2023#6 31. Jahrgang

BSI Forum

offizielles Organ des BSI
Bundesamt
für Sicherheit in der
Informationstechnik

# Ransomware, Schwachstellen und Resilienz

## Die Lage der IT-Sicherheit in Deutschland 2023

***Einmal im Jahr berichtet das Bundesamt für Sicherheit in der Informationstechnik über die Lage der IT-Sicherheit in Deutschland. In seinem diesjährigen Bericht kommt das BSI zu dem Schluss: Die Bedrohung ist so hoch wie nie zuvor. Die Professionalisierung der Angreifer im Cyberraum schreitet ungemindert voran. Staat, Wirtschaft und Gesellschaft brauchen eine entsprechende Abwehr.***

### Ransomware bleibt die größte Bedrohung

Bei Cyberangriffen mit Ransomware beobachtet das BSI eine Verlagerung der Attacken: Nicht mehr nur große, zahlungskräftige Unternehmen stehen im Mittelpunkt, sondern zunehmend auch kleine und mittlere Organisationen sowie staatliche Institutionen und Kommunen. Besonders von erfolgreichen Cyberangriffen auf Kommunalverwaltungen und kommunale Betriebe sind die Bürger:innen unseres Landes oft auch unmittelbar betroffen: So kann es dazu kommen, dass bürgernahe Dienstleistungen eine Zeitlang nicht zur Verfügung stehen oder persönliche Daten in die Hände Krimineller gelangen.

### Auf dem Vormarsch: Cybercrime as a Service

Wie die Realwirtschaft setzen auch Cyberkriminelle zunehmend auf Arbeitsteilung, einen wachsenden Dienstleistungscharakter und eine enge Vernetzung über Länder- und Branchengrenzen hinweg. Mit dem Konzept des „Cybercrime as a Service“ agieren Cyberkriminelle immer professioneller, denn die Spezialisierung auf bestimmte Dienstleistungen ermöglicht es ihnen, ihre „Services“ gezielt zu entwickeln und einzusetzen.

### Schwachstellen bei Software auf besorgniserregendem Niveau

Das BSI registriert immer mehr Schwachstellen in Software. Diese Schwachstellen sind oft das Einfallstor für Cyberkriminelle auf ihrem Weg zu einer Kompromittierung von Systemen und Netzwerken. Das BSI hat mit durchschnittlich knapp 70 neuen Schwachstellen in Software-Produkten *pro Tag* nicht nur rund ein Viertel mehr registriert als im Berichtszeitraum davor – mit



## Inhalt



## Impressum

Redaktion:
Katrin Alberts (verantwortlich)
E-Mail: katrin.alberts@bsi.bund.de

Bundesamt für Sicherheit
in der Informationstechnik (BSI)
Referat Öffentlichkeitsarbeit
Postfach 20 03 63
53133 Bonn

Hausanschrift:
Godesberger Allee 185–189
53175 Bonn

Telefon: +49 228 999582-0
Telefax: +49 228 999582-5455

Web: www.bsi.bund.de

Das BSI-Forum, Organ des Bundesamtes für Sicherheit in der Informationstechnik in Bonn, ist Bestandteil der <kes> – Die Zeitschrift für Informations-Sicherheit

Die Beiträge der einzelnen Autoren spiegeln deren persönliche Meinung wider, die nicht unbedingt der Position des BSI entsprechen muss.

31. Jahrgang 2023

der Anzahl stieg auch ihre potenzielle Schadwirkung: Immer mehr Lücken (etwa jede sechste) werden als *kritisch* eingestuft.

### Generative KI sorgt für neue Risiken, aber auch für neue Chancen

Mit ChatGPT, Bard und LlaMa sowie einer Vielzahl weiterer Tools ist künstliche Intelligenz (KI) in einer breiten, auch wenig technikaffinen Öffentlichkeit angekommen. Diese Tools sind einfach zu bedienen und liefern eine hohe Qualität. Dabei können sie auch für kriminelle Zwecke missbraucht werden: So können sie dafür sorgen, dass sogenannte Deepfakes – manipulierte Bilder, Videos und Stimmen – immer authentischer werden und dadurch immer schwerer zu entlarven sind. Auch kann KI Phishing-Mails glaubwürdiger machen, im Social Web zu Desinformationskampagnen beitragen oder selbst Schadcode generieren – und das wesentlich schneller und zum Teil wesentlich besser als menschliche Cyberkriminelle. KI kann auch selbst zur Schwachstelle werden: Sie kann gehackt und missbräuchlich eingesetzt werden. Das stellt das Schwachstellenmanagement in Unternehmen und Behörden vor noch nie da gewesene Herausforderungen.

