

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 1

Einsatz kryptographischer Verfahren

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 2

Inhaltsverzeichnis

1 Einleitung	5
1.1 Einführung	5
1.2 Zielsetzung	5
2 Kryptographische Verfahren	6
2.1 Kryptographische Schutzziele	6
2.2 Grundsätze für die Auswahl kryptographischer Produkte	6
2.2.1 Organisatorische Aspekte	7
2.2.2 Betrieb	7
2.2.3 Technische Aspekte	7
2.2.4 Wirtschaftliche Aspekte	8
2.2.5 Kryptographische Software	8
2.2.5.1 Installation	8
2.2.6 Kryptographische Hardware	9
2.2.6.1 Installation	9
2.3 Integrität	9
2.4 Vertraulichkeit	10
2.4.1 Symmetrische Verfahren	10
2.4.2 Asymmetrische Verfahren	11
2.4.3 Hybride Verfahren	12
2.5 Authentizität	12
2.5.1 Message Authentication Codes	12
2.5.2 Signaturverfahren	13
2.6 Schlüsselaustausch	14
3 Sicherheitsprotokolle	16

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 3

3.1 TLS	16
3.1.1 TLS v1.2	16
3.1.2 TLS v1.3	20
3.2 IPsec	22
3.2.1 IKE	23
3.2.2 ESP	26
3.2.3 AH	27
3.3 SSH	28
3.4 Kerberos	30
3.5 S/MIME	30
3.6 OpenPGP	30
3.7 WPA	31
4 Vorgehensweisen und Rahmenbedingungen	32
4.1 Zertifikatsmanagement und PKI	32
4.2 Schlüsselmanagement	35
4.2.1 Schlüsselgenerierung	35
4.2.2 Schlüsselverteilung	35
4.2.3 Schlüsselspeicherung	36
4.2.4 Schlüssellöschung	36
4.2.5 Schlüsselwiederherstellung und Notfallverfahren	36
4.2.6 Sitzungsschlüssel	36
4.3 Zufallszahlengeneratoren	37
4.4 Umgang mit Passwörtern	37
4.4.1 Passwörter zum Starten von Diensten	38
4.4.2 Passwörter zum Authentisieren von Nutzern	38
4.5 Umgang mit vertraulichen Daten	39

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 4

5 Policy Prozess	40
------------------	----

Glossar	41
---------	----

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 5

1 Einleitung

1.1 Einführung

Kryptographische Verfahren finden Anwendung in vielen Bereichen des täglichen IT-Betriebs, zum Beispiel bei sicheren Internet-Verbindungen, sicherer E-Mail-Nutzung, sicherem Datentransfer, sicherer Datenablage oder beim Einsatz von Virtual Private Networks.

Die Sicherheit kryptographischer Methoden hängt dabei wesentlich von der Stärke der zugrundeliegenden Algorithmen, sowie der verwendeten Schlüssellänge ab. In dieser Konkretisierung werden kryptographische Verfahren samt Schlüssellängen empfohlen, die nach aktuellem Stand der Technik als sicher gelten. Weitere Faktoren für die Sicherheit sind die korrekten Implementierungen der Algorithmen und die Zuverlässigkeit von Hintergrundsystemen, wie beispielsweise Public-Key-Infrastrukturen für den sicheren Austausch von Zertifikaten.

Es kann erforderlich sein, dass kryptographische Verfahren miteinander kombiniert werden, um Sicherheitsanforderungen zu erfüllen. Die Vertraulichkeit von Informationen kann zum Beispiel durch ein kryptographisches Verschlüsselungsverfahren gewährleistet werden. Die Unveränderbarkeit der Information und die Echtheit des Absenders einer Information, können durch ein anderes kryptographisches Verfahren sichergestellt werden. Dies unterstützt das Erreichen der Schutzziele Integrität und Authentizität.

Weiter ist die Kombination von verschiedenen Ebenen der Anwendung von Verschlüsselungsverfahren je nach Einsatzkontext zu bedenken und zu planen. Beispielsweise sind bei Web-basierten Diensten neben der Verschlüsselung der verwendeten Datenbanken auch die Verschlüsselung der notwendigen Kommunikationswege zwischen den beteiligten End-Geräten zu planen und zu gestalten.

Bei der Auswahl kryptographischer Komponenten für eine Anwendung ist darauf zu achten, dass die Stärke eines kryptographischen Systems nicht höher sein kann als die schwächste kryptographische Komponente. Das kryptographische System soll so ausgelegt sein, dass ein Übergang zu größeren Schlüssellängen und stärkeren kryptographischen Verfahren möglich ist.

Für jeden Anwendungsbereich großer Systeme von kryptographischen Verfahren (z.B. sichere E-Mail-Nutzung) ist ein entsprechendes spezifisches Konzept zum Einsatz der Kryptographie zu erstellen. Ziel eines spezifischen Konzeptes zum Einsatz der Kryptographie ist die Sicherstellung und Beschreibung eines im Anwendungskontext sinnvollen Einsatzes von kryptographischen Verfahren. Das spezifische Konzept zum Einsatz der Kryptographie muss dabei die Abstimmung und die gegenseitige Ergänzung von kryptographischen Verfahren in der Anwendungslogik (z.B. Datenspeicherung, Datenvermittlung) einer Anwendung und verwendeten IT-Technologien adressieren. Verschiedene Verfahren sollen gegebenenfalls sinnvoll kombiniert werden.

1.2 Zielsetzung

Dieses Muster dient als Vorlage für die Umsetzung der DB-Mindestanforderungen IS zum Thema Kryptographie. Nach diesem Muster können Regelungen für die sichere und effiziente Planung und Nutzung von kryptographischen Verfahren festgelegt werden.

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 6

2 Kryptographische Verfahren

2.1 Kryptographische Schutzziele

Kryptographische Verfahren dienen der Erreichung folgender Schutzziele:

- **Vertraulichkeit:** Der Schutz vor unbefugter Preisgabe von Daten
- **Integrität:** Die Sicherstellung der Korrektheit (Unversehrtheit) von Daten
- **Authentizität:** Die Sicherstellung der Identität eines Kommunikationspartners bzw. einer Datenquelle

Zur Gewährleistung dieser Schutzziele müssen, die in den folgenden Kapiteln freigegebenen kryptographischen Verfahren eingesetzt werden. Eine Verwendung alternativer Verfahren sind nur in begründeten Ausnahmefällen zulässig und vom verantwortlichen IT-SiM/ CISO GF/SE im IS-Risikomanagement zu dokumentieren.

Kryptographische Verfahren sind nicht dazu geeignet, das Schutzziel Verfügbarkeit zu gewährleisten.

Beim Einsatz kryptographischer Verfahren sind grundsätzlich zu berücksichtigen:

- Auswirkungen auf die Datensicherung
- Auswirkungen auf das Notfallkonzept
- zusätzlich benötigte Rechenleistung und -zeit

2.2 Grundsätze für die Auswahl kryptographischer Produkte

Die Auswahl kryptographischer Produkte hat auf Grundlage einer Schutzbedarfsanalyse in den Schutzzielen Vertraulichkeit und Integrität und je nach Anwendungskontext Authentizität zu erfolgen. Der Einfluss der Kryptographie auf das Schutzziel Verfügbarkeit ist in jedem Falle zu erläutern. Hierauf aufbauend ist die Identifizierung der geeigneten und zulässigen Verfahren inklusive Mindestschlüssellängen gemäß der Kapitel 2.3 bis 2.6 durchzuführen. Die Auswahl der kryptographischen Verfahren und deren Sicherheitsniveau sind dem Schutzbedarf entsprechend auszuwählen. Bei Bedarf sind entsprechende Fachexperten hinzuzuziehen.

Das von dieser Rahmenrichtlinie angestrebte Mindestsicherheitsniveau beträgt 120 Bit. Dieses Sicherheitsniveau bietet ausreichend Spielraum gegenüber möglichen zukünftigen Fortschritten bei der Krypto-Analyse der präsentierten Algorithmen, um den Schutzbedarf der damit geschützten Daten für die angegebenen Zeiträume zu gewährleisten. Die folgende Tabelle stellt die dazu notwendigen Schlüssellängen verschiedener kryptographischer Verfahren beispielhaft gegenüber:

Blockchiffre, MAC	DH, RSA	ECDH, ECDSA
128	2048 (bis Ende Jahr 2023) 3072 (ab Jahr 2024)	250

Tabelle 1: Mindestschlüssellängen verschiedener kryptographischer Verfahren

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 7

Bei der Auswahl ist der Lebenszyklus des kryptographischen Produkts in den Phasen Installation und Betrieb zu bewerten, da zur sicheren Anwendung der eingesetzten kryptographischen Verfahren zum Teil Zusatzbedingungen an die Hard- und Software gestellt werden müssen.

Kryptographische Produkte sind zu bevorzugen, wenn sie:

- Common Criteria (im Folgenden „CC“ genannt, ISO 15408) oder
- einen äquivalenten Nachweis wie Vorgaben oder Empfehlungen durch staatliche Stellen

erbringen. Kryptographische Produkte sollen im Allgemeinen so ausgelegt sein, dass ein Übergang zu einem höheren Sicherheitsniveau (z.B. durch größere Schlüssellängen oder aktuellere Protokollversionen) mit angemessenem Aufwand möglich ist. Die kryptographischen Algorithmen müssen hierfür modular implementiert werden, um eine schnelle Anpassung an neue Anforderungen zu ermöglichen.

2.2.1 Organisatorische Aspekte

Folgende organisatorischen Aspekte müssen berücksichtigt werden, bevor und während ein kryptographisches Verfahren eingeführt wird:

- Einsatzbereich (z.B. Geschäftsfeld, Behörde, extern, bilateral, usw.),
- Rahmenbedingungen und Regelungen sowie deren Bekanntmachung (Verantwortung und Zuständigkeit für die Pflege des Systems),
- Anweisungen für die Nutzung von Verschlüsselungsmodulen zur Vermeidung von Manipulationen und Fehlbedienungen,
- Migrationskonzept (Umsetzungsplanung),
- Zeitplan für die Umsetzung (Projektplanung),
- Datensicherung und Archivierung – Schlüsselmanagement bei einer Verschlüsselung (Konzept zur Wiederherstellung von verschlüsselten Daten),
- Trust Center, Vertrauensdienste wie Authentifizierungsdienste nach Konkretisierung Authentifizierung, Schlüsselaufbewahrungsdienste, Identitätsdienste, u.a.

2.2.2 Betrieb

Für den Betrieb eines kryptographischen Produkts sind folgende Aspekte zu definieren:

- Prüfung auf Existenz und Einspielen von Updates in einer gesicherten Umgebung,
- Grundsätze für das technische Schlüsselmanagement (u.a. Ablage, kryptographische Bearbeitung),
- Technische Schlüsselungsmaßnahmen (u.a. Kapazität und Verfügbarkeit),
- organisatorische Maßnahmen (z.B. Umsetzung eines Zugriffskonzepts, Betrieb von Vertrauensdiensten und Treuhänder).

