Arbeitsrichtlinie Kryptographie

VAV Versicherungs-Aktiengesellschaft

Klassifikation: Intern
Version 21.0

VAV VERSICHERUNGEN

Dokumenteneigenschaften

Titel	Arbeitsrichtlinie Kryptographie
Version	21.0
Geltungsbereich	Siehe Geltungsbereich Richtlinie Informationssicherheit
Erstmalige Freigabe	05.12.2019
Verabschiedet durch	Daniel Fürdauer (Informationssicherheitsbeauftragter)
Klassifikation	Intern
Verantwortlicher Verantwortliche Abteilung	Daniel Fürdauer Datenschutz und Informationssicherheit
Fachlicher Ansprechpartner	Daniel Fürdauer (daniel.fuerdauer@vav.at)
Letztes Review	November 2021

Dokumentenhistorie

Version	Datum	Beschreibung der Änderung	Ersteller
19.0	05.12.2019	Ersterstellung in Anlehnung an die entsprechende Arbeitsrichtlinie der VHV in der Version 19.0.	Daniel Fürdauer
20.0	04.12.2020	Ergänzung Kerckhoffs'sches Prinzip und Ergänzung der Schlüsselerzeugung und –speicherung um erklärende Beispiele	Daniel Fürdauer
21.0	30.11.2021	Ergänzung neues Kapitel Zertifikate nach X.509, Anpassung der jeweiligen Verschlüsselungsvorgaben, Umbenennung von „Hash-Algorithmen" in „Kennwort-Hash-Algorithmen"	Daniel Fürdauer

Hinweis zur Schreibweise

Die verwendete männliche Sprachform dient der leichteren Lesbarkeit und meint immer alle Geschlechter (m/w/d). Die verkürzte Sprachform hat nur redaktionelle Gründe und beinhaltet keine Wertung.

INHALTSVERZEICHNIS

Inhaltsverzeichnis **3**

Abkürzungsverzeichnis **4**

Tabellenverzeichnis **4**

1. Zielsetzung **5**

2. Adressaten **5**

3. Grundlagen **5**

4. Pflicht zur Verschlüsselung **6**

5. Schlüsselmanagement **6**

5.1. Einleitung 6

5.2. Schlüsselerzeugung 6

5.3. Schlüsseltrennung 7

5.4. Schlüsselverteilung 7

5.5. Schlüsselinstallation 7

5.6. Schlüsselspeicherung 7

5.7. Schlüsselarchivierung & -hinterlegung 7

5.8. Schlüsselwechsel 7

5.9. Schlüsselvernichtung 8

5.10. Schutz von Schlüsseln 8

6. Zertifikate nach X.509 ..... **8**

7. Technische Anforderungen **9**

7.1. Datenträgerverschlüsselung 9

7.2. HTTPS/TLS-Verschlüsselung 10

7.3. E-Mail-Verschlüsselung 10

7.4. SSH-Verschlüsselung 11

7.5. VPN-Verschlüsselung 11

7.6. Smartphone-Verschlüsselung 11

7.7. Kennwort Hash-Algorithmen 13

ABKÜRZUNGSVERZEICHNIS

BSI ..... Bundesamt für Sicherheit in der Informationstechnik

HTTPS ..... Hypertext Transfer Protocol Secure

PGP ..... Pretty Good Privacy

PSK ..... Pre-Shared Key

SCP ..... Secure Copy

SFTP ..... Secure File Transfer Protocol

SSH ..... Secure Shell

SSL ..... Secure Sockets Layer

TLS ..... Transport Layer Security

VPN ..... Virtual Private Network

WLAN ..... Wireless Local Area Network

TABELLENVERZEICHNIS

Tabelle 1 Übersicht von Zertifikatstypen und deren Einsatzvorgaben 9

Tabelle 2: Zulässige Datenträgerverschlüsselung 9

Tabelle 3: TLS-Versionseinsatz 10

Tabelle 4: Passwort-Hash-Algorithmen 13

Tabelle 5: Parameter für Hashalgorithmen 13

1. ZIELSETZUNG

In dieser Richtlinie werden die grundsätzlichen Regelungen zum Einsatz kryptographischer Verfahren aufgeführt. Ziel ist die Gewährleistung einer sicheren Übertragung und Speicherung vertraulicher, streng vertraulicher oder personenbezogener Informationen innerhalb und außerhalb des VAV Netzwerks sowie eine verschlüsselte Speicherung dieser Informationen auf mobilen Endgeräten und Wechseldatenträgern.

