**Zeitschrift:** Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology

**Herausgeber:** Swisscom

**Band:** 74 (1996)

**Heft:** 12

**Artikel:** Schutz vor Informationsgaunern mittels Verschlüsselung und digitaler Signatur

**Autor:** Keller, Peter M.

**DOI:** https://doi.org/10.5169/seals-876806

**Nutzungsbedingungen**

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

**Conditions d'utilisation**

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

**Terms of use**

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

**Download PDF:** 06.07.2025

**ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch**

GRUNDLAGEN DER KRYPTOGRAPHIE UND TRUSTED THIRD PARTIES

# SCHUTZ VOR INFORMATIONSGAUNERN MITTELS VERSCHLÜSSELUNG UND DIGITALER SIGNATUR

Verschlüsselung, symmetrische und asymmetrische Algorithmen, private und öffentliche Schlüssel, digitale Signatur, Zertifizierungsinstanzen, Schlüsselzertifikate, Revocation Lists und Trusted-Third-Party-Dienste sind alles Begriffe, welche in der heutigen Zeit des elektronischen Datenverkehrs und des Internets an Bedeutung gewonnen haben. Wie solche Sicherheitssysteme aufgebaut werden, wird in diesem Beitrag ausgeführt.

PETER M. KELLER, BERN

Seit einiger Zeit lässt sich ein Trend zur Abkehr vom Dokumentenaustausch mittels Papier beobachten. Immer mehr Geschäftsinformationen fliessen heute auf elektronischem Weg von einer Abteilung zur anderen oder von einer Firma zur anderen. Fax und E-mail sind zwei Beispiele dafür. Bei der Übermittlung von wichtigen oder vertraulichen Dokumenten stellt sich dabei automatisch die Frage nach der Sicherheit. Leider genügen viele heute bestehenden Applikationen und Systeme den hohen Sicherheitsanforderungen, die bei der Übermittlung und Verarbeitung von heiklen Daten Voraussetzung sein sollten, nicht. Ein Internet-E-mail zum Beispiel kann mit ein wenig Aufwand relativ einfach abgefangen, gelesen und verändert werden. Sogar der Name des Absenders kann ohne weiteres gefälscht werden. Dasselbe gilt grundsätzlich für jegliche Art von Datentransfer (EDI, Fax, X.400, File Transfer, Netzwerkprotokolle usw.), bei der ungeschützte, das heisst nicht durch kryptographische Massnahmen gesicherte Informationen übertragen werden. Nehmen wir beispielsweise an, jemand loggt sich von zu Hause mittels Terminal in den Zentralrechner seiner Firma ein. Die meisten heute im Einsatz stehenden Systeme verlangen dafür einen Benutzernamen und ein Passwort, das vom Benutzer zu Hause in sein Terminal getippt wird und zum Zentralrechner übermittelt wird. Dieser überprüft den Benutzernamen und das Passwort und öffnet dem Benutzer den Zugriff auf das System. Falls nun die Übertragung des Terminals zum Zentralrechner nicht mit kryptographischen Mechanismen geschützt ist, und das ist in der überwiegenden Mehrheit der Fälle so, dann kann theoretisch jeder, der sich auf irgendeine Weise Zutritt zu der Telefonleitung des Benutzers verschaffen kann, die ganze Session, beispielsweise auf Tonband, aufnehmen. Dieses kann er anschliessend in Ruhe analysieren, und er kann den Benutzernamen und das Passwort herausfinden. Nun kann er sich selber in das System einloggen, da er nun alles hat, was er dazu braucht, nämlich den Benutzernamen und das Passwort. Dieses Beispiel veranschaulicht die Problematik, die entsteht, wenn Passwörter oder allgemein schützenswerte Daten offen übermittelt werden. Dabei spielt es keine Rolle, über welche Kanäle die Übermittlung stattfindet. Die Situation ist dieselbe für eine Telefonleitung, ein LAN, ein Mobiltelefon oder eine Satellitenverbindung.