2.2.3 Technische Aspekte

Folgende technische Aspekte müssen berücksichtigt werden, bevor und während ein kryptographisches Verfahren umgesetzt wird:

- Betroffene Benutzungsdienste und Anwendungen,
- betroffene Benutzende,
- Anforderungen an die Netzinfrastruktur,

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 8

- Anforderungen an die IT-Endgeräte (Performance, Verfügbarkeit),
- Verhalten bei Ausfall von Verschlüsselungsmodulen und
- Verhalten bei Fehlern in verschlüsselten Daten.

2.2.4 Wirtschaftliche Aspekte

Folgende wirtschaftliche Aspekte müssen berücksichtigt werden, bevor und während ein kryptographisches Verfahren umgesetzt wird:

- Anschaffungskosten (einmalige Investitionen, Lizenzgebühren),
- Einführungskosten (Installation, Konfiguration, Schulung von Beschäftigten),
- Administrationskosten (laufende Kosten, Personal),
- Wartungs- und Betreuungskosten (regelmäßige Überprüfung, Updates und so weiter),
- Aufwand, da eine Komprimierung von Daten nicht mehr möglich ist (das heißt unter Umständen höhere Anforderung an Speicher- oder Übertragungskapazitäten),
- Kosten durch Trust Center (zum Beispiel für Zertifikate) und Zeitaufwände (Personalkosten) für Schlüsselmanagement und Schlüsselverteilung und
- Rationalisierungseffekte.

Der Nutzen der Anwendung von kryptographischen Verfahren ergibt sich aus einem angenommenen höheren Sicherheitsniveau sowie aus den zusätzlichen Möglichkeiten der gesicherten Kommunikation.

2.2.5 Kryptographische Software

Kryptographische Softwareprodukte implementieren kryptographische Verfahren innerhalb von Anwendungssoftware. Oftmals werden folgende Eigenschaften als Vorteil genannt:

- Softwarelösungen sind meist kostengünstiger als Hardwarelösungen.
- Implementierungsfehler und Backdoors lassen sich leichter erkennen.
- Nachträgliche Anpassungen sind leichter durchzuführen.
- Softwarelösungen sind leichter auf andere Systeme portierbar.

Die sichere Anwendung hängt entscheidend von der Installation und der Einsatz- und Betriebsumgebung, dem historischen Umgang mit der Information sowie dem Support des Softwareprodukts ab.

Zur Vermeidung von Implementierungsfehlern sind gängige Standardprotokolle zur Verschlüsselung zu verwenden (zum Beispiel SSH, TLS). Die gewählten Protokolle sollten mit quelloffenen Standardbibliotheken implementiert werden, welche von Fachexperten hinreichend bewertet wurden (beispielsweise OpenSSL).

2.2.5.1 Installation

Für die Installation müssen deshalb die folgenden Informationen erhoben und mit dem Einsatzzweck und der -umgebung abgeglichen werden:

- Erfordernis weiterer Komponenten (z.B. Sicherheitskomponenten der Informations- und Kommunikationssysteme, Support, Smartcards),
- Kompatibilität zu dem Betriebssystem und den weiteren Komponenten,
- bekannte Inkompatibilitäten mit anderen Softwareprodukten,

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 9

- Möglichkeit einer Signierung und Signaturprüfung bei Installation zu dem Integritäts- und Authentizitätscheck und
- Transparenz durch offengelegte Open-Source.

2.2.6 Kryptographische Hardware

Kryptographische Geräte implementieren kryptographische Verfahren direkt in Hardware (z.B. als separates Sicherheitsmodul oder Smartcard). Sie bieten folgende Eigenschaften:

- In Hardware implementierte Verfahren sind schneller als Softwareimplementierungen.
- Es besteht eine geringere Anfälligkeit gegenüber Malware-Attacken und gezielter Manipulation.
- Es besteht eine erschwerte Analysierbarkeit der internen Implementierung.
- Die Speicherbarkeit geheimer Schlüssel ohne Möglichkeit des Auslesens ist gewährleistet.
- Die physische Portabilität ist grundsätzlich sichergestellt.
- Der Zugriff auf die kryptographische Hardware kann als „Authentisierung durch Besitz“ verwendet werden.

Die sichere Anwendung hängt entscheidend von der Einrichtung und der Einsatz- und Betriebsumgebung der kryptographischen Hardware, sowie von der Vertrauenswürdigkeit der Zuliefererkette ab.

2.2.6.1 Installation

Für die Installation müssen die folgenden Informationen erhoben und mit dem Einsatzzweck und der -umgebung abgeglichen werden:

- Standort des Geräts,
- Verbindung zu weiteren Geräten und
- Einsatz bestimmter Kabel und Verbindungen (u.a. Abstrahlsicherheit, Jitter, Beamform bei elektromagnetischer Strahlung).

2.3 Integrität

Unter dem Schutzziel Integrität wird die Vollständigkeit und Unverfälschtheit von Daten für den Zeitraum verstanden, in dem die Daten von einer autorisierten Person erstellt, übertragen oder gespeichert werden.

Für die Sicherung der Integrität von Daten werden Hashverfahren eingesetzt, welche aus einer beliebigen Nachricht einen Hashwert fester Länge erzeugen. Die Sicherheit eines solchen Hashverfahrens hängt maßgeblich von dieser Länge ab und soll in der Folge mindestens 240 Bit umfassen.

Zulässige Hashverfahren können der folgenden Tabelle entnommen werden.

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 10

#	SHA-Version	Verfahren	Integrität
1	SHA-2	SHA-256 SHA-384 SHA-512 SHA-512/256	hoch
2	SHA-3	SHA3-256 SHA3-384 SHA3-512	hoch

Tabelle 2: Zulässige Hashverfahren

2.4 Vertraulichkeit

Das Schutzziel Vertraulichkeit soll sicherstellen, dass schutzbedürftige Daten durch unautorisierte Dritte nicht eingesehen werden können. Dies betrifft insbesondere die Erstellung, Speicherung und die Übertragung von Daten.

Es werden für die Kryptographie zwei Schemata zur Einstufung des Risikos der Informationssicherheit verwendet. Befinden sich die Daten im Transport oder Übertragung wird das Schema „Data in Motion“ betrachtet. Befinden sich die Daten auf einem Speicher wird das Schema „Data in Rest“ betrachtet. Beide Schemata sind im Risikomanagement der Informationssicherheit zu betrachten.

2.4.1 Symmetrische Verfahren

Symmetrische Verfahren nutzen für die Ver- und Entschlüsselung den gleichen Schlüssel. Der Schlüssel muss von beiden Kommunikationspartnern vorher über einen sicheren Übertragungsweg ausgetauscht worden sein.

Der Vorteil der symmetrischen Verschlüsselung ist die höhere Geschwindigkeit dieser Verfahren im Vergleich zu asymmetrischen Verschlüsselungsverfahren.

Symmetrische Verschlüsselungsverfahren werden in Blockchiffren und Stromchiffren unterteilt. Blockchiffren bearbeiten die Daten in Blöcken fester Größe, wohingegen Stromchiffren bitweise arbeiten.

Zulässige Blockchiffren müssen eine Mindestblockgröße von 128 Bit haben und können der folgenden Tabelle entnommen werden.

#	Verfahren	Schlüssellänge (Bit)	Vertraulichkeit
1	AES-128	128	normal
2	AES-192	192	hoch
3	AES-256	256	sehr hoch

Tabelle 3: Zulässige symmetrische Verschlüsselungsverfahren

Aktuell sind keine Stromchiffren zur Verwendung freigegeben.

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 11

Blockchiffren können in verschiedenen Betriebsarten verwendet werden, um Daten beliebiger Länge zu verschlüsseln. Die folgenden Betriebsarten sind für die freigegebenen Blockchiffren zulässig:

- Galois Counter Mode (GCM)
- Cipher Block Chaining (CBC)
- Counter Mode (CTR)
- Cipher Block Chaining Message Authentication (CCM)

Bei der Verwendung des CBC-Modus muss der letzte Klartextdatenblock vor der Verschlüsselung über ein sogenanntes Paddingverfahren auf die Blockgröße der Blockchiffre aufgefüllt werden, sofern die Klartextdaten kürzer als die Blockgröße sind. Die folgenden Paddingverfahren sind zulässig:

- ISO-Padding gemäß ISO/IEC 9797-1:2011 Methode 2 und NIST Special Publication 800-38A Anhang A
- Padding gemäß RFC 5562 Kapitel 6.3
- ESP-Padding gemäß RFC 4303 Kapitel 2.4

2.4.2 Asymmetrische Verfahren

Asymmetrische Verfahren beruhen auf der Nutzung eines Schlüsselpaares, das aus einem privaten und einem öffentlichen Schlüssel besteht, die miteinander in einer mathematischen Beziehung stehen, die so gestaltet ist, dass aus der Kenntnis des öffentlichen Schlüssels nicht auf den privaten Schlüssel geschlossen werden kann.

Mit einem Schlüssel verschlüsselte Daten können nur mit dem anderen entschlüsselt werden. Man kann also mit dem öffentlichen Schlüssel verschlüsselte Daten nur mit dem zugehörigen privaten Schlüssel entschlüsseln.

Asymmetrische Verfahren sind erheblich rechenintensiver als symmetrische Verfahren.

Öffentliche Schlüssel werden genutzt zur

- Verschlüsselung von Daten
- Datenauthentisierung durch den Prüfer
- Instanzauthentisierung durch den Prüfer

Private Schlüssel werden genutzt zur

- Entschlüsselung von Daten
- Datenauthentisierung durch den Beweisenden
- Instanzauthentisierung durch den Beweisenden

Die Anforderungen an die Haltung des privaten Schlüssels sind mit den Anforderungen zur Haltung von symmetrischen Schlüsseln gleichzusetzen.

Die Sicherheit asymmetrischer Verfahren ist wie im Fall symmetrischer Verfahren im Wesentlichen durch die Schlüssellänge festgelegt.

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 12

Zulässige asymmetrische Verschlüsselungsverfahren können der folgenden Tabelle entnommen werden.

#	Verfahren	Schlüssellänge (Bit)	Vertraulichkeit
1	RSA	2048 (bis Ende Jahr 2023) 3072 (ab Jahr 2024)	hoch
2	RSA	4096	sehr hoch

Tabelle 4: Zulässige asymmetrische Verschlüsselungsverfahren

2.4.3 Hybride Verfahren

Hybride Verfahren nutzen kombinierend die Vorteile der symmetrischen und asymmetrischen Verfahren. Dabei werden die Daten mit einem symmetrischen Schlüssel verschlüsselt, der wiederum mit dem öffentlichen Schlüssel jedes Empfängers verschlüsselt wird. Auf diese Weise können nur die gewünschten Empfänger den symmetrischen Schlüssel ermitteln und damit die Daten entschlüsseln.