2. ADRESSATEN

Diese Richtlinie richtet sich an die Verantwortlichen und Betreiber von Informationstechnik und Kommunikationsdiensten.

3. GRUNDLAGEN

Als kryptographische Verfahren werden mathematische Funktionen verstanden, die einen Schutz von Informationen vor unautorisierter Kenntnisnahme (durch Verschlüsselung) sowie unbemerkter Manipulation (durch digitale Signaturen) bieten.
Die zugrunde liegenden mathematischen Funktionen werden dabei so ausgewählt, dass eine effiziente Lösung die Kenntnis geheimer Informationen (den sogenannten Schlüssel) voraussetzt. Das Schutzniveau wird entsprechend durch den Aufwand bestimmt, den ein potenzieller Angreifer für die Lösung der mathematischen Funktionen oder durch bloßes Ausprobieren (Brute Force) ohne Kenntnis des geheimen Schlüssels benötigt.
Die Komplexität der kryptographischen Verfahren wird sowohl durch die mathematische Funktion (den Algorithmus) als auch durch die Länge des gewählten Schlüssels bestimmt. Um einen angemessenen Schutz der Daten der VAV zu gewährleisten, ist ausschließlich der Einsatz solcher kryptographischen Verfahren zulässig, die für den jeweiligen Einsatzzweck freigegeben wurden. Sollten neue oder veränderte Einsatzzwecke die Auswahl eines geeigneten Verfahrens nötig machen, ist dies vorher mit der Stabstelle Datenschutz und Informationssicherheit abzustimmen und diese sind so auszuwählen, dass sie grundsätzlich dem Kerckhoffs'schen Prinzip folgen. Es besagt unter anderem, dass die Sicherheit eines Verschlüsselungsverfahrens auf der Geheimhaltung des Schlüssels beruht, anstatt auf der Geheimhaltung des Verschlüsselungsalgorithmus. Somit ist der Einsatz von nicht ohne Zugriffsbeschränkung weltweit offengelegten Verfahren untersagt.
Die Notwendigkeit zum Einsatz kryptographischer Verfahren bzw. der Stärke der Verschlüsselung richtet sich nach dem aus der Risikoeinschätzung erwachsenen Schutzbedarf der zu verarbeitenden Informationen.
Wird ein kryptographisches Verfahren eingesetzt, ist durch die IT mindestens jährlich zu prüfen, ob das Verfahren zulässig ist.
Private Schlüssel sind wie Kennwörter bezüglich ihrer Vertraulichkeit zu behandeln. Öffentliche Schlüssel sind, sofern sie nicht ausschließlich intern verwendet werden, bezüglich ihrer Informationsklassifizierung als „offen“ anzusehen. Soweit einem Mitarbeiter ein privater Schlüssel zugänglich ist, darf dieser nicht an Dritte weitergegeben werden. Zulässige Speicherorte für private Schlüssel werden durch den IT-Betrieb festgelegt. Die Mitarbeiter sind ausschließlich zur Speicherung von privaten Schlüsseln an diesen Ablageorten berechtigt.

4. PFLICHT ZUR VERSCHLÜSSELUNG

Werden interne Informationen durch einen Mitarbeiter außerhalb der Räumlichkeiten der VAV gespeichert, übertragen oder transportiert, sind diese zu verschlüsseln. Dies betrifft:

- Den Versand von E-Mails an externe Empfänger.
- Das Mitführen von sensiblen Informationen auf Datenträgern aller Art, also Laptops, Mobiltelefonen, Speicherkarten (auch in Kameras, Mobiltelefonen und so weiter), USB-Sticks etc.
- Die Verwendung eines Remotezugangs (zum Beispiel im Rahmen von Telearbeit / Home Office Tätigkeiten).
- Die Übertragung über Leitungen die mindestens teilweise außerhalb der Standorte der VAV verlegt sind, nach Möglichkeit.

