

Security-Guide für digitale Services

Richtlinie Security für digitale Services

Version 02.95.00

22. März 2026



**”Zufall ist ein Wort ohne Sinn;
nichts kann ohne Ursache existieren.”**

Philosophisches Taschenwörterbuch Band 6, Artikel Philosophie, Sektion IV (deutsche Übersetzung), 1764, Voltaire (1694-1778), eigtl. François-Marie Arouet, frz. Philosoph u. Schriftsteller

Kapitel 16

Signaturen

16.1 Grundlagen

[SOLL] Für digitale Dokumente gibt es verschiedene Arten von Signaturen, die sich nach rechtlicher Verbindlichkeit, Sicherheitsniveau und technischer Umsetzung unterscheiden.

16.2 Signaturtypen für Dokumente

16.2.1 Einfache elektronische Signatur (*EES*)

Die *EES* ist jede Form elektronischer Daten, die zur Unterzeichnung genutzt wird. Zum Beispiel eingescannte Unterschriften, Checkboxes (*„Ich stimme zu“*) oder einfache Namen unter E-Mails.

Ziel

Niederschwellige Form zur Kenntlichmachung einer Zustimmung oder Willenserklärung ohne hohen Sicherheitsanspruch.

16.2.2 Fortgeschrittene elektronische Signatur (*FES*)

Die *FES* ist eindeutig einer Person zugeordnet, ermöglicht ihre Identifizierung und erkennt Änderungen am Dokument nach der Signatur. Sie basiert meist auf kryptografischen Verfahren mit persönlichem Schlüssel.

Ziel

Höhere Beweiskraft und Sicherheit als *EES*, geeignet für vertrauliche oder rechtlich relevante Dokumente, z. B. Geschäftsverträge.

16.2.3 Qualifizierte elektronische Signatur (*QES*)

Die *QES* erfüllt alle Anforderungen der *FES* und basiert zusätzlich auf einem qualifizierten Zertifikat einer anerkannten Vertrauensstelle. Sie erfordert eine überprüfte Identifizierung (z. B. *eID*, *VideoIdent*).

Ziel

Rechtsverbindliche digitale Unterschrift mit gleichem Stellenwert wie eine handschriftliche Unterschrift – z. B. für Behörden, Gerichte, notarielle Vorgänge.

16.2.4 Digitale Signatur (*im engeren technischen Sinn*)

Dies ist ein kryptografisches Verfahren, bei dem mit einem privaten Schlüssel ein Hashwert des Dokuments signiert wird. Es dient primär der Integritätsprüfung und Authentizität.

Ziel

Nachweis, dass ein Dokument unverändert ist und vom angegebenen Absender stammt unabhängig von rechtlicher Verbindlichkeit. Grundlage aller oben genannten Signaturarten.

16.2.5 Übersicht**16.2.5.1 Dokumente (z.B. *PDFs*, *Verträge*, *Bescheide*)**

Signaturart	geeignet für	Rechtswirkung	Tools/Formate
Einfache elektronische Signatur (<i>EES</i>)	Interne Freigaben, informelle Schreiben	Gering – anfechtbar	PDF-Tools (Adobe, Foxit), Word
Fortgeschrittene elektronische Signatur (<i>FES</i>)	Geschäftliche Dokumente, sensible Unterlagen	Beweiskräftig, mittleres Sicherheitsniveau	DocuSign, FP Sign, Adobe Sign
Qualifizierte elektronische Signatur (<i>QES</i>)	Verträge mit hoher Rechtsverbindlichkeit, behördliche Akte	Gleichwertig zur handschriftlichen Unterschrift	D-Trust, A-Trust, SwissSign, <i>EU</i> -zertifizierte Anbieter
Digitale Signatur (<i>technisch</i>)	Integritätssicherung (z. B. bei <i>Formularen</i> , <i>Gutachten</i>)	Technisch sicher, rechtlich je nach Zertifikat	Signieren per OpenSSL, PGP, S/MIME

Tabelle 16.1: Übersicht Signaturen für Dokumente

16.2.5.2 E-Mails

Methode	Zweck	geeignet für	Tools/Technologien
S/MIME	Digitale Signatur + Verschlüsselung	Geschäftskommunikation, Behörden, Justiz	Outlook, Thunderbird, Apple Mail
PGP/GPG (<i>OpenPGP</i>)	Signatur + Verschlüsselung	Entwickler, Aktivisten, IT-Security	Thunderbird mit Enigmail, Gpg4win
Signatur-Bild/Disclaimer	Keine echte Signatur, nur visuell	Marketing, nicht rechtlich bindend	Outlook, Mail-Templates

Tabelle 16.2: Übersicht Signaturen für E-Mails

16.3 spezielle Signaturtypen

16.3.1 Sichtbare vs. unsichtbare Signatur

- **Sichtbare Signatur:** Unterschriftenfeld mit Name, Datum etc. im [PDF](#).
- **Unsichtbare Signatur:** In den Metadaten des Dokuments eingebettet und dient der Integritätsprüfung.

