



Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Technische Richtlinie TR-02102-3 Kryptographische Verfahren: Empfehlungen und Schlüssellängen

Teil 3 – Verwendung von Internet Protocol Security (IPsec) und Internet Key Exchange (IKEv2)



Änderungshistorie

Tabelle 1: Änderungshistorie

Version	Datum	Beschreibung
2019-01	11.02.2019	Anpassung der Verwendungszeiträume, Empfehlung des CCM-Modus
2020-01	31.01.2020	Anpassung der Verwendungszeiträume, Abkündigung von HMAC-SHA-1
2021-01	12.03.2021	Anpassung der Verwendungszeiträume
2022-01	24.01.2022	Anpassung der Verwendungszeiträume
2023-01	17.01.2023	Anhebung des Sicherheitsniveaus auf 120 Bit, Anpassung der Verwendungszeiträume
2024-01	29.02.2024	Anpassung der Verwendungszeiträume
2024-02	13.09.2024	Empfehlung zusätzlicher Schlüssellängen für RSA-PSS-Signaturen

Inhalt

1	Einleitung.....	4
1.1	Spezifikationen und Internetstandards.....	4
2	Grundlagen.....	5
2.1	IKEv2.....	5
2.1.1	Schlüsselableitung und Schlüsselerzeugung.....	6
2.1.2	Lifetime.....	7
2.1.3	Rekeying.....	7
2.1.4	RNG/Zufall.....	7
2.1.5	Perfect Forward Secrecy (PFS).....	8
2.2	IPsec.....	8
2.2.1	ESP und AH.....	8
2.2.2	Tunnel- und Transportmodus.....	8
2.2.3	SAD und SPD.....	8
3	Empfehlungen.....	10
3.1	Allgemeine Hinweise.....	10
3.1.1	Verwendungszeiträume.....	10
3.1.2	Sicherheitsniveau.....	10
3.2	IKEv2.....	10
3.2.1	Verschlüsselung der IKE-Nachrichten.....	10
3.2.2	Pseudo-Zufallsfunktion zur Schlüsselerzeugung.....	11
3.2.3	Integritätsschutz der IKE-Nachrichten.....	11
3.2.4	Gruppen für den Diffie-Hellman-Schlüsselaustausch.....	11
3.2.5	Authentisierungsverfahren.....	12
3.3	IPsec.....	13
3.3.1	Verschlüsselung der ESP-Pakete.....	13
3.3.2	Integritätsschutz der ESP-Pakete.....	14
3.3.3	Integritätsschutz der AH-Pakete.....	14
3.4	SA-Lifetime und Rekeying.....	14
	Literaturverzeichnis.....	15

1 Einleitung

Diese Technische Richtlinie (TR) gibt Empfehlungen für die Verwendung von kryptographischen Mechanismen in den Protokollen IPsec (Kurzform für Internet Protocol Security) und IKE (Kurzform für Internet Key Exchange). Sie enthält ausschließlich Empfehlungen für die Version 2 des IKE-Protokolls (IKEv2). In dieser TR werden keine Aussagen zu IKEv1 getroffen; die Verwendung des neueren Protokolls IKEv2 wird für Neuentwicklungen grundsätzlich empfohlen. IKEv2 besitzt Vorteile gegenüber IKEv1, die aber hauptsächlich mit der Komplexität des Protokolls und der benötigten Bandbreite beim Aufbau einer Security Association (siehe auch weiter unten) zu tun haben.

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 Informationen gewährleistet werden können. 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 Schutzziele zusätzlich den Schutz der Vertraulichkeit.

Die hier aufgeführten Schutzziele werden durch kryptographische Sicherheitsmechanismen erreicht. IPsec bietet darüber hinaus noch weitere Schutzmechanismen wie z. B. einen Schutz gegen das Wiedereinspielen (Replay-Attacke) von bereits verarbeiteten IPsec-Paketen. Diese werden in der vorliegenden TR nicht betrachtet.

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 IKEv2 kann eine 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 basierend auf der vorher ausgehandelten SA. Der Begriff SA existiert analog für IKEv2. Dabei werden IPsec-SAs (Child-SAs) von vorher ausgehandelten IKE-SAs abgeleitet.

Hinweis: Auch bei Beachtung aller Vorgaben für die Verwendung von IKEv2 und IPsec können Daten in erheblichem Umfang aus einem kryptographischen System abfließen, z. B. durch Ausnutzung von Seitenkanälen (Messung von Timing-Verhalten, Stromaufnahme, Datenraten etc.) oder durch fehlerhafte Konfiguration der Sicherheitsprotokolle auf den Ablaufplattformen. Daher sollte der Entwickler unter Hinzuziehung von Experten auf diesem Gebiet mögliche Seitenkanäle identifizieren und entsprechende Gegenmaßnahmen umsetzen. Je nach Anwendung gilt dies auch für Fault-Attacken.

Hinweis: Für Definitionen kryptographischer Begriffe in diesem Dokument siehe das Glossar in [TR-02102-1].

1.1 Spezifikationen und Internetstandards

Die Protokolle IKEv2 (bzw. IKE) und IPsec wurden in verschiedenen RFCs spezifiziert. Für IKEv2 (bzw. IKE) gibt es die RFCs 2409, 4306, 4718, 5282, 5996, 5998, 7296, 7427, und 8247 (ersetzt RFC 4307). Für IPsec gelten beispielsweise die RFCs 4106, 4301, 4302, 4303, 4308, 4309, 4543 und 8221 (ersetzt RFCs 7321 und 4835).

Diese Technische Richtlinie gibt Empfehlungen für die Protokolle IKEv2 und IPsec, und orientiert sich primär an den zurzeit aktuellen Protokollversionen und RFCs. Für Implementierungen ist RFC 7296 (Vorgängerversion RFC 5996) besonders wichtig, da er eine umfangreiche Überarbeitung von vorigen Standards sowie Klarstellungen aus RFC 4718 enthält.