Die Notwendigkeit der Verschlüsselung wird dabei ausschließlich durch die Vertraulichkeitsanforderungen der Informationen bestimmt. Im Unterschied hierzu sind Datenträger auch dann zu verschlüsseln, wenn der Transport nur über eine geringe Distanz, zum Beispiel zwischen zwei Standorten der VAV, erfolgt.
Der IT-Betrieb stellt grundsätzlich die notwendigen IT-Systeme und Anwendungen bereit, die eine Verschlüsselung gemäß den gültigen Vorgaben dieses Dokuments ermöglichen. Es sind ausschließlich solche IT-Systeme und Anwendungen zu verwenden, die dem Mitarbeiter explizit durch den IT-Betrieb für die Verwendung bereitgestellt wurden. Neben der persönlichen Übergabe durch den IT-Betrieb oder einen berechtigten Vertreter gelten alle zur Verfügung gestellten IT-Systeme grundsätzlich als bereitgestellt im Sinne dieser Regelung.

5. SCHLÜSSELMANAGEMENT

5.1. Einleitung

Eine wesentliche Aufgabe beim Einsatz von Kryptographie ist die Verwaltung der zugehörigen Schlüssel. Um den sicheren Betrieb zu gewährleisten, müssen organisatorische Prozesse und technische Vorkehrungen implementiert werden. Die für die Schlüsselverwaltung notwendigen Prozesse müssen dokumentiert sein. Insbesondere muss klar geregelt sein, wer Zugriff auf welchen Schlüssel erhält und wie dieser vor unautorisierter Verwendung geschützt wird.

5.2. Schlüsselerzeugung

Die Schlüsselerzeugung sollte in sicherer Umgebung und unter Einsatz geeigneter kryptographischer Schlüsselgeneratoren erfolgen, die unvorhersehbare, statistisch gleichverteilte Zufallsfolgen unter Ausnutzung des gesamten möglichen Schlüsselraums erzeugen.. Werden Benutzereingaben zur Schlüsselerzeugung genutzt, so sollten diese schwer vorhersehbar sein. Wenn möglich und in sicherer Umgebung sollte der erzeugte Schlüssel seine Erzeugungsumgebung nicht mehr verlassen (z. B. verbleibt ein privater Schlüssel für ein Zertifikat auf dem gehärteten und dort erzeugten Server und wird nicht via Mail, Instant-Messenger o. ä. verschickt).

5.3. Schlüsseltrennung

Kryptographische Schlüssel sollten möglichst nur für einen Einsatzzweck verwendet werden. Insbesondere muss es eine Trennung des privaten und des öffentlichen Schlüssels geben.

5.4. Schlüsselverteilung

Die Verteilung der Schlüssel muss unter Berücksichtigung des Schutzbedarfes durch geeignete Maßnahmen abgesichert werden (z. B. Verschlüsselung, persönliche Übergabe…).

5.5. Schlüsselinstallation

Im Zuge der Schlüsselinstallation ist die authentische Herkunft sowie die Integrität der Schlüsseldaten zu überprüfen.

5.6. Schlüsselspeicherung

Beim Einsatz kryptographischer Verfahren ist auf die Frage der Datensicherung zu achten. Kryptographische Schlüssel sollten so gespeichert bzw. aufbewahrt werden, dass Unbefugte sie nicht auslesen können. Die Systeme, auf denen Schlüssel gespeichert werden, müssen besonders geschützt sein und der Zugriff ist auf wenige Personen zu beschränken. Daher ist z. B. die Speicherung von Schlüsseln oder deren Kennwort in Versionsverwaltungssystemen untersagt. Stattdessen ist ein Ende-zu-Ende und Punkt-zu-Punkt verschlüsseltes und authentifiziertes Schlüsselverwaltungssystem einzusetzen. Im Fall eines gesicherten Speichers, wie beispielsweise bei einem HSM („Hardware Security Module“), kann auch nur ein Punkt-zu-Punkt verschlüsseltes und authentifiziertes Schlüsselverwaltungssystem zum Einsatz kommen.

5.7. Schlüsselarchivierung & -hinterlegung

Es dürfen lediglich Schlüssel hinterlegt bzw. archiviert werden, die zur Verschlüsselung von Daten verwendet werden und auf die der Zugriff von Dritten notwendig ist, z.B. falls ein Mitarbeiter das Unternehmen verlässt oder wegen Krankheit längere Zeit ausfällt. Private Signaturschlüssel dürfen nicht archiviert werden.

