Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Moderne Messenger – heute verschlüsselt, morgen interoperabel?

Sicher im
digitalen Alltag

Änderungshistorie

Version	*Datum*	*Name*	*Beschreibung*
1.0	November 2021	BSI	Erstausgabe

Tabelle 1: Änderungshistorie

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582- 111
E-Mail: service-center@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhalt

1 Einleitung 4
2 Grundsätzliche Funktionsweise moderner Messenger 6
3 Sicherheitsanforderungen und -eigenschaften moderner Messenger 7
3.1 Ende-zu-Ende- und Transportverschlüsselung 7
3.2 Double-Ratchet-Protokoll und Messaging Layer Security 7
3.3 Kryptographische Eigenschaften von Messenger-Protokollen 9
3.4 Weitere Sicherheitseigenschaften und -mechanismen von Messengern 10
3.5 Open-Source-Software, Zertifizierung und Sicherheitsaudits 10
4 Metadaten / Datenschutzaspekte 12
5 Aktivitäten des BSI 14
6 Zusammenfassung 15
Glossar 16

1 Einleitung

Neben Telefon und E-Mail haben moderne Messenger mit dem Siegeszug von Smartphones längst Einzug in unseren Alltag gehalten und die klassische SMS nahezu vollständig verdrängt. Abgesehen von Textnachrichten erlauben es die meisten Messenger ebenfalls, Bilder, Sprachnachrichten oder Dateien zu versenden oder Audio-/Videoanrufe durchzuführen – und zwar jeweils mit einem einzelnen Kommunikationspartner oder in größeren Gruppen.

Aktuell gibt es eine Vielzahl von Messengern verschiedener Anbieter, die jedoch – im Gegensatz zu Telefon und E-Mail – im Allgemeinen nicht miteinander kompatibel sind. Als Konsequenz können Nutzer verschiedener Messenger in der Regel nicht miteinander kommunizieren. Die Gründe dafür sind vielfältig; eine zentrale technische Hürde stellen in diesem Zusammenhang unterschiedliche Ansätze in puncto „Verschlüsselung“ dar. In der Tat arbeiten die meisten Messenger heutzutage verschlüsselt, um Vertraulichkeit, Integrität und Authentizität der ausgetauschten Inhalte zu schützen. Die dabei zum Einsatz kommenden kryptographischen Protokolle sind jedoch bislang nicht standardisiert und daher im Detail teilweise sehr unterschiedlich.

Mehr noch als bei Telefon oder E-Mail fallen bei der Nutzung eines Messengers eine Vielzahl von Metadaten an, die es erlauben, detaillierte Nutzerprofile zu erstellen. Neben Sicherheitsaspekten (z. B. Vertraulichkeit) spielen daher zunehmend Datenschutzaspekte eine wichtige Rolle bei der Entscheidung für oder gegen einen bestimmten Messenger.

Aus Verbraucherschutzperspektive werden neben Datensicherheit und Datenschutz noch weitere Aspekte diskutiert. So wirken sich eine wachsende Marktkonzentration auf wenige große Messenger-Anbieter und daraus resultierende Netzwerk- und Lock-In-Effekte potentiell negativ auf Interessen der Verbraucherinnen und Verbraucher aus. Im politischen Diskurs steht daher die Frage im Raum, ob z. B. große Messenger-Anbieter mit einer Interoperabilitätsverpflichtung (oder ähnlichen Markteingriffen) belegt werden sollen oder inwiefern eine Standardisierung der Kommunikationsprotokolle zu einer Auflösung von Grenzen zwischen verschiedenen Messengern beitragen kann.

Verschiedene Akteure aus dem Bereich des Digitalen Verbraucherschutzes befassen sich aktuell mit diesem Themenfeld. So hat u. a. die Bundesnetzagentur im Mai 2020 Zahlen einer repräsentativen Umfrage zur Verbreitung und Nutzung von Messengern durchgeführt.[1] Der Verbraucherzentrale Bundesverband (vzbv) hat im Mai 2021 ein Diskussionspapier zu Interoperabilität bei Messenger-Diensten mit Blick auf mögliche regulatorische und technische Ausgestaltungen vorgelegt.[2] Schließlich hat das Bundeskartellamt im November 2020 eine verbraucherrechtliche Sektoruntersuchung zu Messenger- und Video-Diensten eingeleitet und eine große Zahl von Messenger-Anbietern unmittelbar befragt.[3] Bei der Sektoruntersuchung des Bundeskartellamts ist Interoperabilität zwischen verschiedenen Messengern ebenfalls einer der zentralen Untersuchungsschwerpunkte – neben Fragen zu einer möglichen Irreführung der Verbraucherinnen und Verbraucher bezüglich Verschlüsselung sowie zu möglichen Datenschutzverstößen. Das BSI steht im Rahmen von Kooperationsvereinbarungen sowohl mit dem vzbv als auch mit dem Bundeskartellamt im Austausch. Insbesondere unterstützt das BSI das Bundeskartellamt bei der Sektoruntersuchung Messenger- und Video-Dienste mit technischer Expertise. Im November 2021 veröffentlichte das Bundeskartellamt einen ersten Zwischenbericht zur Sektoruntersuchung, welcher einen Branchenüberblick und ein erstes Stimmungsbild der befragten Marktakteure zur Interoperabilität von Messengern liefert.

[1] Bundesnetzagentur (Mai 2020). Nutzung von OTT-Kommunikationsdiensten in Deutschland.
[2] Verbraucherzentrale Bundesverband e.V. (vzbv) (Mai 2021). Interoperabilität bei Messengerdiensten.
[3] Bundeskartellamt (o.J.). Verbraucherrechtlichen Sektoruntersuchungen des Bundeskartellamts, https://www.bundeskartellamt.de/DE/Verbraucherschutz/Verfahren/verfahren_node.html (abgerufen am 24.09.2021). Bundeskartellamt (2020). Bundeskartellamt leitet Sektoruntersuchung zu Messenger-Diensten ein (Pressemitteilung vom 12.11.2020), https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2020/12_11_2020_SU_Messenger_Dienste.html.

Der vorliegende Artikel befasst sich mit einer technischen Sicht auf das Thema Messenger und erläutert die verschiedenen Faktoren, die zur Gesamtsicherheit eines Messengers beitragen. Anstelle der Betrachtung einzelner Messenger werden die grundlegende Funktionsweise moderner Messenger erklärt, die dabei verwendeten Kommunikationsprotokolle und ihre Sicherheitseigenschaften dargestellt sowie weitere Aspekte identifiziert, die bei der sicheren Verwendung eines Messengers eine Rolle spielen, darunter insbesondere Datenschutzaspekte. Ziel ist es, die interessierten Leserinnen und Leser umfassend über das Thema „Sichere Messenger“ zu informieren und sie in die Lage zu versetzen, die Sicherheit eines Messengers anschließend selbst auf Basis öffentlich verfügbarer Informationen beurteilen zu können.

