Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Elektronische Signaturen und Optisch verifizierbare Digitale Siegel auf Verwaltungsdokumenten

Möglichkeiten der optischen Verifikation integritätsgeschützter Dokumente

Frau Lampe und Herr Sauer beleuchten die Frage, wie digitale Urkunden bei anderen Behörden vorgelegt werden…

Das Standesamt meines Geburtsortes sendet die Geburtsurkunde also direkt an mein Nutzerkonto. Woher weiß das Standesamt am Hochzeitsort aber, dass die Geburtsurkunde tatsächlich von dort stammt?

Das ist ganz einfach: Die digitale Geburtsurkunde wird vom ausstellenden Amt elektronisch gesiegelt. Du musst sie dann nur noch elektronisch an das Standesamt des Hochzeitsorts weiterleiten.

Was ist eine elektronische Signatur?

- **„irgendwie wie eine Unterschrift – nur eben digital, statt auf Papier“(?)**
- eIDAS-VO, Artikel 3 Nr. 10:
  "Elektronische Signatur“ sind Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verbunden werden und die der Unterzeichner zum Unterzeichnen verwendet."
- eIDAS-VO, Artikel 25 Nr. 2:
  - Eine **qualifizierte elektronische Signatur** hat die gleiche Rechtswirkung wie eine **handschriftliche Unterschrift**.

Und was sind (qualifizierte) elektronische Siegel?

- **technisch dasselbe wie (qualifizierte) elektronische Signaturen.**
- Mit Bezug zu juristischer (Siegelersteller) statt natürlicher Person (Unterzeichner) → **Herkunftsnachweis statt Willenserklärung**

Frau Lampe und Herr Sauer erläutern das „optisch verifizierbare Siegel“ für Bescheide am Beispiel des Anwohnerparkausweises...

Aber, wenn der Bürger seinen Anwohnerparkausweis elektronisch erhält, liegt am Ende ja nur ein Ausdruck davon hinter der Windschutzscheibe. Wie kann das Ordnungsamt die Echtheit prüfen?

Der Anwohnerparkausweis wird mit einem optisch verifizierbaren Siegel in Form eines Barcodes versehen. Damit können Beschäftigte des Ordnungsamts die Gültigkeit und Echtheit durch die Windschutzscheibe zweifelsfrei prüfen.

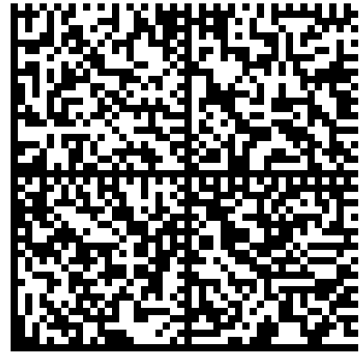
Ausgangslage

- Im Zuge der Digitalisierung werden viele **Genehmigungen, Nachweise und Bescheide nur noch elektronisch** ausgestellt.
- **Qualifizierte elektronische Signaturen und Siegel** liefern Herkunftsnachweis und Integritätsschutz.
- **Herkunftsnachweis und Integritätsschutz** können am Endgerät mit entsprechender Software (z. B. PDF Reader) überprüft werden.

- Ausgedruckte oder am Endgerät vorgezeigte Nachweise verfügen jedoch über **keine physikalischen Sicherheitsmerkmale**.
- Eine **Erkennung von Fälschungen** ist daher i. d. R. **nicht möglich**.