5.8. Schlüsselwechsel

Um einer möglichen Kompromittierung entgegenzutreten ist ein regelmäßiger Schlüsselwechsel durchzuführen. Bei der Einführung der Nutzung von kryptographischen Verfahren ist die Wechselfrequenz für Schlüssel von der betriebsverantwortlichen Organisationseinheit mit der Stabstelle Datenschutz und Informationssicherheit abzustimmen. Die Wechselfrequenz ist von verschiedenen Faktoren abhängig:

- Art des Mediums (z.B. Langzeitdatenträger, Datenübertragungsmedium)
- Kryptographischer Algorithmus
- Schlüssellänge
- Detektion von Angriffen (z.B. Diebstahl oder Verlust eines Schlüssels)
- Schutzbedarf der Daten

- Häufigkeit des Schlüsseleinsatzes
- Volumen der verschlüsselten Daten
- Relevantes Bedrohungspotential
- Sicherheit der Aufbewahrung der Schlüssel

Insbesondere im Falle einer Kompromittierung oder im Verdachtsfall einer Kompromittierung sind durch die betriebsverantwortlichen Organisationseinheiten umgehend die Schlüssel zu wechseln.

5.9. Schlüsselvernichtung

Nicht mehr benötigte Schlüssel (z.B. Schlüssel, deren Gültigkeitsdauer abgelaufen ist) sind auf sichere Art zu löschen bzw. zu vernichten (z.B. durch mehrfaches Löschen/Überschreiben und/oder mechanische Zerstörung des Datenträgers).

5.10. Schutz von Schlüsseln

Schlüssel sind gegen Modifikation, Verlust und Zerstörung zu schützen. Mitarbeiter und externe Partner sind dazu verpflichtet, mit den ihnen zur Verfügung gestellten Schlüsseln ordnungsgemäß umzugehen. Private und geheime Schlüssel dürfen nicht an andere Personen weitergegeben werden, auch nicht zu Vertretungszwecken. Die Hardware, auf welcher Schlüssel generiert, verteilt, gespeichert und archiviert werden, ist durch entsprechende physikalische Sicherheitsmaßnahmen zu schützen.

6. ZERTIFIKATE NACH X.509

Zertifikate nach dem X.509-Standard werden in vielen unterschiedlichen Bereichen eingesetzt. Die wohl bekannteste Verwendung findet sich bei HTTPS-Verbindungen im Internet. Ihr primäres Sicherheitsziel ist die Bestätigung der Authentizität und Integrität der Gegenstelle, wie z. B. einem Server. Dabei werden die Zertifikate in drei unterschiedliche Typen unterschieden, die angeben, wie intensiv die ausstellende Zertifizierungsstelle – auch kurz CA genannt – die Daten im Zertifikat überprüft hat. Die nachfolgende Tabelle beschreibt diese Typen und gibt an, wann welcher Typ in der VAV mindestens zu verwenden ist:

TYP	BESCHREIBUNG	VORGABEN
Domain Validation (DV)	Es wird nur das Recht des Antragstellers geprüft, den Domainnamen zu verwenden. Unternehmensinformationen werden nicht überprüft oder im Zertifikat hinterlegt.	Ist bei allen Nicht-Produktionssystemen einzusetzen. Der Einsatz von kostenlosen Let's Encrypt-Zertifikaten ist erlaubt.
Organization Validation (OV)	Prüfung wie bei einem DV-Zertifikat und es wird vereinfacht geprüft, ob es das Unternehmen gibt. Die Unternehmensinformationen werden im Zertifikat hinterlegt.	Ist bei allen Produktionssystemen einzusetzen.

Extended Validation (EV)	Prüfung wie bei einem OV-Zertifikat und die Unternehmensinformationen werden gründlicher geprüft. Die Unternehmensinformationen werden im Zertifikat hinterlegt.	Keine Vorgabe[1]
Zertifikate, die nur innerhalb der VAV CA-Umgebung genutzt werden, sind immer OV-Zertifikate und werden von der VAV CA beglaubigt, wohingegen außerhalb der VAV CA-Umgebung zur Beglaubigung öffentliche Zertifizierungsstellen verwendet werden.		