2 Grundsätzliche Funktionsweise moderner Messenger

Die meisten Messenger sind heutzutage in irgendeiner Form verschlüsselt. Welche Inhalte verschlüsselt werden – also ob nur Textnachrichten oder auch Bilder, Dateien und Audio-/Videotelefonate, ob nur in Einzel- oder auch in Gruppenkonversationen – und wie diese verschlüsselt werden – also ob Ende-zu-Ende- oder Transportverschlüsselung – ist dabei aber sehr unterschiedlich und mitunter auch eine Sache der gewählten Einstellungen. Bevor näher auf die Details der Verschlüsselung eingegangen wird, sollen zunächst die grundlegende Funktionsweise und die verschiedenen Verschlüsselungsarten erläutert werden, insbesondere da einige Begriffe wie beispielsweise Ende-zu-Ende-Verschlüsselung in diesem Kontext nicht immer einheitlich bzw. korrekt verwendet werden.

Das generelle Funktionsprinzip eines Messengers ist in Abbildung 1 dargestellt: Sämtliche Kommunikation der Nutzer findet zwischen den sogenannten *Clients* (Frontend) und einem vom Anbieter des Messengers betriebenen *Server* (Backend) statt. Ein Nutzer kann dabei durchaus mehrere Clients besitzen, indem er den Messenger z. B. in der Smartphone-App, als Desktop-Anwendung oder über einen Internetbrowser nutzt. Die Daten (z. B. Textnachrichten, Bilder, Dateien, Sprach- oder Videopakete), die ein Sender-Client an den Server schickt, werden dort für den Empfänger-Client aufbewahrt, bis dieser das nächste Mal online ist und seine Daten abruft. Die Kommunikation ist damit *asynchron*, d. h. nicht alle Kommunikationspartner müssen zur gleichen Zeit online sein. Der Server kümmert sich ferner um die Synchronisation zwischen den verschiedenen Clients eines Nutzers oder die Verwaltung von Gruppen, indem sämtliche Daten an alle beteiligten Clients verteilt werden.

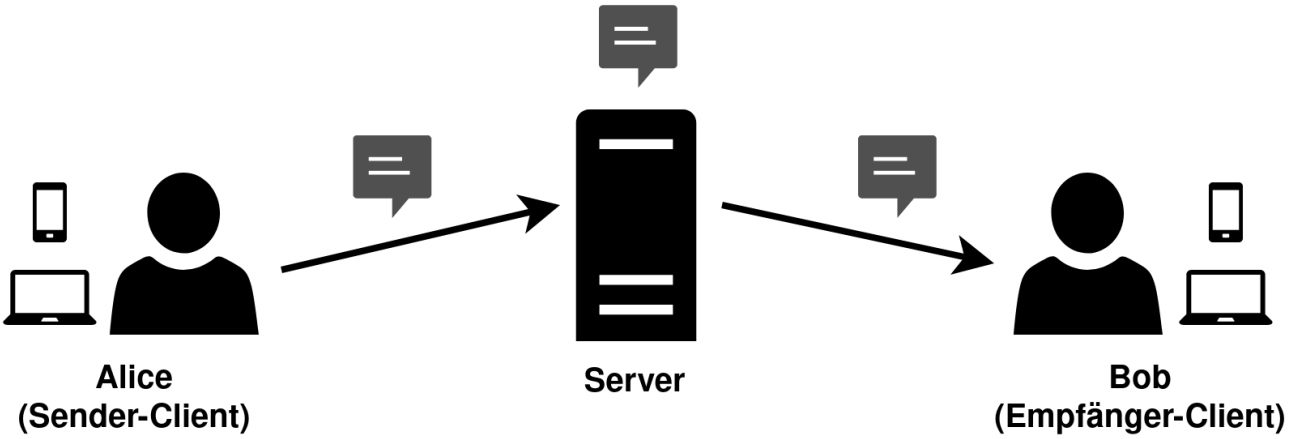


Abbildung 1. Grundsätzliche Funktionsweise eines Messenger-Systems bestehend aus Nutzer-Clients (Alice, Bob) und Server.

Bei vielen Messenger-Anbietern ist auf den ersten Blick nicht ersichtlich, in welchem Land sich die Server befinden. Teilweise verwenden die Anbieter auch mehrere Standorte oder greifen bei der Serverinfrastruktur auf Firmen wie Google, Amazon oder Microsoft zurück. Messenger, die statt der anbietereigenen Serverinfrastruktur auch ein *Hosting-on-Premise* (Server in einem eigenen, also anbieterfremden Rechenzentrum) erlauben, können auf diesem Wege durch den Betreiber an eigene Sicherheitsanforderungen angepasst werden. Zudem lässt sich auch der Zugriff auf Daten und Metadaten besser kontrollieren.

3 Sicherheitsanforderungen und -eigenschaften moderner Messenger

3.1 Ende-zu-Ende- und Transportverschlüsselung

Die von Messengern versendeten Daten können auf zwei verschiedene Arten gegen unerwünschtes Mitlesen geschützt werden: Zum einen bei der Übertragung zwischen Nutzer-Client und Server durch eine sogenannte *Transportverschlüsselung*, die es Außenstehenden unmöglich macht, die übertragenen Inhalte zu lesen, nicht jedoch dem Serverbetreiber, da sie auf dem Server im Klartext vorliegen. Um dies zu verhindern, ist eine zusätzliche Verschlüsselung der Inhalte zwischen den Endpunkten der Kommunikation (den Nutzer-Clients von Sender und Empfänger(n) auf den Endgeräten) notwendig, was mittels einer *Ende-zu-Ende-Verschlüsselung* erreicht werden kann.

Kurz zusammengefasst sichert eine Transportverschlüsselung den Kanal der Übertragung, eine Ende-zu-Ende-Verschlüsselung den übertragenen Inhalt. Grundsätzlich ist zum Schutz vor einem unbefugten Zugriff auf die Daten eine Ende-zu-Ende-Verschlüsselung alleine ausreichend. Eine zusätzliche Transportverschlüsselung in Form von *TLS 1.2/1.3 (Transport Layer Security)* ist heutzutage jedoch Standard und bedeutet nur einen geringen Zusatzaufwand. Kritiker einer Ende-zu-Ende-Verschlüsselung führen unter anderem an, dass auf diesem Weg auch unbemerkt Schadsoftware verschickt werden kann und ferner Strafverfolgung erschwert wird, falls es keine Hintertür *(Backdoor, Lawful Interception)* für gewisse Berechtigte gibt.