Lösungsansatz: Digitale Siegel

- **Digitale Siegel** in Form **zweidimensionaler Barcodes** stellen digitale Daten in **optisch verifizierbarer** Form dar.
- Sie enthalten die **wesentlichen Daten** des Dokuments sowie eine **Integritätssicherung**.
- Digitale Siegel können **auf Papier ausgedruckt vorgelegt** oder auf dem Mobilgerät vorgezeigt und **mit einer Smartphone-App zweifelsfrei verifiziert** werden.
- Die Verifikation kann **vollständig offline** erfolgen, eine Ergänzung um Online-Informationen ist natürlich möglich.
- Digitale Siegel beruhen auf denselben Algorithmen wie qualifizierte elektronische Signaturen und Siegel und erreichen daher **denselben mathematischen Beweiswert**.
- Werden Digitale Siegel mittels qualifizierter Zertifikate erstellt, handelt es sich um **qualifizierte Signaturen bzw. Siegel**.



Standardisierte Lösungen: BSI-TR-03137

- Die **Technische Richtlinie TR-03137 des BSI** liefert Vorgaben für den optisch verifizierbaren kryptographischen Schutz nicht-elektronischer Dokumente.
- Teil 1 enthält **Profile für hoheitliche Dokumente** wie
  - Ankunftsnachweise
  - Sozialversicherungsausweise
  - Aufenthaltserlaubnisse
- **Digitale Siegel auf Ankunftsnachweisen** werden seit 2016 flächendeckend an alle Asylsuchenden ausgegeben.
- Die TR-03137-1 wurde mittlerweile in den **internationalen ICAO-Standard** „Visible Digital Seals for non-electronic Documents“ **integriert**.

Anwendungen digitaler Siegel

>> Ein- und Ausfuhrgenehmigungen

Handel

>> Außengastronomie

>> Marktstände

>> Anwohnerparkausweis

Verkehr

>> Temporäres Parkverbot

>>

>> Schulzeugnis

Urkunden

>>Personenstandsurkunden

>> Geburtsurkunden

>> Fischereischein

Freizeit

>> Genehmigung ...

>> ...

>> Versicherungsnachweise

Finanzwirtschaft

>> Steuerrelevante Belege

>> Kontoauszüge

>> Ankunftsnachweis

Hoheitliche Dokumente

>> Sozialversicherungsnachweis

>> Visum

Bundesamt
für Sicherheit in der
Informationstechnik

BSI-TR-031XX: Digitale Siegel auf Verwaltungsdokumenten

- **Teil 1** der TR-03137 enthält Profile für bestimmte hoheitliche Dokumente. Die **Datenfelder** und deren Typen sind dabei **fest definiert**.
- Der Entwurf sieht **variable Profile für Verwaltungsdokumente** vor.
- Erstellung und Verifizierung der digitalen Siegel geschieht dabei **wie bei hoheitlichen Dokumenten**.
- Lediglich die jeweiligen **Profile** müssen dafür **definiert**, bereitgestellt und herangezogen werden.
- Profile können **bundesweit standardisiert oder individuell** durch einzelne Behörden definiert werden.
- Erstellung und Verifikation sind dennoch durch **einheitliche Anwendungen** (efa) möglich.
- **Individuell verwendete Zertifikate** müssen zur Verifikation bereitgestellt werden.

Digitale Siegel auf Verwaltungsdokumenten Schritt 1: Erstellung eines Profils

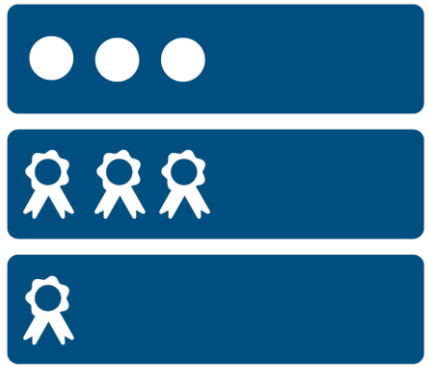
- Für jeden **Typ eines Verwaltungsdokuments** (z. B. Schulzeugnis, Anwohnerparkausweis, Fischereigenehmigung) ist ein **Profil** zu erstellen, das die Datenfelder beschreibt, die im digitalen Siegel geschützt werden sollen. In der Regel sind dies die variablen Daten eines Dokuments.
- Das Profil wird **mittels einer einfachen Excel-Tabelle** durch die fachlich Verantwortlichen erstellt und als XML-Datei exportiert.
- Profile können **individuell** durch Behörden und Kommunen festgelegt **oder bundes- oder landesweit einheitlich** vorgegeben werden.
- Profile müssen den Stellen, die digitale Siegel prüfen sollen, bekannt gemacht werden (dies können auch die Betroffenen selbst sein). Dazu ist eine Profilverwaltung vorgesehen, die als zentraler Dienst (efa) angeboten werden kann.

