Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Technische Richtlinie TR-02102-4 Kryptographische Verfahren: Empfehlungen und Schlüssellängen

Teil 4 – Verwendung von Secure Shell (SSH)

Änderungshistorie

Tabelle 1: Änderungshistorie

Version	***Datum***	***Beschreibung***
2019-01	22.02.2019	Anpassung der Verwendungszeiträume, Empfehlung von Diffie-Hellman Gruppen aus RFC 8268
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, Abkündigung der Empfehlung von DSA ab 2029

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-0
E-Mail: TR02102@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhalt

1 Einleitung

Diese Technische Richtlinie gibt Empfehlungen für den Einsatz des kryptographischen Protokolls *Secure Shell (SSH)*. Mit diesem Protokoll kann ein sicherer Kanal in einem unsicheren Netzwerk aufgebaut werden. Die gängigsten Anwendungen des SSH-Protokolls sind das Anmelden auf einem entfernten System (remote command-line login) und das Ausführen von Befehlen bzw. Applikationen auf entfernten Systemen.

Die vorliegende Technische Richtlinie enthält Empfehlungen für die zu verwendende Protokollversion und die kryptographischen Algorithmen als Konkretisierung der allgemeinen Empfehlungen in Teil 1 dieser Technischen Richtlinie (siehe [TR-02102-1]).

Diese Richtlinie enthält keine Empfehlungen für konkrete Anwendungen, keine Risikobewertungen sowie keine Angriffsmöglichkeiten, die sich aus Fehlern in der Implementierung des Protokolls ergeben.

Hinweis: Auch bei Beachtung aller Empfehlungen für die Verwendung von SSH können Daten in erheblichem Umfang aus einem kryptographischen System abfließen, zum Beispiel durch Ausnutzung von Seitenkanälen (Messung von Timing-Verhalten, Stromaufnahme, Datenraten etc.). 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].

2 Grundlagen

Das SSH-Protokoll besteht aus den drei Unter-Protokollen *Transport Layer Protocol*, *User Authentication Protocol* und *Connection Protocol*.

Das Transport Layer Protocol (siehe [RFC 4253]) ermöglicht Serverauthentisierung, Verschlüsselung, Integritätssicherung und optional Datenkompression. Es setzt logisch auf dem TCP/IP-Protokoll auf.

Das User Authentication Protocol (siehe [RFC 4252]) ist dafür da, den Benutzer gegenüber dem Server zu authentisieren. Es setzt auf dem Transport Layer Protocol auf.

Das Connection Protocol (siehe [RFC 4254]) ist für die Erzeugung und Verwaltung logischer Kanäle innerhalb des verschlüsselten Tunnels zuständig. Es setzt auf dem User Authentication Protocol auf.

Für weitergehende Informationen über die Protokollarchitektur von SSH siehe [RFC4251].

Die umfangreiche Spezifikation des SSH-2-Protokolls (siehe Abschnitt 3.2) findet sich in folgenden RFCs:

- RFC 4250: The Secure Shell (SSH) Protocol Assigned Numbers (Januar 2006)
- RFC 4251: The Secure Shell (SSH) Protocol Architecture (Januar 2006)
- RFC 4252: The Secure Shell (SSH) Authentication Protocol (Januar 2006)
- RFC 4253: The Secure Shell (SSH) Transport Layer Protocol (Januar 2006)
- RFC 4254: The Secure Shell (SSH) Connection Protocol (Januar 2006)
- RFC 4256: Generic Message Exchange Authentication for the Secure Shell Protocol (SSH) (Januar 2006)
- RFC 4335: The Secure Shell (SSH) Session Channel Break Extension (Januar 2006)
- RFC 4344: The Secure Shell (SSH) Transport Layer Encryption Modes (Januar 2006)

Die folgenden RFCs enthalten Erweiterungen und Ergänzungen des SSH-Protokolls:

