gemäß nachfolgendem Schema zu erstellen.

[1] https://fimportal.de/
[2] https://www.xoev.de/die_standards/lateinische_zeichen_in_unicode-4813

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
           elementFormDefault="qualified">

   <xs:element name="profile">
      <xs:complexType>
         <xs:sequence>
            <xs:element name="profileNumber" type="xs:string" />
            <xs:element name="profileName" type="xs:string" />
            <xs:element name="creator" type="xs:string" />
            <xs:element name="category" type="xs:string" minOccurs="0"/>
            <xs:element name="leikaID" type="xs:string" minOccurs="0"/>
            <xs:element name="entry" type="entryType" minOccurs="1"
maxOccurs="251" />
         </xs:sequence>
      </xs:complexType>
      <xs:unique      name="tagNo">
         <xs:selector xpath="entry" />
         <xs:field    xpath="@tag" />
      </xs:unique>
   </xs:element>

   <xs:complexType name="entryType">
      <xs:sequence>
         <xs:element name="name" type="xs:string" />
         <xs:element name="description" type="xs:string" />
         <xs:element name="length" type="xs:positiveInteger" minOccurs="0" />
         <xs:element name="type" type = "typeType" />
         <xs:element name="defaultValue" type="xs:string" minOccurs="0" />
      </xs:sequence>
      <xs:attribute name="tag"    type="tagType" use="required" />
      <xs:attribute name="optional" type="xs:boolean" />
   </xs:complexType>

   <xs:simpleType name="typeType">
      <xs:restriction base="xs:string">
         <xs:enumeration value="alphanum" />
         <xs:enumeration value="string" />
         <xs:enumeration value="multistring" />
         <xs:enumeration value="binary" />
         <xs:enumeration value="date" />
      </xs:restriction>
   </xs:simpleType>

   <xs:simpleType name="tagType">
      <xs:restriction base="xs:integer">
         <xs:minInclusive value="4"/>
         <xs:maxInclusive value="254"/>
      </xs:restriction>
   </xs:simpleType>

</xs:schema>
```

Literaturverzeichnis

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.

TR-03137-1. Technical Guideline TR-03137: Optically Verifiable Cryptographic Protection of non-electronic Documents (Digital Seal).

TR-SEAL. ICAO: Technical Report Visible Digital Seals for non-electronic Documents Version 1.7, March 2018.