Ein gutes Beispiel für diese Problematik ist das Internet. Die Basis jeder Kommunikation über das Internet ist TCP/IP – eine Serie von Kommunikationsprotokollen, die heute aber auch für Netze, die nicht am Internet angeschlossen sind, eingesetzt werden. TCP/IP ist heute sogar das am meisten verwendete Transportprotokoll. Das Basisprotokoll der TCP/IP-Serie ist das Internet-Protokoll (IP). Nun haben die Erfinder von IP es seinerzeit unterlassen, Sicherheitsmechanismen in das Protokoll einzubauen. Die Grundeinheit des IP, das IP-Paket, kann somit unbemerkt durch jeden, der auf dessen Reise Zugriff darauf hat, abgeändert werden. So enthält das IP-Paket beispielsweise die Absender- und die Empfängeradresse des Pakets und wie diese beliebig ausgewechselt und verfälscht werden können. Das gleiche Problem bietet sich für die anderen Protokolle der TCP/IP-Serie.

Es gibt darum diverse (neue) Protokolle, die zwar alle auf TCP/IP aufbauen können, deren Sicherheit jedoch in der

Applikationsebene selber implementiert ist.
Solche neue Protokolle oder Dateiformate sind beispielsweise:
- PEM (Privacy Enhanced Mail): Internet-Standard für sicheres E-mail.
- X.400 (ITU/ISO-Standard für E-mail): Enthält Sicherheitsfunktionen ab Version 1988.
- SET (Secure Electronic Transactions): Industriestandard für On-line-Kreditkartentransaktionen (VISA, Mastercard, IBM, Netscape, Microsoft usw.).
- S-HTTP (Secure Hypertext Transport Protocol): Sicheres WWW-Grundprotokoll.
- SSL (Secure Socket Layer): Sicheres Kommunikationsprotokoll, basierend auf TCP/IP. Industriestandard. Wird heute unter anderem im Netscape Navigator und im Microsoft Explorer (die am meisten gebrauchten WWW-Browser) eingesetzt.
- IPv6 (Internet Protokoll Version 6): Neue Version des Basisprotokolls der TCP/IP-Serie. Enthält neu Sicherheitsfunktionen.

Alle diese sicheren Protokolle und Formate bauen auf sogenannten Public-Key-Systemen auf.

## Sicherheitsanforderungen

Beim Austausch von Daten unterscheidet man zwischen folgenden Anforderungen an die Sicherheit:
- *Vertraulichkeit:* Sicherstellung, dass eine Information nicht für Unbefugte zugänglich oder lesbar gemacht wird.
- *Authentifikation:* Prozess, in dem die Authentizität überprüft wird.
- *Authentizität:* Beweis einer Identität. Er bewirkt die Gewissheit, dass eine Person, eine Maschine oder ein Prozess tatsächlich derjenige ist, für den er sich ausgibt.
- *Authentizität einer Information:* Gewissheit, dass der Absender/Hersteller einer Information (Person, Maschine, Prozess) authentisch ist.
- *Nichtabstreitbarkeit des Ursprungs und Herkunftsbeweis:* Der Absender einer Information kann *nicht abstreiten,* dass die Information von ihm stammt.
- *Integrität:* Sicherstellung der Konsistenz der Information, das heisst Schutz vor Veränderung, Hinzufügung oder Löschung von Informationen.

