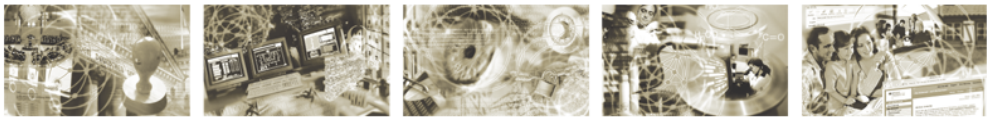
Bundesamt
für Sicherheit in der
Informationstechnik



Technische Richtlinie TR-02102-3

Kryptographische Verfahren: Empfehlungen und Schlüssellängen

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

(Version 2017-01)

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
E-Mail: TR02102@bsi.bund.de
Internet: https://www.bsi.bund.de
© Bundesamt für Sicherheit in der Informationstechnik 2017

Änderungshistorie

Dokument-Version	Wichtige Änderungen
2015-01	Anpassung der Verwendungszeiträume
2015-02	Empfehlung neuer Authentisierungs-Verfahren für IKEv2 auf Basis von RFC 7427 in Abschnitt 3.2.5
2016-01	Anpassung der Verwendungszeiträume, RFC 4835 wird durch RFC 7321 ersetzt, elliptische Kurven mit 224 Bit werden abgekündigt
2017-01	Anpassung der Verwendungszeiträume, Ankündigung der Erhöhung des Sicherheitsniveaus auf 120 Bit ab 2023, Ankündigung der Erhöhung der Bitlängen von RSA, DH und DSA auf 3000 Bit ab 2023

Inhaltsverzeichnis

Tabellenverzeichnis

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 Schutzzielen 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 und 7427 (siehe Hinweis

unten). Für IPsec gelten beispielsweise die RFCs 4106, 4301, 4302, 4303, 4307, 4308, 4309, 4543 und 7321 (ersetzt RFC 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, siehe Hinweis unten) besonders wichtig, da er eine umfangreiche Überarbeitung von vorigen Standards sowie Klarstellungen aus RFC 4718 enthält.

Hinweis: Der RFC 7296 ist im Oktober 2014 veröffentlicht worden und ersetzt die bisherige IKEv2-Spezifikation in RFC 5996. Für die Änderungen gegenüber RFC 5996 siehe Abschnitt 1.8 in RFC 7296. Die Verwendung des neuen RFCs wird empfohlen.

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. IP-Sec-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 [RFC7296] verwiesen.

Für Details zum IKE-Ablauf wird auf das IETF-Dokument [RFC7296] 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-Random-Function (PRF).

Die Berechnung für das Schlüsselmaterial für die IKA-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-Random-Function (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 $\mathbb{Z}_p^x$ oder elliptische Kurvenparameter zusammen mit einem Basispunkt als Generator einer Untergruppe der Punktegruppe. Es werden dabei lediglich die standardisierten Bezeichner einer DH-Gruppe übertragen. Für die Bezeichner gelten standardisierte Werte, die 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 unverhersagbar erzeugt, und darf nur einmal verwendet werden.

Die Nonce-Werte `Ni` und `Nr` 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 [RFC7296]):

- Das *Diffie-Hellman shared secret* `g^ir`
- Die Größe *`SKEYSEED := prf(Ni | Nr, g^ir)`*

  Die Nonce-Werte `Ni` und `Nr` sind in der `IKE_SA_INIT`-Nachricht vom Initiator zum Responder übertragen worden (`Ni` an Responder) und umgekehrt (`Nr` 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-Random-Funktion.

- Aus `SKEYSEED`, den Nonces `Ni` und `Nr` sowie den SPI-Werten[2] 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.