### Auswirkungen des Ukraine-Kriegs auf die IT-Sicherheitslage in Deutschland

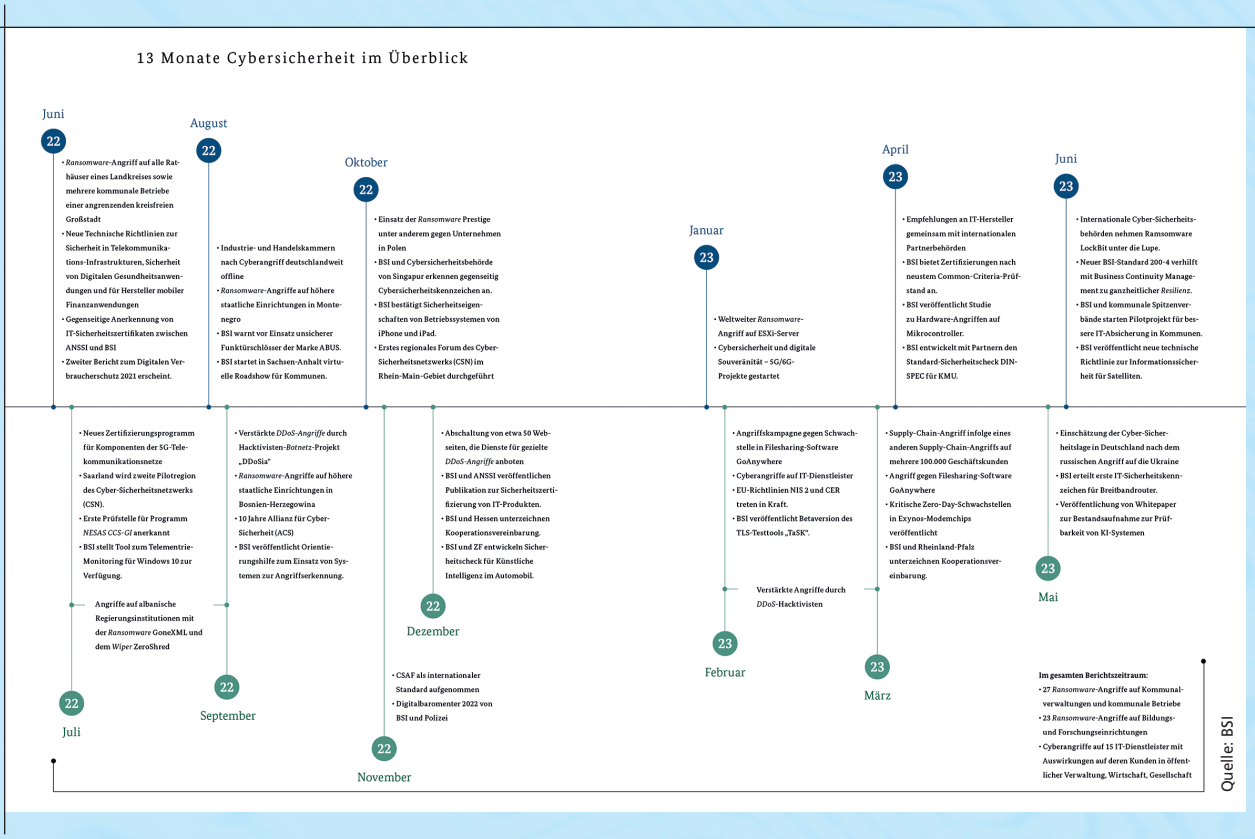
Der russische Angriffskrieg gegen die Ukraine nahm im Berichtszeitraum weiterhin einen zentralen Platz in der öffentlichen Wahrnehmung ein. Vom BSI registrierte Distributed-Denial-of-Service-(DDoS)-Angriffe prorussischer Aktivisten haben bisher aber nur wenig bis keinen bleibenden Schaden anrichten können. Das BSI ordnet die bisherigen Angriffe eher dem Bereich Propaganda zu. Sie sollen Verunsicherung stiften und das Vertrauen in den Staat untergraben. Allerdings kann sich diese Strategie auch ändern, die Vergangenheit hat das gezeigt.

### Wachsende Resilienz gegen zunehmende Bedrohungen

Eine hundertprozentige Sicherheit gegen Angriffe auf IT-Infrastrukturen und softwaregesteuerte Geräte kann es in einer umfassend vernetzten Gesellschaft nicht geben. Den besten Schutz vor solchen Angriffen bietet aber eine ausgeprägte Cyberresilienz. Dabei geht es darum, die Widerstandsfähigkeit von IT zu erhöhen und Angriffen besser begegnen zu können.

Es werden mehr qualifizierte Sicherheitsexpert:innen benötigt, um IT-Systeme resilienter zu machen, Angriffe abzuwehren und, im Falle eines erfolgreichen Angriffs, die negativen Folgen zu mindern. Hier hilft eine Professionalisierung auf Abwehrseite – unter anderem durch Standardisierung, Zentralisierung und Automatisierung. Staat und Zivilgesellschaft stehen den vielfältigen Bedrohungen im Cyberspace nicht wehrlos gegenüber, sondern können ihnen durchaus erfolgreich begegnen. Dabei steht ihnen das BSI als Cybersicherheitsbehörde des Bundes zur Seite. ■

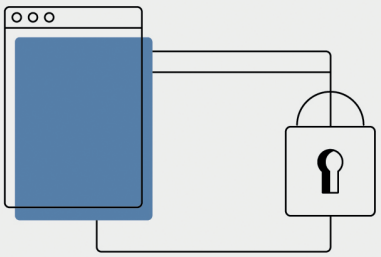
*Abbildung 1: 13 Monate Cybersicherheit im Überblick*



# Ransomware

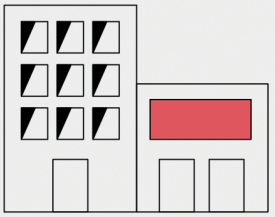
**ist weiterhin die größte Bedrohung.**

**2** **Ransomware-Angriffe** auf Kommunalverwaltungen oder kommunale Betriebe wurden durchschnittlich pro Monat bekannt.



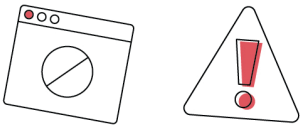
**68** erfolgreiche **Ransomware-Angriffe auf Unternehmen** wurden bekannt.

**15** davon richteten sich gegen **IT-Dienstleister.**

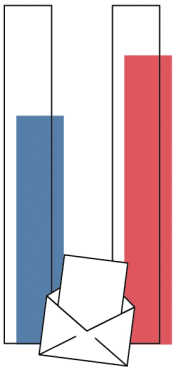


Mehr als **2.000** **Schwachstellen** in Softwareprodukten **(15 % davon kritisch)** wurden im Berichtszeitraum durchschnittlich im Monat bekannt. Das ist ein **Zuwachs von 24 %.**

**Eine Viertelmillion**
neue **Schadprogramm-Varianten** wurden durchschnittlich an jedem Tag im Berichtszeitraum gefunden.



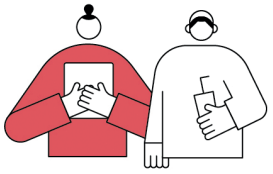
**66%**
aller **Spam-Mails** im Berichtszeitraum waren Cyberangriffe:
**34 %** Erpressungsmails,
**32 %** Betrugsmails



**84%**
aller betrügerischen E-Mails waren **Phishing-E-Mails** zur Erbeutung von Authentisierungsdaten, meist bei Banken und Sparkassen.

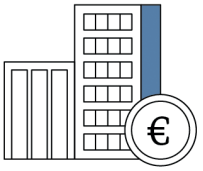
## Top-3-Bedrohungen je Zielgruppe:

### Gesellschaft



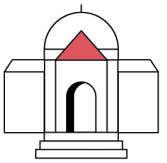
***Identitätsdiebstahl***
Sextortion
Phishing

### Wirtschaft

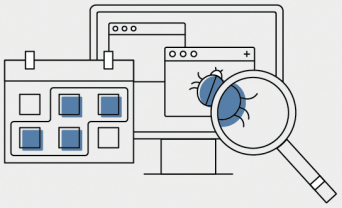


***Ransomware***
Abhängigkeit innerhalb der IT-Supply-Chain
Schwachstellen, offene oder falsch konfigurierte Onlineserver

### Staat und Verwaltung



***Ransomware***
APT
Schwachstellen, offene oder falsch konfigurierte Onlineserver



Rund **21.000** **infizierte Systeme** wurden täglich im Berichtszeitraum erkannt und vom BSI an die deutschen Provider gemeldet.