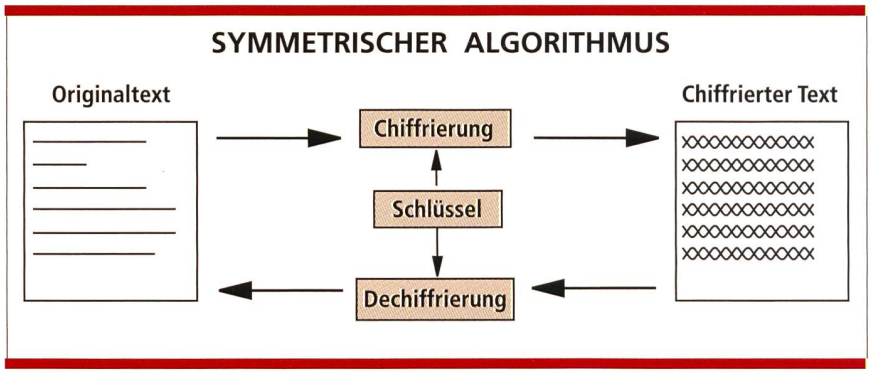


**Bild 1. Symmetrischer Algorithmus.**

Nachfolgend wird hier statt des Begriffs «Information» der Begriff «Meldung» verwendet. Eine Meldung ist eine Information[1], die von einem Absender an einen Empfänger übermittelt wird. Die Begriffe «Absender» und «Empfänger» sind hier sehr weit gefasst. Als Absender oder Empfänger können Personen, Maschinen, einzelne Hardwaremodule oder sogar einzelne Prozesse gemeint sein.
Die Authentizität des Absenders, die Integrität der Information und die Nichtabstreitbarkeit des Ursprungs der Information werden durch die Verwendung einer sogenannten *digitalen Signatur* erreicht. Eine digitale Signatur ist ein kryptographischer Code (d. h. eine Bitsequenz), der für eine bestimmte Information einzigartig ist und für dessen Herstellung ein privater Schlüssel (ebenfalls eine Bitsequenz), den nur der Verfasser besitzt, benötigt wird. Die digitale Signatur kann demnach nur vom Besitzer des privaten Schlüssels hergestellt werden. Sie wird normalerweise der Originalmeldung beigefügt.
Die Vertraulichkeit der Informationsübertragung wird durch *Verschlüsselung* erreicht. Sie besteht darin, dass die Meldung mit einem Verschlüsselungsalgorithmus und eines kryptographischen Schlüssels (Bitsequenz) in einen unleserlichen Zustand verwandelt wird. Aus der auf diese Art verwandelten Meldung kann die Ursprungsinformation nicht zurückgewonnen werden, es sei denn, man kenne den zum Entschlüsseln notwendigen Schlüssel.

## Symmetrische und asymmetrische Verschlüsselung

Man unterscheidet zwei Arten von Verschlüsselungsalgorithmen:

*Symmetrisch*

Zum Chiffrieren und Dechiffrieren (Chiffrieren = Verschlüsseln) einer Information wird derselbe kryptographische Schlüssel verwendet (Bild 1). Folglich müssen der Absender und der Empfänger im Besitz des gleichen Schlüssels sein. Ohne diesen Schlüssel ist es unmöglich[2], die Originalinformation wieder zurückzubekommen. Der heute am häufigsten verwendete symmetrische Algorithmus ist *DES* (Digital Encryption Standard). Andere Algorithmen sind beispielsweise IDEA, RC2 und RC4.

*Asymmetrisch*

Zum Chiffrieren und Dechiffrieren werden zwei verschiedene, komplementäre Schlüssel verwendet *(Schlüsselpaar),* das heisst, die Meldung wird mit dem Schlüssel 1 chiffriert und mit dem Schlüssel 2 dechiffriert (Bild 2). Diese Prozedur ist umkehrbar, das heisst, es kann auch der Schlüssel 2 zum Chiffrieren und der Schlüssel 1 zum Dechiffrieren benutzt werden. Es

[1] Als Information wird hier eine Bitfolge bezeichnet. Sie kann verschiedenste Inhalte darstellen: Text, Bild, Video, Ton, Programmcode usw.
[2] Unmöglich heisst hier, dass mit der heute mit Grossrechnern zur Verfügung stehenden Rechenleistung mehrere tausend Jahre benötigt werden, um einen Schlüssel zu knacken.

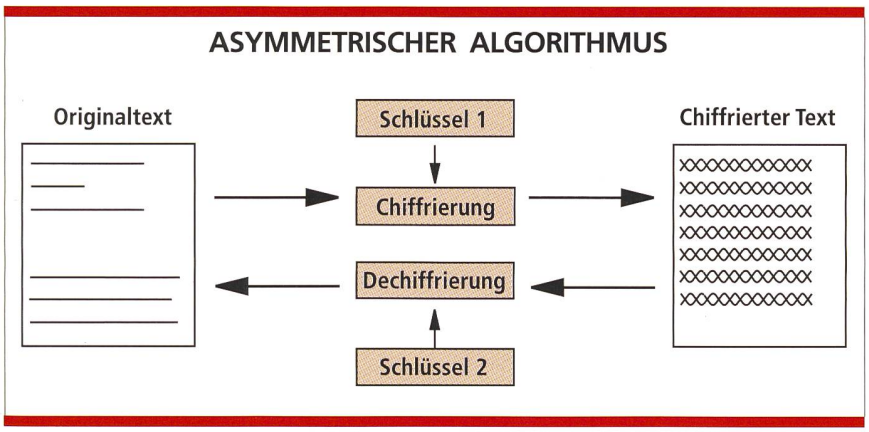


Bild 2. Asymmetrischer Algorithmus.