16.3.2 Zeitstempel (*Timestamp*)

- Ergänzung zur Signatur zur Bestätigung des genauen Signaturzeitpunkts.
- Besonders wichtig für Langzeitarchivierung oder gerichtliche Nachweise.

Kapitel 23

Web-Infrastruktur

23.1 Grundlagen

[MUSS] Diese Richtlinie definiert die verbindlichen technischen und organisatorischen Anforderungen an die Informationssicherheit und die forensische Handlungsfähigkeit für den Betrieb der Web-Infrastruktur sowie der zugehörigen Autorensysteme.

Aufgrund der Einstufung des Zielsystems als wesentliche Einrichtung gemäß NIS-2-Richtlinie [25] [26] bzw. als Kritische Infrastruktur (*KRITIS*) [6] ist die Umsetzung des Stands der Technik zwingend. Die Richtlinie adressiert zudem die Anforderungen zur Verarbeitung von Sozialdaten gemäß § 393 SGB V [2] sowie den Schutz besonderer Kategorien personenbezogener Daten gemäß Art. 9 DSGVO [27].

23.2 Infrastruktur und Digitale Souveränität

23.2.1 Hosting und Datenresidenz

[SOLL] Sämtliche Instanzen der Applikations- und Datenbankebene sowie alle Backup-Systeme müssen innerhalb der Europäischen Union (*EU*) betrieben werden. Der Einsatz von US-amerikanischen Hyperscalern (z.B. *AWS*, *Azure*, *Google Cloud Platform*) ist, ungeachtet des Rechenzentrumsstandorts, aufgrund des Konfliktpotenzials mit dem US Cloud Act und der angestrebten digitalen Souveränität zu vermeiden.

23.2.2 Cloud-Compliance (*BSI C5*)

[MUSS] Sofern Cloud-Dienste (*IaaS*, *PaaS* oder *SaaS* für Autorensysteme) zum Einsatz kommen, muss der Anbieter ein gültiges Testat gemäß dem BSI Cloud Computing Compliance Criteria Catalogue (*C5*) vorlegen. Dies ist Voraussetzung für die optionale Verarbeitung von Sozialdaten.

23.2.3 Netzsegmentierung

[MUSS] Die Infrastruktur ist in logisch getrennte Zonen (*DMZ*, *Applikation*, *Datenhaltung*) zu unterteilen. Der Datenaustausch zwischen den Zonen erfolgt nach dem Prinzip des geringsten Privilegs (*Least Privilege*) über zustandsorientierte Firewalls mit einem "Default Deny"-Regelwerk.

23.3 Applikations- und Schnittstellensicherheit

23.3.1 Web Application Firewall (WAF)

- [SOLL] Der Web-Infrastruktur ist eine [WAF](#) vorzuschalten. Diese soll das [OWASP](#) ModSecurity Core Rule Set ([CRS](#)) im Paranoia-Level 2 oder höher anwenden. Ein prozessual definiertes False-Positive-Handling sowie ein kontinuierliches Tuning der Regeln sind sicherzustellen.

23.3.2 Container- und DevOps-Security

- [MUSS] Bei Nutzung von Container-Technologien müssen Images automatisiert auf Schwachstellen ([CVE](#)) geprüft werden. Die Konfiguration der Infrastruktur ([IaC](#)) ist vor dem Deployment gegen Sicherheits-Best-Practices zu prüfen.

23.3.3 API-Sicherheit

- [MUSS] Schnittstellen müssen eine strikte Validierung von Eingangs- und Ausgangsdaten (*Input/Output Validation*) vollziehen. Die Authentifizierung erfolgt über gesicherte Protokolle ([OAuth 2.0](#), [mTLS](#) oder [JWT](#)).

23.4 Kryptographie und Identitätsmanagement

23.4.1 Schlüsselmanagement ([KMS](#)/[HSM](#))

- [MUSS] Kryptografische Schlüssel sind in einem nach [FIPS 140-2](#) Level 3 [\[28\]](#) zertifizierten Hardware-Sicherheitsmodul ([HSM](#)) oder einem äquivalenten Key Management System ([KMS](#)) zu verwalten. Eine logische Trennung zwischen Schlüssel- und Datenebene ist zwingend. Master-Keys unterliegen einem jährlichen Rotationszyklus gemäß [BSI TR-02102-1](#) [\[29\]](#).

23.4.2 Secrets Management

- [MUSS] Die Speicherung von Identitätsmerkmalen, [API](#)-Schlüsseln oder Datenbank-Credentials im Quellcode ist untersagt. Der Zugriff erfolgt über einen zentralen Secrets-Management-Dienst mit automatisierter Rotation.

23.4.3 Identitätsmanagement und [MFA](#)

- [MUSS] Administrative Zugriffe müssen über einen zentralen Identity Provider ([IdP](#)) mittels phishing-resistenter Multi-Faktor-Authentifizierung ([MFA](#)), bevorzugt [FIDO2](#) oder hardwarebasierte Token, abgesichert werden. Für cloud-basierte Autorensysteme sind ausschließlich "Federated IDs" (z.B. [EntraID](#)) zu verwenden.