Durchschnittlich rund **775** **E-Mails mit Schadprogrammen** wurden an jedem Tag im Berichtszeitraum in deutschen Regierungsnetzen abgefangen.

**370** **Webseiten** wurden im Durchschnitt an jedem Tag des Berichtszeitraums für den Zugriff aus den Regierungsnetzen gesperrt. **Der Grund:** Die Seiten enthielten Schadprogramme.

6.220
2022

5.100
2021

**7.120**
Teilnehmer hatte die **Allianz für Cyber-Sicherheit** im Jahr 2023.

Deutschland
**Digital•Sicher•BSI•**

# Digitale Siegel machen hoheitliche Papierdokumente fälschungssicher

## Ob schwarz-weiß oder Farbe – das BSI gestaltet internationale Standards

***Im vergangenen Jahr wurden in Europa die ersten Schengen-Visa mit digitalen Siegeln ausgegeben. In Hamburg startete die Wohnsitz-Ummeldung via Online-Ausweisfunktion, bei der die Adressänderungsaufkleber fälschungssicher mit digitalem Siegel abgesichert sind. Damit findet der Einsatz kryptografisch signierter 2D-Barcodes auf hoheitlichen Dokumenten immer weitere Anwendungsfelder. Durch die internationale Standardisierung des vom BSI entwickelten farbigen JAB-Codes ist es zudem möglich, die Datenkapazität noch einmal deutlich zu erhöhen.***

*Von Dr. Guido Frank und Nicolas Thenée, Referat eID-Strukturen für die Digitalisierung*

Während die Integrität elektronischer Ausweisdokumente heute mit kryptografischen Mechanismen wie digitalen Signaturen abgesichert ist, gibt es weiterhin Bedarf an hoheitlichen Papierdokumenten. Dabei ist die Nutzung eines speziellen Sicherheitspapiers häufig allerdings nicht mehr ausreichend, um Fälschungen zu verhindern.

Mit der Technischen Richtlinie (TR) BSI TR-03137-1 [1] hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) den Grundstein für die kryptografische Absicherung von hoheitlichen Papierdokumenten gelegt. Diese TR definiert ein optisch verifizierbares digitales Siegel, welches in Form eines digital signierten zweidimensionalen Barcodes (DataMatrix) auf dem Dokument aufgebracht wird und dadurch die Prüfung der Echtheit und Unversehrtheit der aufgedruckten Daten ermöglicht. Die TR spezifiziert den Aufbau und die Nutzung digitaler Siegel im Kontext hoheitlicher Dokumente.

Die im digitalen Siegel codierten Daten werden mit dem geheimen Schlüssel (Private Key) des Dokumentenherstellers über ein Online-Personalisierungssystem signiert und können mit einem entsprechenden Lesegerät (etwa ein Smartphone mit einer passenden App) einfach verifiziert werden. Eine prototypische Android-App (SealVa) zur Prüfung der digitalen Siegel nach TR-03137-1 steht unter https://play.google.com/store/apps/details?id=de.tsenger.sealver zur Verfügung.

Aufgrund der meist stark begrenzten Druckfläche, die auf dem Barcode zur Verfügung steht, werden die Zertifikate für Signaturprüfung jedoch in der Regel nicht im Barcode codiert, sondern müssen auf den entsprechenden Lesegeräten vorliegen. Der Barcode selbst enthält eine Referenz auf das zur Prüfung zu verwendende Zertifikat.

Bei einer ungültigen Signatur ist von einer Fälschung auszugehen und das Dokument abzulehnen. Bei einer erfolgreichen Signaturprüfung müssen die im Siegel enthaltenen Daten noch mit denen des Aufdrucks abgeglichen werden, um sicherzustellen, dass das Dokument authentisch ist und nicht manipuliert wurde.

Als Infrastruktur für die Verifikation der digitalen Siegel dienen im Hintergrund bewährte Systeme, die bereits für elektronische Reisepässe und eID-Dokumente eingesetzt werden. Das BSI betreibt die „Nationale Wurzelzertifizierungsstelle“ („Country Signing Certification Authority“, CSCA) für hoheitliche Dokumente und stellt die benötigten Zertifikate für den Dokumentenhersteller aus. Dieser einheitliche Ansatz ermöglicht Flexibilität und schnelle Reaktionen auf politische Entwicklungen.

### Anwendungsfälle

Durch diese Flexibilität fand das digitale Siegel im Rahmen der Flüchtlingssituation 2015 mit dem Ankunftsnachweis (Abb. 1) für Asylsuchende seine Anwendung. Dieser konnte innerhalb kurzer Zeit eingeführt werden und half dabei, die Identifizierung von Asylsuchenden zu verbessern und so die Asylverfahren in Deutschland zu beschleunigen.

Danach wurde die TR des BSI in die Standards für maschinenlesbare Reisedokumente (Doc-9303-Serie) der Internationalen Luftfahrtorganisation (International Civil Aviation Organization, ICAO) überführt. Damit ist nun auch die länderübergreifende und interoperable


*Abbildung 1: Bild eines Ankunftsnachweises mit digitalem Siegel nach TR-03137-1 [1]*


*Abbildung 2: Muster eines Visa-Stickers mit digitalem Siegel*

Nutzung der digitalen Siegel möglich. Auf Basis der Entscheidung der EU-Kommission C(2020) 2672 schützt das digitale Siegel seit 2022 auch ausgestellte Visa in Europa vor Fälschungen und erhöht damit die Sicherheit der Grenzkontrolle (Abb. 2).

Auch auf nationaler Ebene spielt die TR-03137-1 eine wichtige Rolle: In der Freien und Hansestadt Hamburg startete in der zweiten Jahreshälfte 2022 die Möglichkeit der Online-Ummeldung. Diese ermöglicht mithilfe der Online-Ausweisfunktion des Personalausweises die Ummeldung von zu Hause aus – niemand muss dafür mehr beim Amt erscheinen. Bei der Ummeldung werden nicht nur die Adressdaten auf dem Chip geändert, sondern – über einen digital gesiegelten Adressaufkleber – auch die auf dem Ausweis aufgedruckte Adresse. Der Aufkleber erreicht die Antragsteller:inn:en auf dem Postweg.

Zudem wird aktuell geplant, die ausländerrechtlichen Papierdokumente wie beispielsweise Fiktionsbescheinigungen, Ausweisersatz, Notreiseausweis et cetera, deren Design gerade in Überarbeitung ist, in Zukunft ebenfalls mit einem digitalen Siegel zu versehen und diese Dokumente somit gegen Fälschungen zu schützen.