Hybride Verschlüsselung verbindet die Schnelligkeit der symmetrischen mit dem Komfort der asymmetrischen Verschlüsselung und wird unter anderem bei den Netzwerkprotokollen IPsec und TLS und zum Verschlüsseln von E-Mails mittels S/MIME oder PGP/GPG verwendet.

Zulässige hybride Verschlüsselungsverfahren ergeben sich durch die Kombination der in den Kapiteln 2.4.1 und 2.4.2 freigegebenen symmetrischen und asymmetrischen Verschlüsselungsverfahren. Darüber hinaus ist die Verwendung der folgenden hybriden Verschlüsselungsverfahren zulässig.

#	Verfahren	Schlüssellänge (Bit)	Vertraulichkeit
1	DLIES	2048 (bis Ende Jahr 2022) 3078 (ab Jahr 2023)	sehr hoch
2	ECIES	250	sehr hoch

Tabelle 5: Zulässige hybride Verschlüsselungsverfahren

2.5 Authentizität

Das Schutzziel Authentizität soll die Identität eines Kommunikationspartners bzw. die Identität einer Datenquelle, wie z.B. eines Dokumentenverfassers, sicherstellen.

2.5.1 Message Authentication Codes

Message Authentication Codes (MAC) werden zur Sicherung der Integrität und Authentizität von Daten eingesetzt. Dazu werden symmetrische Verschlüsselungs- und Hashverfahren auf Basis eines gemeinsamen Geheimnisses genutzt. Die Berechnung eines MACs ist dabei im Vergleich zur Berechnung einer digitalen Signatur wesentlich leichtgewichtiger, da keine asymmetrische Kryptographie zum Einsatz kommt.

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 13

Zulässig sind die folgenden MAC-Verfahren (grundsätzlich im Modus „Encrypt-then-MAC“), wenn sie mit den genannten Basisverfahren, Mindestschlüssellängen und Mindestprüfsummenlängen verwendet werden.

Zulässig sind die folgenden MAC-Verfahren.

#	MAC-Verfahren	Basis-Verfahren	Schlüssellänge (Bit)	Prüfsummenlänge (Bit)	Integrität
1	HMAC	Hashverfahren gemäß Kapitel 2.3	128	96	hoch
2	CMAC	Symmetrische Blockchiffre gemäß Kapitel 2.4.1	128	96	hoch
3	GMAC	Symmetrische Blockchiffre gemäß Kapitel 2.4.1	128	96	hoch

Tabelle 6: Zulässige MAC-Verfahren

2.5.2 Signaturverfahren

Signaturverfahren werden zur Authentisierung von Kommunikationsteilnehmern und zur Sicherung der Integrität und Authentizität von Daten eingesetzt. Die Signatur wird dabei durch die Anwendung des privaten Schlüssels eines asymmetrischen Verschlüsselungsverfahrens auf den Hashwert der zu schützenden Daten erstellt. Alle freigegebenen Signaturverfahren können sowohl zur Signierung von Daten, als auch zum Ausstellen von Zertifikaten genutzt werden.

Für digitale Signaturen dürfen die Hashverfahren gemäß Kapitel 2.3 verwendet werden.

Die folgenden asymmetrischen Verfahren zur Erzeugung von digitalen Signaturen sind zulässig.

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 14

#	Verfahren	Schlüssellänge (Bit)	Authentizität
1	RSA gemäß Kapitel 2.4.2 mit EMSA-PSS- oder DS-Padding 2 oder 3	2048 (bis Ende Jahr 2023) 3072 (ab Jahr 2024)	hoch
2	DSA	2048 (bis Ende Jahr 2022) 3072 (ab Jahr 2023)	hoch
3	ECDSA	250	sehr hoch
4	ECKCDSA	250	sehr hoch
5	ECGDSA	250	sehr hoch
6	Merkle-Signatur auf Basis der Hashverfahren gemäß Kapitel 2.3	nicht zutreffend ¹	sehr hoch

Tabelle 7: Zulässige Signaturverfahren

2.6 Schlüsselaustausch

Schlüsselaustauschverfahren dienen dem Austausch eines Verschlüsselungsschlüssels bzw. eines Geheimnisses zur Ableitung eines solchen über einen unsicheren Kanal. Diese Verfahren müssen unbedingt mit einem Authentisierungsverfahren zur Authentisierung des Kommunikationspartners kombiniert werden. Ansonsten besteht keine Möglichkeit zu entscheiden, mit welcher Partei der Schlüsselaustausch durchgeführt wird.

Werden kryptographische Schlüssel mit einem Schlüsselaustauschverfahren ausgehandelt, so besitzen die kryptographischen Verfahren, die diese Schlüssel verwenden, maximal das gleiche Sicherheitsniveau wie das Schlüsselaustauschverfahren. Daraus schlussfolgernd dürfen derartige Schlüssel nicht mehr verwendet werden, sobald das zugrundeliegende Schlüsselaustauschverfahren die Freigabe durch diese Rahmenrichtlinie verliert.

Die folgenden Verfahren sind zum Schlüsselaustausch zulässig.

¹¹Die Sicherheit von Merkle-Signaturen basiert ausschließlich auf der Sicherheit des eingesetzten Hashverfahrens.

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 15

#	Verfahren	Schlüssellänge (Bit)	Vertraulichkeit
1	Symmetrische Verfahren gemäß Kapitel 2.4.1		
2	Asymmetrische Verfahren gemäß Kapitel 2.4.2		
3	DH	2048 (bis Ende Jahr 2022) 3072 (ab Jahr 2023)	hoch
4	DH	4096	sehr hoch
5	ECDH	250	sehr hoch

Tabelle 8: Zulässige Schlüsselaustauschverfahren

Zu beachten ist, dass die symmetrischen Verfahren gemäß Kapitel 2.4.1 und die asymmetrischen Verfahren gemäß Kapitel 2.4.2 gegenüber den Verfahren DH und ECDH nicht über die Eigenschaft der Perfect Forward Secrecy verfügen. Dies bedeutet, dass ein Angreifer, der in den Besitz des ausgetauschten Geheimnisses gelangt, aus dem die Verschlüsselungsschlüssel abgeleitet werden, dennoch nicht diese kompromittieren kann. Aus diesem Grund sind letztere Verfahren gegenüber ersteren zu bevorzugen.

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 16

3 Sicherheitsprotokolle

Die vorgenannten kryptographischen Verfahren werden im Rahmen von Sicherheitsprotokollen miteinander kombiniert. Zulässig sind grundsätzlich solche Protokolle, welche die in den Kapiteln 2.3 bis 2.6 spezifizierten kryptographischen Verfahren mit den geforderten Sicherheitsparametern einsetzen.

Die im Folgenden aufgelisteten Verfahren sind mit einem Verwendungszeitraum versehen. Die Angabe einer Jahreszahl bedeutet hierbei, dass die Nutzung des jeweiligen Verfahrens bis zum Ende des angegebenen Jahres freigegeben ist. Ist die Jahreszahl mit einem „+“-Zeichen gekennzeichnet, so bedeutet dies, dass dieser Verwendungszeitraum möglicherweise in einer zukünftigen Version dieser Rahmenrichtlinie verlängert wird.

3.1 TLS

Transport Layer Security (TLS) ist ein Protokoll zur sicheren Datenübertragung. In einem der eigentlichen Datenübertragung vorangestellten Handshake können sich die Kommunikationspartner authentisieren und die Sicherheitseigenschaften für die anschließende Datenübertragung aushandeln und aktivieren.

Erlaubte Protokollversionen: 1.2 und 1.3

Für die erlaubten Schlüssellängen der Teilverfahren gilt das in den Kapiteln 2.3 bis 2.6 Gesagte.

3.1.1 TLS v1.2

Bei TLS v1.2 sind die Sicherheitseigenschaften in Form von Vertraulichkeit, Integrität und Authentizität, sowie deren Güte, der Authentisierungsmodus (anonym, nur serverseitig, gegenseitig), das Authentisierungsverfahren und das Schlüsselaustauschverfahren in Form sogenannter Cipher Suites zusammengefasst. Deren Bezeichner ist wie folgt aufgebaut:

TLS_[Schlüsselaustausch]_[Authentisierung]_WITH_[symmetrische Verschlüsselung]_[Hash]

Erlaubte Cipher Suites sind:

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 17

#	Cipher Suite	Verwendung bis
1	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	2026+
2	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	2026+
3	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	2026+
4	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	2026+
5	TLS_ECDHE_ECDSA_WITH_AES_128_CCM	2026+
6	TLS_ECDHE_ECDSA_WITH_AES_256_CCM	2026+
7	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	2026+
8	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	2026+
9	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	2026+
10	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	2026+
11	TLS_DHE_DSS_WITH_AES_128_CBC_SHA256	2026+
12	TLS_DHE_DSS_WITH_AES_256_CBC_SHA256	2026+
13	TLS_DHE_DSS_WITH_AES_128_GCM_SHA256	2026+
14	TLS_DHE_DSS_WITH_AES_256_GCM_SHA384	2026+
15	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	2026+
16	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	2026+
17	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	2026+
18	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	2026+
19	TLS_DHE_RSA_WITH_AES_128_CCM	2026+
20	TLS_DHE_RSA_WITH_AES_256_CCM	2026+

Tabelle 9: Zulässige TLS v1.2 Cipher Suites

Sollen bei einer TLS-Verbindung zusätzliche, vorab ausgetauschte Daten in den Schlüsselaustausch einfließen, können Cipher-Suites mit einem Pre-Shared Key (kurz PSK) verwendet werden. Hierzu sind folgende Cipher Suites erlaubt:

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 18

#	Cipher Suite	Verwendung bis
1	TLS_ECDHE_PSK_WITH_AES_128_CBC_SHA256	2026+
2	TLS_ECDHE_PSK_WITH_AES_256_CBC_SHA384	2026+
3	TLS_ECDHE_PSK_WITH_AES_128_GCM_SHA256	2026+
4	TLS_ECDHE_PSK_WITH_AES_256_GCM_SHA384	2026+
5	TLS_ECDHE_PSK_WITH_AES_128_CCM_SHA256	2026+
6	TLS_DHE_PSK_WITH_AES_128_CBC_SHA256	2026+
7	TLS_DHE_PSK_WITH_AES_256_CBC_SHA384	2026+
8	TLS_DHE_PSK_WITH_AES_128_GCM_SHA256	2026+
9	TLS_DHE_PSK_WITH_AES_256_GCM_SHA384	2026+
10	TLS_DHE_PSK_WITH_AES_128_CCM	2026+
11	TLS_DHE_PSK_WITH_AES_256_CCM	2026+

Tabelle 10: Zulässige TLS v1.2 PSK Cipher Suites

Alle erlaubten Cipher Suites gewährleisten Perfect Forward Secrecy.

Zu beachten ist, dass beide Kommunikationspartner die Cipher Suite unterstützen müssen, auf die man sich einigen will und dass ein Kommunikationspartner, der sich authentisieren soll, ein zum Authentisierungsverfahren passendes Zertifikat besitzt.