Mit einer guten Ende-zu-Ende-Verschlüsselung muss ein Endnutzer nur den Endpunkten der Kommunikation vertrauen: Sich selbst, dem Gegenüber und den Clients. Dazwischen – im Internet und auf den Servern – ist die Kommunikation sicher. Die Ende-zu-Ende-Verschlüsselung geht mit einem leicht erhöhten Rechenaufwand und damit einem höheren Strom-/Akkuverbrauch einher, was für heutige Smartphones (und PCs erst recht) jedoch kein Hindernis mehr darstellt. Dennoch ist sie bei einigen Messengern nicht standardmäßig aktiviert oder teilweise nur gegen Zusatzkosten hinzubuchbar.

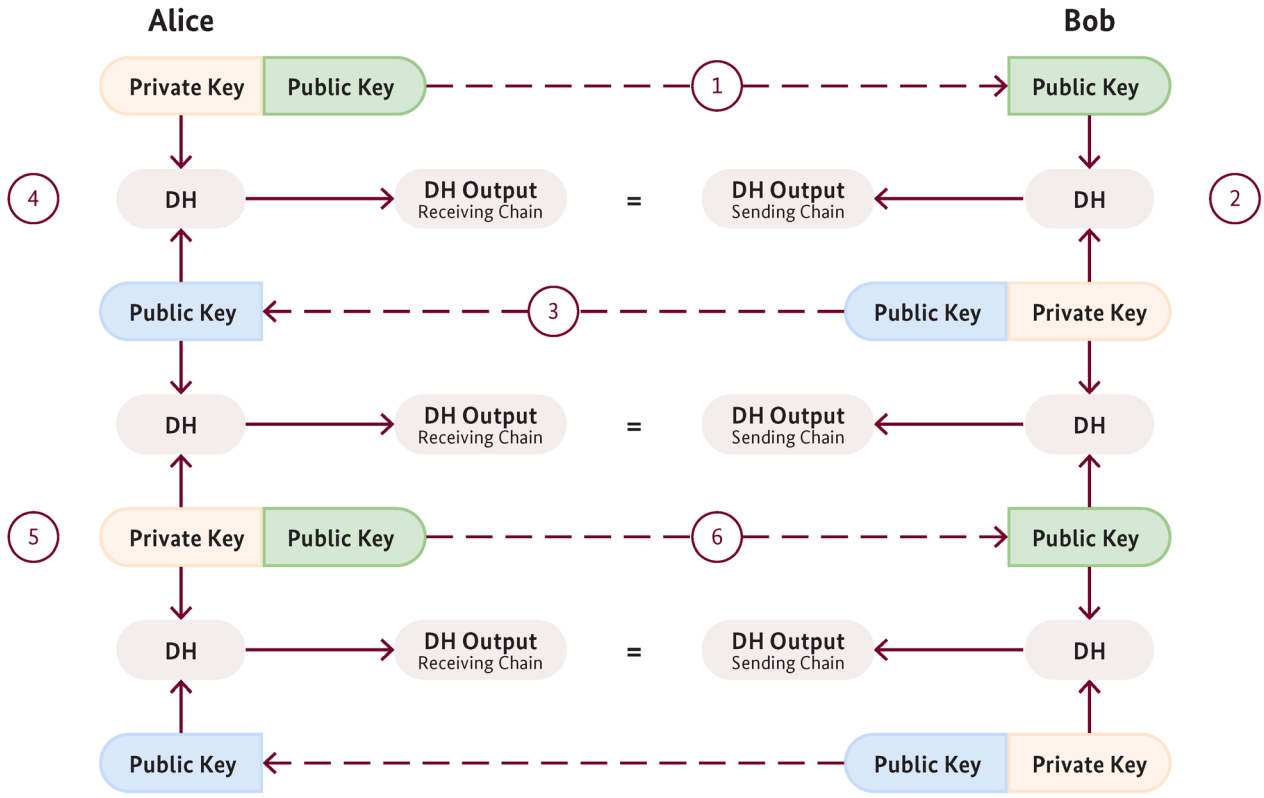
3.2 Double-Ratchet-Protokoll und Messaging Layer Security

Die Nachrichtenverschlüsselung vieler moderner Ende-zu-Ende-verschlüsselten Messenger basiert auf dem sogenannten *Double-Ratchet-Protokoll*.[4] Die Sicherheit des Protokolls, welches derzeit als Stand der Technik gilt, wurde inzwischen in einer Reihe von Forschungsarbeiten analysiert.[5] Das Protokoll kann als Weiterentwicklung des *Off-the-Record-Protokolls (OTR)* angesehen werden. Beide wurden von den Entwicklern des Messengers *Textsecure* (heute *Signal)* entworfen. Das Double-Ratchet-Protokoll kommt mit leichten Modifikationen auch in anderen Messengern zum Einsatz und wird so derzeit von mehr als einer Milliarde Menschen weltweit genutzt. Das Protokoll besteht im Wesentlichen aus drei Phasen: einem initialen Schlüsselaustausch *(X3DH, Extended Triple Diffie-Hellman)* zur Erzeugung eines gemeinsamen Geheimnisses, in welches die an den Nutzer-Client gebundenen Langzeitschlüssel der Kommunikationspartner einfließen, sowie einer asymmetrischen „Ratsche“ und einer symmetrischen „Ratsche“, die zusammen dem Protokoll auch seinen Namen geben. Eine der grundlegenden Ideen des Protokolls ist es, mit jeder versendeten Nachricht stets auch neue (Sitzungs-)Schlüssel zu versenden und die alten zu löschen. Das Schlüsselmaterial wird also quasi wie bei einer Ratsche „vorwärts geratscht“, sodass es für einen Angreifer

[4] Perrin und Marlinspike (2016). The Double Ratchet Algorithm (Revision 1), https://signal.org/docs/specifications/doubleratchet/doubleratchet.pdf (abgerufen am 24.09.2021).