  `prf+` bedeutet gemäß [RFC7296], Abschnitt 2.13 die iterierte Anwendung der vereinbarten Pseudo-Random-Function, 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:

1 Im Zusammenhang mit der Verwendung von elliptischen Kurven zur Schlüsselvereinbarung sei auf RFC6954 [RFC6954], 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]

Schlüssel	*Verwendung*
SK_d	Ableitung von Schlüsseln für Child-SAs
SK_ei	Symmetrischer Schlüssel zur Verschlüsselung aller weiteren IKE-Nachrichten (IKE_AUTH, CREATE_CHILD_SA, INFORMATIONAL) vom Initiator zum Responder
SK_ai	Schlüssel für den Integritätsschutz aller weiteren IKE-Nachrichten (IKE_AUTH, CREATE_CHILD_SA, INFORMATIONAL) vom Initiator zum Responder
SK_er	Symmetrischer Schlüssel zur Verschlüsselung aller weiteren IKE-Nachrichten (IKE_AUTH, CREATE_CHILD_SA, INFORMATIONAL) vom Responder zum Initiator
SK_ar	Schlüssel für den Integritätsschutz aller weiteren IKE-Nachrichten (IKE_AUTH, CREATE_CHILD_SA, INFORMATIONAL) vom Responder zum Initiator
SK_pi	Schlüssel zur Generierung der AUTH-Payload zur Authentisierung des Initiators beim Responder (beim IKE_AUTH-Exchange). Vgl. auch Abschnitt 2.15 in [RFC7296].
SK_pr	Schlüssel zur Generierung der AUTH-Payload zur Authentisierung des Responders beim Initiator (beim IKE_AUTH-Exchange). Vgl. auch Abschnitt 2.15 in [RFC7296].

Tabelle 1: Übersicht der wichtigsten Schlüssel

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-Funktion gewählt werden.

2.1.2 Lifetime

Eine IKE-SA als auch eine IPsec-SA 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 [RFC4301], Abschnitt 4.4.2.1, muss eine IPsec-Implementierung beide Kriterien unterstützen, wobei das Zeitkriterium vorrangig zum Volumenkriterium zu behandeln ist. 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 [RFC7296]).

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 [RFC7296] 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 [AIS20/31], vgl. auch Kapitel 9 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 [RFC7296] *optional* unter Verwendung eines erneuten Diffie-Hellman-Schlüsselaustausches geschehen. Dazu werden nach Abschnitt 1.3.1 in [RFC7296] die öffentlichen Diffie-Hellman-Schlüssel zwischen Initiator und Responder übertragen und anschließend auf beiden Seiten das gemeinsame Diffie-Hellman-Geheimnis berechnet, welches gemäß [RFC7296], 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 [RFC4302] (für AH) sowie auf [RFC4303] (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 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.

Eine genaue Beschreibung der beiden Betriebsmodi für AH findet sich in [RFC4302] in den Abschnitten 3.1.1 und 3.1.2. [RFC4303] 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 [RFC4301]). 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 [RFC4301] 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. Es liegt zurzeit bei 100 Bit.

Hinweis: Ab dem Jahr 2023 wird ein Sicherheitsniveau von 120 Bit angestrebt. Siehe dazu auch Abschnitt 1.1 in [TR-02102-1].

3.1.3 Schlüssellängen bei Verfahren mit elliptischen Kurven

Für einen Einsatzzeitraum bis Ende 2022 sind die Schlüssellängen bei Verfahren, die auf elliptischen Kurven basieren, etwas größer (im Vergleich zu RSA) gewählt worden, um einen Sicherheitsspielraum für diese Verfahren zu erreichen. Für eine Begründung und weitere Erläuterungen siehe Bemerkung 4, Kapitel 3 in [TR-02102-1].

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 Empfohlene Verschlüsselungsverfahren für den Schutz 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:

Lfd. Nr.	*Verfahren*	*IANA-Nr.*	*Spezifiziert in*	*Schlüssellänge von SK_ei und SK_er*	*Verwendungszeitraum*
1	ENCR_AES_CBC	12	[RFC7296]	128	2023+
2	ENCR_AES_CTR	13	[RFC5930]	128	2023+
3	AES-GCM with a 16 octet ICV	20	[RFC5282]	128/256	2023+
4	AES-GCM with a 12 octet ICV	19	[RFC5282]	128/256	2023+

Tabelle 2: Empfohlene Verschlüsselungsverfahren

Hinweis: Die ersten beiden Verfahren in Tabelle 2 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 zur Betriebsart GCM siehe Abschnitt 2.1.2 in [TR-02102-1]. Wird diese Betriebsart eingesetzt, darf gemäß Abschnitt 8 in [RFC5282] kein Algorithmus zum Integritätsschutz der übertragenen Nachrichten verwendet werden.