Die freigegebenen Cipher Suites verwenden alle (EC)DHE für den Schlüsselaustausch. Das hintere E steht für ephemeral, was bedeutet, dass das Diffie Hellman Schlüsselpaar nur temporär und für jede Session neu generiert wird. Der Client kann dem Server die unterstützten elliptischen Kurven bzw. multiplikativen Gruppen mittels der Supported Groups Erweiterung mitteilen, die eine gemäß der eigenen Präferenz sortierte Liste darstellt. Diese Erweiterung soll bei der Verwendung einer TLS_ECDH-Cipher Suite und kann bei der Verwendung einer TLS_DH-Cipher Suite gesendet werden. Die folgenden elliptischen Kurven und multiplikativen Gruppen sind freigegeben:

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 19

#	Supported Groups Erweiterung	Verwendung bis
1	secp256r1	2026+
2	secp384r1	2026+
3	brainpoolP256r1tls13	2026+
4	brainpoolP384r1tls13	2026+
5	brainpoolP512r1tls13	2026+
6	ffdhe2048	2022
7	ffdhe3072	2026+
8	ffdhe4096	2026+

Tabelle 11: Zulässige elliptische Kurven und multiplikative Gruppen für die TLSv1.2 Supported Groups Erweiterung

Der Client kann dem Server mittels der Signature Algorithms Erweiterung mitteilen, welche Signaturverfahren er für Daten- und Zertifikatssignaturen akzeptiert. Diese Erweiterung soll gesendet werden. Die Angabe des Signaturverfahrens erfolgt dabei aus der Kombination von Signatur- und Hashalgorithmus.

Die folgenden Signaturalgorithmen sind freigegeben:

#	Signatur Algorithmus	Verwendung bis
1	rsa	2025
2	dsa	2026+
3	ecdsa	2026+

Tabelle 12: Zulässige Signaturverfahren für die TLSv1.2 Signature Algorithms Erweiterung

Die folgenden Hashalgorithmen sind freigegeben:

#	Hash Algorithmus	Verwendung bis
1	sha256	2026+
2	sha384	2026+
3	sha512	2026+

Tabelle 13: Zulässige Hashverfahren für die TLSv1.2 Signature Algorithms Erweiterung

Des Weiteren ist zu beachten:

- Durch den Client initiiertes Neuaushandeln der Sicherheitseigenschaften einer Session, sogenanntes Session Renegotiation, muss vom Server abgelehnt werden.
- Die in RFC 6066 definierte Erweiterung zur Verkürzung der Ausgabe des HMAC auf 80 Bit darf nicht verwendet werden.

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 20

- Die in TLS vorgesehene Möglichkeit, die übertragenen Daten vor der Verschlüsselung zu komprimieren, darf nicht genutzt werden.
- Die in RFC 6520 definierte Heartbeat-Erweiterung darf nicht genutzt werden.

3.1.2 TLS v1.3

Bei TLS v1.3 werden der Authentisierungsmodus (anonym, nur serverseitig, gegenseitig), das Authentisierungsverfahren und das Schlüsselaustauschverfahren separat von den Cipher Suites ausgehandelt, die nur noch die Sicherheitseigenschaften in Form von Vertraulichkeit, Integrität und Authentizität zusammenfassen. Deren Bezeichner ist wie folgt aufgebaut:

TLS_[symmetrische Verschlüsselung]_[Hash]

Erlaubte Cipher Suites sind:

#	Cipher Suite	Verwendung bis
1	TLS_AES_128_GCM_SHA256	2026+
2	TLS_AES_256_GCM_SHA384	2026+
3	TLS_AES_128_CCM_SHA256	2026+

Tabelle 14: Zulässige TLS v1.3 Cipher Suites

Soll der Kommunikationspartner sich authentisieren, so muss ihm mittels der Signature Algorithms und der Signature Algorithms Certificate Erweiterung mitgeteilt werden, welche Signaturverfahren man selbst für eine Daten- respektive Zertifikatssignatur akzeptiert.

Die folgenden Signaturverfahren sind für Datensignaturen freigegeben:

#	Signatur Algorithms Erweiterung	Verwendung bis
1	rsa_pss_rsae_sha256	2026+
2	rsa_pss_rsae_sha384	2026+
3	rsa_pss_rsae_sha512	2026+
4	rsa_pss_pss_sha256	2026+
5	rsa_pss_pss_sha384	2026+
6	rsa_pss_pss_sha512	2026+
7	ecdsa_secp256r1_sha256	2026+
8	ecdsa_secp384r1_sha384	2026+
9	ecdsa_brainpoolP256r1tls13_sha256	2026+
10	ecdsa_brainpoolP384r1tls13_sha384	2026+
11	ecdsa_brainpoolP512r1tls13_sha512	2026+

Tabelle 15: Zulässige Signaturverfahren für die TLSv1.3 Signature Algorithms Erweiterung
Fachautor: Guthoff, Nora | TOC(5) | Tel.: +49 1523 741 3897

Gültig ab: 15.01.2023

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 21

Die folgenden Signaturverfahren sind für Zertifikatssignaturen freigegeben:

#	Signatur Algorithms Certificate Erweiterung	Verwendung bis
1	rsa_pkcs1_sha256	2025
2	rsa_pkcs1_sha384	2025
3	rsa_pkcs1_sha512	2025
4	rsa_pss_rsae_sha256	2026+
5	rsa_pss_rsae_sha384	2026+
6	rsa_pss_rsae_sha512	2026+
7	rsa_pss_pss_sha256	2026+
8	rsa_pss_pss_sha384	2026+
9	rsa_pss_pss_sha512	2026+
10	ecdsa_secp256r1_sha256	2026+
11	ecdsa_secp384r1_sha384	2026+
12	ecdsa_brainpoolP256r1tls13_sha256	2026+
13	ecdsa_brainpoolP384r1tls13_sha384	2026+
14	ecdsa_brainpoolP512r1tls13_sha512	2026+

Tabelle 16: Zulässige Signaturverfahren für die TLSv1.3 Signature Algorithms Certificate Erweiterung

Der Schlüsselaustausch erfolgt in TLSv1.3 grundsätzlich mit (EC)DHE. Das hintere E steht für ephemeral, was bedeutet, dass das Diffie Hellman Schlüsselpaar nur temporär und für jede Session neu generiert wird. Dem Kommunikationspartner müssen die eigenen öffentlichen Schlüssel und die unterstützten elliptischen Kurven bzw. multiplikativen Gruppen mitgeteilt werden. Ersteres erfolgt mittels der Key Shares Erweiterung, letzteres mittels der Supported Groups Erweiterung, die eine gemäß der eigenen Präferenz sortierte Liste darstellt. Die folgenden elliptischen Kurven und multiplikativen Gruppen sind freigegeben:

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 22

#	Supported Groups Erweiterung	Verwendung bis
1	secp256r1	2026+
2	secp384r1	2026+
3	brainpoolP256r1tls13	2026+
4	brainpoolP384r1tls13	2026+
5	brainpoolP512r1tls13	2026+
6	ffdhe2048	2022
7	ffdhe3072	2026+
8	ffdhe4096	2026+

Tabelle 17: Zulässige elliptische Kurven und multiplikative Gruppen für die TLSv1.3 Supported Groups Erweiterung

TLS v1.3 hat die Pre-Shared Key Cipher Suites und den Session Resumption Mechanismus älterer TLS Protokollversionen kombiniert. Dies ist einleuchtend, da es konzeptionell keine Rolle spielt, ob das gemeinsame Geheimnis, das man zur Ableitung neuen Schlüsselmaterials wiederverwenden möchte, in einer früheren TLS-Verbindung oder extern generiert wurde. Will ein Client ein existierendes Geheimnis für eine neue Verbindung wiederverwenden, so muss er dies dem Server mittels der Pre-Shared Key und der Pre-Shared Key Exchange Modes Erweiterungen anzeigen. Erstere referenziert das gemeinsame Geheimnis, letztere die Art und Weise, wie man es wiederverwenden möchte. Die folgenden Modi sind freigegeben:

#	Pre-Shared Key Exchange Modes Erweiterung	Verwendung bis
1	psk_dhe_ke	2026+

Tabelle 18: Zulässige Handshake-Modi für die TLSv1.3 Pre-Shared Key Exchange Modes Erweiterung

Des Weiteren ist zu beachten:

- Die Early Data Indication-Erweiterung darf nicht genutzt werden.

3.2 IPsec

Internet Protocol Security (IPsec) ermöglicht eine sichere Übertragung von Informationen in IP-basierten Datennetzwerken, wobei insbesondere die Vertraulichkeit, die Integrität und die Authentizität der mittels des IP-Protokolls übertragenen Daten gewährleistet wird. Es gibt zwei IPsec-Protokolle:

- Authentication Header (AH) gewährleistet die Integrität sowie die Authentizität der mittels des IP-Protokolls übertragenen Daten. Es findet kein Schutz der Vertraulichkeit der übertragenen Daten statt.
- Encapsulated Security Payload (ESP) gewährleistet neben den durch AH realisierten Schutzzielen zusätzlich den Schutz der Vertraulichkeit.

Sowohl AH als auch ESP können in zwei Betriebsmodi verwendet werden:

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 23

- Tunnelmodus: Die IPsec-Schutzmechanismen werden auf das gesamte IP-Paket (d. h. IP-Header inklusive Schicht-4-Protokoll) angewendet und ein neuer IP-Header vorangestellt. Dieser neue Header enthält die Adressen der kryptographischen Endpunkte (Tunnelenden).
- Transportmodus: Die IPsec-Schutzmechanismen werden nur auf die Nutzdaten des IP-Pakets angewendet und weiterhin der ursprüngliche IP-Header verwendet. Im Gegensatz zum Tunnelmodus werden also die Adressen der gesichert kommunizierenden Systeme nicht verborgen. Ein Angreifer würde beim Abhören der geschützten Verbindung also ggf. Informationen über das Kommunikationsverhalten bzw. über das gesicherte Netz erhalten.

Ein fundamentales Konzept von IPsec ist die Security Association (SA). Dabei handelt es sich um eine IPsec-gesicherte Verbindung zwischen zwei Kommunikationspartnern inkl. der zugehörigen kryptographischen Parameter, Algorithmen, Schlüssel und Betriebsmodi für diese Verbindung. Mit dem Protokoll Internet Key Exchange (IKE) kann eine IKE-SA ausgehandelt werden. Die Vorgaben dafür müssen im Voraus durch einen Sicherheitsadministrator festgelegt werden. IPsec ermöglicht dann die eigentliche gesicherte Nutzdatenübertragung auf der Ebene von IP-Paketen, indem von der vorher ausgehandelten IKE-SA eine verbindungspezifische IPsec-SA abgeleitet wird. Dabei muss zwingend ein erneuter Schlüsselaustausch im CRE-ATE_CHILD_SA-Austausch durchgeführt werden, um Perfect Forward Secrecy zu erzielen. Die Lebensdauer einer SA muss je nach Sicherheitsanforderung der Anwendung festgelegt werden. Dies gilt sowohl für IKE-SAs als auch für IPsec-SAs, wobei die IKE-SA-Lifetime maximal 24 h und die IPsec-SA-Lifetime maximal 4 h betragen darf.