2 Grundlagen

2.1 IKEv2

Das IKE-Protokoll läuft zwischen zwei IP-basierten Kommunikationssystemen ab, die über ein (möglicherweise) unsicheres Netz mittels IPsec verschlüsselt kommunizieren möchten. IKE ermöglicht die Aushandlung und ggf. Erneuerung (Schlüsselwechsel) des dafür zu verwendenden Schlüsselmaterials.

Das IKE-Protokoll existiert in zwei Versionen: Die erste Version (IKEv1) wurde im Jahre 1998 in RFC 2409 spezifiziert. Die derzeit aktuelle Version IKEv2 ist in den drei IETF-Dokumenten RFC 4306, RFC 5996 sowie RFC 7296 spezifiziert. RFC 7296 ist eine Überarbeitung von RFC 5996 sowie RFC 4306. Die Aufgaben des IKE-Protokolls können wie folgt zusammengefasst werden:

1. Aushandlung der für IKE zu verwendenden Kryptoalgorithmen und Kryptoparameter für den Aufbau eines verschlüsselten und integritätsgesicherten Kanals, der zwischen zwei über das IP-Protokoll in einem nicht vertrauenswürdigen Netz kommunizierenden Parteien aufgebaut werden soll
2. Aufbau eines verschlüsselten und integritätsgesicherten Kanals unter Verwendung der in Punkt 1 ausgehandelten kryptographischen Verfahren
3. Gegenseitige Authentisierung der beiden Parteien
4. Aushandlung der für IPsec zu verwendenden kryptographischen Algorithmen, Betriebsarten, Schlüssellängen sowie des IPsec-Protokolls (AH oder ESP). Diese Aushandlung geschieht unter dem Schutz des in 2. aufgebauten Kanals
5. Erzeugung der IPsec-Schlüssel bei beiden Kommunikationspartnern unter Berücksichtigung der in 4. ausgehandelten Algorithmen

Alle Kommunikationsabläufe innerhalb von IKE bestehen immer aus einer *Request*- und einer *Response*-Nachricht. Beide Nachrichten zusammen bilden einen *Austausch*. Die beiden beteiligten Systeme bzw. Kommunikationspartner heißen im IKE-Protokoll traditionell *Initiator* und *Responder*.

Bei IKEv2 gibt es die vier folgenden Austauscharten:

- IKE_SA_INIT
- IKE_AUTH
- CREATE_CHILD_SA
- INFORMATIONAL

IKE_SA_INIT (Schritte 1 und 2) und IKE_AUTH (Schritte 3 und 4) werden dabei zu Beginn des IKE-Ablaufes durchgeführt. Nach erfolgreichem Abschluss von IKE_AUTH sind bei beiden kommunizierenden Parteien IKE-Sicherheitsbeziehungen (IKE Security Association, kurz IKE-SAs) sowie Sicherheitsbeziehungen für die IPsec-Protokolle AH oder ESP (Child-SAs, d. h. IPsec-SAs) vorhanden. Die IKE-SA beinhaltet die gegenseitige Authentisierung von Initiator und Responder sowie das Vorhandensein einer verschlüsselten und integritätsgesicherten Verbindung zwischen beiden (Schritte 1 bis 3 erfolgreich durchlaufen). Ein CREATE_CHILD_SA-Austausch ist optional und ermöglicht zum Beispiel das Erneuern des Schlüsselmaterials einer vorhandenen IPsec-SA auf Basis einer bestehenden IKE-SA. Dies bedeutet die Wiederholung der Schritte 4 und 5 unter dem Schutz der bestehenden IKE-SA und wird nach Ablauf der vorher festgelegten Lifetime durchgeführt.

Weiterhin gibt es auch INFORMATIONAL-Exchanges für den Austausch von Fehlermeldungen und anderer Nachrichten zwischen Initiator und Responder. Für Details wird auf die Abschnitte 1.4 und 1.5 in [RFC 7296] verwiesen.

Für Details zum IKE-Ablauf wird auf das IETF-Dokument [RFC 7296] verwiesen.

2.1.1 Schlüsselableitung und Schlüsselerzeugung

Der Begriff *Schlüsselableitung* beschreibt hier das Erzeugen von kryptographischem Schlüsselmaterial sowohl für IKE-SAs als auch für IPsec-SAs. Ein wesentliches Kernelement der Schlüsselableitung in IKE ist ein Diffie-Hellman-Schlüsselaustausch sowie die Berechnung des Schlüsselmaterials mit einer sog. Pseudo-Zufallsfunktion (engl. pseudorandom function, kurz PRF).

Die Berechnung für das Schlüsselmaterial für die IKE-SA findet zeitlich nach dem `IKE_SA_INIT`-Austausch und vor dem `IKE_AUTH`-Austausch statt. Die *erste* `IKE_SA_INIT`-Nachricht enthält in der SA-Payload folgende Vorschläge des Initiators bzgl. der zu verwendenden Algorithmen:

1. Symmetrischer Verschlüsselungsalgorithmus für die Verschlüsselung der IKE-Nachrichten des `IKE_AUTH`-Austausches und des optionalen `CREATE_CHILD_SA`-Austausches sowie eventuelle `INFORMATIONAL`-Austauschvorgänge
2. Pseudo-Zufallsfunktion (PRF) zur Schlüsselableitung
3. Algorithmus zum Integritätsschutz der anschließend übertragenen IKE-Nachrichten
4. Diffie-Hellman-Gruppe für die Diffie-Hellman-Schlüsselvereinbarung. Eine Diffie-Hellman-Gruppe ist dabei entweder eine Primzahl p zusammen mit einem Generator g der zyklischen Gruppe $(Z_p)^*$ oder elliptische Kurvenparameter zusammen mit einem Basispunkt als Generator einer Untergruppe der Punktgruppe. Es werden dabei lediglich die standardisierten Bezeichner einer DH-Gruppe übertragen. Für die Bezeichner gelten standardisierte Werte, die unter „Transform Type 4“ unter [IANA] eingesehen werden können.