3.2.2 Empfohlene Pseudo-Zufallsfunktionen 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:

Lfd. Nr.	*Verfahren*	*IANA-Nr.*	*Spezifiziert in*	*Verwendungszeitraum*
1	PRF_AES128_XCBC	4	[RFC4434]	2023+
2	PRF_AES128_CMAC	8	[RFC4615]	2023+
3	PRF_HMAC_SHA1	2	[RFC2104]	2018+
4	PRF_HMAC_SHA2_256	5	[RFC4868]	2023+
5	PRF_HMAC_SHA2_384	6		
6	PRF_HMAC_SHA2_512	7		

Tabelle 3: Empfohlene PRFs zur Erzeugung von Schlüsselmaterial

Hinweis: Die Länge des erzeugten Schlüssels (Ausgabelänge der PRF) muss mindestens so groß sein wie die empfohlene Schlüssellänge des eingesetzten Verschlüsselungs-Verfahrens aus Tabelle 2. Es ist zu beachten, dass die PRF gemäß Abschnitt 2.13 in [RFC7296] ggf. mehrfach iterativ aufgerufen werden muss.

Bei Verwendung der Verfahren Nr. 1 und Nr. 2 aus Tabelle 3 müssen die entsprechenden Hinweise aus Abschnitt 2.14 in [RFC7296] beachtet werden.

3.2.3 Empfohlene Verfahren zum Integritätsschutz der IKE-Nachrichten

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

Lfd. Nr.	*Verfahren*	*IANA-Nr.*	*Spezifiziert in*	*Verwendungs-zeitraum*
1	AUTH_HMAC_SHA1_96	2	[RFC7296]	2018+
2	AUTH_AES_XCBC_96	5	[RFC7296]	2023+
3	AUTH_HMAC_SHA2_256_128	12	[RFC4868]	2023+
4	AUTH_HMAC_SHA2_384_192	13		
5	AUTH_HMAC_SHA2_512_256	14		

Tabelle 4: Empfohlene Verfahren zum Integritätsschutz

Hinweis: Die Schlüssellänge für die in Tabelle 4 genannten Verfahren muss mindestens den geforderten Schlüssellängen in den jeweils angegebenen RFCs entsprechen.

Für Neuentwicklungen wird eines der auf SHA-2 basierenden Verfahren (Nr. 3-5) in Tabelle 4 empfohlen.

3.2.4 Empfohlene Gruppen für den Diffie-Hellman-Schlüsselaustausch

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

Lfd. Nr.	*Name*	*IANA-Nr.*	*Spezifiziert in*	*Verwendung bis*
1	2048-bit MODP Group	14	[RFC3526]	2022
2	3072-bit MODP Group	15	[RFC3526]	2023+
3	4096-bit MODP Group	16	[RFC3526]	2023+
4	256-bit random ECP group	19	[RFC5903]	2023+
5	384-bit random ECP group	20	[RFC5903]	2023+
6	521-bit random ECP group	21	[RFC5903]	2023+
7	2048-bit MODP Group with 256-bit Prime Order Subgroup	24	[RFC5114]	2022
8	brainpoolP256r1	28	[RFC6954]	2023+
9	brainpoolP384r1	29		
10	brainpoolP512r1	30		

Tabelle 5: Empfohlene Gruppen für den Diffie-Hellman-Schlüsselaustausch

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 [RFC6989]) wird empfohlen. Diese Tests werden besonders beim Einsatz von elliptischen Kurven empfohlen; siehe dazu Abschnitt 2.3 in [RFC6989].

Hinweis 4: Bei den elliptischen Kurven mit den IANA-Nr. 19, 20 und 21 handelt es sich um NIST-Kurven. In Tabelle 5 werden die IANA-Bezeichnungen verwendet. Für alternative Bezeichnungen der Kurven (z. B. von NIST) siehe Kapitel 5 in [RFC4753].