- RFC 4255: Using DNS to Securely Publish Secure Shell (SSH) Key Fingerprints (Januar 2006)
- RFC 4419: Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol (März 2006)
- RFC 4432: RSA Key Exchange for the Secure Shell (SSH) Transport Layer Protocol (März 2006)
- RFC 4462: Generic Security Service Application Program Interface (GSS-API) Authentication and Key Exchange for the Secure Shell (SSH) Protocol (Mai 2006)
- RFC 4716: The Secure Shell (SSH) Public Key File Format (November 2006)
- RFC 4819: Secure Shell Public Key Subsystem (März 2007)
- RFC 5647: AES Galois Counter Mode for the Secure Shell Transport Layer Protocol (August 2009)
- RFC 5656: Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer (Dezember 2009)
- RFC 6187: X.509v3 Certificates for Secure Shell Authentication (März 2011)
- RFC 6239: Suite B Cryptographic Suites for Secure Shell (SSH) (Mai 2011)
- RFC 6594: Use of the SHA-256 Algorithm with RSA: Digital Signature Algorithm (DSA): and Elliptic Curve DSA (ECDSA) in SSHFP Resource Records (April 2012)
- RFC 6668: SHA-2 Data Integrity Verification for the Secure Shell (SSH) Transport Layer Protocol (Juli 2012)
- RFC 8268: More Modular Exponentiation (MODP) Diffie-Hellman (DH) Key Exchange (KEX) Groups for Secure Shell (SSH) (Dezember 2017)

- RFC 8270: Increase the Secure Shell Minimum Recommended Diffie-Hellman Modulus Size to 2048 Bits (Dezember 2017)
- RFC 9142: Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH) (Januar 2022)

3 Empfehlungen

Dieses Kapitel enthält Empfehlungen für die Verwendung des SSH-Protokolls. Diese beziehen sich auf die zu verwendenden kryptographischen Verfahren und die SSH-Versionen. Die vorliegende Technische Richtlinie enthält keine Konfigurationsanleitungen für konkrete Implementierungen des SSH-Protokolls, sondern grundsätzliche kryptographische Empfehlungen, die für alle SSH-Implementierungen verwendet werden können.

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 SSH-Versionen

Im Jahr 1995 wurde die erste Version des SSH-Protokolls von Tatu Ylönen, einem Forscher an der Helsinki University of Technology, entwickelt. Diese Version wird heute SSH-1 genannt. Im Jahr 2006 wurde eine überarbeitete Version des Protokolls als Internet Standard (RFC) durch die IETF verabschiedet; diese Version heißt SSH-2.

Es gelten folgende Empfehlungen für die Auswahl der SSH-Protokollversion:

- Die Verwendung von SSH-2 wird empfohlen.
- Der Einsatz von SSH-1 wird **nicht empfohlen**, da diese Protokollversion kryptographische Schwächen enthält.

3.2.1 Konformität zur SSH-Spezifikation

Die Spezifikation des SSH-Protokolls enthält kryptographische Algorithmen, die von standardkonformen Anwendungen unterstützt werden müssen. In der vorliegenden Technischen Richtlinie werden davon möglicherweise nicht alle empfohlen.

Wenn eine Anwendung vollständig konform zur SSH-Spezifikation sein muss, dann sollte wie folgt vorgegangen werden: Die Anwendung sollte die im vorliegenden Dokument empfohlenen Algorithmen *und* die in der Spezifikation festgelegten Verfahren unterstützen, aber so konfiguriert sein, dass die hier empfohlenen (kryptographisch starken) Algorithmen mit hoher Priorität und die (möglicherweise kryptographisch schwachen oder veralteten) Algorithmen aus der SSH-Spezifikation mit niedriger Priorität bzw. nach Möglichkeit nicht verwendet werden.

3.3 Schlüsseleinigung

Im Rahmen des SSH-Verbindungsaufbaus wird ein Schlüsselaustausch (Key Exchange) durchgeführt, um gemeinsame Sitzungsschlüssel für die Authentisierung und die Verschlüsselung zu erzeugen und auszutauschen.