Die erste `IKE_SA_INIT`-Nachricht (request) enthält weiterhin:

- Eine Key-Exchange-Payload, die einen öffentlichen Diffie-Hellman-Schlüssel enthält, der vor der Übertragung unter Verwendung der vorgeschlagenen Diffie-Hellman-Gruppe und dem privaten Diffie-Hellman-Schlüssel erzeugt wurde. Für die Erzeugung des privaten Diffie-Hellman-Schlüssel gelten die Empfehlungen aus [TR-02102-1]¹.
- Den sog. Nonce-Wert des Initiators. Dieser wird zufällig und unvorhersagbar erzeugt, und darf nur einmal verwendet werden.

Die Nonce-Werte N_i und N_r von Initiator und Responder müssen eine Größe von mindestens 16 Byte und maximal 256 Byte haben (siehe [RFC 7296], Abschnitt 3.9). Beide Parteien (Initiator, Responder) berechnen nach dem `IKE_SA_INIT`-Austausch unabhängig voneinander (siehe Abschnitt 2.14 in [RFC 7296]):

- Das Diffie-Hellman shared secret g^{ir}
- Die Größe `SKEYSEED` := `prf(Ni | Nr, gir)`
Die Nonce-Werte N_i und N_r sind in der `IKE_SA_INIT`-Nachricht vom Initiator zum Responder übertragen worden (N_i an Responder) und umgekehrt (N_r an Initiator). Sie gehen aneinandergehängt (konkateniert) als Schlüssel in die PRF-Berechnung mit ein. g^{ir} ist der gemeinsame geheime Schlüssel nach abgeschlossener Diffie-Hellman-Schlüsselvereinbarung. Der Wert `SKEYSEED` hat die Ausgabelänge der verwendeten Pseudo-Zufallsfunktion.
- Aus `SKEYSEED`, den Nonces N_i und N_r sowie den SPI-Werten² werden mehrere Schlüssel berechnet:
`prf+(SKEYSEED, Ni | Nr | SPIi | SPIr) = {SK_d | SK_ai | SK_ar | SK_ei | SK_er | SK_pi | SK_pr}`
Dabei sind `SPIi` und `SPIr` die eindeutigen Kennzeichner der auszuhandelnden IKE-SA, die jeweils vom Initiator und Responder gebildet werden.

¹ Im Zusammenhang mit der Verwendung von elliptischen Kurven zur Schlüsselvereinbarung sei auf [RFC 6954], Abschnitt 3 hingewiesen: „..., the private Diffie-Hellman keys should be selected with the same bit length as the order of the group generated by the base point G and with approximately maximum entropy.“

² Siehe Abschnitt 2.6 in [RFC 7296].

$\text{prf}+$ bedeutet gemäß [RFC 7296], Abschnitt 2.13 die iterierte Anwendung der vereinbarten Pseudo-Zufallsfunktion, um eine ausreichende Ausgabelänge für die Gesamtmenge der zu erzeugenden Schlüssel zu erreichen. Die Anzahl der Iterationen des PRF-Aufrufes muss dabei so bemessen werden, dass die Summe der Bitlängen von SK_d , SK_{ai} , SK_{ar} , SK_{ei} , SK_{er} , SK_{pi} und SK_{pr} erreicht wird. Diese Schlüssel haben folgende Bedeutung:

Tabelle 2: Übersicht der wichtigsten Schlüssel

Schlüssel	Verwendung
SK_d	Ableitung von Schlüsseln für Child-SAs
SK_{ei}	Symmetrischer Schlüssel zur Verschlüsselung aller weiteren IKE-Nachrichten (<code>IKE_AUTH</code> , <code>CREATE CHILD SA</code> , <code>INFORMATIONAL</code>) vom Initiator zum Responder
SK_{ai}	Schlüssel für den Integritätsschutz aller weiteren IKE-Nachrichten (<code>IKE_AUTH</code> , <code>CREATE CHILD SA</code> , <code>INFORMATIONAL</code>) vom Initiator zum Responder
SK_{er}	Symmetrischer Schlüssel zur Verschlüsselung aller weiteren IKE-Nachrichten (<code>IKE_AUTH</code> , <code>CREATE CHILD SA</code> , <code>INFORMATIONAL</code>) vom Responder zum Initiator
SK_{ar}	Schlüssel für den Integritätsschutz aller weiteren IKE-Nachrichten (<code>IKE_AUTH</code> , <code>CREATE CHILD SA</code> , <code>INFORMATIONAL</code>) vom Responder zum Initiator
SK_{pi}	Schlüssel zur Generierung der AUTH-Payload zur Authentisierung des Initiators beim Responder (beim <code>IKE_AUTH</code> -Exchange). Vgl. auch Abschnitt 2.15 in [RFC 7296].
SK_{pr}	Schlüssel zur Generierung der AUTH-Payload zur Authentisierung des Responders beim Initiator (beim <code>IKE_AUTH</code> -Exchange). Vgl. auch Abschnitt 2.15 in [RFC 7296].

Die Längen (in Bit) aller oben gelisteten Schlüssel müssen entsprechend den in Kapitel 3 empfohlenen Verfahren und deren Bitlängen gewählt werden. Insbesondere sollen die Schlüssellängen von SK_d , SK_{pi} und SK_{pr} gemäß der vereinbarten PRF gewählt werden.