Daneben hat das BSI mit der BSI TR-03171 eine weitere Richtlinie für den optisch verifizierbaren Schutz von Verwaltungsdokumenten entwickelt (vgl. https://bsi.

bund.de/dok/digitale-siegel). Ziel ist es, Bescheide, Genehmigungen oder andere Dokumente, die bisher durch eine Behörde mit Stempel und Unterschrift versehen wurden, mit einem digitalen Siegel abzusichern. Solche Dokumente können damit elektronisch zugestellt und zweifelsfrei in elektronischer oder gedruckter Form überprüft werden.

## Datenstruktur

Das digitale Siegel nach TR-03137-1 besteht aus einem Header, einer Message-Zone (enthält die eigentlichen Nutzdaten) und einer Signature-Zone. Innerhalb des Headers (Abb. 3) werden Informationen wie Ausstellerland, eine Referenz auf das für die Signaturprüfung benötigte Zertifikat, das Ausstellungsdatum, Signaturerstellungsdatum, Dokumentenart (z. B. Visum oder Ankunftsnachweis) und ein Identifier, der angibt, welche Daten in welcher Reihenfolge codiert werden, angegeben.

Die Daten in der Message-Zone werden mittels einer Tag-Length-Value-Datenstruktur codiert. Hierbei beschreibt das Tag (1 Byte) den Typ des codierten Datenelements und die Länge (1–5 Bytes) gibt die Länge der zu codierenden Daten für dieses Tag an. Abhängig von der Versionsnummer werden die Längenbytes der TLV Struktur in einem Byte (Versionsnummer 3) oder in DER-TLV-Length-Encoding (Versionsnummer 4) dargestellt.

Innerhalb der Message-Zone können die Daten auf unterschiedliche Weise codiert werden:

- Alphanumerische Zeichen (A–Z, 0–9 und Leerzeichen) werden als C40-Bytes codiert. Dies führt dazu, dass aus drei Zeichen, zwei Bytes platzsparend codiert werden können.
- Beliebige Binärdaten (ohne weiteres Encoding)
- Für positive Integer wird Unsigned-Integer-Repräsentierung verwendet.
- Datumsangaben werden in einem Datumsformat codiert. Hier wird zunächst das Datum als ganzzahliger Wert durch Konkatenation von Monat, Tag und Jahr dargestellt. Dieser ganzzahlige Wert wird dann in 3 Bytes abgebildet.

Die nach den Nutzdaten folgende Signatur wird mit dem Tag 0xFF gekennzeichnet, welches den Start der digitalen Signatur (siehe Abb. 3) definiert. Nach dem Tag folgen die Codierung der Länge (1–5 Bytes) der Signaturdaten sowie die Signatur selbst. Die Signatur wird über den Header und die gesamte Message-Zone gebildet. Für die digitalen Siegel kommen Signaturen auf Basis von elliptischen Kurven, gemäß den Vorgaben der TR-03116-2 [2] zum Einsatz.

## In Farbe: JAB-Code

Die Integration von digitalen Siegeln auf hoheitlichen Dokumenten stellt Behörden vor die Herausforderung, dass aus Platz-