Tabelle 1 Übersicht von Zertifikatstypen und deren Einsatzvorgaben

Je nach Zertifikatstyp sind auch sogenannte Wildcard-Zertifikate möglich, also Zertifikate, die für eine ganze Domain gelten, wie z. B. *.vav.at (gültig für mein.vav.at etc.). Die Verwendung von Wildcard-Zertifikaten ist immer dann erlaubt, wenn der private Schlüssel des Zertifikats nur durch Systeme mit demselben Schutzbedarf und denselben Zugriffsregeln auf den Schlüssel selbst genutzt wird.

7. TECHNISCHE ANFORDERUNGEN

Alle nachfolgenden Anforderungen basieren auf der jeweils aktuellen Version der technischen Richtlinie TR-02102-1 des Bundesamts für Sicherheit in der Informationstechnik (BSI („Bundesamt für Sicherheit in der Informationstechnik“)) und sind als Minimalanforderung zu verstehen. Für HTTPS („Hypertext Transfer Protocol Secure“) / TLS („Transport Layer Security“) Verbindungen gilt ergänzend die technische Richtlinie TR-02102-2. Sofern das BSI Techniken „(grundsätzlich) empfiehlt“, so gelten diese Vorgaben als verpflichtend in Sinne dieser Richtlinie. Wird in den technischen Richtlinien von „nicht empfohlen“ gesprochen, so ist dies mit dem grundsätzlichen Verbot des Einsatzes dieser Technik gleichzusetzen.

7.1. Datenträgerverschlüsselung

Wird ein Datenträger oder werden einzelne Dateien eines Datenträgers (Container) verschlüsselt, ist das nachfolgende kryptographischen Verfahren zu verwenden:

ALGORITHMUS	SCHLÜSSELLÄNGE (MINIMAL)
AES	256 Bit

Tabelle 2: Zulässige Datenträgerverschlüsselung

Um Schwächen der Implementierung auszuschließen, sind nur solche Produkte für die Verschlüsselung zulässig, die durch die Stabstelle Datenschutz und Informationssicherheit freigegeben wurden.

[1] Viele Browser zeigten eine „Grüne Adressleiste“ an. Diese wurde aber von vielen Benutzern nach Untersuchungen ignoriert, daher wird dieser Unterschied zu OV-Zertifikaten zukünftig komplett wegfallen. Somit ist kein Mehrwert für den Benutzer zur Verifikation des Servers im Browser im Vergleich zu OV-Zertifikaten mehr gegeben, daher erfolgt in dieser Richtlinie hierzu keine Vorgabe.

7.2. HTTPS/TLS-Verschlüsselung

Bei der Transport Layer Security (im Folgenden „TLS“ genannt) handelt es sich um eine Protokollfamilie. Die Sicherheit einer TLS gesicherten Verbindung wird dabei durch eine Auswahl der verwendeten Algorithmen zum Schlüsselaustausch, der Authentifizierung, der Hashbildung sowie der Verschlüsselung bestimmt – diese Auswahl wird nachfolgend als „Cipher Suite“ bezeichnet.
Die Schlüssel bzw. der Signierungsalgorithmus der dazugehörigen Zertifikate orientiert sich an der technischen Richtlinie TR-02102-1 und sieht aktuell RSA mit mindestens 2048 Bit und SHA-256 Bit vor. Es können statt RSA auch elliptische Kurven nach technischer Richtlinie eingesetzt werden.
Die IT-Systeme der VAV sind so zu konfigurieren, dass grundsätzlich nur solche Cipher Suites verwendet werden, die durch das BSI empfohlen werden. Die aktuellen Empfehlungen des BSI sind der technischen Richtlinie TR-02102-2 zu entnehmen. Aktuell werden folgende Anforderungen gestellt:

BEZEICHNUNG	VORGABE
TLS 1.3	Wenn möglich, zu verwenden
TLS 1.2	Ist zu verwenden
TLS 1.0; 1.1	Grundsätzlich **nicht** zu verwenden
SSL v2, v3	**Nicht** zu verwenden