23.5 Datenerfassung und Transfer

23.5.1 Zero-Knowledge-Verschlüsselung

- [SOLL] Sensible Nutzerdaten aus Formularen sind unmittelbar nach der Erfassung auf Applikationsebene asymmetrisch zu verschlüsseln (z.B. [RSA-4096](#)). Der private Schlüssel verbleibt ausschließlich in der Sphäre des Auftraggebers.

23.5.2 Datentransfer (E-Mail und VPN)

- [MUSS] Der Transfer verschlüsselter Datenpakete an den Auftraggeber erfolgt via E-Mail. Die beteiligten Mail-Gateways müssen eine Transportverschlüsselung mittels [mTLS](#) oder Forced [TLS](#) erzwingen. Optional ist eine Site-to-Site VPN-Verbindung bereitzustellen.

23.6 Detektion, Forensik und Incident Response

23.6.1 SOC-Anbindung und SzA

- [MUSS] Der Auftragnehmer implementiert ein System zur Angriffserkennung ([SzA](#)). Detektierte Sicherheitsereignisse sind in Echtzeit an die definierte Meldestelle des Auftraggeber-SOC (*Security Operations Center*) zu übermitteln. Die Weiterleitung von Roh-Logs an das [SIEM](#) des Auftraggebers ist als Option vorzusehen.

23.6.2 Digitale Forensik

- [SOLL] Die Beweissicherung soll den Standards ISO/IEC 27037 [\[30\]](#) und dem [BSI](#) Leitfaden Digitale Forensik [\[31\]](#) entsprechen. Im Falle eines Sicherheitsvorfalls sind vor invasiven Maßnahmen flüchtige Daten (*RAM-Dumps*) und sektorengenaue Abbilder der Datenträger (*Images*) anzufertigen. Die Integrität ist durch kryptografische Hashes und eine lückenlose Chain-of-Custody-Dokumentation zu wahren.

23.6.3 Logging-Spezifikation

- [MUSS] Ereignisprotokolle sind manipulationssicher für mindestens sechs Monate vorzuhalten. Personenbezogene Daten in Payloads sind vor der Protokollierung zu anonymisieren oder zu entfernen.

23.7 Business Continuity und Schwachstellenmanagement

23.7.1 Verfügbarkeit ([SLA](#))

23.7.1.1 Recovery Time Objective ([RTO](#))

- [MUSS] Die Wiederherstellung des Gesamtsystems muss innerhalb von 24 Stunden abgeschlossen sein.

23.7.1.2 Recovery Point Objective ([RPO](#))

- [MUSS] Der maximal zulässige Datenverlust beträgt 12 Stunden.

23.7.2 Backup-Strategie

- [SOLL] Es ist eine 3-2-1-1-Backup-Strategie anzuwenden. Mindestens eine Kopie muss unveränderbar (*Immutable*) und offline (*Air-Gapped*) vorgehalten werden. Jährliche Wiederherstellungstests sind zu dokumentieren.

23.7.3 Vulnerability Management und Pentests

- [SOLL]

Sämtliche Komponenten sind kontinuierlichen Schwachstellenscans zu unterziehen. Kritische Schwachstellen müssen innerhalb von 48 Stunden behoben werden. Ein jährlicher Penetrationstest durch einen unabhängigen Dritten ist obligatorisch.

23.8 Meldepflichten gemäß **NIS-2** und **KRITIS**

Der Auftragnehmer ist verpflichtet, erhebliche Sicherheitsvorfälle innerhalb von 24 Stunden nach Kenntniserlangung dem Auftraggeber zu melden, um die gesetzliche Frühwarnpflicht gegenüber den Aufsichtsbehörden zu gewährleisten.

Kapitel 24

CAPTCHA

24.1 Grundlagen

CAPTCHA (Abkürzung für *”Completely Automated Public Turing test to tell Computers and Humans Apart”*) ist ein Sicherheitstest im Internet. Auf Deutsch bedeutet der Name: *”Vollautomatischer öffentlicher Turing-Test, um Computer und Menschen auseinanderzuhalten.”*

Definition

CAPTCHA ist ein kleiner Test, den nur ein Mensch leicht bestehen soll, während ein Computerprogramm (*ein ”Bot”*) daran scheitert.

Ziel

Das wesentliche Ziel eines CAPTCHAs ist die Sicherheit einer Website, indem es sicherstellt, dass eine Aktion von einem Menschen und nicht von einem Computerprogramm (Bot) durchgeführt wird.

Hinweis

Ein CAPTCHA ist im Wesentlichen der *”Türsteher”* für Formulare im Internet.

24.2 Anforderungen

[MUSS] Die Konzeption und Implementierung von CAPTCHA-Verfahren basiert auf einem Katalog spezifischer Anforderungen. Diese Kriterien zielen darauf ab, eine funktionale Balance zwischen der notwendigen Sicherheitsfunktion und der Gebrauchstauglichkeit für den Menschen zu etablieren.