[5] Siehe u. a. Cohn-Gordon, Cremers, Dowling, Garratt und Stebil (2019). A Formal Security Analysis of the Signal Messaging Protocol, https://eprint.iacr.org/2016/1013.pdf und Alwen, Coretti und Dodis (2020). The Double Ratchet: Security Notions, Proofs, and Modularization for the Signal Protocol. *Annual International Conference on the Theory and Applications of Cryptographic Techniques*. https://eprint.iacr.org/2018/1037.pdf (beide abgerufen am 24.09.2021).

nicht möglich ist, von einem späteren zu einem früheren Zeitpunkt zurückzukehren und vorangegangene Nachrichten zu entschlüsseln. Eine vereinfachte, schematische Darstellung der asymmetrischen Ratsche ist in Abbildung 2 erläutert.



1. Alice sendet eine Nachricht zusammen mit ihrem Public Key an Bob
2. Bob berechnet mit Alices Public Key und seinem Private Key ein gemeinsames Diffie-Hellman-Geheimnis (DH)
3. Bob sendet seinen Public Key zusammen mit seiner nächsten Nachricht an Alice
4. Alice berechnet mit Bobs Public Key und ihrem Private Key das gemeinsame Diffie-Hellman-Geheimnis
5. Alice generiert ein neues Schlüsselpaar
6. Alice sendet eine Nachricht zusammen mit ihrem neuen Public Key an Bob (usw.)

Abbildung 2. Vereinfachte Darstellung eines Ausschnittes der asymmetrischen (Diffie-Hellman-) Ratsche.

Die Verschlüsselung von Gruppenchats wird aktuell erreicht, indem diese als Einzelchats aller Gruppenmitglieder untereinander implementiert werden. Bei einer Gruppe mit n Mitgliedern gibt es $n(n-1)/2$ dieser Einzelchats, sodass der Verschlüsselungsaufwand quadratisch mit der Anzahl der Teilnehmer wächst und bei größeren Gruppen (>100 Teilnehmer) schnell zum Problem wird. Bei einigen Messengern sind ebenfalls (Gruppen-) Audio-/Videotelefonate Ende-zu-Ende verschlüsselt. Hier kommt zumeist das *WebRTC-Protokoll*, in der Regel im Zusammenspiel mit *DTLS-SRTP (Datagram Transport Layer Security – Secure Real-Time Transport Protocol)*, zum Einsatz.

Der quadratische Aufwand bei der Verschlüsselung von Gruppenchats stellt einen der Hauptgründe dar, der zur Gründung einer *IETF-Arbeitsgruppe* geführt hat, die sich mit einer Weiterentwicklung des Double-Ratchet-Protokolls beschäftigt, dem *Messaging-Layer-Security-Protokoll (MLS)*, welches insbesondere ein effizientes Gruppenhandling ermöglichen soll.[6]

Ein weiteres, ebenfalls wichtiges Ziel, das mit einer Standardisierung von MLS erreicht werden soll, ist die Interoperabilität verschiedener Messenger. In der Tat ist es aktuell so, dass jeder Messenger seine eigene, in

[6] IETF Working Group “Messaging Layer Security (MLS)”, https://datatracker.ietf.org/wg/mls/about/ (abgerufen am 24.09.2021).

der Regel leicht modifizierte Form des Double-Ratchet-Protokolls implementiert. Dadurch sind verschiedene Messenger nicht miteinander kompatibel und es sind ferner auch keine einheitlichen Sicherheitsanalysen möglich. Dem soll begegnet werden, indem MLS als IETF-Standard verabschiedet wird. Die Etablierung des Standards, an dessen Ausarbeitung verschiedene Unternehmen (u. a. *Mozilla, Twitter, Cisco, Google, Facebook)*, Forschungseinrichtungen *(INRIA)* und Universitäten *(MIT, University of Oxford)* beteiligt sind, ist für Mitte 2022 geplant. Mit MLS als Standard stellt die Verschlüsselung für die Interoperabilität verschiedener Messenger kein Hemmnis mehr dar. Für eine praktische Interoperabilität benötigen die verschiedenen Systeme jedoch über MLS hinaus noch weitere Funktionalitäten, so vor allem Schnittstellen zum Austausch der MLS-verschlüsselten Informationen. Demzufolge ist derzeit noch offen, wie die interoperable Kommunikation zwischen Messengern praktisch umgesetzt wird, z. B. wie sich Nutzer aus unterschiedlichen Messenger-Systemen "finden" können. Dazu müssen neben Anpassungen an den Messenger-Clients auch Erweiterungen an der Netzwerkinfrastruktur der Messenger-Server – z. B. am *Domain Name System (DNS)* – vorgenommen werden. Auch das Thema Föderation, also eine Serverübergreifende Kommunikation, rückt mit dem MLS-Standard in greifbarere Nähe, auch wenn sich die Ausarbeitung von Konzepten hier noch in den Anfängen befindet und es bislang nur wenige praktische, kryptographisch abgesicherte Lösungsansätze gibt.

3.3 Kryptographische Eigenschaften von Messenger-Protokollen

Das Double-Ratchet- und auch das zukünftige MLS-Protokoll weisen neben den klassischen Sicherheitseigenschaften der Kryptographie (Vertraulichkeit, Integrität, Authentizität, Verfügbarkeit, (Nicht-) Abstreitbarkeit) und der Ende-zu-Ende-Verschlüsselung eine Reihe weiterer Sicherheitseigenschaften auf, die insbesondere bei Messengern von besonderer Bedeutung sind und im Folgenden kurz erläutert werden sollen.[7, 8]

Post-Compromise Security, auch *Future Secrecy* oder *Backward Secrecy*, bezeichnet die Eigenschaft eines kryptographischen Protokolls, gemäß derer sich die Sicherheit der Kommunikation auch nach der Kompromittierung eines Schlüssels wieder „heilt“, d. h., dass neue Nachrichten auch ohne Zutun der Nutzer wieder sicher sind.

(Perfect) Forward Secrecy macht es einem Angreifer unmöglich, durch die Kenntnis eines geheimen Haupt- oder Langzeitschlüssels einen Sitzungsschlüssel zu rekonstruieren. Die Sitzungsschlüssel sind nur für eine definierte Zeit gültig und nicht voneinander ableitbar. Eine aufgezeichnete verschlüsselte Kommunikation ist damit selbst bei der Kenntnis des Langzeitschlüssels nicht nachträglich zu entschlüsseln.