Hinweis 5: Die Verfahren Nr. 1 und Nr. 7 werden nur noch bis zum Jahr 2022 empfohlen. Ab dem Jahr 2023 werden Schlüssellängen von mindestens 3000 Bit für diese Verfahren empfohlen. Siehe dazu auch Kapitel 3.1.2.

3.2.5 Empfohlene Authentisierungs-Verfahren

Im Januar 2015 wurde [RFC7427] veröffentlicht. In diesem Dokument wird eine breite Unterstützung von Signaturverfahren und Hashfunktionen spezifiziert. Mit diesem RFC ist es nun bei IKEv2 möglich, weitere elliptischen Kurven, neue Hashfunktionen sowie weitere Signaturverfahren einzusetzen.

Bisher waren der Signaturalgorithmus und die Hashfunktion fest verbunden und mit nur *einer gemeinsamen* IANA-Nummer für die Authentication Method versehen (siehe [IANA1]). Daher wurde in [RFC7427] die Authentication Method Nr. 14 eingeführt; hierbei 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.

Es werden folgende Authentisierungs-Verfahren empfohlen:

Lfd. Nr.	*Verfahren*	*Bitlänge*	*Hash-Funktion*	*IANA-Nr. der Authentication Method*	*Spezifiziert in*	*Verwendungszeitraum*
1	ECDSA-256 mit Kurve secp256r1	256	SHA-256	9	[RFC4753] und [RFC4754]	2023+
2	ECDSA-384 mit Kurve secp384r1	384	SHA-384	10		
3	ECDSA-512 mit Kurve secp521r1	512	SHA-512	11		
4	ECDSA-256 mit Kurve brainpoolP256r1	256	SHA-256	14	[RFC7427]	2023+
5	ECDSA-384 mit Kurve brainpoolP384r1	384	SHA-384			
6	ECDSA-512 mit Kurve brainpoolP512r1	512	SHA-512			
7	RSASSA-PSS	2048	SHA-256	14	[RFC7427] und [RFC4055]	2022
8	RSASSA-PSS	4096	SHA-384	14	[RFC7427] und [RFC4055]	2023+
9	ECGDSA-256 mit Kurve brainpoolP256r1[3]	256	SHA-256	14	[RFC7427]	2023+
10	ECGDSA-384 mit Kurve brainpoolP384r1[3]	384	SHA-384			
11	ECGDSA-512 mit Kurve brainpoolP512r1[3]	512	SHA-512			

Tabelle 6: Empfohlene Authentisierungs-Verfahren

Hinweis 1: Die Verfahren RSA (IANA-Nr. 1) und DSS (IANA-Nr. 3) sind in [RFC7296] nur in Verbindung mit der Hashfunktion SHA-1 spezifiziert. SHA-1 sollte aber aufgrund von Angriffen gegen seine Kollisionsresistenz-Eigenschaften grundsätzlich nicht mehr für die Erstellung von Signaturen verwendet werden. Siehe dazu auch Bemerkung 13, Kapitel 4 in [TR-02102-1]. Stattdessen sollte RSASSA nur in Verbindung mit PSS (siehe Abschnitte 8.1 und 9.1 in [RFC3447]) 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 [RFC7296] im Abschnitt 2.15 beschrieben. Die erstellte Signatur wird in der Authentication Payload übertragen.

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.

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 [RFC4303] verwiesen.

Lfd. Nr.	*Verfahren*	*IANA-Nr.*	*Spezifiziert in*	*Bemerkungen*	*Verwendungszeitraum*
1	ENCR_AES_CBC	12	[RFC3602]	Muss mit einem Verfahren aus Abschnitt 3.3.2 kombiniert werden.	2023+
2	ENCR_AES_CTR	13	[RFC3686]		
3	AES-GCM with a 16 octet ICV	20	[RFC4106]	Bei Verwendung der Betriebsart GCM kann ein separater Integritätsschutz der ESP-Pakete entfallen.	2023+
4	AES-GCM with a 12 octet ICV	19			

Tabelle 7: Verschlüsselung der ESP-Pakete

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 [RFC4303], Abschnitt 3.1.1 und Abschnitt 3.1.2, verwiesen.