	Profilnr.	FISCH1		
	Profilname	Fischereigenehmigung		
	Ersteller	Digitalisierungslabor		
	Kategorie			
	LeiKa-ID	99042001000000		
Tag	***Feldname***	***Beschreibung***	***maximale Länge***	***Typ***
4	id	Ausweisnummer	20	alphanum
5	name	Name	40	string
6	firstname	Vorname	100	string
7	birthdate	Geburtsdatum		date
8	birthplace	Geburtsort	100	string
9	issuer	Aussteller	100	string
10	validTo	Gültig bis		date

```
−<profile xsi:schemaLocation="http://www.bsi.bund.de sealprofile.xsd">
    <profileNumber>FISCH1</profileNumber>
    <profileName>Fischereigenehmigung</profileName>
    <creator>Digitalisierungslabor</creator>
    <leikaID>99042001000000</leikaID>
  −<entry tag="4">
      <name>id</name>
      <description>Ausweisnummer</description>
      <length>20</length>
      <type>alphanum</type>
    </entry>
  −<entry tag="5">
      <name>name</name>
      <description>Name</description>
      <length>40</length>
      <type>string</type>
    </entry>
  −<entry tag="6">
      <name>firstname</name>
      <description>Vorname</description>
      <length>100</length>
      <type>string</type>
    </entry>
```

Digitale Siegel auf Verwaltungsdokumenten
Schritt 2: Signatur- oder Siegelzertifikat

- Zur Erstellung eines digitalen Siegels wird ein **Signatur- oder Siegelzertifikat** benötigt. Grundsätzlich kann dasselbe Zertifikat verwendet werden, das auch für die Erstellung elektronischer Signaturen bzw. Siegel zum Einsatz kommt.
- **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.
- Da digitale Siegel eine **begrenzte Kapazität** haben, können nur Zertifikate auf Basis **elliptischer Kurven** zum Einsatz kommen.
- Da digitale Siegel eine begrenzte Kapazität haben, enthalten sie nur eine **Referenz auf das verwendete Zertifikat**, nicht das Zertifikat selbst.
- Das Zertifikat muss daher über eine **Zertifikatsverwaltung** zur Verfügung gestellt werden. Diese kann als zentraler Dienst (efa) angeboten werden.