2.1.2 Lifetime

Sowohl IKE-SAs als auch IPsec-SAs sollen nur für eine begrenzte Zeit gültig sein und nach Ablauf dieser Zeit neu ausgehandelt werden. Alternativ kann als Kriterium für die Neuaushandlung einer IPsec-SA auch das übertragene Datenvolumen herangezogen werden. Nach [RFC 4301], Abschnitt 4.4.2.1, muss eine IPsec-Implementierung beide Kriterien unterstützen. Die Angabe von verbindlichen Gültigkeitszeiträumen bzw. einer Obergrenze für das Datenvolumen ist Teil einer Sicherheitspolitik und muss vom Systemadministrator festgelegt werden. Im Gegensatz zum alten Protokoll IKEv1 ist die Lifetime von SAs bei IKEv2 nicht mehr aushandelbar (vgl. Seite 37 in [RFC 7296]).

2.1.3 Rekeying

Unter Rekeying versteht man das erneute Aushandeln einer abgelaufenen und damit nicht mehr gültigen Sicherheitsbeziehung. Dies bezieht sich sowohl auf IKE-SAs als auch auf SAs für IPsec. Für beide Fälle wird auf die Beschreibung in [RFC 7296] verwiesen.

2.1.4 RNG/Zufall

Für die Generierung von Zufallszahlen, z. B. für die Erzeugung kryptographischer Schlüssel, für die Signaturerzeugung und für die Erzeugung von Nonces müssen geeignete Zufallszahlengeneratoren eingesetzt werden.

Empfohlen wird ein Zufallszahlengenerator aus einer der Klassen DRG.3, DRG.4, PTG.3 oder NTG.1 gemäß [AIS 20/31], vgl. auch Kapitel 8 in [TR-02102-1].

2.1.5 Perfect Forward Secrecy (PFS)

Perfect Forward Secrecy bedeutet, dass eine abgehörte Verbindung auch bei Kenntnis der Langzeit-Schlüssel der Kommunikationspartner nachträglich nicht entschlüsselt werden kann.

Durch den IKE_AUTH-Austausch entsteht sowohl das Schlüsselmaterial für die IKE-SA als auch für eine Child-SA. Sollen auf Basis der bestehenden IKE-SA weitere Child-SAs ausgehandelt werden, kann dies nach Abschnitt 2.17 in [RFC 7296] optional unter Verwendung eines erneuten Diffie-Hellman-Schlüsselaustausches geschehen. Dazu werden nach Abschnitt 1.3.1 in [RFC 7296] die öffentlichen Diffie-Hellman-Schlüssel zwischen Initiator und Responder übertragen und anschließend auf beiden Seiten das gemeinsame Diffie-Hellman-Geheimnis berechnet, welches gemäß [RFC 7296], Abschnitt 2.17, in die Sitzungsschlüsselberechnung eingeht.

Die Nutzung von PFS wird grundsätzlich empfohlen.

2.2 IPsec

2.2.1 ESP und AH

Die Sicherheitsdienste der beiden IPsec-Protokolle ESP und AH wurden im Abschnitt 1 genannt. Für eine genaue Beschreibung wird auf [RFC 4302] (für AH) sowie auf [RFC 4303] (für ESP) verwiesen.

2.2.2 Tunnel- und Transportmodus

Sowohl AH als auch ESP können in zwei Betriebsmodi verwendet werden: *Tunnelmodus* und *Transportmodus*. Im Tunnelmodus werden die IPsec-Schutzmechanismen 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).

Im Transportmodus hingegen werden die IPsec-Schutzmechanismen nur auf die Nutzdaten des IP-Pakets angewendet und weiterhin der ursprüngliche IP-Header verwendet. Im Gegensatz zum Tunnelmodus werden also die Adressen der gesicherten kommunizierenden Systeme nicht verborgen. Ein Angreifer würde beim Abhören der geschützten Verbindung also ggf. Informationen über das Kommunikationsverhalten bzw. über das gesicherte Netz erhalten.

Eine genaue Beschreibung der beiden Betriebsmodi für AH findet sich in [RFC 4302] in den Abschnitten 3.1.1 und 3.1.2. [RFC 4303] enthält in den Abschnitten 3.1.1 und 3.1.2 die Beschreibung der beiden Betriebsmodi für ESP. Die Wahl für den Tunnel- oder Transportmodus hängt von der vorliegenden Anwendung ab (siehe hierzu auch Abschnitt 4 in [RFC 4301]). Grundsätzlich sollte bei der Verwendung von ESP jedoch der Tunnelmodus gegenüber dem Transportmodus bevorzugt werden, da beim Tunnelmodus durch die Verschlüsselung des gesamten inneren IP-Pakets keine verdeckten Kanäle von dem zu schützenden Netzwerk in das nicht vertrauenswürdige Netzwerk bestehen. Zusätzlich ist bei der Verwendung von ESP im Tunnelmodus keine vollständige Verkehrsflussanalyse möglich, weil die Adressinformationen des inneren IP-Headers durch die Verschlüsselung verborgen werden.

2.2.3 SAD und SPD

Die *Security Association Database (SAD)* und die *Security Policy Database (SPD)* sind zwei wichtige IPsec-Datenbanken, die bei der Verarbeitung von IPsec-Paketen verwendet werden (siehe Abschnitte 4.4.1 und 4.4.2 in [RFC 4301] für Details).

Die SPD enthält Regeln, die bestimmen, wie ein- und ausgehende Pakete durch IPsec verarbeitet werden. Dabei werden alle Pakete (auch nicht-IPsec-Pakete) anhand der Regeln in der SPD bearbeitet. Beispielsweise gibt es Regeln, die festlegen, wie die Verbindung zwischen zwei Kommunikationspartnern gesichert ist. Die Sicherung selbst kann dann durch AH oder ESP erfolgen.

In der SAD werden die SAs verwaltet; für jede Verbindung gibt es einen Eintrag in der SAD, der z. B. die Schlüssel für das vereinbarte Sicherheitsprotokoll der Verbindung enthält. Für AH und ESP gibt es separate Einträge in der Datenbank.