- **Robustheit gegenüber automatisierten Systemen**

Ein primäres Ziel eines CAPTCHA ist die zuverlässige Differenzierung zwischen menschlichen Nutzern und automatisierten Agenten, sogenannten Bots. Das Verfahren muss daher eine signifikante Robustheit gegenüber Lösungsversuchen durch Software, insbesondere durch Systeme künstlicher Intelligenz, aufweisen. Die gestellte Aufgabe sollte so konzipiert sein, dass sie für Computerprogramme kognitiv oder technisch schwer zu interpretieren und zu lösen ist, während sie für den Menschen lös-

bar bleibt. Die Effektivität der Bot Abwehr ist ein zentraler Indikator für die Qualität des Verfahrens.

- **Hohe Benutzerfreundlichkeit (*Usability*)**

Parallel zur Sicherheitsfunktion ist die Gebrauchstauglichkeit für den menschlichen Anwender von erheblicher Bedeutung. Die Interaktion mit dem CAPTCHA sollte den Nutzerfluss nur minimal beeinträchtigen. Dies bedingt, dass die Aufgabe für den Menschen kognitiv einfach und zeitnah zu bewältigen ist. Verfahren, die eine hohe kognitive Last erzeugen oder viel Zeit beanspruchen, können die Nutzerakzeptanz reduzieren und die Konversionsrate einer Webseite negativ beeinflussen.

- **Gewährleistung der Barrierefreiheit**

Eine wichtige Anforderung ist die Zugänglichkeit des Verfahrens für Menschen mit unterschiedlichen physischen oder kognitiven Einschränkungen. Ein CAPTCHA, das ausschließlich auf visueller Erkennung basiert, schließt beispielsweise Personen mit Sehbehinderungen aus. Moderne Verfahren sollten daher alternative Modalitäten anbieten, wie etwa auditive Ausgaben (*vorgelesene Ziffern oder Wörter*) oder auf Verhaltensanalysen basierende, unsichtbare Prüfungen, um eine breite Nutzergruppe nicht von der Interaktion auszuschließen.

- **Vollständige Automatisierung**

Die Definition eines CAPTCHA impliziert bereits die vollständige Automatisierung des Prozesses. Sowohl die Generierung der Prüfungsaufgabe als auch die Validierung der vom Nutzer eingegebenen Lösung müssen serverseitig und ohne menschliche Intervention erfolgen. Dieser Aspekt stellt die Skalierbarkeit des Verfahrens für Webanwendungen sicher.

- **Performanz und Datenschutz**

In der praktischen Anwendung werden zusätzlich Anforderungen an die technische Performanz gestellt. Die Integration des CAPTCHA darf die Ladezeiten der Webseite nicht signifikant verzögern. Des Weiteren ist der Datenschutz von Relevanz. Insbesondere bei verhaltensbasierten Analysen, die Mausbewegungen oder Eingabemuster protokollieren, müssen datenschutzrechtliche Bestimmungen, wie die der Datenschutz Grundverordnung (*DSGVO*) in Europa, beachtet werden. Die Erhebung und Verarbeitung von Daten sollte auf das für die Sicherheitsprüfung notwendige Maß beschränkt sein.

24.3 Moderne CAPTCHA-Verfahren

[SOLL] Die Entwicklung im Bereich der Boterkennung hat zu einer signifikanten Diversifizierung der eingesetzten Prüfverfahren geführt. Während klassische Interaktionstests an Effektivität verlieren, gewinnen passive Analysemethoden und risikobasierte Modelle zunehmend an Bedeutung. Die Effektivität moderner Systeme beruht oft auf der intelligenten Kombination verschiedener, im Hintergrund agierender Komponenten. Die folgende Aufstellung gliedert die wesentlichen technischen Ansätze, die aktuell zur Differenzierung von menschlichen Nutzern und automatisierten Systemen dienen.

- **Verhaltensbasierte Erkennung**

Analyse von Mausbewegungen, Tippmustern, Scrollverhalten, Interaktionsgeschwindigkeit. Bots erzeugen unnatürliche Muster. Bewertung erfolgt unsichtbar im Hintergrund.

- **Risikobasierte Modelle**
Geräte-Fingerprinting, IP-Reputation, Browser-Telemetrie, Historie der Sitzung. Bei niedrigem Risiko wird gar kein sichtbares CAPTCHA mehr angezeigt.
- **Unsichtbare CAPTCHAs**
Beispiel: invisible reCAPTCHA v3. Liefert eine numerische Risikobewertung anhand von Nutzerinteraktionen. Nur bei hohem Risiko erfolgt ein Zusatztest.
- **Proof-of-Work-Mechanismen**
Der Client muss eine kleine Rechenaufgabe lösen. Vorteil: hohe Hürde für Massenzugriffe. Kommt in einigen Privacy-orientierten Lösungen vor.
- **Herausforderungen mit Kontext**
Klassisches Bilder- oder Audiocaptcha wird nur noch als Fallback genutzt. Fokus auf Tasks, die schwer zu automatisieren sind (*z.B. temporäre visuelle Puzzle*).
- **Hardware-gebundene Nachweise**
Nutzung sicherer Umgebungen (*Passkeys/WebAuthn*) als Nachweis, dass ein echter Benutzer am Gerät sitzt. Entlastet CAPTCHA-Systeme in sensiblen Anwendungen.
- **Serverseitige Anomalieerkennung**
Machine-Learning-Modelle, die Traffic-Muster in Echtzeit auswerten und Botnetz-typische Merkmale erkennen.