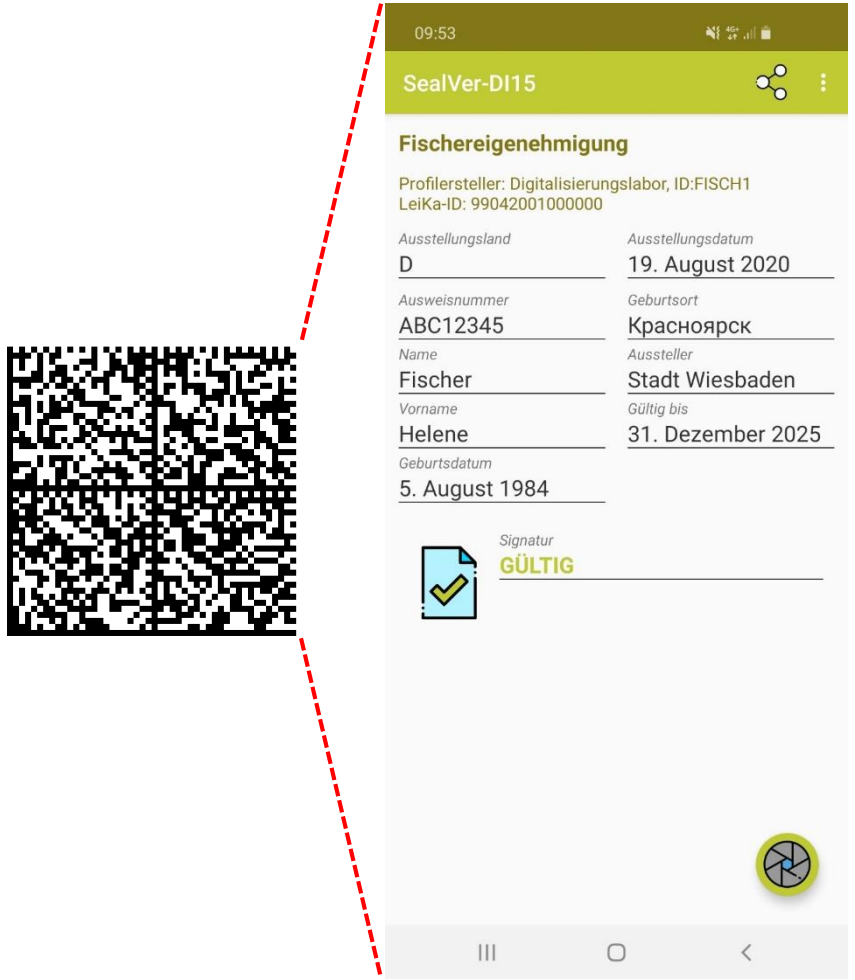


Digitale Siegel auf Verwaltungsdokumenten
Schritt 3: Erstellung gesiegeltes Dokument

- Ein Verwaltungsdokument wird i. d. R. aus einer Vorlage (Formular) und **individuellen Inhaltsdaten** (z. B. Identitätsdaten eines Antragstellers) erstellt. Aus dem im 1. Schritt erzeugten Profil kann dazu auch ein **Eingabeformular** generiert werden.
- Das Dokument (i. d. R. PDF) wird an einen **Siegelserver** übergeben. Zusätzlich werden die **Inhaltsdaten als Datensatz** übergeben. Das Format ergibt sich dabei aus dem Profil.
- Der Siegelserver erzeugt mittels einer einheitlichen (efa-)Anwendung ein **digitales Siegel gemäß TR-031XX** und fügt dies dem erzeugten PDF-Dokument hinzu.
- Das Dokument kann anschließend **zusätzlich elektronisch (qualifiziert) signiert oder gesiegelt** und zugestellt werden.
- Ein **qualifiziert signiertes Dokument** ersetzt (in elektronischer Form) die **Schriftform**.
- Ausgedruckt verliert es diese Eigenschaft, das **digitale Siegel ermöglicht jedoch die Prüfung von Herkunft und Integrität** auf demselben Niveau.