(Plausible) Deniability (Glaubhafte Abstreitbarkeit) erlaubt es einem Kommunikationspartner, das Versenden einer gegebenen Nachricht im Nachhinein glaubhaft abstreiten zu können. Es gibt im Wesentlichen zwei Implementierungsmöglichkeiten: Entweder teilen alle Kommunikationsteilnehmer ein Geheimnis, welches es ihnen im Prinzip ermöglicht, die ausgetauschten Nachrichten im Nachhinein zu modifizieren, oder die Signatur einer Nachricht, die eine manipulationssichere Übertragung sicherstellen soll, wird nur bei Empfang überprüft und unmittelbar danach gelöscht. Das Konzept ist eng verwandt mit dem der allgemeineren *deniable encryption*, einer Verschlüsselungstechnik, bei der das Vorhandensein einer verschlüsselten Datei oder Nachricht in dem Sinne geleugnet werden kann, als dass ein Gegner nicht beweisen kann, dass der Klartext existiert.

[7] Unger, Dechand, Bonneau, Fahl, Perl, Goldberg und Smith (2015). SoK: Secure Messaging. *2015 IEEE Symposium on Security and Privacy*. https://www.ieee-security.org/TC/SP2015/papers-archived/6949a232.pdf (abgerufen am 24.09.2021).

[8] Vatandas, Gennaro, Ithurburn und Krawczyk (2021). On the Cryptographic Deniability of the Signal Protocol. *International Conference on Applied Cryptography and Network Security*. https://eprint.iacr.org/2021/642.pdf (abgerufen am 24.09.2021).

3.4 Weitere Sicherheitseigenschaften und -mechanismen von Messengern

Neben dem Schutz der eigentlichen Kommunikationsinhalte tragen weitere, nachfolgend aufgeführte Eigenschaften und Mechanismen eines Messengers und der zugrundeliegenden Plattform zur Gesamtsicherheit eines Messenger-Systems bei.

Ein wichtiger Aspekt bei der Nutzung eines Messengers ist das Thema *Authentifizierung*, sowohl die eigene gegenüber dem Messenger-Dienst als auch die Gesprächspartner-Authentifizierung. Bezüglich ersterer ist eine *Zwei-Faktor-Authentifizierung* erstrebenswert, bei der der Identitätsnachweis getrennt über zwei unterschiedliche Komponenten erfolgt, um das Sicherheitsniveau zu erhöhen. Diese beiden Faktoren stammen aus den Kategorien Wissen (z. B. Passwort, PIN, Antwort auf Sicherheitsfrage), Besitz (z. B. Smartcard, TAN-Liste) oder Biometrie (z. B. Fingerabdruck, Gesichtserkennung). Die Stärken der beiden Faktoren werden kombiniert, sodass ihre sicherheitsrelevanten Schwächen eine weniger gewichtige Rolle spielen. Fehlt einer der beiden Faktoren oder ist dieser nicht korrekt, wird der Zugriff verweigert.

Die Authentifizierung insbesondere neuer Kommunikationspartner stellt sicher, dass die Kommunikation tatsächlich mit der gewünschten Person erfolgt und sich keine fremde Person als diese ausgibt. Aktuell gibt es dafür verschiedene Ansätze, z. B. über den telefonischen Vergleich einer übertragenen Prüfsumme oder durch das Einscannen eines QR-Codes.

Die Speicherung von Langzeitgeheimnissen und anderen sensiblen Daten stellt ein weiteres sicherheitsrelevantes Thema dar. Eine *Ablageverschlüsselung* stellt sicher, dass lokal abgelegte Daten (z. B. Nachrichtenverläufe) sicher gespeichert und ausschließlich von der entsprechenden Messenger-App ausgelesen und verwendet werden können.

Aktuell sind Messenger-Lösungen meist rein softwarebasiert implementiert. Der geheime Schlüssel des Nutzers wird dabei softwareseitig auf dem Mobiltelefon gespeichert. Bei Verlust oder bei Befall durch Malware greifen dann auch lediglich softwarebasierte Sicherungsmechanismen (wie z. B. *Sandboxing* der Applikation), um eine Kompromittierung des Schlüssels zu verhindern. Viele Mobiltelefone verfügen allerdings inzwischen über hardwarebasierte Sicherheitselemente, die eine sichere Speicherung des geheimen Schlüssels ermöglichen (z. B. in Form eines *Trusted Execution Environment (TEE)*, der *Android StrongBox* bzw. des *Cryptographic Service Provider* (BSI-CC-PP-0104-2019) oder der *Apple Secure Enclave)*. Der Zugriff auf ein solches Sicherheitselement ist jedoch aktuell nicht standardisiert und oft durch die Hersteller reglementiert, weswegen nach derzeitigem Kenntnisstand keine der aktuellen Messenger-Lösungen davon Gebrauch macht.

3.5 Open-Source-Software, Zertifizierung und Sicherheitsaudits

Theoretische Eigenschaften kryptographischer Protokolle und ihre praktische Umsetzung sind zwei verschiedene Seiten einer Medaille. In der Tat ist eine korrekte Umsetzung eines Verfahrens eine komplexe Angelegenheit. In der Vergangenheit haben häufig nicht theoretische Schwachstellen, sondern Implementierungsfehler zu Sicherheitslücken geführt.

Neben unabhängig durchgeführten Sicherheitsaudits kann eine Zertifizierung des Anbieters nach ISO 27001, die Veröffentlichung der kryptographischen Designkriterien und / oder des Source Codes einer Software dazu beitragen, das Vertrauen in die Korrektheit einer Implementierung zu erhöhen. Die Hoffnung ist, dass Fehler oder möglicherweise absichtlich eingebaute Funktionen oder Hintertüren, sogenannte *Backdoors*, bei der Code-Analyse durch unabhängige Experten auffallen würden, auch wenn dies in Anbetracht der enormen Menge an Source Code in modernen Messenger-Lösungen ein anspruchsvolles Unterfangen bleibt.

Offen zugänglicher Source Code erlaubt es aber zu überprüfen, ob und wenn ja, in welcher Form ein Messenger Inhalte Ende-zu-Ende-verschlüsselt. In der Vergangenheit sind wiederholt Hersteller aufgefallen, die ihre Messenger als Ende-zu-Ende-verschlüsselt beworben haben, auch wenn diese in der Realität „nur“ transportverschlüsselt waren. In Open-Source-Produkten lassen sich solche Aussagen vergleichsweise einfach verifizieren.