Kapitel 25

WebFormulare als Service

25.1 Grundlagen

Im Rahmen moderner Webarchitekturen kann die Notwendigkeit bestehen, Formularfunktionalitäten an externe Dienstleister auszulagern, anstatt diese auf der eigenen Infrastruktur zu betreiben. Ein solches Szenario impliziert die Übermittlung und Verarbeitung personenbezogener Daten im Sinne der Datenschutz-Grundverordnung (*DSGVO*) sowie den potenziellen Transfer sensibler Dateianhänge über Drittsysteme.

Aus dieser Konstellation ergeben sich spezifische Anforderungen an die IT-Sicherheit, um die Vertraulichkeit und Integrität der übertragenen Informationen zu gewährleisten. Insbesondere die Exponierung von Eingabeschnittstellen im öffentlichen Netz erfordert effektive Abwehrmechanismen gegen automatisierte Zugriffe und Missbrauch (*z.B. durch Bots oder Spam-Skripte*).

Folglich ist die Implementierung einer CAPTCHA-Lösung (*Completely Automated Public Turing test to tell Computers and Humans Apart*) unabdingbar, die dem aktuellen Stand der Technik entspricht. Veraltete Verfahren bieten oft keinen hinreichenden Schutz gegen moderne maschinelle Lernverfahren.

25.2 Exemplarisches Szenario

Zur Schaffung einer fundierten Grundlage wird im folgenden ein exemplarisches Szenario konzipiert, das als Referenzmodell dient. Der Fokus liegt auf einem Web-Formular-Prozess, der zwar in seinem Aufbau als grundlegend betrachtet wird, jedoch die wesentlichen Kernkomponenten und Interaktionen einer typischen Datenerfassung im Webumfeld abbildet und den Datenaustausch beschreibt.

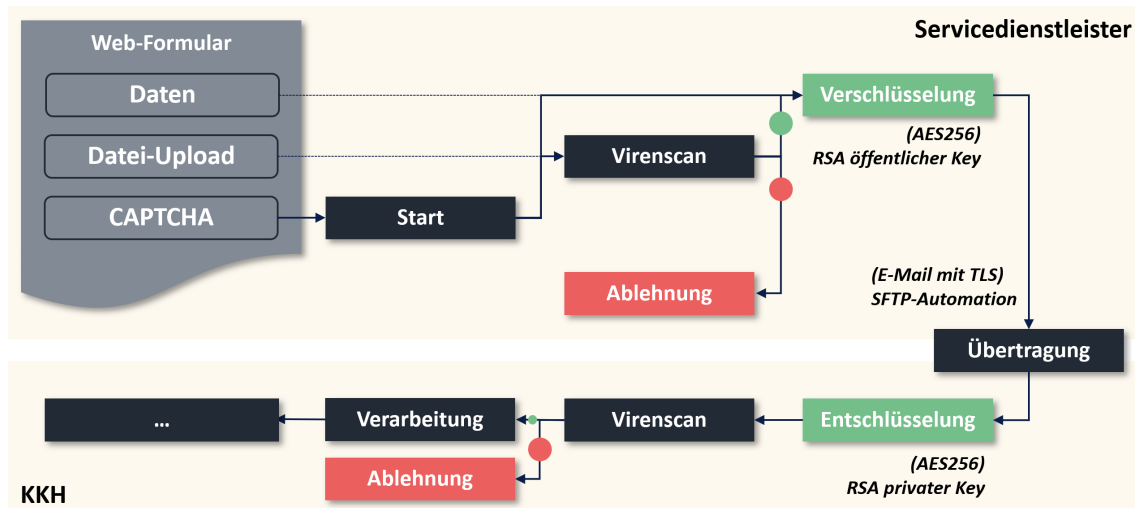


Abbildung 25.1: Exemplarisches Szenario Webformular Servicedienstleister

25.2.1 Web-Formular

[MUSS] Ein Webformular muss klare und eindeutig beschriftete Eingabefelder bereitstellen, Eingaben validieren und Fehler nachvollziehbar anzeigen, Datenübertragung ausschließlich verschlüsselt durchführen, nur notwendige Daten abfragen, manipulationssichere Server-Validierung nutzen, barrierefreie Bedienbarkeit gewährleisten, missbrauchsrelevante Funktionen durch Schutzmechanismen, Rate-Limiting und Captcha absichern und eine zuverlässige Verarbeitung sowie sichere Speicherung der übermittelten Informationen garantieren. Dabei sind die Angriffsvektoren (z.B. *Cross Site Scripting*) zu beschreiben und entsprechende Maßnahmen abzuleiten.