Die IPsec-Datenbanken Security Policy Database (SPD) mit den Regeln, wie ein- und ausgehende Pakete durch IPsec verarbeitet werden, und Security Association Database (SAD) mit den SA-spezifischen Informationen müssen gesichert gespeichert werden um sie vor unautorisierter Manipulation zu schützen.

Für die erlaubten Schlüssellängen der jeweiligen Teilverfahren gilt das in den Kapiteln 2.3 bis 2.6 Gesagte.

3.2.1 IKE

Erlaubte Protokollversionen: 2

Für den Vertraulichkeitsschutz der IKE-Nachrichten sind folgende symmetrische Verschlüsselungsverfahren freigegeben, wobei die ersten beiden Verfahren mit einem Verfahren zur Integritätssicherung kombiniert werden müssen und die restlichen Verfahren mit keinem Verfahren zur Integritätssicherung kombiniert werden dürfen, da sie bereits implizit durch die Betriebsart CCM bzw. GCM erfolgt.:

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 24

#	Verschlüsselungsverfahren	Schlüssellänge (Bit)	Verwendung bis
1	ENCR_AES_CBC	128 / 256	2026+
2	ENCR_AES_CTR	128 / 256	2026+
3	ENCR_AES_GCM_12	128 / 256	2026+
4	ENCR_AES_GCM_16	128 / 256	2026+
5	ENCR_AES_CCM_12	128 / 256	2026+
6	ENCR_AES_CCM_16	128 / 256	2026+

Tabelle 19: Zulässige symmetrische Verschlüsselungsverfahren für IKE

Zur Erzeugung der symmetrischen Verschlüsselungsschlüssel ist ein Pseudo-Zufallszahlengenerator notwendig. Wichtig dabei ist, dass die Ausgabe des Pseudo-Zufallszahlengenerators mindestens genauso groß ist wie die Schlüssellänge des eingesetzten symmetrischen Verschlüsselungsverfahrens. Die folgenden Pseudo-Zufallszahlengeneratoren sind zulässig:

#	Pseudo-Zufallszahlengenerator	Verwendung bis
1	PRF_AES128_XCBC	2026+
2	PRF_AES128_CMAC	2026+
3	PRF_HMAC_SHA2_256	2026+
4	PRF_HMAC_SHA2_384	2026+
5	PRF_HMAC_SHA2_512	2026+

Tabelle 20: Zulässige Pseudo-Zufallszahlengeneratoren für IKE

Für den Integritätsschutz der IKE-Nachrichten sind folgende MAC-Verfahren freigegeben, wobei Neuentwicklungen nur noch mittels der auf SHA2-basierenden Verfahren erfolgen sollen:

#	MAC-Verfahren	Verwendung bis
1	AUTH_AES_XCBC_96	2026+
2	AUTH_HMAC_SHA2_256_128	2026+
3	AUTH_HMAC_SHA2_384_192	2026+
4	AUTH_HMAC_SHA2_512_256	2026+

Tabelle 21: Zulässige MAC-Verfahren für IKE

Für den Schlüsselaustausch per (EC)DH sind folgende elliptische Kurven und multiplikative Gruppen freigegeben:

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 25

#	(EC)DH Schlüsselaustausch auf Basis von	Verwendung bis
1	2048-bit MODP Group	2022
2	3072-bit MODP Group	2026+
3	4096-bit MODP Group	2026+
4	256-bit random ECP group	2026+
5	384-bit random ECP group	2026+
6	521-bit random ECP group	2026+
7	2048-bit MODP Group with 256-bit Prime Order Subgroup	2022
8	brainpoolP256r1	2026+
9	brainpoolP384r1	2026+
10	brainpoolP512r1	2026+

Tabelle 22: Zulässige elliptische Kurven und multiplikative Gruppe für den (EC)DH Schlüsselaustausch in IKE

Zur Authentisierung der Kommunikationspartner sind folgende Verfahren freigegeben:

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 26

#	Signaturverfahren	Schlüssellänge (Bit)	Hashverfahren	Verwendung bis
1	ECDSA-256 mit Kurve secp256r1	256	SHA-256	2026+
2	ECDSA-384 mit Kurve secp384r1	284	SHA-384	2026+
3	ECDSA-512 mit Kurve secp521r1	512	SHA-512	2026+
4	ECDSA-256 mit Kurve brainpoolP256r1	256	SHA-256	2026+
5	ECDSA-384 mit Kurve brainpoolP384r1	384	SHA-384	2026+
6	ECDSA-512 mit Kurve brainpoolP512r1	512	SHA-512	2026+
7	RSASSA-PSS	2048	SHA-256	2023
8	RSASSA-PSS	4096	SHA-384	2026+
9	ECGDSA-512 mit Kurve secp512r1	512	SHA-512	2026+
10	ECGDSA-256 mit Kurve brainpoolP256r1	256	SHA-256	2026+
11	ECGDSA-384 mit Kurve brainpoolP384r1	384	SHA-384	2026+

Tabelle 23: Zulässige Signaturverfahren für IKE

3.2.2 ESP

Bei der Verwendung von ESP soll der Tunnelmodus eingesetzt werden.

Für den Vertraulichkeitsschutz der ESP-Pakete sind folgende symmetrische Verschlüsselungsverfahren freigegeben, wobei die ersten beiden Verfahren mit einem Verfahren zur Integritätssicherung kombiniert werden müssen:

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 27

#	Verschlüsselungsverfahren	Schlüssellänge (Bit)	Verwendung bis
1	ENCR_AES_CBC	128 / 256	2026+
2	ENCR_AES_CTR	128 / 256	2026+
3	ENCR_AES_GCM_12	128 / 256	2026+
4	ENCR_AES_GCM_16	128 / 256	2026+
5	ENCR_AES_CCM_12	128 / 256	2026+
6	ENCR_AES_CCM_16	128 / 256	2026+

Tabelle 24: Zulässige symmetrische Verschlüsselungsverfahren für ESP

Für den Integritätsschutz der ESP-Pakete sind folgende MAC-Verfahren freigegeben, wobei Neuentwicklungen nur noch mittels der auf SHA2-basierenden Verfahren erfolgen sollen:

#	MAC-Verfahren	Verwendung bis
1	AUTH_AES_XCBC_96	2026+
2	AUTH_AES_CMAC_96	2026+
3	AUTH_HMAC_SHA2_256_128	2026+
4	AUTH_HMAC_SHA2_384_192	2026+
5	AUTH_HMAC_SHA2_512_256	2026+

Tabelle 25: Zulässige MAC-Verfahren für ESP

3.2.3 AH

Für den Integritätsschutz der AH-Pakete sind folgende Verfahren freigegeben, wobei Neuentwicklungen nur noch mittels der auf SHA2-basierenden Verfahren erfolgen sollen:

#	MAC-Verfahren	Verwendung bis
1	AUTH_AES_XCBC_96	2026+
2	AUTH_AES_CMAC_96	2026+
3	AUTH_HMAC_SHA2_256_128	2026+
4	AUTH_HMAC_SHA2_384_192	2026+
5	AUTH_HMAC_SHA2_512_256	2026+

Tabelle 26: Zulässige MAC-Verfahren für AH

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 28

3.3 SSH

Secure Shell (SSH) ist ein Protokoll zum Aufbau eines sicheren Kanals in einem unsicheren Netzwerk. Die gängigsten Anwendungen des SSH-Protokolls sind das Anmelden auf einem entfernten System und das Ausführen von Befehlen auf entfernten Systemen.

Das SSH-Protokoll besteht aus drei Unter-Protokollen:

- Das Transport Layer Protocol ermöglicht Serverauthentisierung, Verschlüsselung, Integritätssicherung und optional Datenkompression. Es setzt logisch auf TCP/IP auf.
- Das User Authentication Protocol ist dafür da, den Benutzer gegenüber dem Server zu authentisieren. Es setzt auf dem Transport Layer Protocol auf.
- Das Connection Protocol ist für die Erzeugung und Verwaltung logischer Kanäle innerhalb des verschlüsselten Tunnels zuständig. Es setzt auf dem User Authentication Protocol auf.

Erlaubte Protokollversionen: 2.0

Für die erlaubten Schlüssellängen der Teilverfahren gilt das in den Kapiteln 2.3 bis 2.6 Gesagte.

Der Schlüsselaustausch dient dem Generieren von gemeinsamen Sitzungsschlüsseln für die Daten-Authentisierung und -Verschlüsselung. Folgende Verfahren sind freigegeben:

#	Schlüsselaustauschverfahren	Verwendung bis
1	diffie-hellman-group-exchange-sha256	2026+
2	diffie-hellman-group14-sha256	2022
3	diffie-hellman-group15-sha512	2026+
4	diffie-hellman-group16-sha512	2026+
5	rsa2048-sha256	2023
6	ecdh-sha2-nistp256	2026+
7	ecdh-sha2-nistp384	2026+
8	ecdh-sha2-nistp521	2026+

Tabelle 27: Zulässige Schlüsselaustauschverfahren für SSH

Im Rahmen des Schlüsselaustauschs einigen sich Client und Server auf einen symmetrischen Verschlüsselungsalgorithmus sowie einen gemeinsamen Verschlüsselungsschlüssel. Die folgenden Verschlüsselungsverfahren sind freigegeben, wobei die Verfahren im GCM-Modus bereits eine Integritäts- und Authentizitätssicherung enthalten und bevorzugt werden sollen:

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 29

#	Verschlüsselungsverfahren	Verwendung bis
1	AEAD_AES_128_GCM	2026+
2	AEAD_AES_256_GCM	2026+
3	aes128-cbc	2024
4	aes192-cbc	2024
5	aes256-cbc	2024
6	aes128-ctr	2026+
7	aes192-ctr	2026+
8	aes256-ctr	2026+

Tabelle 28: Zulässige symmetrische Verschlüsselungsverfahren für SSH

Wird ein Verschlüsselungsverfahren ohne GCM-Modus eingesetzt, so muss zusätzlich noch ein MAC-Verfahren zur Integritäts- und Authentizitätssicherung der übertragenen Daten ausgehandelt werden. Die folgenden MAC-Verfahren sind freigegeben:

#	MAC-Verfahren	Verwendung bis
1	hmac-sha2-256	2026+
2	hmac-sha2-512	2026+

Tabelle 29: Zulässige MAC-Verfahren für SSH

Der Server authentisiert sich im Rahmen des Transport Layer Protocols, indem er seine Schlüsselaustausch-Nachrichten digital signiert. Folgende Signaturverfahren sind freigegeben:

#	Signaturverfahren	Schlüssellänge (Bit)	Verwendung bis
1	pgp-sign-rsa	2048	2020
2	pgp-sign-dss	2048 / 250 3072 / 250	2022 ab 2023
3	ecdsa-sha2-nistp256	250	2026+
4	ecdsa-sha2-nistp384	250	2026+
5	ecdsa-sha2-nistp521	250	2026+
6	x509v3-rsa2048-sha256	2048	2020
7	x509v3-ecdsa-sha2-nistp256	250	2026+
8	x509v3-ecdsa-sha2-nistp384	250	2026+
9	x509v3-ecdsa-sha2-nistp521	250	2026+

Tabelle 30: Zulässige Signaturverfahren für SSH
Fachautor: Guthoff, Nora | TOC(5) | Tel.: +49 1523 741 3897

Gültig ab: 15.01.2023

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 30

Die Client-Authentisierung findet im Rahmen des User Authentication Protocols statt. Es existieren dazu 3 Mechanismen:

- Public Key Authentication
- Password Authentication
- Host-based Authentication

Die Client-Authentisierung soll per Public Key Authentication stattfinden. Dazu sind die gleichen Signaturverfahren freigegeben wie für die Server-Authentisierung.