Folgende Key Exchange Methods werden empfohlen:

Tabelle 2: Empfohlene Key Exchange Methods

Nr.	*Key Exchange Method*	*Spezifikation*	*Verwendung bis*
1	`diffie-hellman-group-exchange-sha256`	[RFC 4419], Abschnitt 4.2 [RFC 8270]	2030+
2	`diffie-hellman-group15-sha512`	[RFC 8268]	2030+
3	`diffie-hellman-group16-sha512`	[RFC 8268]	2030+
4	`ecdh-sha2-nistp256`	[RFC 5656]	2030+
5	`ecdh-sha2-nistp384`	[RFC 5656]	2030+
6	`ecdh-sha2-nistp521`	[RFC 5656]	2030+

Bemerkung zu Key Exchange Method Nr. 1: Unter Verwendung der Bezeichnungen aus Kapitel 3 in [RFC 4419]:

1. Die Länge der Primzahl p soll mindestens 3000 Bit betragen (siehe dazu auch Abschnitt 2.3.5 in [TR-02102-1]).
2. Die Ordnung des Erzeugers g soll mindestens 2^{250} groß sein (siehe dazu auch Abschnitt 2.3.5 in [TR-02102-1]).
3. Gemäß Kapitel 3 in [RFC 4419] soll p eine Safe Prime sein, das heißt mit $p = 2q+1$ sind sowohl p als auch q prim.

Da p eine Safe Prime ist, gilt $p-1 = 2q$, das heißt die Ordnung des Erzeugers g kann nur 2 oder q sein. Beachtet man die Empfehlung in Punkt 2, so bleibt nur q als mögliche Ordnung übrig. Aufgrund der zusätzlichen Forderung in Punkt 3 (Safe Prime) ist die Bitlänge von q viel größer als in Punkt 2 mindestens empfohlen wird. Dieser Umstand ist zu akzeptieren, wenn die Implementierung konform zu [RFC 4419], [TR-02102-1] und der vorliegenden Technischen Richtlinie sein soll.

Hinweis: Bei dieser Key Exchange Method muss SHA-256 auch für die key derivation pseudo-random function (PRF) verwendet werden.

Bemerkung zu Key Exchange Methods Nr. 4-6: Die zugehörige Hashfunktion aus der SHA-2-Familie muss in Abhängigkeit der Bitlänge der Kurve gemäß Abschnitt 6.2.1 in [RFC 5656] gewählt werden.

3.3.1 Key Re-Exchange

Es ist sinnvoll, das Schlüsselmaterial einer Verbindung nach einer bestimmten Zeit oder einer bestimmten Menge übertragener Daten zu erneuern, um einen Angriff auf die Sitzungsschlüssel zu erschweren. Bei SSH kann das Erneuern der Sitzungsschlüssel durch das Senden der Nachricht `SSH_MSG_KEXINIT` erreicht werden. Sowohl Client als auch Server können diesen Vorgang initiieren.

Es wird empfohlen, ein Key Re-Exchange gemäß Kapitel 9 in [RFC 4253] durchzuführen, das heißt die Sitzungsschlüssel werden nach einer Stunde oder nach der Übertragung von einem Gigabyte (je nachdem, was zuerst eintritt) erneuert.

3.4 Verschlüsselungsalgorithmen

Während des Key Exchange einigen sich Client und Server auf einen Verschlüsselungsalgorithmus sowie einen gemeinsamen Verschlüsselungsschlüssel. Hierzu werden die folgenden Verschlüsselungsverfahren empfohlen:

Tabelle 3: Empfohlene Verschlüsselungsverfahren

Nr.	*Verschlüsselungsverfahren*	*Spezifikation*	*Verwendung bis*
1	`AEAD_AES_128_GCM`	[RFC 5647], Abschnitt 6.1	2030+

Nr.	*Verschlüsselungsverfahren*	*Spezifikation*	*Verwendung bis*
2	`AEAD_AES_256_GCM`	[RFC 5647], Abschnitt 6.2	2030+
3	`aes128-ctr`	[RFC 4344]	2030+
4	`aes192-ctr`	[RFC 4344]	2030+
5	`aes256-ctr`	[RFC 4344]	2030+

Hinweis: Bei den Verfahren Nr. 1 und Nr. 2 ist durch den GCM-Modus schon eine MAC-Sicherung enthalten.