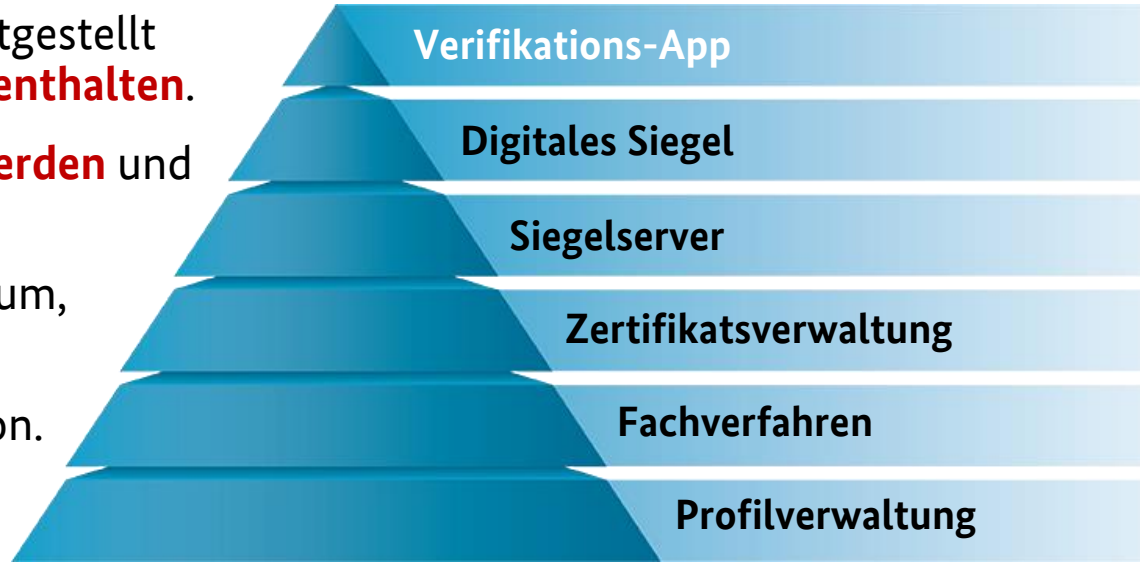
Digitale Siegel auf Verwaltungsdokumenten
Schritt 4: Verifikation eines digitalen Siegels

- Das mit dem digitalen Siegel versehene Dokument kann **ausgedruckt oder auf einem Mobilgerät vorgezeigt** werden.
- Zur **Verifikation mittels einheitlicher App** wird 1. das verwendete **Zertifikat** und 2. das jeweilige **Profil** benötigt. Diese können über die Zertifikats- bzw. Profilverwaltung **online abgefragt oder zur offline-Nutzung vorab heruntergeladen** werden.
- Der **Download kann** bei Bedarf auf Zertifikate/Profile bestimmter Behörden oder z. B. der eigenen Kommune **begrenzt werden**; auch eine Begrenzung der Profile auf bestimmte Einsatzgebiete (z. B. unter Verwendung der LeiKa-ID) ist vorgesehen.
- Die Verifikation erfolgt mit **Mobilgerät** mit eingebauter Kamera.
- Die Bezeichnungen der angezeigten **Datenfelder** sind im Profil hinterlegt, die **Inhaltsdaten** im digitalen Siegel.
- Es wird angezeigt, ob der **Integritätsschutz** verifiziert werden konnte.