Die eigenen privaten SSH-Schlüssel müssen sicher gespeichert und verarbeitet werden, d.h. ihr Schutz vor Kopieren, missbräuchlicher Nutzung und Manipulation muss gewährleistet werden, z.B. durch Nutzung eines HSMs. Des Weiteren müssen die öffentlichen Schlüssel von vertrauenswürdigen Stellen manipulationssicher gespeichert werden.

3.4 Kerberos

Kerberos soll eine sichere und einheitliche Authentifizierung in einem ungesicherten TCP/IP-Netzwerk auf sicheren Hostrechnern bieten. Die Authentifizierung übernimmt eine vertrauenswürdige dritte Partei. Diese dritte Partei ist ein besonders geschützter Kerberos-5-Netzwerkdienst. Kerberos ermöglicht Single Sign-on, d.h. ein Benutzer muss sich nur einmal anmelden. Im Anschluss kann er alle verfügbaren Netzwerkdienste nutzen, ohne ein weiteres Mal sein Passwort eingeben zu müssen.

Kerberos wird von Microsoft als Standardprotokoll für die Authentisierung innerhalb einer Domäne verwendet, wobei die Kerberos-Schlüssel im Active Directory gespeichert werden.

Erlaubte Protokollversionen: 5

3.5 S/MIME

Secure / Multipurpose Internet Mail Extensions (S/MIME) ist ein Standard zur hybriden Verschlüsselung und zum Signieren von MIME-Objekten, die z.B. bei E-Mails zum Einsatz kommen.

Erlaubte Protokollversionen: 4.0

3.6 OpenPGP

Open Pretty Good Privacy (PGP) ist ein Standard zur hybriden Verschlüsselung und zum Signieren von beliebigen Daten, wie z.B. E-Mails. Im Gegensatz zu S/MIME verwendet OpenPGP keine X.509-Zertifikate und basiert damit auf keinem hierarchischen Vertrauensmodell. Sein Web of Trust genanntes Vertrauensmodell ist dezentral organisiert. Jeder Teilnehmer verwendet ein selbstsigniertes Zertifikat, dem der Kommunikationspartner entweder explizit vertrauen muss oder implizit über Vertrauensketten anderer Teilnehmer, denen ersterer vertraut.

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 31

Aufgrund des fehlenden zentralen Vertrauensmodells wird OpenPGP im kommerziellen Umfeld heute nur noch in Legacy-Anwendungen eingesetzt und wird für Neuentwicklungen nicht mehr empfohlen.

3.7 WPA

Wi-Fi Protected Access (WPA) ist ein Protokoll zur Absicherung von Drahtlosnetzwerken (WLAN).

Erlaubte Protokollversionen: 2 und 3

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 32

4 Vorgehensweisen und Rahmenbedingungen

4.1 Zertifikatsmanagement und PKI

Zum Einsatz der asymmetrischen kryptographischen Verfahren zur Sicherung von Vertraulichkeit und Authentizität werden Zertifikate benötigt. Ein Zertifikat bindet einen öffentlichen Schlüssel an eine Identität, hat eine begrenzte Gültigkeit und wird durch eine Zertifizierungsstelle ausgestellt. Die Zertifikatsbeantragung erfolgt durch den Zertifikatsinhaber selbst oder durch einen autorisierten Dritten. Eine Zertifizierungsstelle ist logisch in die Funktionen Registration Authority (RA) zum Authentisieren und Legitimieren des Antragsstellers und Certificate Authority (CA) zum Ausstellen des beantragten Zertifikats aufgeteilt.

Zur Sicherung der Integrität und Authentizität der Zertifikatsdaten sind diese von der CA digital signiert. Dazu besitzt auch die CA ein asymmetrisches Schlüsselpaar, dessen öffentlicher Schlüssel in einem Zertifikat enthalten ist, das seinerseits von einer übergeordneten CA ausgestellt und signiert wurde. Die oberste CA wird als Wurzel-Zertifizierungsstelle (Root-CA) bezeichnet. Sämtliche Zertifikate, die entweder direkt oder über untergeordnete CAs indirekt von der Root-CA abgeleitet sind, bilden einen hierarchischen Vertrauensraum und werden als Public Key Infrastruktur (PKI) bezeichnet.

Ein Certification Practice Statement (CPS) dokumentiert die Arbeitsweise einer Zertifizierungsstelle, insbesondere im Hinblick auf deren Zertifikat Lifecycle Management, sowie weitere technische, geschäftliche und rechtliche Themen. Das CPS muss auf einer Webseite veröffentlicht werden, die für alle PKI-Teilnehmer erreichbar ist.

Eine Certificate Policy (CP) definiert den Verwendungszweck eines Zertifikats und wird von diesem referenziert. Die CP ermöglicht es dem Prüfenden, zu entscheiden, ob das Zertifikat und die darin enthaltene Bindung von öffentlichem Schlüssel zu Identität hinreichend vertrauenswürdig für die angestrebte Nutzung ist. Daraus folgt, dass alle Zertifikate einer Zertifikatskette dieselbe CP referenzieren müssen. Eine Ausnahme stellt dabei das Zertifikat der Root-CA dar, das keine CP enthält und damit zu allen CPs kompatibel ist. Will man unterschiedliche CPs innerhalb einer PKI ermöglichen, so kann dies auf Ebene einer untergeordneten CA umgesetzt werden. Ob getrennte CP-Vertrauensräume per dedizierter PKI oder per Policy CAs aufgezogen werden, oder aber per CA umgesetzt werden, die Endnutzer-Zertifikate mit unterschiedlichen CPs ausstellt, ist eine Design-Frage und im CPS dokumentiert.

Jede Zertifizierungsstelle benötigt zur Inbetriebnahme ein CPS gemäß [] und für jede CP, für die sie Zertifikate ausstellt, eine CP gemäß []. CPS und CP einer konzernweit operierenden CA müssen vom CISO DB abgenommen werden, CPS und CP einer GF/SE weit operierenden CA vom jeweiligen IT SiM/CISO GF/SE. CPS und CP werden jährlich durch Audit auf Aktualität geprüft.

Das Root-CA-Zertifikat muss auf den Systemen bzw. in den Anwendungen der jeweiligen PKI-Teilnehmer als Vertrauensanker konfiguriert sein, um den Vertrauensraum aufzuspannen.

Zur Absicherung der Kommunikation mit Externen muss auf eine öffentliche CA zurückgegriffen werden, da eigene CAs bei Externen kein Vertrauen genießen und ihre Zertifikatsstatusinformationen von extern nicht abfragbar sind.

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 33

Der Assetverantwortliche einer CA ist verantwortlich für

- Erstellen und Pflege von CPS und CP
- Erzeugen des kryptographischen Schlüsselpaars der CA
- Beantragen des CA-Zertifikats bei der übergeordneten CA und für dessen Einspielen
- Veröffentlichen der folgenden Informationen:
 - a) aktuell gültige CA-Zertifikate mit Gültigkeitszeitraum und Datum der Inbetriebnahme
 - b) URLs der zugehörigen OCSP-Server
 - c) URLs der zugehörigen CRLDPs
- Inbetriebnahme eines neuen CA-Zertifikats, bevor das aktuelle aufgrund des Schalenmodells keine profilkonformen Zertifikate mehr ausstellen kann
- Bereitstellen jeweils einer separaten CA-Instanz aus getrennten PKIs in der Entwicklungs- und Testumgebung für jede CA-Instanz der Produktivumgebung
- Sperren eines gültigen CA-Zertifikats, wenn der zugehörige private Schlüssel kompromittiert wurde
- Informieren der betroffenen PKI-Teilnehmer über die Sperrung des CA-Zertifikats und die durchzuführenden notwendigen Maßnahmen
- Erzeugen eines neuen kryptographischen Schlüsselpaars, Beantragen eines neuen CA-Zertifikats und dessen Einspielen zwecks Wieder-Inbetriebnahme der CA nach einer Schlüssel-Kompromittierung
- Sperren eines gültigen CA-Zertifikats, wenn die CA außer Betrieb genommen wird und es sich bei der CA um keine Root-CA handelt

Der Assetverantwortliche einer Root-CA ist darüber hinaus zusätzlich verantwortlich für

- rechtzeitiges Informieren sämtlicher PKI-Teilnehmer über die geplante Inbetriebnahme eines neuen Root-CA-Zertifikats inklusive des Datums der Inbetriebnahme
- Verteilen des Root-CA-Zertifikats vor der Inbetriebnahme an die PKI-Teilnehmer. Dabei muss den PKI-Teilnehmern ausreichend Zeit gewährt werden, das Root-CA-Zertifikat als Vertrauensanker in ihren Systemen und Anwendungen zu konfigurieren, bevor es in Betrieb genommen werden darf.
- Außerbetriebnahme der PKI, wenn der private Schlüssel der Root-CA kompromittiert wurde
- Informieren sämtlicher PKI-Teilnehmer über die Außerbetriebnahme der PKI und die durchzuführenden notwendigen Maßnahmen

Der IT-Assetverantwortliche einer Anwendung oder einer IT-Infrastrukturkomponente, deren Sicherheitsanforderungen den Einsatz von PKI erfordern, ist verantwortlich für

- Erzeugen des kryptographischen Schlüsselpaars der Anwendung bzw. der IT-Infrastrukturkomponente
- Beantragen des Zertifikats und dessen Einspielen zur Inbetriebnahme der Anwendung bzw. der IT-Infrastrukturkomponente
- Verlängerung des Zertifikats der Anwendung bzw. der IT-Infrastrukturkomponente und Einspielen des neuen Zertifikats, bevor das aktuelle abläuft
- erfolgreiche Prüfung eines erhaltenen Zertifikats auf Gültigkeit und Vertrauenswürdigkeit vor dessen Nutzung, sowohl für das beantragte Zertifikat, als auch für ein CA- oder ein Root-CA-Zertifikat

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 34

- Sperren eines gültigen Zertifikats, wenn der zugehörige private Schlüssel kompromittiert wurde, sowie Informierung des Security Incident Managements, falls der kompromittierte Schlüssel in der Produktivumgebung eingesetzt wurde
- Sperren eines gültigen Zertifikats, wenn es nicht mehr zur Erfüllung der Sicherheitsanforderung benötigt wird
- Sperren aller gültigen Zertifikate der Anwendung bzw. der IT-Infrastrukturkomponente, wenn diese außer Betrieb genommen wird

Der IT-Assetverantwortliche kann Schlüsselgenerierung, Zertifikatsbeantragung, Zertifikatsverlängerung und Sperrung bei Außerbetriebnahme an einen autorisierten Dritten delegieren. Die Verantwortung bleibt jedoch bei ihm.