25.2.1.1 Daten

[MUSS] Die Verarbeitung von Daten, insbesondere wenn sie personenbezogene Daten im Sinne der Datenschutz-Grundverordnung (*DSGVO*) umfassen, unterliegt einem fundamentalen rechtlichen und operativen Paradigma: Die erforderlichen Schutzmaßnahmen sind nicht uniform, sondern müssen sich an der Sensibilität und dem Risiko der jeweiligen Information orientieren.

25.2.1.2 Datei-Upload

[MUSS] Die Funktionalität des Datei-Uploads (*Dateianhang*) stellt eine signifikante Erweiterung der reinen Formular-Datenerfassung dar. Sie ermöglicht es Anwendern, die strukturiert eingegebenen Daten (*Formularfelder*) durch unstrukturierte Informationen in Form von Dateien (z.B. *Dokumente, Bilder, Nachweise*) zu ergänzen.

Diese angehängten Dateien sind datenschutzrechtlich den Formulardaten (*siehe Abschnitt 25.2.1.2*) gleichzusetzen. Sofern sie personenbezogene Daten enthalten, was bei Dokumenten wie Lebensläufen, ärztlichen Bescheinigungen oder Antragsunterlagen die Regel ist, unterliegen sie vollumfänglich den Verarbeitungsprinzipien und Schutzanforderungen der Datenschutz-Grundverordnung (*DSGVO*).

Neben dieser datenschutzrechtlichen Dimension (*Schutz der Inhalte*) muss die kritische Dimension der Informations- und IT-Sicherheit (*Schutz der verarbeitenden Systeme*) betrachtet werden.

Dateiupload-Schnittstellen gelten als exponierte Angriffsvektoren. Sie können missbraucht werden, um schadhafte Dateien (*Malware*) in die Systemumgebung einzuschleusen. Bestimmte Dateiformate bergen ein inhärentes Risiko, da sie die Ausführung von Skripten, Makros oder eingebettetem Code (*z.B. JavaScript in HTML-Dateien, Makros in Office-Dokumenten*) ermöglichen. Solche Dateien können zur Kompromittierung des Servers, zur Infektion nachgelagerter Systeme (*wie dem Virens Scanner selbst oder internen Laufwerken*) oder zur Vorbereitung von Cross-Site-Scripting (*XSS*)-Angriffen genutzt werden.

Um dieser Gefährdungslage adäquat zu begegnen und der Sorgfaltspflicht zur Sicherung der IT-Systeme nachzukommen (*vgl. Art. 32 DSGVO, "Sicherheit der Verarbeitung"*), ist eine restriktive Steuerung der zulässigen Dateitypen unumgänglich.

Zugelassene Dokumentenformate (*Stand: 16.11.2025*)

- **PDF** (*statisch, kein eingebettetes JavaScript*)
- **PNG**
- **JPG/JPEG**
- **TXT**

25.2.1.3 CAPTCHA

[MUSS] Die Bereitstellung öffentlich zugänglicher Webformulare birgt das inhärente Risiko des Missbrauchs durch automatisierte Skripte, sogenannte "Bots". Diese autonomen Software-Agenten können Schnittstellen für diverse illegitime Zwecke nutzen, wie beispielsweise das massenhafte Versenden von Spam-Nachrichten, die Durchführung von Credential-Stuffing-Angriffen oder die künstliche Überlastung von Back-End-Ressourcen (*Denial of Service*). Diese Bedrohungslage erfordert die Implementierung spezifischer technischer Abwehrmaßnahmen (*u.a. CAPTCHA in Abschnitt 24*), um die Systemintegrität zu wahren und die Datenqualität sicherzustellen.

25.2.2 Start

[SOLL] Nach erfolgreicher Durchführung der CAPTCHA-Prüfung beginnt der technische Ablauf zur weiteren Verarbeitung des übermittelten Formulars.

25.2.3 Virens Scan

[MUSS] Nach dem Hochladen der Dateien ist eine Überprüfung mit einem aktuellen und fachlich freigegebenen Virens Scanner erforderlich. Die Prüfung dient der Feststellung, ob schädliche Inhalte vorliegen, die den weiteren Verarbeitungsprozess oder die nachgelagerten Systeme beeinträchtigen könnten.

25.2.4 Ablehnung

- [MUSS] Fällt die Virenprüfung negativ aus, ist das gesamte Formular als nicht verarbeitbar einzustufen. Der Vorgang ist vollständig in den zuständigen Log-Dateien zu protokollieren. Die weitere Behandlung des Vorfalls liegt im Verantwortungsbereich des fachlich zuständigen Teams, das geeignete Maßnahmen zur Analyse und Bewertung einzuleiten hat.