3.5 MAC-Sicherung

Für die MAC-Sicherung werden die folgenden Verfahren empfohlen:

Tabelle 4: Empfohlene Verfahren zur MAC-Sicherung

Nr.	*MAC-Verfahren*	*Spezifikation*	*Verwendung bis*
1	`hmac-sha2-256`	[RFC 6668], Kapitel 2	2030+
2	`hmac-sha2-512`	[RFC 6668], Kapitel 2	2030+

3.6 Server-Authentisierung

Der Server authentisiert sich gegenüber dem Client; dies läuft im Rahmen des Transport Layer Protocol ab. In Kapitel 7 von [RFC 4253] wird dazu die *Explicit Server Authentication* beschrieben. Dabei enthalten die Key Exchange-Nachrichten eine digitale Signatur des Servers (oder einen anderen Nachweis), um dessen Authentizität zu beweisen. Der Client kann die Signatur mit dem Public Key des Servers überprüfen und somit die Authentizität des Servers feststellen.

Die Algorithmen für digitale Signaturen werden in [RFC 4253] „Public Key Algorithms“ genannt (vgl. Abschnitt 6.6 in [RFC 4253]).

Folgende Signaturverfahren für die Server-Authentisierung werden empfohlen:

Tabelle 5: Empfohlene Signaturverfahren für die Server-Authentisierung

Nr.	*Signaturverfahren*	*Spezifikation*	*Verwendung bis*
1	`pgp-sign-dss`	[RFC 4253], Abschnitt 6.6	2029
2	`ecdsa-sha2-*`	[RFC 5656]	2030+
3	`x509v3-ecdsa-sha2-*`	[RFC 6187]	2030+

Bemerkung zu Signaturverfahren Nr. 1: Unter Verwendung der Bezeichnungen aus Abschnitt 13.6 in [RFC 4880] werden mindestens 3000 Bit für die Länge der Primzahl p und mindestens 250 Bit für die Länge der Ordnung q empfohlen (siehe dazu auch Abschnitt 2.3.5 in [TR-02102-1]). Als zugehörige Hashfunktion wird SHA-256, SHA-384 oder SHA-512 empfohlen.

Die Nutzung des Signaturverfahrens `pgp-sign-dss` wird aufgrund der geringen Verbreitung und der Abkündigung in [FIPS 186-5] nur noch bis 2029 empfohlen (siehe auch Bemerkung 5.7 in [TR-02102-1]).

Bemerkung zu den Signaturverfahren Nr. 2-3: Das „`*`“-Zeichen wird ersetzt durch den Bezeichner einer elliptischen Kurve aus Abschnitt 10.1 in [RFC 5656]. Zurzeit werden die folgenden elliptischen Kurven empfohlen:

- `nistp256`, `nistp384`, `nistp521`

Die zugehörige Hashfunktion aus der SHA-2-Familie muss in Abhängigkeit der Bitlänge der Kurve gemäß Abschnitt 6.2.1 in [RFC 5656] gewählt werden.

Für die Authentisierung innerhalb von Projekten des Bundes sind die Vorgaben der Technischen Richtlinie [TR-03116-4] in der jeweils aktuellen Fassung zu beachten.

3.7 Client-Authentisierung

Die Client-Authentisierung findet (im Gegensatz zur Server-Authentisierung) nicht im Transport Layer Protocol, sondern im User Authentication Protocol statt; dieses Protokoll setzt logisch auf dem Transport Layer Protocol auf.

Die wichtigsten Verfahren für die Client-Authentisierung sind:

- Public key authentication
- Password authentication
- Host-based authentication

Empfehlung: Für die Client-Authentisierung wird die „Public key authentication“ zusammen mit einem der Verfahren aus Tabelle 5, Abschnitt 3.6 empfohlen.

Anmerkung: Die Public key authentication muss gemäß [RFC 4252] von jeder SSH-Implementierung unterstützt werden. Der dazugehörige Authentication Method Name gemäß [RFC 4250], Abschnitt 4.8 lautet „publickey“. Die Authentisierungs-Methode wird in Kapitel 7 von [RFC 4252] beschrieben.

Für die Authentisierung innerhalb von Projekten des Bundes sind die Vorgaben der Technischen Richtlinie [TR-03116-4] in der jeweils aktuellen Fassung zu beachten.