Für eine Person, deren Sicherheitsanforderungen den Einsatz von PKI erfordern, gilt das Gleiche wie für den IT-Assetverantwortlichen einer Anwendung.

Eine RA muss

- eine Schnittstelle anbieten, über die Zertifikate beantragt werden können
- muss den Zertifikat-Antragsteller authentifizieren
- prüfen, dass die Identität, für die ein Zertifikat beantragt wird, im zentralen Asset-Register bzw. im Benutzermanagement registriert ist
- prüfen, dass der Antragsteller berechtigt ist, Zertifikate für die beantragte Identität zu beantragen
- gibt einen erfolgreich geprüften Zertifikatsantrag zur Bearbeitung durch die CA frei
- eine Schnittstelle anbieten, über die Zertifikate gesperrt werden können
- den Sperr-Antragsteller authentifizieren
- prüfen, dass der Antragsteller berechtigt ist, Zertifikate für die beantragte Identität zu sperren
- prüfen, dass das Zertifikat, dessen Sperrung beantragt wird, aktuell gültig ist
- gibt einen erfolgreich geprüften Sperrantrag zur Bearbeitung durch die CA frei
- einen Zertifikats- oder Sperrantrag für ein CA-Zertifikat nach dem 4-Augen-Prinzip prüfen und freigeben
- eine CA nach dem 4-Augen-Prinzip in und außer Betrieb nehmen

Eine CA

- stellt ein Zertifikat für einen Zertifikatsantrag aus, nachdem dieser von der RA freigegeben wurde.
- muss gewährleisten, dass maximal 2 Zertifikate pro Zertifikatsinhaber gleichzeitig gültig sind, wobei der Zertifikatsinhaber Auskunft gibt über die zertifizierte Identität und gegebenenfalls die Anwendung. Im Normalfall existiert also genau ein gültiges Zertifikat pro Zertifikatsinhaber und bei der Verlängerung im Überschneidungszeitraum zwei.
- muss eine Schnittstelle anbieten, über die ausgestellte Zertifikate abgeholt werden können
- soll den Antragsteller benachrichtigen, dass das Zertifikat ausgestellt wurde
- muss den Antragsteller benachrichtigen, wenn das Zertifikat abgeholt werden muss
- sperrt das im Sperrantrag referenzierte Zertifikat, nachdem dieser von der RA freigegeben wurde
- muss den Antragsteller benachrichtigen, dass das Zertifikat gesperrt wurde
- muss regelmäßig CRLs ausstellen mit Informationen zu gesperrten Zertifikaten

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 35

- muss eine Schnittstelle zur Abholung von CRLs anbieten
- kann eine Schnittstelle zur Abfrage des Status eines Zertifikats per OCSP anbieten
- soll den PKI-Teilnehmer rechtzeitig über das zeitnahe Ablaufen seines Zertifikats informieren

Des Weiteren muss,

- Zertifikatsbeantragungsprozess dokumentiert werden
- Zertifikatssperrprozess dokumentiert werden
- ein ausgestelltes Zertifikat PKIX-konform sein
- ein ausgestelltes Zertifikat auf seine CP verweisen
- eine ausgestellte CRL PKIX-konform sein
- zur Verlängerung eines Zertifikats ein neues kryptographisches Schlüsselpaar generiert werden

4.2 Schlüsselmanagement

Dieses Kapitel enthält technische und organisatorische Anforderungen an den Umgang mit Schlüsseln, die in den kryptographischen Verfahren und Sicherheitsprotokollen eingesetzt werden.

4.2.1 Schlüsselgenerierung

Für die Schlüsselgenerierung gelten folgende Anforderungen:

- Schlüssel für eine Dokumentenverschlüsselung und zur Authentisierung technischer Nutzer müssen von einer zentralen Stelle, wie z.B. einem Key Management System, bereitgestellt werden. Alle anderen Schlüssel können vom Schlüsselinhaber selbst erstellt werden.
- Die Schlüssel einer CA müssen nach dem 4-Augen-Prinzip generiert werden.
- Es sollen keine selbstsignierten Zertifikate verwendet werden, sondern nur Zertifikate der Konzern-PKI. Stellt die Konzern-PKI keine geeigneten Zertifikate zur Verfügung, kann per Ausnahmegenehmigung auf eine geschäftsprozess-spezifische PKI zurückgegriffen werden.
- Es sollen unterschiedliche Schlüssel für unterschiedliche Einsatzzwecke (z.B. Authentisierung, Verschlüsselung, Signatur) verwendet werden.

4.2.2 Schlüsselverteilung

Für die Schlüsselverteilung gelten folgende Anforderungen:

- Symmetrische und private asymmetrische Schlüssel dürfen nur unter Wahrung von Vertraulichkeit, Integrität und Authentizität verteilt werden. Hierzu stehen die kryptographischen Verfahren des Kapitels 2 und das PKCS#12 Format zur Verfügung.
- Zertifikatsanfragen und nicht-selbstsignierte Zertifikate sind per digitaler Signatur gegen Veränderung gesichert und können über einen unsicheren Kanal übertragen werden.
- Die Verteilung selbstsignierter Zertifikate, z.B. Root-CA-Zertifikate, muss die Authentizität des Zertifikats gewährleisten.
- Die Verteilung von Smartcards und Tokens muss die Sicherheitsanforderungen an die Verteilung der enthaltenen Schlüssel gemäß dieses Kapitels erfüllen.

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 36

4.2.3 Schlüsselspeicherung

Für die Schlüsselspeicherung gelten folgende Anforderungen:

- Symmetrische und private asymmetrische Schlüssel sollen nur verschlüsselt gespeichert werden.
- Da Root-CA-Zertifikate Vertrauensbäume aufspannen, müssen sie so gespeichert werden, dass eine Manipulation durch unbefugte Dritte ausgeschlossen ist.
- Symmetrische und private asymmetrische Schlüssel müssen so gespeichert werden, dass das Auslesen des Schlüssels durch unbefugte Dritte nicht möglich ist (z.B. Smartcard, HSM). Bei einer Speicherung von Schlüsseln im Dateisystem, müssen die Zugriffsrechte so gesetzt werden, dass der Zugriff durch unbefugte Dritte ausgeschlossen ist. Dies ist insbesondere wichtig, falls eine kryptographische Sicherung der Objekte technisch nicht möglich ist.
- Symmetrische und private asymmetrische Schlüssel dürfen weder in ein Versionskontrollsystem eingecheckt noch in Container-Images gespeichert werden.
- Ist die Verfügbarkeit eines zentral gespeicherten Schlüssels Voraussetzung für die Verfügbarkeit einer Anwendung, so muss er redundant gespeichert werden.
- Schlüssel, die von einer zentralen Stelle generiert werden, müssen zentral so gespeichert werden, dass ihre Wiederherstellung im Notfall möglich ist.
- Alle technischen Sicherheitsmaßnahmen zur Endpunktsicherung müssen umgesetzt werden (z.B. Zugriffsschutz, Einsatz von Firewalls oder Virens Scanner).

4.2.4 Schlüssellöschung

Für die Schlüssellöschung gelten folgende Anforderungen:

- Nicht mehr benötigte symmetrische und private asymmetrische Schlüssel müssen gelöscht werden.
- Nicht mehr benötigte Tokens oder Smartcards müssen vernichtet werden.

4.2.5 Schlüsselwiederherstellung und Notfallverfahren

Für die Schlüsselwiederherstellung und Notfallverfahren gelten folgende Anforderungen:

- Alle Verfahren zur Wiederherstellung von Schlüsseln Dritter müssen das 4-Augen-Prinzip umsetzen.
- Die Länge eines Wiederherstellungsschlüssels, englisch Personal Unblocking Key (PUK), muss mindestens 120 Bit betragen.
- Wiederherstellungsschlüssel müssen zur Gewährleistung des 4-Augen-Prinzips mit mindestens zwei Teilschlüsseln verschlüsselt gespeichert werden.
- Zugriffe auf Schlüssel im Notfall sowie Vertretungsregelungen müssen explizit definiert und dokumentiert werden.
- Das Notfallverfahren einer Anwendung muss den Zugriff auf verschlüsselt gespeicherte Anwendungsdaten gewährleisten. Gegebenenfalls muss das Notfallverfahren um Maßnahmen zur Schlüsselwiederherstellung und Restauration der Vertrauensanker ergänzt werden.

4.2.6 Sitzungsschlüssel

Sitzungsschlüssel zur Verschlüsselung, Integritäts- oder Authentizitätssicherung der Kommunikation zweier Kommunikationspartner werden durch die Verfahren in Kapitel 2.6 erzeugt.

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 37

Die Ableitung von Sitzungsschlüsseln für eine zeitlich befristete Kommunikation aus einem Passwort soll mittels Password Authenticated Connection Establishment (PACE) gemäß BSI TR-03110-2 oder Simple Password Exponential Key Exchange (SPEKE) gemäß ISO/IEC 11770-4:2017 erfolgen.

Sitzungsschlüssel müssen regelmäßig gewechselt werden. Zur Bestimmung der Wechselhäufigkeit sind folgende Faktoren zu berücksichtigen:

- ausgetauschtes Datenvolumen
- Verbindungsdauer
- Sicherheitsniveau des lokalen Schlüsselspeichers
- Information über die Kompromittierung eines verwendeten Schlüssels

Sitzungsschlüssel müssen nach Beendigung der Sitzung sofort und sicher gelöscht werden.

4.3 Zufallszahlengeneratoren

Eine große Zahl kryptographischer Verfahren benötigt Zufallszahlen, etwa zur Schlüsselgenerierung oder zur Instanzenauthentisierung. Dies betrifft symmetrische und asymmetrische Verschlüsselungsverfahren ebenso wie Signatur- und Authentisierungsverfahren und Paddingverfahren.

Dabei sind Unvorhersagbarkeit und Geheimhaltung der Zufallszahlen bzw. der aus ihnen abgeleiteten Werte unverzichtbar. Selbst wenn ein Angreifer lange Teilfolgen von Zufallszahlen kennt, soll ihn dies nicht in die Lage versetzen, Vorgänger oder Nachfolger zu bestimmen. Ungeeignete Zufallszahlengeneratoren können grundsätzlich starke kryptographische Mechanismen entscheidend schwächen. Daher müssen für kryptographische Anwendungen geeignete Zufallszahlengeneratoren eingesetzt werden.