25.2.5 Verschlüsselung

- [MUSS] Die verschlüsselte Speicherung der übermittelten Dateien stellt einen grundlegenden Bestandteil der Schutzmaßnahmen dar. Für die Umsetzung kommen zwei Verfahren in Betracht.
- [KANN] Erstens kann eine symmetrische Verschlüsselung eingesetzt werden. Dieses Verfahren erfordert jedoch einen sensibel zu verwaltenden Schlüssel, der auf der Internetseite theoretisch unbemerkt kompromittiert werden könnte. Als Mindestanforderung ist die Verwendung eines AES-256-Verfahrens festgelegt.
- [SOLL] Zweitens kann eine asymmetrische Verschlüsselung genutzt werden. Dieses Verfahren reduziert die Risiken eines Schlüsselabflusses, erfordert aber mehr Rechenressourcen sowie ein abgestimmtes und dokumentiertes Schlüsselmanagement zwischen Dienstleister und Auftraggeber. Vorgabe ist die Nutzung eines RSA-4096-Schlüssels.

25.2.6 Übertragung

- [MUSS] Die Übertragung der Daten an interne Systeme soll über ein nachvollziehbares und revisionssicheres Verfahren erfolgen. Eine weniger geeignete, aber in Einzelfällen genutzte Möglichkeit stellt die Übermittlung per E-Mail dar, die aufgrund des Protokollstandards keine zuverlässige Bestätigung über erfolgreiche Zustellung bietet und daher zusätzliche technische Implementierungen (*u. a. TLS*) erfordert. Zu bevorzugen ist ein automatisierter elektronischer Datenaustausch über SFTP mit definiertem Quittungsmechanismus.

25.2.7 Entschlüsselung

- [MUSS] Die Entschlüsselung der Daten erfolgt nach dem jeweils angewendeten Verschlüsselungsverfahren. Der eingesetzte Algorithmus bestimmt die konkreten Schritte des kryptografischen Rückprozesses.

25.2.8 Virensan

- [MUSS] Nach dem Eingang der Daten im internen System ist eine erneute Virenprüfung vorzusehen. Diese zweite Prüfung dient der Absicherung der internen Infrastruktur und ergänzt die Maßnahmen, die bereits auf der Upload-Strecke durchgeführt wurden.

25.2.9 Verarbeitung

- [SOLL] Die weitere Verarbeitung der Daten richtet sich nach den fachlichen, organisatorischen und regulatorischen Vorgaben des Unternehmens. Die konkrete Ausgestaltung dieses Verarbeitungsschritts wird im Rahmen dieses Kapitels nicht behandelt.

Quellenverzeichnis

- [1] *ISO/IEC 27001:2022 – Information security management systems – Requirements*, Internationale Norm, ISO/IEC, 2022. besucht am 19. Juni 2025. Adresse: <https://www.iso.org/standard/27001>
- [2] *Sozialgesetzbuch (SGB) Fünftes Buch – Gesetzliche Krankenversicherung – (SGB V)*. Berlin: Bundesministerium der Justiz, 2025, zuletzt abgerufen am 21.09.2025. Adresse: https://www.gesetze-im-internet.de/sgb_5/
- [3] *Gesetz zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung (NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz - NIS2UmsuCG)*, <https://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/CI1/nis2umsucg.html>, Regierungsentwurf vom Juli 2024, Gesetzgebungsverfahren läuft — Referentenentwürfe und Kabinettsfassung (Stand Juli 2025) liegen vor; ein Inkrafttreten wird bis Ende 2025 erwartet, 2024.
- [4] The European Parliament and the Council of the European Union, “Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC,” Official Journal of the European Union, Regulation L 257/73, Aug. 2014.
- [5] *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG)*, https://www.gesetze-im-internet.de/bsig_2009/, Zuletzt geändert durch Artikel 4 des Gesetzes vom 23. Juni 2021 (BGBl. I S. 1858), 2009.
- [6] Bundesamt für Sicherheit in der Informationstechnik (BSI). “Erstellung branchenspezifischer Sicherheitsstandards (B3S).” Abgerufen am 02. August 2025, besucht am 2. Aug. 2025. Adresse: https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/KRITIS-FAQ/FAQ-zur-Erstellung-von-B3S/faq-zur-erstellung-von-b3s_node.html
- [7] “Branchenspezifischer Sicherheitsstandard für gesetzliche Kranken- und Pflegeversicherer (B3S-GKV/PV), Version 1.4,” GKV Spitzenverband, Berlin, Technischer Bericht, 2025, Feststellung durch BSI am 09.04.2025, gültig bis April 2028. besucht am 19. Juni 2025. Adresse: https://www.gkv-datenaustausch.de/media/dokumente/sicherheitsstandard_b3s/B3S_GKV-PV_V.1.4_final.pdf
- [8] Bundesamt für Sicherheit in der Informationstechnik, *Business Continuity Management - BSI-Standard 200-4*. Bonn: BSI, 2023, Version 2023, abgerufen am 02. August 2025. besucht am 2. Aug. 2025. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BSI_Standards/standard_200_4.pdf?__blob=publicationFile&v=8
- [9] Bundesamt für Sicherheit in der Informationstechnik, *IT-Grundschutz-Kompendium, Edition 2023*. Bonn: BSI, 2023, Version 2023, abgerufen am 19. Juni 2025. besucht