Hinweis: Die Datenbanken SAD und SPD müssen gesichert gespeichert werden, damit keine Manipulationen durch Angreifer möglich sind.

3 Empfehlungen

3.1 Allgemeine Hinweise

3.1.1 Verwendungszeiträume

Die Empfehlungen in dieser Technischen Richtlinie sind mit Verwendungszeiträumen versehen. Die Angabe der Jahreszahl bedeutet hierbei, dass das entsprechende Verfahren bis zum Ende des angegebenen Jahres empfohlen wird. Ist die Jahreszahl mit einem „+“-Zeichen gekennzeichnet, so bedeutet dies, dass dieser Verwendungszeitraum möglicherweise in einer zukünftigen Version dieser Technischen Richtlinie verlängert wird.

3.1.2 Sicherheitsniveau

Das Sicherheitsniveau für alle kryptographischen Verfahren in dieser Technischen Richtlinie richtet sich nach dem in Abschnitt 1.1 in [TR-02102-1] angegebenen Sicherheitsniveau und liegt bei 120 Bit.

3.2 IKEv2

In diesem Abschnitt werden Empfehlungen für die folgenden IKE-Komponenten festgelegt:

1. Verschlüsselung der IKE-Nachrichten
2. Funktion zur Schlüsselableitung bzw. -erzeugung
3. Integritätsschutz der IKE-Nachrichten
4. Gruppen für den Diffie-Hellman-Schlüsselaustausch
5. Verfahren zur gegenseitigen Authentisierung

3.2.1 Verschlüsselung der IKE-Nachrichten

Die Empfehlungen betreffen die Verschlüsselung der im IKE_AUTH-, CREATE_CHILD_SA- sowie INFORMATIONAL-Exchange ausgetauschten Nachrichten. Die folgenden Verschlüsselungsverfahren für IKE werden empfohlen:

Tabelle 3: Empfohlene Verschlüsselungsverfahren für IKE-Nachrichten

Nr.	Verfahren	IANA-Nr.	Spezifikation	AES-Schlüssellänge	Verwendung bis
1	ENCR_AES_CBC	12	[RFC 7296]	128 / 256	2030+
2	ENCR_AES_CTR	13	[RFC 5930]	128 / 256	2030+
3	ENCR_AES_GCM_16	20	[RFC 5282] [RFC 8247]	128 / 256	2030+
4	ENCR_AES_GCM_12	19	[RFC 5282] [RFC 8247]	128 / 256	2030+
5	ENCR_AES_CCM_16	16	[RFC 5282]	128 / 256	2030+
6	ENCR_AES_CCM_12	15	[RFC 5282]	128 / 256	2030+

Hinweis: Die ersten beiden Verfahren in Tabelle 3 müssen mit einem der in Abschnitt 3.2.3 genannten Verfahren zum Schutz der Integrität kombiniert werden. Die Schlüssel für die Verfahren in obiger Tabelle werden nach der in Abschnitt 2.1.1 angegebenen Vorschrift berechnet. Die hier zur Anwendung kommenden Schlüssel sind SK_{ei} und SK_{er} .

Für weitere Informationen zu den Betriebsarten GCM und CCM siehe Abschnitt 3.1.2 in [TR-02102-1]. Werden diese Betriebsarten eingesetzt, darf gemäß Abschnitt 8 in [RFC 5282] kein Algorithmus zum Integritätsschutz der übertragenen Nachrichten verwendet werden.

3.2.2 Pseudo-Zufallsfunktion zur Schlüsselerzeugung

Wie in Abschnitt 2.1.1 erläutert, wird zur Erzeugung von Schlüsselmaterial eine Pseudo-Zufallsfunktion (engl. pseudorandom function, kurz PRF) eingesetzt. Die folgenden PRFs werden empfohlen:

Tabelle 4: Empfohlene PRFs zur Schlüsselerzeugung

Nr.	Verfahren	IANA-Nr.	Spezifikation	Verwendung bis
1	PRF AES128 XCBC	4	[RFC 4434]	2030+
2	PRF AES128 CMAC	8	[RFC 4615]	2030+
3	PRF HMAC SHA2 256	5	[RFC 4868]	2030+
4	PRF HMAC SHA2 384	6	[RFC 4868]	2030+
5	PRF HMAC SHA2 512	7	[RFC 4868]	2030+

Hinweis: Die Länge des erzeugten Schlüssels (Ausgabelänge der PRF) muss mindestens so groß sein wie die empfohlene Schlüssellänge des eingesetzten Verschlüsselungsverfahrens aus Tabelle 3. Es ist zu beachten, dass die PRF gemäß Abschnitt 2.13 in [RFC 7296] ggf. mehrfach iterativ aufgerufen werden muss.

Bei Verwendung der Verfahren Nr. 1 und Nr. 2 aus Tabelle 4 müssen die entsprechenden Hinweise aus Abschnitt 2.14 in [RFC 7296] beachtet werden.

3.2.3 Integritätsschutz der IKE-Nachrichten

Die folgenden Verfahren werden für die Integritätssicherung der im IKE_AUTH-, CREATE_CHILD_SA- sowie INFORMATIONAL-Exchange ausgetauschten Nachrichten empfohlen:

Tabelle 5: Empfohlene Verfahren zum Integritätsschutz der IKE-Nachrichten

Nr.	Verfahren	IANA-Nr.	Spezifikation	Verwendung bis
1	AUTH AES XCBC 96	5	[RFC 7296]	2030+
2	AUTH HMAC SHA2 256 128	12	[RFC 4868]	2030+
3	AUTH HMAC SHA2 384 192	13	[RFC 4868]	2030+
4	AUTH HMAC SHA2 512 256	14	[RFC 4868]	2030+

Hinweis: Die Schlüssellänge für die in Tabelle 5 genannten Verfahren muss den geforderten Schlüssellängen in den jeweils angegebenen RFCs entsprechen.