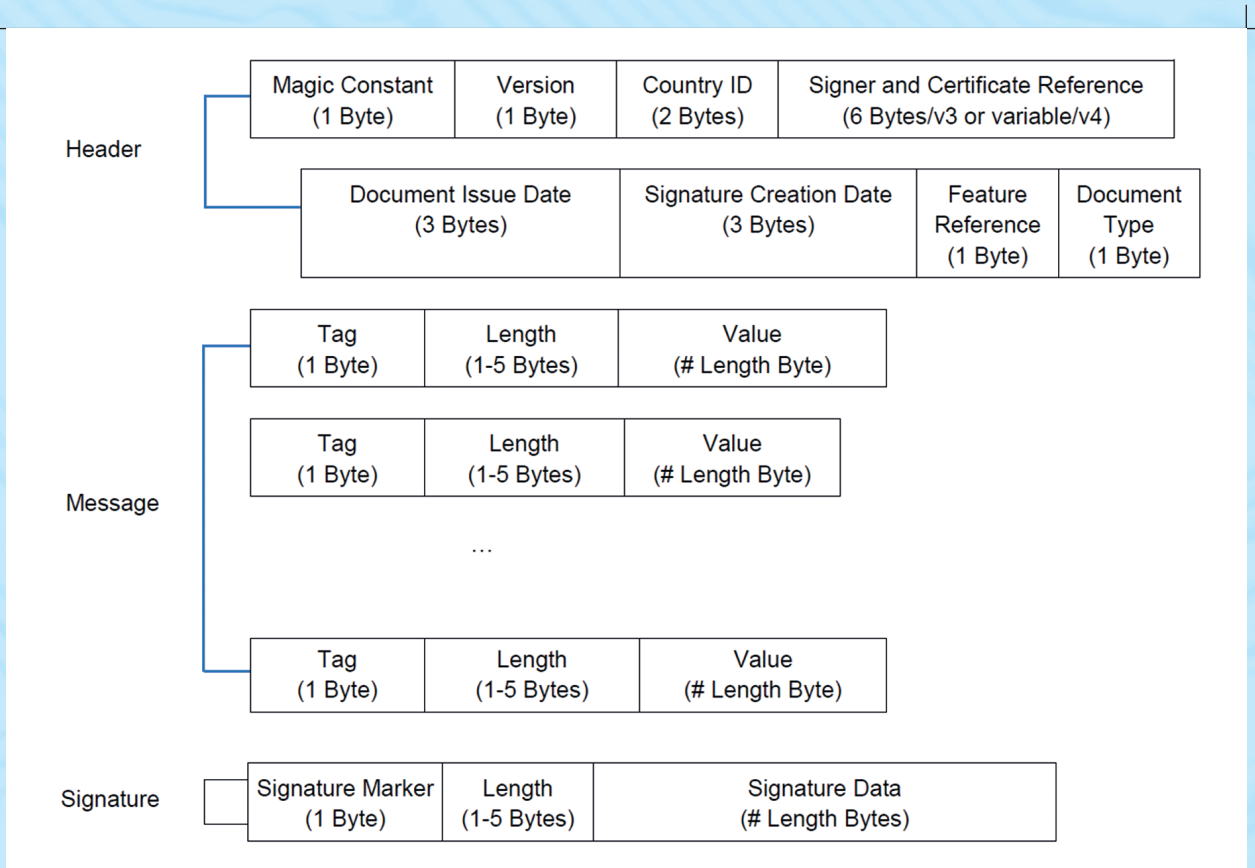



*Abbildung 3: Generische Datenstruktur für digitale Siegel gemäß [3]*

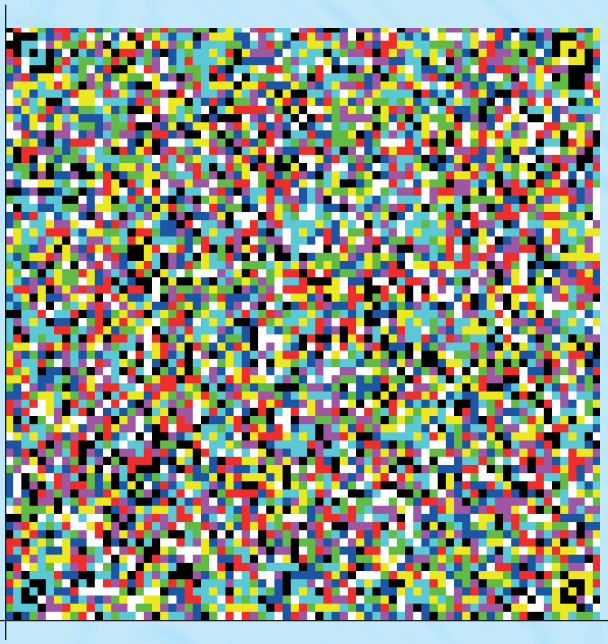


*Abbildung 4: Beispieldarstellung eines JAB-Codes mit Gesichtsbild, MRZ, Passnummer und AZR-Nummer*

gründen meist nur eine sehr kleine Fläche für den Druck zur Verfügung steht. Dies führt dazu, dass die 2D-Barcodes in ihrer Speicherkapazität meist stark eingeschränkt sind und nicht alle aufgedruckten Merkmale (darunter das Gesichtsbild) im Barcode codiert werden können.

Um dieses Problem zu lösen, hat das BSI in Zusammenarbeit mit dem Fraunhofer SIT den farbigen „JAB-Code" entwickelt und diesen in die Standardisierung eingebracht. Seit April 2022 steht der JAB-Code als internationaler Standard ISO/IEC 23634 [4] zur Verfügung. Durch die verwendeten Farben kann eine wesentlich höhere Datendichte als bei monochromen Barcodes erreicht werden – so lassen sich bei gleicher Größe wesentlich mehr Daten speichern.

Der JAB-Code ist ein aus mindestens vier und maximal acht Farben bestehender 2D-Barcode der sowohl rechteckig als auch quadratisch sein kann. Durch diese Beschaffenheit lassen sich durch Kombination der rechteckigen und quadratischen Module beliebige Formen erzeugen. Der JAB-Code kann demnach formflexibel auf dem Trägerdokument aufgebracht werden.

Der JAB-Code besteht aus vier Suchmustern, die an den jeweiligen Ecken platziert sind: Durch die Platzierung der Suchmuster im Barcode und der Ausgestaltung der Form und Farbe kann beim JAB-Code auf eine Ruhezone verzichtet werden. Ohne diese Ruhezone ist der Barcode flexibel einsetzbar und stellt somit auch eine höhere Speicherdichte zur Verfügung.

Diese Eigenschaften machen den JAB-Code besonders interessant für den Einsatz auf hoheitlichen Papierdokumenten. So könnte es mit dem JAB-Code künftig möglich sein, unter geeigneten Rahmenbedingungen alle aufgedruckten Daten im Barcode abzusichern und so die Fälschungssicherheit auf ein neues Niveau zu heben. Der in Abbildung 4 dargestellte JAB-Code zeigt prototypisch die Codierung eines Gesichtsbilds, zusätzlich zu den aufgedruckten Daten wie MRZ, Passnummer und AZR-Nummer (Ausländerzentralregister) – dieser Barcode kann mit der App „JABPro" verifiziert werden (https://play.google.com/store/apps/details?id=org.jabcode.jabpro.twa). ■

## Literatur


**[1]** Bundeamt für Sicherheit in der Informationstechnik (BSI), Technische Richtlinie BSI TR-03137-1: Optically Verifiable Cryptografic Protection of non-electronic Documents (Digital Seal), Version 2.5, Dezember 2021, www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03137/BSI-TR-03137_Part1.pdf?__blob=publicationFile&v=7

**[2]** Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie BSI TR-03116-2: Kryptographische Vorgaben für die Projekte der Bundesregierung, März 2023, www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03116/TR-03116_node.html

**[3]** International Civil Aviation Organization (ICAO), Machine Readable Travel Documents, Doc 9303, Eighth Edition Part 13: Visible Digital Seal, 2021, www.icao.int/publications/Documents/9303_p13_cons_en.pdf

**[4]** International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), ISO/IEC 23634 Information technology – Automatic identification and data capture techniques, JAB Code polychrome bar code symbology specification, April 2022, verfügbar via https://www.iso.org/standard/76478.html (kostenpflichtig)

**[5]** Bundeamt für Sicherheit in der Informationstechnik (BSI), Technische Richtlinie BSI TR 03137-2: JAB Code (Just Another Bar Code), Color Bar Code Symbology Specification, Version 1.0, Juli 2020, www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03137/BSI-TR-03137_Part2.pdf?__blob=publicationFile&v=1

## Amtliche Mitteilungen

1. **Im Vergleich zur letzten Ausgabe dieser amtlichen Mitteilungen sind inzwischen folgende Zertifizierungen des BSI gemäß Common Criteria und ITSEC abgeschlossen worden:**