4 Metadaten / Datenschutzaspekte

Neben den reinen Kommunikationsinhalten fallen bei der Verwendung eines Messengers eine Reihe weiterer Daten, sogenannte *Metadaten*, an. Einige dieser Metadaten fallen bei normaler Nutzung rein technisch bedingt an und sind kaum zu vermeiden. So sieht ein Server beispielsweise wann und von wo sich Clients mit ihm verbinden und welche Nutzer wann und wie häufig kommunizieren. Andere Metadaten, z. B. Profilinformationen, werden durch manche Betreiber gezielt von den Nutzern erhoben.

Diese Metadaten werden zu verschiedenen Zwecken genutzt. Einerseits erlauben sie es, den Nutzern bestimmte Komfortfunktionen zu ermöglichen, wie das einfachere Finden von Kontakten über den Abgleich mit dem Adressbuch oder ein automatisches Anzeigen des Online-Status, und können darüber hinaus dem Hersteller beim Identifizieren von Fehlerursachen helfen. Anderseits können diese Daten aber auch zu eigenen Werbezwecken genutzt, an Dritte weiterverkauft oder anderweitig systematisch ausgewertet werden. In datensparsamen Messengern werden von vornherein so wenig wie möglich personalisierte Metadaten erfasst und diese schnellstmöglich wieder gelöscht.

Der Art der Daten sind dabei kaum Grenzen gesetzt, folgende Informationen können beispielsweise von Interesse sein:

- **Persönliche Daten:**
  Profilbilder, Vor- bzw. Nachname des Nutzers, Benutzername oder Pseudonym (z. B. Nickname), Geburtsdatum, Alter, Geschlecht, Nationalität, E-Mail-Adresse, Telefonnummer, Kontoinformationen
- **Geräte- / Konfigurationsdaten:**
  IP-Adresse, Betriebssystem, Netzbetreiber, Gerätetyp, Geräte IDs, Benutzerkonten, Passwörter, Zertifikate, installierte Apps, Regions- und Spracheinstellungen
- **Standort- / Bewegungsdaten:**
  Aufenthaltsorte, Aufenthaltszeitpunkte, Aufenthaltsdauer, Bewegungsprofile
- **Kontakte / Daten Dritter:**
  Kontaktverzeichnis, Adressbücher
- **Gruppenmitgliedschaften:**
  Teilnehmer oder Host in Chatgruppen, Telefonkonferenzen, Videokonferenzen
- **Nutzungsverhalten:**
  Häufigkeit und Dauer der Nutzung einer Messenger-App, Online-/Offline-Status, Browserchronik, Nutzung verschiedener Endgeräte, Zeitpunkte / Dauer / Teilnehmer eines Austauschs per Textnachricht / Telefonat / Videotelefonat

Eine Veröffentlichung des entsprechenden Source Codes eines Messengers kann helfen nachzuvollziehen, welche weiteren Daten ein Client und – falls der entsprechende Code ebenfalls einsehbar ist – ein Server erhebt und in welcher Form diese verarbeitet, gespeichert und ggf. weitergeleitet werden. Oftmals werden die Daten dabei an unterschiedlichen Orten gespeichert, intern auf dem Endgerät eines Nutzers, auf Servern inner- oder außerhalb der EU oder in der Cloud inner- oder außerhalb der EU. Die Unterscheidung zwischen inner- und außerhalb der EU ist insofern relevant, als dass der genaue Standort Auskunft darüber gibt, welchem Datenschutzrecht die Kommunikationsdaten unterworfen sind. Bei vielen Anbietern ist auf den ersten Blick allerdings nicht ersichtlich, in welchem Land sich die Server befinden, teilweise verwenden die Anbieter auch mehrere Standorte.

Die Betrachtung von Metadaten ist umso wichtiger, als dass diese ebenfalls sensible Informationen enthalten können. So lassen sich beispielsweise aus der Kenntnis, wann jemand wie oft und wie lange mit wem und auf welche Art und Weise kommuniziert hat, bereits weitreichende Schlussfolgerungen ziehen, auch ohne die genauen Inhalte zu kennen. Zusammen mit weiteren gespeicherten Merkmalen (z. B. Standort, Suchanfragen, Zahlungsinformationen) erlauben es diese Informationen, ein detailliertes Nutzerprofil zu

erstellen. Daher sind bei der Auswahl eines Messengers insbesondere auch Datenschutzaspekte zu berücksichtigen, darunter vor allem die Information, welche Daten in welcher Form (verschlüsselt / unverschlüsselt, anonymisiert oder nicht), von wem, wo und zu welchem Zweck erhoben und gespeichert werden, und ob sie nach einem gewissen Zeitraum gelöscht werden oder nicht. Berücksichtigt werden sollten auch "indirekte" Metadaten, die nicht beim Messenger selbst, sondern im Ökosystem des Betriebssystems (z. B. iOS, Android) anfallen. Dazu gehören Push Notifications, die sensible Informationen enthalten können und über die Netzwerkinfrastruktur des Betriebssystem-Anbieters (z. B. Apple, Google) laufen.

Aus den zuvor genannten Gründen kann daher ein Blick in die Datenschutzerklärung ratsam sein, zu deren Erstellung die Betreiber eines Messengers verpflichtet sind und in der Art und Umfang der erhobenen Daten und deren Nutzung aufgeführt werden.

5 Aktivitäten des BSI

Abschließend soll kurz auf die Rolle und Aktivitäten des BSI im Kontext von sicherem Messaging eingegangen werden. Neben der allgemeinen Beobachtung verschiedener Messenger führt das BSI eine tiefergehende Evaluierung einzelner, ausgewählter Messenger hinsichtlich eines zugelassenen Einsatzes in der Bundesverwaltung durch.[9] In diesem Zusammenhang arbeitet das BSI auch an der Etablierung eines VS-Anforderungsprofils, welches Anforderungen für die Verarbeitung, Übertragung und Speicherung von Verschlusssachen im Kontext des Messagings formuliert. Ebenso verfolgt und unterstützt das BSI die Standardisierung des MLS-Protokolls und strebt eine Proof-of-Concept-Implementierung an. Das BSI kooperiert mit dem Bundeskartellamt und weiteren Akteuren im Bereich des Digitalen Verbraucherschutzes und unterstützt diese mit technischer Expertise zum Thema Messenger. Für Verbraucherinnen und Verbraucher stellt das BSI ferner Empfehlungen zusammen, worauf bei einem sicheren Einsatz von Messengern geachtet werden sollte.[10] Zentrales Anliegen des BSI mit allen diesen Maßnahmen ist es insbesondere, umfassend über das Thema "Sicheres Messaging" zu informieren sowie die IT-Sicherheit von Messengern für Staat, Wirtschaft und Gesellschaft langfristig zu erhöhen.