Für Neuentwicklungen wird eines der auf SHA-2 basierenden Verfahren (Nr. 2-4) in Tabelle 5 empfohlen.

3.2.4 Gruppen für den Diffie-Hellman-Schlüsselaustausch

Die folgenden Gruppen werden für den Schlüsselaustausch mit dem Diffie-Hellman-Verfahren empfohlen:

Tabelle 6: Empfohlene Gruppen für den Diffie-Hellman-Schlüsselaustausch

Nr.	Name	IANA-Nr.	Spezifikation	Verwendung bis
1	3072-bit MODP Group	15	[RFC 3526]	2030+
2	4096-bit MODP Group	16	[RFC 3526]	2030+
3	256-bit random ECP group	19	[RFC 5903]	2030+
4	384-bit random ECP group	20	[RFC 5903]	2030+
5	521-bit random ECP group	21	[RFC 5903]	2030+
6	brainpoolP256r1	28	[RFC 6954]	2030+

Nr.	Name	IANA-Nr.	Spezifikation	Verwendung bis
7	brainpoolP384r1	29	[RFC 6954]	2030+
8	brainpoolP512r1	30	[RFC 6954]	2030+

Hinweis 1: Zur Realisierung der Eigenschaft *Perfect Forward Secrecy (PFS)* kann im `CREATE_CHILD_SA`-Austausch ein erneuter Diffie-Hellman-Schlüsselaustausch durchgeführt werden. Die dabei empfohlenen elliptischen Kurven und Gruppen sind dabei die gleichen wie in obiger Tabelle.

Hinweis 2: Die Verwendung von Brainpool-Kurven wird grundsätzlich empfohlen.

Hinweis 3: Eine Verwendung von zusätzlichen Diffie-Hellman-Tests (siehe [RFC 6989]) wird empfohlen. Diese Tests werden besonders beim Einsatz von elliptischen Kurven empfohlen; siehe dazu Abschnitt 2.3 in [RFC 6989].

Hinweis 4: Bei den elliptischen Kurven mit den IANA-Nr. 19, 20 und 21 handelt es sich um NIST-Kurven. In Tabelle 6 werden die IANA-Bezeichnungen verwendet. Für alternative Bezeichnungen der Kurven (z. B. von NIST) siehe Kapitel 5 in [RFC 5903].

3.2.5 Authentisierungsverfahren

Die folgenden Authentisierungsverfahren werden empfohlen:

Tabelle 7: Empfohlene Authentisierungsverfahren

Nr.	Verfahren	Bitlänge	Hashfunktion	IANA-Nr.	Spezifikation	Verwendung bis
1	ECDSA-256 mit Kurve <code>secp256r1</code>	256	SHA-256	9	[RFC 4754] [RFC 5903]	2030+
2	ECDSA-384 mit Kurve <code>secp384r1</code>	384	SHA-384	10	[RFC 4754] [RFC 5903]	2030+
3	ECDSA-512 mit Kurve <code>secp521r1</code>	512	SHA-512	11	[RFC 4754] [RFC 5903]	2030+
4	ECDSA-256 mit Kurve <code>brainpoolP256r1</code>	256	SHA-256	14	[RFC 7427]	2030+
5	ECDSA-384 mit Kurve <code>brainpoolP384r1</code>	384	SHA-384	14	[RFC 7427]	2030+
6	ECDSA-512 mit Kurve <code>brainpoolP512r1</code>	512	SHA-512	14	[RFC 7427]	2030+
7	RSASSA-PSS	mind. 3000	SHA-256 / SHA-384 / SHA-512	14	[RFC 7427] [RFC 4055]	2030+
8	ECGDSA-256 mit Kurve <code>brainpoolP256r1³</code>	256	SHA-256	14	[RFC 7427]	2030+
9	ECGDSA-384 mit Kurve <code>brainpoolP384r1</code>	384	SHA-384	14	[RFC 7427]	2030+
10	ECGDSA-512 mit Kurve <code>brainpoolP512r1</code>	512	SHA-512	14	[RFC 7427]	2030+

Hinweis 1: Die Verfahren RSA (IANA-Nr. 1) und DSS (IANA-Nr. 3) sind in [RFC 7296] nur in Verbindung mit der Hashfunktion SHA-1 spezifiziert. SHA-1 sollte aber aufgrund von Angriffen gegen seine

³ Für die Kodierung der ECGDSA-Signaturen siehe Abschnitt 5.2.1 in [TR-03111]. Für die OIDs der ECGDSA-Varianten siehe Abschnitt 5.2.1.2 in [TR-03111]. Für das Public-Key-Format wird auf OID 1.3.36.3.3.2.5 sowie [Teletrust] und Abschnitt 4.4 in [ECGDSA] verwiesen.

Kollisionsresistenz-Eigenschaften grundsätzlich nicht mehr für die Erstellung von Signaturen verwendet werden. Siehe dazu auch Bemerkung 4.3 in [TR-02102-1]. Stattdessen sollte RSASSA nur in Verbindung mit PSS (siehe Abschnitte 8.1 und 9.1 in [RFC 8017]) und einer Hashfunktion aus der SHA-2-Familie verwendet werden.

Hinweis 2: Bei der Erstellung einer ECDSA-Signatur ist zu beachten, dass die Nonce k zufällig und gleichverteilt aus dem Intervall $[1, q-1]$ gewählt wird, wobei q die Ordnung des Basispunkts der elliptischen Kurve ist. Die Nonce ist ebenso wie der Langzeitschlüssel geheim zu halten und muss nach einmaliger Verwendung unmittelbar gelöscht werden. Die in IKEv2 zu signierenden Nachrichten werden in [RFC 7296] im Abschnitt 2.15 beschrieben. Die erstellte Signatur wird in der Authentication Payload übertragen.