| Hersteller/Vertreiber | Produkt | Produkt-Typ | Ergebnis<br>ID<br>Zertifizierungsdatum |
|---|---|---|---|
| Eviden Germany GmbH | CardOS V6.0 ID R1.1 | Hoheitliche Dokumente (IC mit Anwendung) | BSI-DSZ-CC-1162-V2-2023<br>2023-10-17 |
| Eviden Germany GmbH | CardOS V6.0 ID R1.1 (BAC) | Hoheitliche Dokumente (IC mit Anwendung) | BSI-DSZ-CC-1172-2022-MA-02<br>2023-10-16 |
| NXP Semiconductors Germany GmbH | NXP Secure Smart Card Controller P6021y VB* including IC Dedicated Software | Smart-Card-Controller | BSI-DSZ-CC-1072-V5-2022-MA-01<br>2023-10-12 |
| EMH metering GmbH & Co.KG | CASA 1.0 and CASA 1.1 | Smart-Meter-Gateway | EAL4+<br>BSI-DSZ-CC-0919-V3-2023<br>2023-10-02 |
| SYSGO GmbH | PikeOS Separation Kernel v5.1.3 for the NXP LS 1023A/LS1043A Processor, Version 3.1.0 | Betriebssystem | EAL5+<br>BSI-DSZ-CC-1185-2023<br>2023-09-18 |
| genua GmbH | genugate 10.0 p14 Firewall Software | Firewall | BSI-DSZ-CC-1154-2023-MA-01<br>2023-09-25 |
| NXP Semiconductors Germany GmbH | NXP Secure Smart Card Controller N7122 with IC Dedicated Software and Crypto Library (R1/R2/R3) | Smart-Card-Controller | EAL6+<br>BSI-DSZ-CC-1149-V2-2023<br>2023-09-13 |
| Stoneridge Electronics AB | SE 5000-8.1, Version C | Digital Tachograph (Vehicle-Unit) | EAL4+<br>BSI-DSZ-CC-1071-V7-2023<br>2023-09-12 |
| EFR GmbH | Secure Smart Grid Hub (SGH-S), V1.00 | Smart-Meter-Gateway | EAL4+<br>BSI-DSZ-CC-1000-2023<br>2023-09-11 |
| Stoneridge Electronics AB | SE 5000-8.1, Version B | Digital Tachograph (Vehicle-Unit) | BSI-DSZ-CC-1071-V6-2023-MA-01<br>2023-08-15 |
| Giesecke+Devrient Mobile Security GmbH | STARCOS 3.7 ID ePA C1, STARCOS 3.7 ID eAT C1, STARCOS 3.7 ID ePass C1 | elektronische Identitätskarte | BSI-DSZ-CC-1077-2020-RA-02<br>2023-08-09 |

| Hersteller/Vertreiber | Produkt | Produkt-Typ | Ergebnis<br>ID<br>Zertifizierungsdatum |
|---|---|---|---|
| Infineon Technologies AG | Infineon Technologies AG OPTIGA™ Trusted Platform Module SLB9672_2.0 v16 and SLB9673_2.0 v26, version v16.10.16488.00, v16.12.16858.00 and v26.10.16688.00 | Trusted-Platform-Module | EAL4+<br>BSI-DSZ-CC-1178-V4-2023<br>2023-08-01 |
| Infineon Technologies AG | Infineon Technologies AG OPTIGA™ Trusted Platform Module SLB9672_2.0 v17 und SLB9673_2.0 v27; v17.10.16488.00, v17.12.16858.00, v17.13.17733.00, v27.10.16688.00 and v27.13.17770.00 | Trusted-Platform-Module | EAL4+<br>BSI-DSZ-CC-1179-V4-2023<br>2023-07-27 |
| Bundesdruckerei GmbH | Bundesdruckerei Document Application with tamper-evident casing 2.5.1, Firmware Version 1.5.8, TOE Casing Version 0 | Hoheitliche Dokumente (Software) | EAL3+<br>BSI-DSZ-CC-1215-2023<br>2023-07-20 |
| Stoneridge Electronics AB | SE 5000-8.1 Version A | Digital Tachograph (Vehicle-Unit) | EAL4+<br>BSI-DSZ-CC-1071-V6-2023<br>2023-07-10 |
| Cherry GmbH | CHERRY eHealth Terminal ST-1506, AFxZ FW 3.0.0, HW 4.0.0 | Kartenterminal (eHealth) | EAL3+<br>BSI-DSZ-CC-1124-V3-2023<br>2023-06-06 |

**Anmerkung:**

– Die zugehörigen Zertifizierungsreporte mit Zertifikaten sind auf der Web-Seite www.bsi.bund.de/zertifizierungsreporte einzusehen.

**2. Im Vergleich zur letzten Ausgabe dieser amtlichen Mitteilungen ist inzwischen für folgende Produkte eine Zertifizierung beantragt worden:**

| Antragsteller | Produktname | Produkttyp | Zertifizierungs-ID |
|---|---|---|---|
| SUSE LLC | SUSE Linux Enterprise Server 15 | Betriebssystem | BSI-DSZ-CC-1231 |
| SUSE LLC | SUSE Linux Enterprise Micro 5.3 | Betriebssystem | BSI-DSZ-CC-1230 |
| planck Security S.A. | planck Secure Email, Version 3.1.0 | E-Mail- und Dateiverschlüsselung | BSI-DSZ-CC-1227 |

**Anmerkungen:**

– Eine Veröffentlichung dieser Angaben erfolgt hier nur, sofern der Antragsteller damit einverstanden ist *und* die Evaluierung begonnen wurde. In der Liste vorhandene Nummerierungslücken betreffen beantragte Zertifizierungen, für die die genannten Voraussetzungen fehlen.

– Bei einigen Produkten handelt es sich um eine Re-Zertifizierung eines bereits zertifizierten Produkts wegen Änderungen am Produkt oder Wechsel der Prüfkriterien.

### 3. Vom BSI erteilte Standortzertifikate

| Antragsteller | Entwicklungs-/ Produktionsstandorte | ID Ausstellungsdatum | gültig bis |
|---|---|---|---|
| Linxens (Thailand) Co Ltd. | Linxens (Thailand) Co Ltd., 142 Moo, Hi-Tech Industrial Estate, Tambon Ban Laean, Amphor Bang-pa-In, 13160 Ayutthaya, Thailand | BSI-DSZ-CC-S-0253-2023 2023-10-10 | 2026-01-26 |
| ASE Singapore Pte. Ltd. | ASE Singapore Pte. Ltd. (ASESG), 2 Woodlands Loop, Singapore 738074 | BSI-DSZ-CC-S-0256-2023 2023-10-10 | 2026-02-04 |
| NXP Manufacturing (Thailand) Inc. | NXP Semiconductor Thailand Ltd. (ATBK) 303 Moo 3 Chaengwattana Rd. Laksi, Bangkok 10210, Thailand | BSI-DSZ-CC-S-0251-2023 2023-09-29 | 2025-11-18 |
| NXP Semiconductors Taiwan Ltd (ATKH) | NXP Semiconductors Taiwan Ltd (ATKH), #10, Chin 5th Road, N.E.P.Z, Kaohsiung 81170, Taiwan, R.O.C. | BSI-DSZ-CC-S-0252-2023 2023-09-29 | 2025-12-20 |
| Polska Wytwórnia Papierów Wartościowych S.A. | PWPW SmartApp Development Site Polska Wytwórnia Papierów Wartościowych S.A. ul. Sanguszki 1, 00-222 Warszawa Poland | BSI-DSZ-CC-S-0245-2023 2023-09-21 | 2025-10-26 |
| GlobalFoundries Singapore Pte. Ltd. | GlobalFoundries Singapore Pte. Ltd. – Fab2, Fab7 and Fab7G | BSI-DSZ-CC-S-0257-2023 2023-09-08 | 2026-02-09 |
| United Microelectronics Corporation (UMC) | United Microelectronics Corporation Fab 12i, No 3, Pasir Ris Drive 12, Singapore 519528 | BSI-DSZ-CC-S-0258-2023 2023-08-22 | 2026-02-02 |
| Theben Smart Energy GmbH | 1. Entwicklungsstandort Theben Smart Energy GmbH, Hohenbergstr. 32, 72401 Haigerloch<br>2. Fertigungsstandort Theben AG, Madertal 22, 72401 Haigerloch<br>3. Entwicklungsstandort Theben Smart Energy GmbH, Bremer Str. 179a, 21073 Hamburg | BSI-DSZ-CC-S-0230-2023-MA-01 2023-07-31 | 2025-07-24 |
| NXP Semiconductors Belgium NV | NXP Semiconductors Belgium NV, Interleuvenlaan 80, B-3001 Leuven, Belgium | BSI-DSZ-CC-S-0241-2023 2023-07-27 | 2025-11-25 |
| Taiwan Semiconductor Manufacturing Company, Limited | Taiwan Semiconductor Manufacturing Company Limited, Fab 18A/18B and Advanced Backend Fab 6A | BSI-DSZ-CC-S-0243-2023 2023-07-21 | 2025-11-04 |