[9] Laus und Peter (2020). Sichere, zeitgemäße Kommunikation innerhalb der Netze des Bundes mit Wire. Mit Sicherheit, BSI-Magazin 2020/02, S. 10-12. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Magazin/BSI-Magazin_2020_02.pdf?__blob=publicationFile&v=3#A_PBIS-2110025_BSI%20Magazin_02-2020_DRUCKDATEI_6.indd%3A.69580%3A585.

[10] Bundesamt für Sicherheit in der Informationstechnik (o.J.). Messenger & Videotelefonie sicher nutzen. https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Onlinekommunikation/Chat-Messenger/Messenger/messenger_node.html (abgerufen am 24.09.2021).

6 Zusammenfassung

In diesem Artikel wurde ein Überblick über das Thema „Sichere Messenger“ gegeben, wobei neben der Erläuterung der grundsätzlichen Funktionsweise eines Messengers insbesondere auf Kommunikationsprotokolle und deren kryptographische Eigenschaften sowie Datenschutzaspekte eingegangen wurde. Die Darstellung zeigt, dass es sich um ein vielschichtigeres und komplexeres Thema handelt, als es die einfache Nutzung eines Messengers vermuten lässt, und dass bei der Wahl eines sicheren Messengers eine Reihe von Faktoren zu berücksichtigen sind. Mit dem MLS-Protokoll wurde zudem ein Ausblick auf ein künftiges, standardisiertes Kommunikationsprotokoll gegeben, welches eine Interoperabilität verschiedener Messenger bei gleichzeitiger Ende-zu-Ende-Verschlüsselung nach dem Stand der Technik ermöglicht – ein wichtiger Schritt, der zeigt, dass eine größere Nutzerfreundlichkeit bei gleichzeitig hoher Sicherheit sich nicht ausschließen.

Glossar

(Nicht-)Abstreitbarkeit ((Non-)Repudiation)
Eines der Sicherheitsziele der Kryptographie, welches sicherstellt, dass kein unzulässiges Abstreiten durchgeführter Handlungen möglich ist, z. B., dass eine Kommunikation nicht im Nachhinein von einem der beteiligten Kommunikationspartner gegenüber Dritten abgestritten werden kann.

Asynchrone Kommunikation
Modus der Kommunikation, der das Versenden und Empfangen von Daten zeitlich versetzt und ohne Verzögerung durch beispielsweise Warten auf die Reaktion des Gegenübers zulässt.

Authentizität
Eines der Sicherheitsziele der Kryptographie, welches besagt, dass der Urheber von Daten oder der Absender einer Nachricht eindeutig identifizierbar und seine Urheberschaft nachprüfbar sein sollen.

Backdoor (engl. Hintertür, auch Trapdoor)
Bezeichnet einen (oft vom Entwickler oder der Entwicklerin eingebauten) Teil einer Software, der es Dritten ermöglicht, unter Umgehung der normalen Zugriffssicherung Zugang zum Computer oder einer sonst geschützten Funktion eines Programms zu erlangen.

Backend
Bei Client-Server-Anwendungen wie beispielsweise den meisten Messenger-Diensten wird das auf dem Client laufende Programm als Frontend (Dienstnutzer) und das auf dem Server laufende Programm als Backend (Dienstleister) bezeichnet.

Backward Secrecy, Future Secrecy, Post-Compromise Security („Selbstheilung")
Eigenschaft eines kryptographischen Protokolls, welche garantiert, dass verschlüsselte Nachrichten auch dann geheim bleiben, wenn in der Vergangenheit ein Schlüssel kompromittiert also beispielsweise entwendet wurde.

Client
Programm oder Anwendung, welche(s) auf dem Endgerät eines Nutzers oder einer Nutzerin ausgeführt wird und mit einem Server (Zentralrechner) kommuniziert.

Cryptographic Service Provider (Kryptographiedienstanbieter)
Module, die kryptographische Funktionen anbieten, beispielsweise das Verschlüsseln und Entschlüsseln von Daten, das sichere Speichern von sensitiven Daten wie geheimen Schlüsseln, eine Authentifizierung mit digitalen Zertifikaten oder die Generierung von (Pseudo-)Zufallszahlen.

Deniable Encryption
Verschlüsselungstechnik, bei denen das Vorhandensein einer verschlüsselten Datei oder Nachricht in dem Sinne geleugnet werden kann, dass ein Gegner oder eine Gegnerin nicht beweisen kann, dass der Klartext existiert.

(Plausible) Deniability (Glaubhafte Abstreitbarkeit)
Eigenschaft eines kryptographischen Protokolls, welche es ermöglicht, das Versenden einer Nachricht im Nachhinein glaubhaft abstreiten zu können.

DNS (Domain Name System)
Ein weltweiter Verzeichnisdienst, der den Namensraum des Internets verwaltet. Die Hauptaufgabe von DNS ist die Beantwortung von Anfragen zur Namensauflösung.

Double-Ratchet-Protokoll
Kryptographisches Protokoll für einen asynchronen (d. h. die Kommunikationspartner müssen nicht gleichzeitig online sein), Ende-zu-Ende-verschlüsselten Nachrichtenaustausch.

DTLS (Datagram Transport Layer Security)

Sicherheitsprotokoll, das auf der Funktionsweise von TLS (Transport Layer Security) basiert. Im Gegensatz zu TLS nutzt DTLS nicht das gesicherte, verbindungsorientierte Transportprotokoll TCP (Transmission Control Protocol), sondern das ungesicherte UDP (User Datagram Protocol) zur verschlüsselten und geschützten Übertragung von Daten. DTLS kommt beispielsweise im WebRTC-Protokoll in Form von DTLS-SRTP für eine sichere Schlüsselaushandlung zum Einsatz.

Encryption at Rest (Ablageverschlüsselung)

Verschlüsselung von Daten (sog. Data at Rest, im Gegensatz zu Data in Transit und Data in Use), die in irgendeiner Form längerfristig im Speicher eines Computers/Endgeräts gespeichert sind.

Ende-zu-Ende-Verschlüsselung

Die Verschlüsselung übertragener Daten über alle Übertragungsstationen hinweg. Nur die Kommunikationspartner als Endpunkte der Kommunikation können die Daten entschlüsseln.

(Perfect) Forward Secrecy (Folgenlosigkeit)

Eigenschaft eines kryptographischen Protokolls die es unmöglich macht, durch die Kenntnis eines geheimen Haupt- oder Langzeitschlüssels einen Sitzungsschlüssel zu rekonstruieren. Eine aufgezeichnete verschlüsselte Kommunikation ist damit selbst bei der Kenntnis des Langzeitschlüssels nicht nachträglich zu entschlüsseln.