Übersicht: Eigenschaften Digitaler Siegel auf Verwaltungsdokumenten

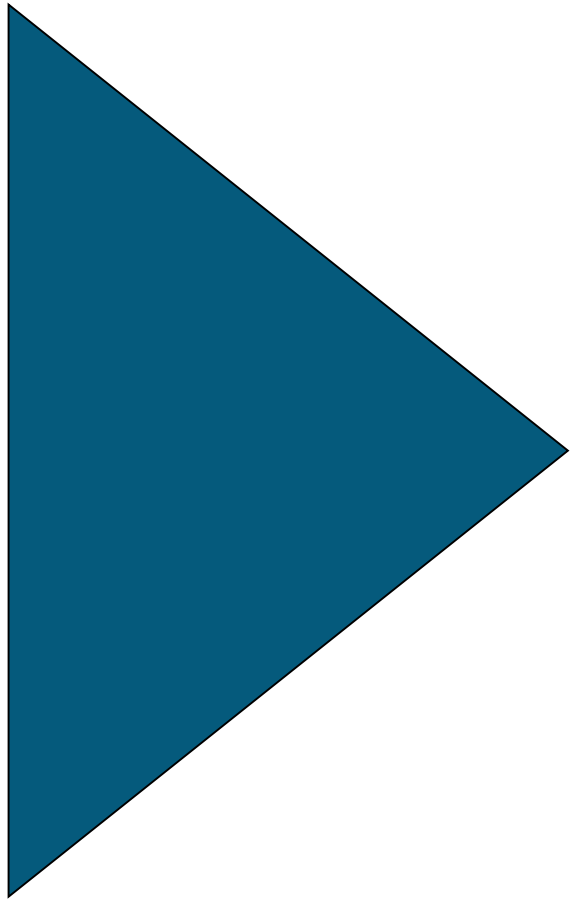
- Eine Überprüfung mit Verifikations-App ist möglich, wenn Digitale Siegel **ausgedruckt oder am Mobilgerät vorgezeigt werden**.
- Die **Größe der** vom Siegelserver erzeugten **Barcodes** hängt ausschließlich von der Länge der darin hinterlegten Daten ab.
- Digitale Siegel auf Verwaltungsdokumenten können **offline überprüft** werden, sofern die verwendeten Profile und Zertifikate vorher heruntergeladen wurden.
- XML-Profile und Zertifikate können als efa-Lösung zentral bereitgestellt werden. **Zertifikate** sind aus Kapazitätsgründen **nicht im Siegel enthalten**.
- **Profile** für Verwaltungsdokumente **können beliebig definiert werden** und bis zu 251 Datenfelder umfassen
- Als **Datentypen** stehen ein- und mehrzeilige Zeichenketten, Datum, alphanumerische (MRZ) und Binärdaten zur Verfügung.
- Auch **URLs** können hinterlegt werden, z.B. zur Online-Verifikation.



Fazit

- Qualifiziert signierte und digital gesiegelte Dokumente ersetzen die Schriftform und können auch ausgedruckt zweifelsfrei auf ihre Herkunft und Integrität überprüft werden.
- Profile für unterschiedlichste Arten von (Verwaltungs-)Dokumenten können gemäß TR-031XX individuell oder vereinheitlicht erstellt werden.
- Erstellung und Verifikation digitaler Siegel können dennoch mit einheitlichen Anwendungen erfolgen.

Video: Praktische Vorführung zur Nutzung der Digitalen Siegel

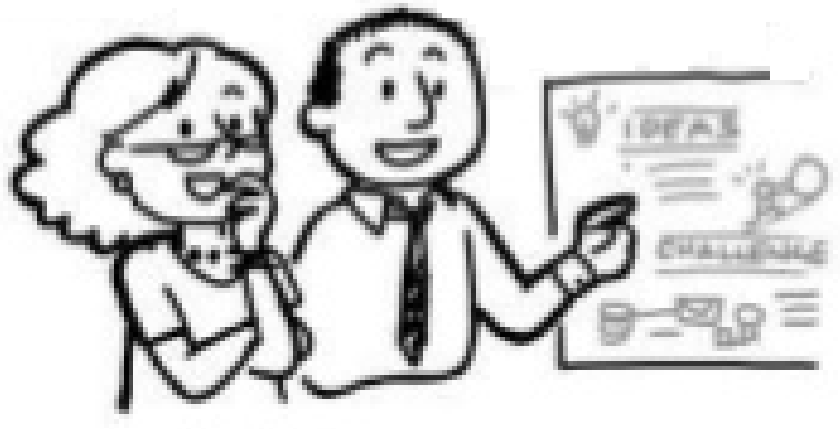


Frau Lampe und Herr Sauer sind auf der Suche nach Pilotpartnern für Digitale Siegel, aber auch weiteren interessanten Themen wie...

...Digitaler Schülerausweis

...App- & Webportal Testing

...Digitales Schulzeugnis



Bundesamt für Sicherheit in der Informationstechnik

Vielen Dank
für Ihre Aufmerksamkeit!

Kontakt

Jasmina Ćejvanović und Ann-Kristin Derst
Referat DI 15 - eID-Lösungen für die digitale Verwaltung

referat-di15@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de
www.bsi-fuer-buerger.de

Bundesamt
für Sicherheit in der
Informationstechnik