**4. Seit der letzten Ausgabe haben folgende Produkte ein Zertifikat der Beschleunigten Sicherheitszertifizierung des BSI erhalten:**

| Hersteller | Produkt | Zertifizierungs-ID | gültig bis |
|---|---|---|---|
| OMICRON electronics GmbH | RBX1 StationGuard, HW-Plattformen RBX1, Produktversion 2.21.0081 | BSI-DSZ-BSZ-0006-2023 | 2025-09-27 |

**5. Vom BSI erteilte ISO-27001-Zertifikate auf der Basis von IT-Grundschutz**

| Zertifikatsnummer | Institution | Untersuchungsgegenstand | gültig bis |
|---|---|---|---|
| BSI-IGZ-0582-2023 | Thüringer Netkom GmbH | Die Thüringer Netkom GmbH betreibt ein Rechenzentrum am Standort Ilmenau und verantwortet hierfür den Rechenzentrumsbetrieb zum Zwecke der Vermarktung durch Bereitstellung von Rechenzentrumsflächen zur Aufstellung (Whitespace) und zum Betrieb von IT-Systemen (Housing) für ihre Kunden. Der Informationsverbund umfasst das Rechenzentrum am Standort Ilmenau, den Geschäftsprozess Rechenzentrumsbetrieb sowie die für den RZ-Betrieb erforderlichen Anwendungen, IT-Systeme, Netzwerk- und Kommunikationsverbindungen bis zu den Kunden-Racks sowie Büro-/Betriebsräume. Nicht zum Geltungsbereich gehören die von den Kunden aufgestellten IT-Systeme in den Racks und deren Backup. Diese liegen im Verantwortungsbereich der jeweiligen Kunden. Das Hosting von IT-Komponenten ist ebenfalls nicht Bestandteil des Geltungsbereichs. | 2026-10-05 |
| BSI-IGZ-0566-2023 | noris network AG | Der Informationsverbund „Housing“ beinhaltet all diejenigen Prozesse und Systeme, die für den Betrieb von Housing/Co-Location der noris-network-eigenen Rechenzentren zuständig sind. Dazu zählt der Betrieb der Rechenzentren und der umgebenden Einheiten wie Klimaanlagen, USVs, (Not-)Strom und Zugangssysteme. Der dazugehörige Geschäftsbereich „Housing“ wird von noris network selbst betrieben, noris network ist für die entsprechenden Services mit eigenen Mitarbeitern an den Standorten komplett verantwortlich. | 2026-09-30 |
| BSI-IGZ-0590-2023 | Rechenzentrum der Finanzverwaltung des Landes Nordrhein-Westfalen | Die elektronische Steuererklärung ELSTER ist ein Projekt der deutschen Steuerverwaltungen aller Länder und des Bundes zur Abwicklung der Steuererklärungen und Steueranmeldungen über das Internet. Die im Rechenzentrum der Finanzverwaltung des Landes Nordrhein-Westfalen (RZF) betriebene ZPS (Zentrale Produktions- und Service-Stelle) erbringt fachliche Dienste im Kontext länderübergreifender Verfahren. Der Untersuchungsgegenstand umfasst die IT-Infrastruktur mit den zentralen fachlichen Basisdiensten und -anwendungen der ZPS am Standort Düsseldorf. | 2026-09-06 |
| BSI-IGZ-0587-2023 | Kommunales Rechenzentrum Niederrhein (KRZN) | Der Untersuchungsgegenstand des Kommunalen Rechenzentrums Niederrhein (KRZN) umfasst den Betrieb der Infrastruktur sowie Fachanwendungen und zugehörige IT-Systeme des Rechenzentrums am Standort Kamp-Lintfort. Zu den Fachanwendungen zählen insbesondere solche aus dem Bereich der öffentlichen Verwaltung. Einzelne Bestandteile der zugehörigen IT-Systeme im Rahmen des Rechenzentrumsbetriebs sind Client-/Server-Umgebungen, SAN, Netzwerke und darüber hinaus die Verwaltung der Gebäude und Räume und die gesamte Gebäudeleittechnik. | 2026-09-06 |