Hinweis 3: Bei der Authentication Method Nr. 14 [RFC 7427] werden das Signaturverfahren und die Hashfunktion als ASN.1-Objekt direkt vor der eigentlichen Signatur innerhalb der Authentication Payload gespeichert. Das ASN.1-Objekt enthält die OIDs der eingesetzten Verfahren.

Die Technische Richtlinie [TR-02103] enthält Empfehlungen zu X.509-Zertifikaten und Zertifizierungspfadvalidierung.

3.3 IPsec

In diesem Abschnitt werden Vorgaben für die IPsec-Protokolle *Encapsulating Security Payload (ESP)* und *Authentication Header (AH)* gemacht. Es werden Vorgaben und Empfehlungen für die folgenden Sicherheitsziele festgelegt:

1. Schutz der Vertraulichkeit der ESP-Pakete durch Verschlüsselung
2. Integritätsschutz der ESP-Pakete
3. Integritätsschutz der AH-Pakete

3.3.1 Verschlüsselung der ESP-Pakete

Die Empfehlungen betreffen die Verschlüsselung des zu verschlüsselnden Bereichs von ESP-Paketen. Die Empfehlungen sind unabhängig davon, ob der Tunnel- oder Transportmodus von ESP verwendet wird. Für Details über die zu verschlüsselnden Bereiche wird auf die Abschnitte 3.1.1 und 3.1.2 in [RFC 4303] verwiesen.

Tabelle 8: Empfohlene Verschlüsselungsverfahren für ESP-Pakete

Nr.	Verfahren	IANA-Nr.	Spezifikation	AES-Schlüssellänge	Verwendung bis
1	ENCR_AES_CBC	12	[RFC 3602]	128 / 256	2030+
2	ENCR_AES_CTR	13	[RFC 3686]	128 / 256	2030+
3	ENCR_AES_GCM_16	20	[RFC 4106] [RFC 8247]	128 / 256	2030+
4	ENCR_AES_GCM_12	19	[RFC 4106] [RFC 8247]	128 / 256	2030+
5	ENCR_AES_CCM_16	16	[RFC 4309]	128 / 256	2030+
6	ENCR_AES_CCM_12	15	[RFC 4309]	128 / 256	2030+

Hinweis: Die ersten beiden Verfahren in Tabelle 8 müssen mit einem der in Abschnitt 3.3.2 genannten Verfahren zum Schutz der Integrität kombiniert werden. Bei Verwendung der Betriebsarten GCM und CCM muss ein separater Integritätsschutz der ESP-Pakete entfallen.

3.3.2 Integritätsschutz der ESP-Pakete

Die folgenden Empfehlungen betreffen den Integritätsschutz von ESP-Paketen. Die Empfehlungen sind unabhängig davon, ob der Tunnel- oder Transportmodus von ESP verwendet wird. Für Details über die zu sichernden Bereiche innerhalb des ESP-Pakets wird auf [RFC 4303], Abschnitt 3.1.1 und Abschnitt 3.1.2, verwiesen.

Tabelle 9: Empfohlene Verfahren für den Integritätsschutz der ESP-Pakete

Nr.	Verfahren	IANA-Nr.	Spezifikation	Verwendung bis
1	AUTH AES XCBC 96	5	[RFC 3566]	2030+
2	AUTH AES CMAC 96	8	[RFC 4494]	2030+
3	AUTH HMAC SHA2 256 128	12	[RFC 4868]	2030+
4	AUTH HMAC SHA2 384 192	13	[RFC 4868]	2030+
5	AUTH HMAC SHA2 512 256	14	[RFC 4868]	2030+

Für Neuentwicklungen wird eines der auf SHA-2 basierenden Verfahren (Nr. 3-5) in Tabelle 9 empfohlen.

3.3.3 Integritätsschutz der AH-Pakete

Die folgenden Empfehlungen betreffen die Berechnung des Integrity Check Values (ICV) für die Anwendung im IPsec-Protokoll *Authentication Header (AH)*. Die Empfehlungen sind unabhängig davon, ob der Tunnel- oder Transportmodus von AH verwendet wird. Für Details über die zu sichernden Bereiche innerhalb des AH-Pakets wird auf [RFC 4302], Abschnitt 3.1.1 und Abschnitt 3.1.2, verwiesen.

Tabelle 10: Empfohlene Verfahren für den Integritätsschutz der AH-Pakete

Nr.	Verfahren	IANA-Nr.	Spezifikation	Verwendung bis
1	AUTH AES XCBC 96	5	[RFC 3566]	2030+
2	AUTH AES CMAC 96	8	[RFC 4494]	2030+
3	AUTH HMAC SHA2 256 128	12	[RFC 4868]	2030+
4	AUTH HMAC SHA2 384 192	13	[RFC 4868]	2030+
5	AUTH HMAC SHA2 512 256	14	[RFC 4868]	2030+

Für Neuentwicklungen wird eines der auf SHA-2 basierenden Verfahren (Nr. 3-5) in Tabelle 10 empfohlen.

3.4 SA-Lifetime und Rekeying

Die Lebensdauer einer SA (SA-Lifetime) soll je nach Sicherheitsanforderung der Anwendung festgelegt werden; dies gilt sowohl für IKE-SAs als auch für IPsec-SAs. In gewöhnlichen Einsatzszenarien soll die IKE-SA-Lifetime maximal 24 h und die IPsec-SA-Lifetime maximal 4 h betragen. Für besondere Szenarien können nach Rücksprache mit einem Experten auch längere SA-Lifetimes verwendet werden.