Tabelle 3: TLS-Versionseinsatz

Beim Einsatz sind im Standard Cipher Suites einzusetzen, die Perfect Forward Secrecy unterstützten. Diese Cipher müssen bei der Verhandlung (TLS-Handshake) zuerst durch den Server angeboten und genutzt werden (beim Apache Webserver beispielsweise durch Setzen der Option „SSLHonorCipherOrder On“ möglich).
Digitale Zertifikate, die im Rahmen der TLS-Verschlüsselung verwendet werden, sind vor ihrer Verwendung auf ihre Gültigkeit zu prüfen. Die Verbindung ist nur zulässig, wenn das digitale Zertifikat des angesprochenen Servers

- für die erwartete Organisationseinheit / URL ausgestellt ist,
- durch eine vertrauenswürdige Stelle (Trusted CA) beglaubigt wurde,
- kein Widerruf vorliegt und
- der Gültigkeitszeitraum nicht in der Vergangenheit endet oder erst in der Zukunft beginnt.

7.3. E-Mail-Verschlüsselung

Grundsätzlich ist der Versand von E-Mails durch die E-Mail-Server der VAV nur unter Verwendung einer TLS gesicherten Verbindung, PGP oder S/MIME verschlüsselt zum Empfangs-E-Mail-Server zulässig. Wird keines der Verfahren durch den Kommunikationspartner unterstützt, wird die E-Mail automatisch mittels VAV SecureMail an den Kommunikationspartner übermittelt. Der unverschlüsselte Versand von E-Mails bedarf der Freigabe durch den Datenschutzbeauftragten bzw. dessen Vertreter.
Die Anforderungen an PGP und S/MIME hängen vom eingesetzten Verschlüsselungsalgorithmus ab. Bei asymmetrischen Verfahren, wie RSA, ist eine Schlüssellänge von mindestens 3.072Bit erforderlich; beim Einsatz von Verfahren, die auf elliptischen Kurven basieren, beträgt die

Minimallänge 256 Bit. Vorgaben bezüglich der TLS-Verschlüsselung sind im vorherigen Kapitel zu finden.
Die Gültigkeit von S/MIME-Zertifikaten beträgt drei Jahre. Sie können nach diesen drei Jahren verlängert werden, ohne einen komplett neuen Schlüssel generieren zu müssen, wenn sie zum Zeitpunkt der Verlängerung noch die Minimalanforderungen an die Kryptographie nach dieser Richtlinie erfüllen. Werden bei Verlängerung höhere Schlüssellängen nach dieser Richtlinie gefordert, ist ein neuer Schlüssel mit dieser neuen Minimallänge zu erstellen. Die Vorgaben für S/MIME gelten analog auch für PGP.
Die Schlüsselvernichtung bei Gültigkeitsablauf hat innerhalb von drei Monaten nach Erreichen der Gültigkeit zu erfolgen. Diese Übergangszeit soll den Kommunikationspartnern die Möglichkeit geben den Schlüssel in ihren Systemen auszutauschen. Der Schlüssel darf nicht vernichtet werden, wenn damit noch Kommunikationsdaten z. B. in einem Archiv entschlüsselt werden müssen. Ist dieser Zweck erreicht, ist der Schlüssel sicher zu löschen.

7.4. SSH-Verschlüsselung

Für die Verwendung des Secure Shell Protokolls (SSH) sowie hierauf aufbauender Dienste wie „SSH File Transfer Protokoll“ (SFTP) und „Secure Copy“ (SCP) ist nur die Protokollversion SSH-2 oder höher zulässig.
Im Rahmen des SSH-Verbindungsaufbaus erfolgt der Austausch eines Sitzungsschlüssels. Die Vorgaben zu diesem Sitzungsschlüssel sind auf Basis der technischen Richtline TR-020102-1 einzustellen. Die Gültigkeit des Sitzungsschlüssels ist nach Möglichkeit auf maximal eine Stunde zu limitieren oder nach einem Gigabyte an Datenvolumen zu erneuern (je nachdem was zuerst eintritt).
Für die Authentifizierung der Benutzer ist grundsätzlich das Public-Key-Verfahren zu verwenden. Die Authentifizierung auf den Servern der VAV ist nach Möglichkeit gegen einen zentralen Verzeichnisdienst einzurichten.