- am 19. Juni 2025. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium/IT_Grundschutz_Kompendium_Edition2023.pdf
- [10] ISO/IEC 22301:2019 – *Security and resilience — Business continuity management systems — Requirements*, Internationale Norm, ISO/IEC, 2019. besucht am 2. Aug. 2025. Adresse: <https://www.iso.org/standard/75106.html>
- [11] ISO/IEC 27035-1:2016 — *Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management*, ISO/IEC 27035-1:2016, Geneva: International Organization for Standardization, 2016.
- [12] S. Bradner, “Key words for use in RFCs to Indicate Requirement Levels,” The Internet Engineering Task Force (IETF), Request for Comments RFC 2119, März 1997. DOI: [10.17487/RFC2119](https://doi.org/10.17487/RFC2119) Adresse: <https://www.rfc-editor.org/info/rfc2119>
- [13] M. Urlaub, *IT-Governance Guide - Richtlinie Governance für digitale Services*, Version 02.00.00, Richtlinie Security für digitale Services, KKH - Kaufmännische Krankenkasse, 2025.
- [14] M. Urlaub, *IT-Forensik Guide - Richtlinie Forensik für digitale Services*, Version 02.00.00, Richtlinie Security für digitale Services, KKH - Kaufmännische Krankenkasse, 2025.
- [15] M. U. Christina Thoma, Schulungsmatrix nach Zielgruppe und Angriffsvektor, in *Awareness*. 16. Aug. 2025.
- [16] K. Kent, M. Souppaya und R. L. Chew, “Guide to Integrating Forensic Techniques into Incident Response,” National Institute of Standards und Technology, Gaithersburg, MD, Techn. Ber. SP 800-86, Aug. 2006. DOI: [10.6028/NIST.SP.800-86](https://doi.org/10.6028/NIST.SP.800-86)
- [17] R. D. Pethia, S. D. Crocker und B. Y. Fraser, “A Plan for the C3 Initial Operational Capability for the Computer Emergency Response Team (CERT),” Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, Techn. Ber. CMU/SEI-89-TR-10, Juni 1989.
- [18] I. Alsmadi und M. Zarour, *Cybersecurity and Incident Response*. Cham: Springer, 2020.
- [19] AXELOS, *ITIL® Foundation, ITIL 4 Edition*. London: The Stationery Office, 2019.
- [20] E. M. Hutchins, M. J. Cloppert und R. J. Amin, “Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains,” Lockheed Martin Corporation, Hanover, MD, White Paper, 2011.
- [21] *Date and time — Representations for information interchange*, International Standard, International Organization for Standardization, 2019.
- [22] G. Klyne und C. Newman, “Date and Time on the Internet: Timestamps,” Internet Engineering Task Force (IETF), Request for Comments RFC 3339, 2002.
- [23] Internet Assigned Numbers Authority (IANA), *Time Zone Database*, <https://www.iana.org/time-zones>, Primary source for global time zone definitions, 2026.
- [24] Center for Internet Security. “CIS Controls.” Abgerufen am 19. Juni 2025, besucht am 19. Juni 2025. Adresse: <https://www.cisecurity.org/controls>
- [25] *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)*, Text with EEA relevance, 14. Dez. 2022. Adresse: <https://eur-lex.europa.eu/eli/dir/2022/2555/oj>

- [26] *Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSIG)*, Artikel 1 des Gesetzes vom 2. Dezember 2025, BGBl. 2025 I Nr. 301; in Kraft seit 6. Dezember 2025, 2. Dez. 2025. Adresse: https://www.gesetze-im-internet.de/bsig_2025/
- [27] *Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)*, 27. Apr. 2016. besucht am 15. Sep. 2025. Adresse: <https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=CELEX:32016R0679>
- [28] National Institute of Standards and Technology, “Security Requirements for Cryptographic Modules,” National Institute of Standards und Technology, Federal Information Processing Standards Publication 140-2, Mai 2001, FIPS PUB 140-2; includes Security Level 3 as one of four defined security levels. Adresse: <https://doi.org/10.6028/NIST.FIPS.140-2>
- [29] Bundesamt für Sicherheit in der Informationstechnik, “Kryptographische Verfahren: Empfehlungen und Schlüssellängen,” Bundesamt für Sicherheit in der Informationstechnik, Technische Richtlinie BSI TR-02102-1, Version 2026-01, 23. Jan. 2026, Abgerufen am 22.03.2026. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102.pdf?__blob=publicationFile
- [30] International Organization for Standardization und International Electrotechnical Commission, *ISO/IEC 27037:2012 – Information technology – Security techniques – Guidelines for identification, collection, acquisition and preservation of digital evidence*, International Standard, ISO/IEC, Geneva, Switzerland, Okt. 2012.
- [31] Bundesamt für Sicherheit in der Informationstechnik (BSI), “Leitfaden „IT-Forensik“,” Bundesamt für Sicherheit in der Informationstechnik, Bonn, Leitfaden, 2011, Version 1.0. besucht am 29. Juni 2025. Adresse: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Leitfaden/Leitfaden_IT-Forensik.pdf?__blob=publicationFile&v=3