Literaturverzeichnis

- [AIS 20/31] BSI: AIS 20/31 – A proposal for: Functionality classes for random number generators, 2011
- [ECGDSA] Erwin Hess, Marcus Schafheutle, Pascale Serf (Siemens AG): The Digital Signature Scheme ECGDSA, 2006, URL: https://www.teletrust.de/fileadmin/files/oid/ecgdsa_final.pdf
- [IANA] Internet Assigned Numbers Authority (IANA): Internet Key Exchange Version 2 (IKEv2) Parameters, URL: <https://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml>
- [RFC 2104] H. Krawczyk, M. Bellare, R. Canetti: RFC 2104, HMAC: Keyed-Hashing for Message Authentication, 1997
- [RFC 2404] C. Madson, R. Glenn: RFC 2404, The Use of HMAC-SHA-1-96 within ESP and AH, 1998
- [RFC 2409] D. Harkins, D. Carrel: RFC 2409, The Internet Key Exchange (IKE), 1998
- [RFC 3526] T. Kivinen, M. Kojo: RFC 3526, More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE), 2003
- [RFC 3566] S. Frankel, H. Herbert: RFC 3566, The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec, 2003
- [RFC 3602] S. Frankel, R. Glenn, S. Kelly: RFC 3602, The AES-CBC Cipher Algorithm and Its Use with IPsec, 2003
- [RFC 3686] R. Housley: RFC 3686, Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP), 2004
- [RFC 4055] J. Schaad, B. Kaliski, R. Housley: RFC 4055, Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, 2005
- [RFC 4106] J. Viega, D. McGrew: RFC 4106, The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP), 2005
- [RFC 4301] S. Kent, K. Seo: RFC 4301, Security Architecture for the Internet Protocol, 2005
- [RFC 4302] S. Kent: RFC 4302, IP Authentication Header, 2005
- [RFC 4303] S. Kent: RFC 4303, IP Encapsulating Security Payload (ESP), 2005
- [RFC 4306] C. Kaufman (Ed.): RFC 4306, Internet Key Exchange (IKEv2) Protocol, 2005
- [RFC 4307] J. Schiller: RFC 4307, Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2), 2005
- [RFC 4308] P. Hoffman: RFC 4308, Cryptographic Suites for IPsec, 2005
- [RFC 4309] R. Housley: RFC 4309, Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP), 2005
- [RFC 4494] JH. Song, R. Poovendran, J. Lee: RFC 4494, The AES-CMAC-96 Algorithm and Its Use with IPsec, 2006
- [RFC 4543] D. McGrew, J. Viega: RFC 4543, The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH, 2006
- [RFC 4615] J. Song, R. Poovendran, J. Lee, T. Iwata: RFC 4615, The Advanced Encryption Standard-Cipher-based Message Authentication Code-Pseudo-Random Function-128 (AES-CMAC-PRF-128) Algorithm for the Internet Key Exchange Protocol (IKE), 2006
- [RFC 4718] P. Eronen, P. Hoffman: RFC 4718, IKEv2 Clarifications and Implementation Guidelines, 2006

- [RFC 4754] D. Fu, J. Solinas: RFC 4754, IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA), 2007
- [RFC 4835] V. Manral: RFC 4835, Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH), 2007
- [RFC 4868] S. Kelly, S. Frankel: RFC 4868, Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec, 2007
- [RFC 5114] M. Lepinski, S. Kent: RFC 5114, Additional Diffie-Hellman Groups for Use with IETF Standards, 2008
- [RFC 5282] D. Black, D. McGrew: RFC 5282, Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol, 2008
- [RFC 5903] D. Fu, J. Solinas: RFC 5903, Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2, 2010
- [RFC 5930] S. Shen, Y. Mao, NSS. Murthy: RFC 5930, Using Advanced Encryption Standard Counter Mode (AES-CTR) with the Internet Key Exchange version 02 (IKEv2) Protocol, 2010
- [RFC 5996] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen: RFC 5996, Internet Key Exchange Protocol Version 2 (IKEv2), 2010
- [RFC 5998] P. Eronen, H. Tschofenig, Y. Sheffer: RFC 5998, An Extension for EAP-Only Authentication in IKEv2, 2010
- [RFC 6954] J. Merkle, M. Lochter: RFC 6954, Using the Elliptic Curve Cryptography (ECC) Brainpool Curves for the Internet Key Exchange Protocol Version 2 (IKEv2), 2013
- [RFC 6989] Y. Sheffer, S. Fluhrer: RFC 6989, Additional Diffie-Hellman Tests for the Internet Key Exchange Protocol Version 2 (IKEv2), 2013
- [RFC 7296] C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, T. Kivinen: RFC 7296, Internet Key Exchange Protocol Version 2 (IKEv2), 2014
- [RFC 7321] D. McGrew, P. Hoffman: RFC 7321, Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH), 2014
- [RFC 7427] T. Kivinen, J. Snyder: RFC 7427, Signature Authentication in the Internet Key Exchange Version 2 (IKEv2), 2015
- [RFC 8017] K. Moriarty, B. Kaliski, J. Jonsson, A. Rusch: RFC 8017, PKCS #1: RSA Cryptography Specification Version 2.2, 2016
- [RFC 8221] P. Wouters, D. Migault, J. Mattsson, Y. Nir, T. Kivinen: RFC 8221, Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH), 2017
- [RFC 8247] Y. Nir, T. Kivinen, P. Wouters, D. Migault: RFC 8247, Algorithm Implementation Requirements and Usage Guidance for the Internet Key Exchange Protocol Version 2 (IKEv2), 2017
- [Teletrust] Teletrust: OID-Datenbank. URL: https://www.teletrust.de/fileadmin/docs/projekte/oid/OID-Liste_1_3_36_3_3.pdf
- [TR-02102-1] BSI: Technische Richtlinie TR-02102-1, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, 2024
- [TR-02103] BSI: Technische Richtlinie TR-02103, X.509 Zertifikate und Zertifizierungspfadvalidierung, Version 1.0, 2020
- [TR-03111] BSI: Technical Guideline TR-03111, Elliptic Curve Cryptography, Version 2.10, 2018