In BSI TR-2102-01 Kapitel 9 werden verschiedene Funktionalitätsklassen für physikalische Zufallszahlengeneratoren (PTG.1 – PTG.3), deterministische Zufallszahlengeneratoren (DRG.1 – DRG.4) und nicht-physikalische nicht-deterministische Zufallszahlengeneratoren (NTG.1) herausgearbeitet und die Verwendung eines Zufallszahlengenerators aus der jeweils höchsten Funktionalitätsklasse (PRG.3, DRG.4, NTG.1) empfohlen. Für die IT bedeutet das außerhalb von zertifizierter kryptographischer Spezialhardware die Verwendung von Zufallszahlengeneratoren der Funktionalitätsklasse NTG.1 unter Verwendung von /dev/random auf Linux und CryptGenRandom auf Windows Systemen.

4.4 Umgang mit Passwörtern

Der Umgang mit Passwörtern ist im „Leitfaden_zur_Auswahl_von_Passwörtern,_PIN“ t definiert.

Passwörter müssen immer vertraulich mithilfe der in dieser Rahmenrichtlinie freigegebenen kryptographischen Verfahren und Sicherheitsprotokolle übertragen werden.

Passwörter dürfen weder in ein Versionskontrollsystem eingecheckt noch in Container-Images gespeichert werden.

Bei der Speicherung von Passwörtern sind mehrere Fälle zu unterscheiden.

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 38

4.4.1 Passwörter zum Starten von Diensten

Benötigt ein Dienst Zugriff auf vertrauliche Daten, so muss sich der Dienst gegenüber den Daten authentisieren. Dies erfolgt in der Regel mit Hilfe eines Passworts. Damit der Dienst automatisch starten kann, muss das Passwort im Klartext in eine Konfigurationsdatei eingetragen werden. Eine derartige Konfigurationsdatei muss auf Dateisystemebene geschützt werden. Dazu müssen die Zugriffsrechte so gesetzt werden, dass der Zugriff durch unbefugte Dritte ausgeschlossen ist. Das Verschleiern des Passworts in der Konfigurationsdatei durch einen im Programmcode hinterlegten Schlüssel stellt keine geeignete Sicherung dar, zumal das Einchecken eines solchen Codes in ein Versionskontrollsystem einen Verstoß gegen diese Rahmenrichtlinie darstellen würde.

4.4.2 Passwörter zum Authentisieren von Nutzern

Nutzer authentisieren sich beim Anmelden an Systemen und Applikationen, als auch beim Zugriff auf vertrauliche Nutzdaten und kryptographische Schlüssel. Kommt dabei eine passwortbasierte Authentisierung zum Einsatz, so dürfen die Passwörter der Nutzer nicht im Klartext gespeichert werden, sondern müssen mit einem Hashverfahren geschützt werden.

Da Hashverfahren deterministisch sind, ergibt das gleiche Passwort immer den gleichen Hashwert. Um Angriffe basierend auf dem Abgleich von erbeuteten Passwort-Hashes gegen vorausberechnete Hashwerte beliebiger Passwörter vorzubeugen, muss in die Hash-Berechnung ein individueller Zufallswert eingerechnet werden. Dieser Zufallswert wird als Salt bezeichnet und muss zusammen mit dem Passwort-Hash abgespeichert werden.

Die Hashverfahren des Kapitels 2.3 sind nicht zur Sicherung von Passwörtern geeignet, weil sie zu performant sind und damit keinen ausreichenden Schutz gegen Brute Force Angriffe bieten. Die folgenden Algorithmen sind zur Sicherung von Passwörtern freigegeben:

#	Hash-Verfahren	Basis-Verfahren	Vertraulichkeit
1	PBKDF2	HMAC-SHA2-256 HMAC-SHA2-384 HMAC-SHA2-512 HMAC-SHA2-512/256	hoch
2	bcrypt		sehr hoch
3	scrypt		sehr hoch
4	argon2	Argon2id	sehr hoch

Tabelle 31: Zulässige Passwort-Hashverfahren

Windows Systeme speichern Passwörter mit bis zu 2 verschiedenen Verfahren ab, per LM-Hash und/oder NT-Hash, wobei für beide Verfahren kein Salt verwendet wird. Der LM-Hash hat ein Sicherheitsniveau von 43 Bit und muss deaktiviert werden. Der NT-Hash nutzt den MD4 Algorithmus, hat damit zwar ein potenzielles Sicherheitsniveau von 128 Bit, ist aber aufgrund von Algorithmen-Schwächen ebenfalls hochgradig unsicher, stellt jedoch das kleinere Übel dar. Der NT-Hash ist ausschließlich zur Sicherung von Passwörtern durch das Windows Betriebssystem selbst freigegeben.

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 39

Ein manuell eingegebenes Passwort muss

- kryptographisch gesichert vom Eingabemedium zum Schlüsselspeicher übertragen werden, wenn der Schlüsselspeicher kontaktbehaftet ist (z.B. Smartcard) und das Eingabemedium kein zertifiziertes Kartenlesegerät ist.
- kryptographisch gesichert vom Eingabemedium zum Schlüsselspeicher übertragen werden, wenn der Schlüsselspeicher über ein Netzwerk angebunden ist (z.B. Netzwerk-HSM).
- per PACE gesichert vom Eingabemedium zum Schlüsselspeicher übertragen werden, wenn der Schlüsselspeicher kontaktlos ist. Die Anzahl der ungültigen Passwort-Eingabeversuche muss auf drei beschränkt werden.

Die Verteilung eines Passworts muss

- entweder auf einem anderen Übertragungskanal erfolgen (z.B. postalisch, persönlich) als die Übertragung des damit gesicherten Geheimnisses
- oder unter Sicherung von Vertraulichkeit und Integrität mit einem der freigegebenen kryptographischen Verfahren gemäß Kapitel 2 erfolgen, wenn zur Übertragung von Passwort und damit gesichertem Geheimnis der gleiche Übertragungskanal genutzt wird.

4.5 Umgang mit vertraulichen Daten

Die Speicherung und Übertragung von Daten unterschiedlicher Vertrauensklassen ist in der RRil 135.2001 „Umgang mit Unternehmensinformationen nach Vertraulichkeitsklassen“ definiert. Zur Erreichung der Schutzziele müssen die freigegebenen kryptographischen Verfahren und Sicherheitsprotokolle dieser Rahmenrichtlinie eingesetzt werden. Nicht mehr benötigte vertrauliche Daten müssen sofort und sicher gelöscht werden.

Bei der Historisierung vertraulicher und damit verschlüsselter Daten stellt sich die Herausforderung des Umgangs mit ablaufenden Verschlüsselungszertifikaten. Es gelten die folgenden Anforderungen:

- Es muss regelmäßig geprüft werden, ob die Daten noch benötigt werden. Falls nein, sind die Daten sofort sicher zu löschen.
- Die Daten müssen rechtzeitig vor Gültigkeitsende des Verschlüsselungszertifikats umgeschlüsselt werden. Dazu müssen sie mit dem zum demnächst ablaufenden Zertifikat zugehörigen privaten Schlüssel entschlüsselt und mit dem neuen Verschlüsselungszertifikat verschlüsselt werden. Die Umschlüsselung soll in einem zusammenhängenden Arbeitsschritt erfolgen. Dabei entstehende Prozess-Artefakte, wie z.B. die Klartextdaten, müssen sicher gelöscht werden.

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 40

5 Policy Prozess

Die zulässigen kryptographischen Verfahren gemäß Kapitel 2, die zulässigen Sicherheitsprotokolle gemäß Kapitel 3 und die empfohlenen Zufallszahlengeneratoren gemäß Kapitel 4.3 basieren auf den Empfehlungen des BSI. Im Rahmen der regelmäßigen Überprüfung dieses Anhangs durch den Policy Prozess müssen die freigegebenen Verfahren und Protokolle mit den BSI-Empfehlungen gemäß den zum Zeitpunkt der Überprüfung aktuellen Versionen der BSI TR-02102 Dokumente abgeglichen werden.

Die freigegebenen Verfahren und Protokolle dieses Anhangs basieren auf den Empfehlungen in folgenden Dokumentversionen:

- BSI TR-02102-1 Kryptographische Verfahren: Empfehlungen und Schlüssellängen v2020-01
- BSI TR-02102-2 Kryptographische Verfahren: Verwendung von TLS v2020-01
- BSI TR-02102-3 Kryptographische Verfahren: Verwendung von IPsec und IKEv2 v2020-01
- BSI TR-02102-4 Kryptographische Verfahren: Verwendung von SSH v2020-01

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 41

Glossar

AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard Algorithmus
AH	Authentication Header
API	Application Programming Interface
BSI	Bundesamt für Sicherheit in der Informationstechnik
CA	Certificate Authority
CBC	Cipher Block Chaining
CC	Common Criteria
CCM	Cipher Block Chaining Message Authentication
CMAC	Cipher-Based Message Authentication Code
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CRLDP	Certificate Revocation List Distribution Point
CTR	Counter Mode
DH	Diffie Hellman Algorithmus
DHE	Diffie Hellman Ephemeral
DLIES	Discrete Logarithm Integrated Encryption Scheme
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
ECDH	Elliptic Curve Diffie Hellman Algorithmus
ECDHE	Elliptic Curve Diffie Hellman Ephemeral
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption Scheme

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 42

ECGDSA	Elliptic Curve German Digital Signature Algorithm
ECKCDSA	Elliptic Curve Korean Certificate-based Digital Signature Algorithm
ESP	Encapsulated Security Payload
GCM	Galois Counter Mode
GMAC	Galois Message Authentication Code
HMAC	Keyed-Hash Message Authentication Code
HSM	Hardware-Sicherheitsmodul
IKE	Internet Key Exchange
IPsec	Internet Protocol Security
ISMS	Informationssicherheitsmanagementsystem
ITSEC	Information Technology Security Evaluation Criteria
MAC	Message Authentication Code
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object ID
PACE	Password Authentication Connection Establishment
PBKDF	Password-Based Key Derivation Function
PGP	Pretty Good Privacy
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
PKIX	PKI using X.509 Certificate and CRL Profile
PSK	Pre-Shared Key
PSS	Probabilistic Signature Scheme
PUK	Personal Unblocking Key
RA	Registration Authority
RSA	Rivest Shamir Adleman Algorithmus

Organisation und Managementsysteme	Informationssysteme
Einsatz kryptographischer Verfahren	Seite 43

RSAE	rsaEncryption OID
RSASSA-PSS	RSA Signatur mit PSS Encoding
SHA	Secure Hash Algorithmus
SPEKE	Simple Password authenticated Exponential Key Exchange
SSH	Secure Shell
S/MIME	Secure / Multipurpose Internet Mail Extensions
TLS	Transport Layer Security
TR	Technische Richtlinie
VPN	Virtual Private Network
WPA	Wi-Fi Protected Access
XCBC	Extended Cipher Block Chaining Encryption