Lfd. Nr.	*Verfahren*	*IANA-Nr.*	*Spezifiziert in*	*Verwendungszeitraum*
1	AUTH_HMAC_SHA1_96	2	[RFC2404]	2018+
2	AUTH_AES_XCBC_96	5	[RFC3566]	2023+
3	AUTH_AES_CMAC_96	8	[RFC4494]	2023+
4	AUTH_HMAC_SHA2_256_128	12	[RFC4868]	2023+
5	AUTH_HMAC_SHA2_384_192	13		
6	AUTH_HMAC_SHA2_512_256	14		

Tabelle 8: Integritätsschutz der ESP-Pakete

Für Neuentwicklungen wird eines der auf SHA-2 basierenden Verfahren (Nr. 4-6) in Tabelle 8 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 [RFC4302], Abschnitt 3.1.1 und Abschnitt 3.1.2, verwiesen.

Lfd. Nr.	*Verfahren*	*IANA-Nr.*	*Spezifiziert in*	*Verwendungszeitraum*
1	AUTH_HMAC_SHA1_96	2	[RFC2404]	2018+
2	AUTH_AES_XCBC_96	5	[RFC3566]	2023+
3	AUTH_AES_CMAC_96	8	[RFC4494]	2023+
4	AUTH_HMAC_SHA2_256_128	12	[RFC4868]	2023+
5	AUTH_HMAC_SHA2_384_192	13		2023+
6	AUTH_HMAC_SHA2_512_256	14		2023+

Tabelle 9: Integritätsschutz der AH-Pakete

Für Neuentwicklungen wird eines der auf SHA-2 basierenden Verfahren (Nr. 4-6) in Tabelle 9 empfohlen.

3.4 SA-Lifetime und Re-Keying

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. Dabei soll die IKE-SA- Lifetime maximal 24 h und die IPSsec-SA-Lifetime maximal 4 h betragen.

4 Literaturverzeichnis

AIS20/31	BSI: W. Killmann, W. Schindler, 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 (abgerufen am 08.05.2015)
IANA	Internet Assigned Numbers Authority (IANA): Internet Key Exchange Version 2 (IKEv2) Parameters, Transform Type 4 - Diffie-Hellman Group Transform IDs, URL: http://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml#ikev2-parameters-8
IANA1	Internet Assigned Numbers Authority (IANA): Internet Key Exchange Version 2 (IKEv2) Parameters, IKEv2 Authentication Method, URL: http://www.iana.org/assignments/ikev2-parameters/ikev2-parameters.xhtml#ikev2-parameters-12

RFC2104	H. Krawczyk, M. Bellare, R. Canetti: RFC 2104, HMAC: Keyed-Hashing for Message Authentication, 1997
RFC2404	C. Madson, R. Glenn: RFC 2404, The Use of HMAC-SHA-1-96 within ESP and AH, 1998
RFC2409	D. Harkins, D. Carrel: RFC 2409, The Internet Key Exchange (IKE), 1998
RFC3447	J. Jonsson, B. Kaliski: RFC 3447, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, 2003
RFC3526	T. Kivinen, M. Kojo: RFC 3526, More Modular Exponential (MODP) Diffie-Hellman groups for Internet Key Exchange (IKE), 2003
RFC3566	S. Frankel, H. Herbert: RFC 3566, The AES-XCBC-MAC-96 Algorithm and Its Use With IPsec, 2003
RFC3602	S. Frankel, R. Glenn, S. Kelly: RFC 3602, The AES-CBC Cipher Algorithm and Its Use with IPsec, 2003
RFC3686	R. Housley: RFC 3686, Using Advanced Encryption Standard (AES) Counter Mode With IPsec Encapsulating Security Payload (ESP), 2004
RFC4055	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
RFC4106	J. Viega, D. McGrew: RFC 4106, The Use of Galois/Counter Mode (GCM) in IPsec Encapsulating Security Payload (ESP), 2005
RFC4301	S. Kent, K. Seo: RFC 4301, Security Architecture for the Internet Protocol, 2005
RFC4302	S. Kent: RFC 4302, IP Authentication Header, 2005
RFC4303	S. Kent: RFC 4303, IP Encapsulating Security Payload (ESP), 2005
RFC4306	C. Kaufman (Ed.): RFC 4306, Internet Key Exchange (IKEv2) Protocol, 2005
RFC4307	J. Schiller: RFC 4307, Cryptographic Algorithms for Use in the Internet Key Exchange Version 2 (IKEv2), 2005
RFC4308	P. Hoffman: RFC 4308, Cryptographic Suites for IPsec, 2005
RFC4309	R. Housley: RFC 4309, Using Advanced Encryption Standard (AES) CCM Mode with IPsec Encapsulating Security Payload (ESP), 2005
RFC4494	JH. Song, R. Poovendran, J. Lee: RFC 4494, The AES-CMAC-96 Algorithm and Its Use with IPsec, 2006
RFC4543	D. McGrew, J. Viega: RFC 4543, The Use of Galois Message Authentication Code (GMAC) in IPsec ESP and AH, 2006
RFC4615	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
RFC4718	P. Eronen, P. Hoffman: RFC 4718, IKEv2 Clarifications and Implementation Guidelines, 2006
RFC4753	D. Fu, J. Solinas: RFC 4753, ECP Groups for IKE and IKEv2, 2007