| Zertifikatsnummer | Institution | Untersuchungsgegenstand | gültig bis |
|---|---|---|---|
| BSI-IGZ-0588-2023 | WOLFF Daten. Menschen. Marketing. GmbH | Der Informationsverbund am Standort Berlin umfasst die gesamte interne Organisation mit der Verwaltung, der Lohn- und Finanzbuchhaltung, dem Bereich Kommunikation und Vertrieb und der IT-Administration. Darüber hinaus die Erstellung von Marketing-Analysen und -Konzepten, das operative Kundendatenmanagement sowie das Management von Hosting und Betrieb individuell realisierter Portal-Lösungen. Ausgenommen ist der Software-Entwicklungs-Bereich. | 2026-09-04 |
| BSI-IGZ-0559-2023 | GEMINI DIRECT marketing solutions GmbH | Am Standort Idstein betreibt die GEMINI DIRECT marketing solutions GmbH einen abgeschotteten Informationsverbund, in dem personenbezogene und schutzbedürftige Daten für Dialogmarketingzwecke gespeichert und verarbeitet (Selektion, Anreicherung, Aufbereitung) werden. Grundlage dieser Leistungen ist eine umfassende Konsumentendatenbank mit einer Vielzahl von Selektionsmerkmalen. | 2026-08-15 |
| BSI-IGZ-0512-2023 | Stadt Nürnberg | Der Informationsverbund für den Netzübergang zum Verbindungsnetz des Bundes (NdB) beinhaltet alle Prozesse, die zum Betrieb des Netzübergangs notwendig sind. Dazu zählen die netztechnischen Komponenten begrenzt zum Städtischen LAN und begrenzt zu den SINA-Boxen. | 2026-07-27 |
| BSI-IGZ-0563-2023 | KENFO – Fonds zur Finanzierung der kerntechnischen Entsorgung | Der Informationsverbund umfasst alle internen Prozesse zur Erfüllung des Stiftungszwecks sowie die dafür notwendigen Anwendungen, IT-Systeme, Netze, Mitarbeiter, die für den Betrieb notwendigen Dienstleister und die Räumlichkeiten des KENFO. | 2026-07-25 |
| BSI-IGZ-0585-2023 | Vodafone Group Services GmbH | Der Informationsverbund umfasst die Referenzarchitektur der Vodafone Cloud & Security in Deutschland (VC&S DE), die für die Bereitstellung der Vodafone Cloud-Dienste erforderlich ist und in den beiden deutschen Rechenzentren der Vodafone Group in Frankfurt am Main und Rüsselsheim in gleicher Weise installiert ist. | 2026-07-20 |
| BSI-IGZ-0570-2023 | DATANET GmbH | Der Untersuchungsgegenstand umfasst den „Informationsverbund Rechnungsdatennachverarbeitung für öffentliche Auftraggeber“ (IV-RDNV-OefA) am Firmenstandort der DATANET GmbH in Bad Münstereifel, welcher der Bereitstellung kundenindividueller Services, zur Datenverarbeitung im Auftrag auf Basis der unternehmenseigenen CT-Services Software-Plattform dient. Die Plattform umfasst die Module CTR (Communication Tool Rebilling/Rerating), CTR+ (Communication Tool Reporting) sowie CTO (Communication Tool Ordering). Die Ergebnisse entsprechen der vertraglich vereinbarten Granularität der „Rechnungsdatennachverarbeitung“ (RDNV). Im Rahmen des IV-RDNV-OefA werden ausschließlich Services für öffentliche Auftraggeber erbracht, welche besonderen Vorgaben an die Informationssicherheit unterliegen. | 2026-07-06 |
| BSI-IGZ-0558-2023 | Stadt Köln | Der Informationsverbund Basisdienste Rechenzentrum Stadt Köln umfasst Dienstleistungen und Betrieb der beiden zentralen städtischen Rechenzentren und somit jeglicher IT-Komponenten, welche für die Datenverarbeitung und die Unterstützung von Verfahren der kommunalen Verwaltung eingesetzt werden. | 2026-07-05 |

| Zertifikatsnummer | Institution | Untersuchungsgegenstand | gültig bis |
|---|---|---|---|
| BSI-IGZ-0555-2023 | centron GmbH | Der Prozess Hosting beinhaltet folgende Teilbereiche: Der Betrieb des Rechenzentrums am Standort Hallstadt und der dazu notwendigen Infrastruktur. Unter der Bereitstellung von Rackspace für Kunden wird die Zurverfügungstellung von Einbauplätzen verstanden. Die centron GmbH stellt das dazu notwendige Rechenzentrum zur Verfügung und betreibt dies. Ebenso wird Strom und ein Netzwerkanschluss bereitgestellt. Seitens der centron GmbH wird die Hardware optional auf Kundenwunsch auf Funktionsfahigkeit überwacht. Bei Defekten werden auf Wunsch des Kunden Hardwarekomponenten ausgetauscht. Weitere IT-Service-Leistungen sind nicht Teil der Bereitstellung von Rackspace. Die Bereitstellung von Servern für Kunden beinhaltet den Betrieb des Rechenzentrums und die Installation, sowie den Betrieb von Serverhardware. Zusätzlich das Monitoring der genannten Serverhardware. Nicht Teil der Bereitstellung von Servern sind die auf den Servern installierten virtuellen Umgebungen, die Betriebssysteme und die installierten Kundenapplikationen. Für diese sind die Kunden vollständig selbst verantwortlich. Der Prozess des Dienstleister-Managements gliedert sich in die Teilbereiche Auswahl, Beauftragung und Überwachung. Zu den relevanten Dienstleistern zählen solche Dienstleister, die Support für die genannten Tätigkeiten und Leistungen der centron GmbH erbringen. Dazu zählen auch insbesondere solche Dienstleister, bei denen Rackspace seitens der centron GmbH angemietet wird. Nicht Teil des Informationsverbundes sind Dienstleister, die Dienstleistungen für die virtuelle Umgebung, Betriebssysteme und Anwendungen der Kunden erbringen. Alle anderen Prozessabläufe der centron GmbH sind nicht Teil des Informationsverbundes. | 2026-07-04 |
| BSI-IGZ-0576-2023 | IHK Gesellschaft für Informationsverarbeitung mbH | Der Informationsverbund „Verbindungsnetz Teilnehmeranschluss (VN-TNA)“ umfasst gemäß den Anschlussbedingungen die unmittelbar an das Verbindungsnetz gekoppelten Netze und IT-Infrastruktur-Komponenten, wie insbesondere Router, Switche und Firewalls sowie die Anschlusstechnik mit CE-Router und SINA Box. Alle erforderlichen Komponenten für den Teilnehmeranschluss zum Verbindungsnetz befinden sich im Rechenzentrum der IHK Gesellschaft für Informationsverarbeitung mbH (IHK-GfI) in Dortmund. Betrieb und Management der unmittelbar angeschlossenen Netze und Netzkomponenten geschieht durch die IHK-Gfl im Bereich Netzwerk Services. | 2026-07-03 |
| BSI-IGZ-0569-2023 | sector27 GmbH | Die sector27 GmbH plant, betreibt und stellt im Auftrag eines Kunden eine standardisierte Basisplattform für fachspezifische Anwendungen bereit. Die fachspezifischen Anwendungen werden entweder durch die Kunden eigenverantwortlich administriert oder auf Wunsch durch die sector27 GmbH.<br>Die Basisplattform besteht aus IT-Systemen mit ihren erforderlichen Betriebssystemen, der Netzwerkinfrastruktur sowie den erforderlichen Management- und Überwachungssystemen.<br>Die Systeme werden in einer sicheren infrastrukturellen Umgebung des Auftraggebers betrieben. Der Zertifizierungsumfang umfasst weiterhin den Betrieb von IT-Grundschutz konformen EMM-Systemen (Enterprise-Mobility-Management-Lösung), die auf der Basisplattform aufsetzen. | 2026-07-02 |