Frontend

Bei Client-Server-Anwendungen wie beispielsweise den meisten Messenger-Diensten wird das auf dem Client laufende Programm als Frontend (Dienstnutzer) und das auf dem Server laufende Programm als Backend (Dienstleister) bezeichnet.

IETF (Internet Engineering Task Force)

Offene, internationale Freiwilligenvereinigung von Netzwerktechnikern, Herstellern, Netzbetreibern, Forschern und Anwendern, die sich mit der technischen Weiterentwicklung des Internets – insbesondere der Standardisierung der im Internet eingesetzten Kommunikationsprotokolle – befasst, um dessen Funktionsweise zu verbessern.

Integrität (Integrity)

Eines der Sicherheitsziele der Kryptographie, welches sicherstellt, dass Daten nicht unbemerkt verändert werden können.

Interoperabilität

Bezeichnet in diesem Artikel die Fähigkeit unabhängiger, heterogener Messenger-Systeme oder Messenger-Clients, in verschieden hohem Maße zusammenarbeiten zu können.

Lawful Interception (auch Legal Interception)

Bezeichnet die vom Gesetzgeber vorgeschriebene technische Einrichtung von Abhörmöglichkeiten in Telekommunikations- und Telefonnetzen, die es Strafverfolgungsbehörden mit Gerichtsbeschluss oder anderer rechtlicher Grundlage ermöglichen, einzelne Teilnehmer selektiv abzuhören.

Messaging (auch Instant Messaging)

Eine Kommunikationsmethode, bei der sich zwei oder mehr Teilnehmende per Textnachrichten beispielsweise über das Internet unterhalten. Die meisten Messenger erlauben es außerdem, Bilder, Sprachnachrichten oder Dateien zu versenden oder Audio-/Videoanrufe durchzuführen. Messaging stellt eine Alternative zum SMS-Versand (Short Message Service) im Mobilfunk dar und ist heute ein vielgenutzter Dienst auf Mobilgeräten.

Messenger-Dienst

Wird in diesem Artikel als Oberbegriff für offene und geschlossene Messenger-Systeme, Messenger-Clients und Multimessenger verwendet, die Messaging-Funktionen und/oder Audio-/Videotelefonie (einzeln und/oder in Gruppen) anbieten.

Messenger-System
Sammelbegriff für das gesamte System, das zum Messaging benötigt wird, bestehend aus Kommunikationsprotokoll, Anwendersoftware (App, Client), Serversoftware und Hardware.

MLS (Messaging Layer Security)
Messagingprotokoll, welches auf dem Double-Ratchet-Protokoll basiert und derzeit im Rahmen einer IETF-Arbeitsgruppe standardisiert wird. Der Standard strebt ein verbessertes Gruppenmanagement sowie die Interoperabilität verschiedener Messenger an.

Personenbezogene Daten
Nach Art. 4 Nr. 1 DSGVO sind dies alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.

(Kommunikations-) Protokoll
Regelsatz, nach der die Datenübertragung zwischen zwei oder mehreren Endpunkten abläuft.

Sandbox
Eine Sandbox bezeichnet einen isolierten Bereich, innerhalb dessen jede Maßnahme keine Auswirkung auf die äußere Umgebung hat.

Schlüsselaustausch
Verfahren in der Kryptographie, um zwei oder mehreren Kommunikationspartnern einen gemeinsamen, geheimen Schlüssel zugänglich zu machen.

(Klassische) Sicherheitsziele der Kryptographie
Vertraulichkeit, Integrität, Authentizität, Verfügbarkeit, (Nicht-)Abstreitbarkeit/Verbindlichkeit, Zurechenbarkeit (siehe jeweilige Glossareinträge).

(S)RTP ((Secure) Real-Time Transport Protocol)
Netzwerkprotokoll für die Übertragung von Audio- und Videodaten über IP-Netzwerke. Bei SRTP handelt es sich im Vergleich zu RTP um eine sicherere Variante des Protokolls, die zusätzlich Verschlüsselung, Authentizität und Integrität der übermittelten Daten sowie Schutz vor Replay-Attacken bietet.

Synchrone Kommunikation
Modus der Kommunikation, bei der das Senden oder Empfangen von Daten stets unmittelbar erfolgt und die Kommunikation somit in Echtzeit stattfindet.

TEE (Trusted Execution Environment)
Eine vertrauenswürdige Ausführungsumgebung (TEE) ist ein Bereich auf dem Hauptprozessor eines Geräts, der vom (Haupt-)Betriebssystem des Systems getrennt ist. Sie gewährleistet, dass Daten in einer sicheren Umgebung gespeichert, verarbeitet und geschützt werden.

TLS (Transport Layer Security)
Verschlüsselungsprotokoll zur sicheren Datenübertragung im Internet; Weiterentwicklung von Secure Sockets Layer (SSL).

Transportverschlüsselung (Punkt-zu-Punk-Verschlüsselung)
Bezeichnung für das Senden von unverschlüsselten Daten über einen verschlüsselten Kanal bezeichnet. Außerhalb des Übertragungsweges und an den Endpunkten liegen die Daten unverschlüsselt vor.

Verfügbarkeit (Availability)
Eines der Sicherheitsziele der Kryptographie, welches den Grad der Funktionalität von IT-Systemen beschreibt und sicherstellt, dass der Zugriff oder die Verarbeitung von Daten innerhalb eines festgelegten Zeitrahmens möglich ist.

Vertraulichkeit (Confidentiality)
Eines der Sicherheitsziele der Kryptographie, welches garantiert, dass Daten vor unautorisiertem Zugriff bzw. Informationsabfluss geschützt sind.

WebRTC (Web Real-Time Communication)
Offener Standard, der eine Sammlung von Kommunikationsprotokollen und Programmierschnittstellen (API) definiert, die Echtzeitkommunikation über Rechner-Rechner-Verbindungen ermöglichen.

Zurechenbarkeit (Accountability)
Eines der Sicherheitsziele der Kryptographie, welches garantiert, dass einem Kommunikationspartner eine durchgeführte Handlung eindeutig zugeordnet werden kann.

Zwei-Faktor-Authentifizierung
Identitätsnachweis eines Nutzers mittels der Kombination zweier unterschiedlicher und insbesondere unabhängiger Komponenten (Faktoren), wie z. B. Passwort und Fingerabdruck.