RFC4754	D. Fu, J. Solinas: RFC 4754, IKE and IKEv2 Authentication Using the Elliptic Curve Digital Signature Algorithm (ECDSA), 2007
RFC4835	V. Manral: RFC 4835, Cryptographic Algorithm Implementation Requirements for Encapsulating Security Payload (ESP) and Authentication Header (AH), 2007
RFC4868	S. Kelly, S. Frankel: RFC 4868, Using HMAC-SHA-256, HMAC-SHA-384, and HMAC-SHA-512 with IPsec, 2007
RFC5114	M. Lepinski, S. Kent: RFC 5114, Additional Diffie-Hellman Groups for Use with IETF Standards, 2008
RFC5282	D. Black, D. McGrew: RFC 5282, Using Authenticated Encryption Algorithms with the Encrypted Payload of the Internet Key Exchange version 2 (IKEv2) Protocol, 2008
RFC5903	D. Fu, J. Solinas: RFC 5903, Elliptic Curve Groups modulo a Prime (ECP Groups) for IKE and IKEv2, 2010
RFC5930	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
RFC5996	C. Kaufman, P. Hoffman, Y. Nir, P. Eronen: RFC 5996, Internet Key Exchange Protocol Version 2 (IKEv2), 2010
RFC5998	P. Eronen, H. Tschofenig, Y. Sheffer: RFC 5998, An Extension for EAP-Only Authentication in IKEv2, 2010
RFC6954	J. Merkle, M. Lochter: RFC 6954, Using the Elliptic Curve Cryptography (ECC) Brainpool Curves for the Internet Key Exchange Protocol Version 2 (IKEv2), 2013
RFC6989	Y. Sheffer, S. Fluhrer: RFC 6989, Additional Diffie-Hellman Tests for the Internet Key Exchange Protocol Version 2 (IKEv2), 2013
RFC7296	C. Kaufman, P. Hoffman, Y. Nir, P. Eronen, T. Kivinen: RFC 7296, Internet Key Exchange Protocol Version 2 (IKEv2), 2014
RFC7321	D. McGrew, P. Hoffman: RFC 7321, Cryptographic Algorithm Implementation Requirements and Usage Guidance for Encapsulating Security Payload (ESP) and Authentication Header (AH), 2014
RFC7427	T. Kivinen, J. Snyder: RFC 7427, Signature Authentication in the Internet Key Exchange Version 2 (IKEv2), 2015
Teletrust	Teletrust: OID-Datenbank. URL: https://www.teletrust.de/projekte/oid/
TR-02102-1	BSI: Technische Richtlinie TR-02102-1, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, 2017
TR-03111	BSI: Technical Guideline TR-03111, Elliptic Curve Cryptography, Version 2.0, 2012