7.5. VPN-Verschlüsselung

Zulässig sind die Verwendung von SSL/TLS-basierten VPNs, sowie die Verwendung von IPsec. Für die SSL/TLS-basierten VPNs gelten die Anforderungen aus Abschnitt 7.2.
Soweit möglich ist eine zertifikatsbasierte Authentifizierung zu verwenden. Die Zertifikate sind unmittelbar zu sperren, wenn die Grundlage für den VPN-Zugang entfällt (zum Beispiel zum Vertragsende) oder wenn Kenntnisse eines (möglichen) Missbrauchs vorliegen.
Soweit ein Pre-shared key (PSK) verwendet wird, ist der Schlüssel regelmäßig, mindestens jährlich, zu wechseln. Soweit der Missbrauch oder die versehentliche Offenlegung des PSK bekannt wird, ist der Schlüssel unmittelbar zu wechseln.

7.6. Smartphone-Verschlüsselung

Die Speicherung von sensiblen Informationen auf Smartphones und die Übertragung von sensiblen Informationen unter Verwendung von Smartphones ist nur nach den Vorgaben der technischen Richtline TR-020102-1 erlaubt.
Die drahtlose Übertragung von sensiblen Informationen ist nur zulässig, wenn die Verbindung mit einem durch die Stabstelle Datenschutz und Informationssicherheit freigegebenen Verfahren

verschlüsselt wird. Als drahtlos wird die Übertragung sowohl in Mobilfunknetzen, im WLAN als auch unter Nutzung sonstiger (Nah-)Funkverbindungen verstanden. Die Verschlüsselung der kabellosen Verbindung ist optional, wenn bereits ein in dieser Richtlinie aufgeführtes Protokoll sicher genutzt wird (zum Beispiel eine TLS-gesicherte Verbindung zum E-Mail-Server).

7.7. Kennwort Hash-Algorithmen

Hashfunktionen werden grundsätzlich nach ihrem Einsatzgebiet unterschieden: Hashes in Datenbanken (Suchoptimierung durch Hashtabellen), Prüfsummen (Manipulationserkennung in Kommunikationsverbindungen) und in der Kryptologie (Signierung von Nachrichten und Erzeugung von Passwort-Hashes). Nachfolgend werden nur die Anforderungen an sichere Passwort-Hashes beschrieben, da hierzu die technische Richtlinie des BSI keine Aussage trifft.
Passwort-Hash-Algorithmen müssen gegen Brute-Force-Attacken und den Einsatz von Rainbow-Tabellen (z. B. durch Einsatz eines kryptographisch sicheren und bei jedem Passwort anderen Einmalwerts, einem sogenannten Salt) weitgehend immun sein. Folgende Algorithmen werden in der angegebenen Reihenfolge empfohlen:

ALGORITHMUS	HINWEIS
Argon2id	Empfohlen für alle Einsatzzwecke
Argon2i	Für Frontend-Server-Authentifizierungen und Festplattenverschlüsselungen
Argon2d	Für Backend-Server-Authentifizierungen
PBKDF2	Falls FIPS-Kompatibilität / Zertifizierbarkeit bestehen soll oder eine Unternehmensunterstützung auf vielen Plattformen erforderlich ist.
Bcrypt	Zu verwenden, wenn vorherige Algorithmen nicht nutzbar.
Scrypt	Zu verwenden, wenn vorherige Algorithmen nicht nutzbar.

Tabelle 4: Passwort-Hash-Algorithmen

Sofern der eingesetzte Passwort-Hash-Algorithmus das Setzen von bestimmen Parametern zur Erzeugung des Hashes anbietet, sind diese nach den jeweiligen Empfehlungen des Algorithmus zu setzen. Nachfolgend am Beispiel Argon2:

PARAMETER	HINWEIS	BEISPIEL: BACKEND-SERVER-AUTHENTIFIZIERUNG
Arbeitsspeicher	So hoch wie möglich und tolerabel	Beispielsweise 4 GB
Zeit(-Kosten)	So hoch wie möglich und tolerabel	Hasherzeugung dauert mindestens 0,5 Sekunden
Parallelismus	Doppelte Anzahl der Prozessorkerne	Bei 4 Kernen: Mindestens 8

Tabelle 5: Parameter für Hashalgorithmen