4 Schlüssel und Zufallszahlen

4.1 Schlüsselspeicherung

Private kryptographische Schlüssel, insbesondere statische Schlüssel und Signaturschlüssel, müssen sicher gespeichert und verarbeitet werden. Dies bedeutet u. a. den Schutz vor Kopieren, missbräuchlicher Nutzung und Manipulation der Schlüssel. Eine sichere Schlüsselspeicherung kann zum Beispiel durch die Verwendung zertifizierter Hardware (Chipkarte, HSM) gewährleistet werden.

Ebenso müssen die öffentlichen Schlüssel von als vertrauenswürdig anerkannten Stellen (Vertrauensanker) manipulationssicher gespeichert werden.

4.2 Umgang mit Ephemer-Schlüsseln

Wenn eine SSH-Verbindung durch ein Verschlüsselungsverfahren gesichert ist, muss sichergestellt werden, dass alle Ephemer-Schlüssel nach ihrer Verwendung unwiderruflich gelöscht werden, und keine Kopien dieser Schlüssel erzeugt wurden. Ephemer- bzw. Sitzungsschlüssel dürfen nur für *eine* Verbindung benutzt werden und grundsätzlich nicht persistent abgespeichert werden.

4.3 Zufallszahlen

Für die Erzeugung von Zufallszahlen, zum Beispiel für kryptographische Schlüssel oder die Signaturerzeugung, 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 Teil 1 dieser Technischen Richtlinie [TR-02102-1].

Literaturverzeichnis

[**AIS 20/31**] BSI: AIS 20/31 – A proposal for: Functionality classes for random number generators, 2011

[**FIPS 186-5**] National Institute of Standards and Technology: Federal Information Processing Standards FIPS PUB 186-5, Digital Signature Standard (DSS), 2023

[**RFC 4251**] T. Ylonen, C. Lonvick: RFC 4251, The Secure Shell (SSH) Protocol Architecture, 2006

[**RFC 4252**] T. Ylonen, C. Lonvick: RFC 4252, The Secure Shell (SSH) Authentication Protocol, 2006

[**RFC 4253**] T. Ylonen, C. Lonvick: RFC 4253, The Secure Shell (SSH) Transport Layer Protocol, 2006

[**RFC 4254**] T. Ylonen, C. Lonvick: RFC 4254, The Secure Shell (SSH) Connection Protocol, 2006

[**RFC 4344**] M. Bellare, T. Kohno, C. Namprempre: RFC 4344, The Secure Shell (SSH) Transport Layer Encryption Modes, 2006

[**RFC 4419**] M. Friedl, N. Provos, W. Simpson: RFC 4419, Diffie-Hellman Group Exchange for the Secure Shell (SSH) Transport Layer Protocol, 2006

[**RFC 4432**] B. Harris: RFC 4432, RSA Key Exchange for the Secure Shell (SSH) Transport Layer Protocol, 2006

[**RFC 4880**] J. Callas, L. Donnerhacke, H. Finney, D. Shaw, R. Thayer: RFC 4880, OpenPGP Message Format, 2007

[**RFC 5647**] K. Igoe, J. Solinas: RFC 5647, AES Galois Counter Mode for the Secure Shell Transport Layer Protocol, 2009

[**RFC 5656**] D. Stebila, J. Green: RFC 5656, Elliptic Curve Algorithm Integration in the Secure Shell Transport Layer, 2009

[**RFC 6668**] D. Bider, M. Baushke: RFC 6668, SHA-2 Data Integrity Verification for the Secure Shell (SSH) Transport Layer Protocol, 2012

[**RFC 8268**] M. Baushke: RFC 8268, More Modular Exponentiation (MODP) Diffie-Hellman (DH) Key Exchange (KEX) Groups for Secure Shell (SSH), 2017

[**RFC 8270**] L. Velvindron, M. Baushke: RFC 8270, Increase the Secure Shell Minimum Recommended Diffie-Hellman Modulus Size to 2048 Bits, 2017

[**RFC 9142**] M. Baushke: RFC 9142, Key Exchange (KEX) Method Updates and Recommendations for Secure Shell (SSH), 2022

[**TR-02102-1**] BSI: Technische Richtlinie TR-02102-1, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, 2024

[**TR-03116-4**] BSI: Technische Richtlinie TR-03116-4, Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 4: Kommunikationsverfahren in Anwendungen, 2024