ist unmöglich[3], aufgrund des Schlüssels 1 den Schlüssel 2 zu rekonstruieren (oder umgekehrt). Ebenso ist es unmöglich, aufgrund der chiffrierten Information den Schlüssel zu berechnen. (Dies ist sogar dann gültig, wenn die Originalinformation bekannt ist.) Der heute mit Abstand am häufigsten verwendete asymmetrische Algorithmus ist *RSA* (benannt nach dessen Erfindern Rivest, Shamir und Adleman). Eine Variante davon ist DSS (Digital Signature Standard).
Mit Hilfe der asymmetrischen Chiffrierung kann eine sogenannte digitale Signatur hergestellt werden.

## Private und öffentliche Schlüssel

Mit Hilfe der asymmetrischen Verschlüsselungstechnik kann ein sogenanntes System von öffentlichen und privaten Schlüsseln realisiert werden (Public-key-Systeme). Dabei wird der eine Schlüssel des komplementären Schlüsselpaars als privat bezeichnet. Er ist im Besitz des Absenders und ist nur ihm bekannt. Er wird deshalb auch geheimer Schlüssel genannt (wobei dieser Begriff normalerweise für symmetrische Schlüssel verwendet wird). Der andere Schlüssel ist der öffentliche Schlüssel. Er ist allgemein zugänglich und wird an alle Teilnehmer verteilt. Wie bereits erwähnt, ist es nicht möglich, aufgrund des öffentlichen Schlüssels den privaten Schlüssel zu berechnen. Jeder Benutzer erhält ein Schlüsselpaar, bestehend aus dem privaten und dem öffentlichen Schlüssel. Dabei kann der Benutzer sein eigenes Schlüsselpaar herstellen, oder er erhält es von einer vertrauenswürdigen Instanz.
Es ist von eminenter Wichtigkeit, dass der private Schlüssel auch wirklich geheim bleibt, das heisst, dass keine andere Person ihn kennt, weil darauf die Sicherheit der digitalen Signatur aufbaut. Darum ist es ratsam, den privaten Schlüssel nur in verschlüsselter Form auf dem PC abzulegen oder noch besser auf einer Chipkarte zu speichern, die mit einem PIN geschützt ist und auf der ausserdem der Chiffrieralgorythmus direkt implementiert ist. Auf diese Weise bleibt der private Schlüssel immer im Chip und verlässt diesen in keinem Moment. Die zu verschlüsselnden Daten werden in den Chip transferiert, dort werden sie verschlüsselt und anschliessend wieder zurückgesendet. Die Tatsache nämlich, dass der private Schlüssel in den Speicher des PC übergeführt wird, könnte nämlich ein Sicherheitsrisiko bedeuten, da es nie ausgeschlossen ist, dass im PC ein Virus steckt (unbemerkt), das systematisch den Speicher eines PC abtastet und so den Schlüssel lesen könnte. Dieser wird dann beispielsweise an eine bestimmte IP-Adresse gesendet. Die Architektur des Chips ist so definiert, dass der private Schlüssel weder mit elektronischen noch mit optischen, mechanischen, chemischen oder elektromagnetischen Mitteln gelesen werden kann.
Im Gegensatz zum privaten Schlüssel ist der öffentliche Schlüssel allgemein bekannt und wird an alle Benutzer verteilt. Der Einfachheit halber wird der öffentliche Schlüssel in der Regel mit jeder Meldung mitgeschickt. Wie wir weiter unten sehen werden, braucht es dabei eine vertrauenswürdige Instanz (Zertifizierungsinstanz), die für die Echtheit der öffentlichen Schlüssel bürgt, da ein Krimineller sein eigenes Schlüsselpaar herstellen und sich als jemand anderen ausgeben kann. Diese Echtheitsgarantie geschieht in Form eines sogenannten Zertifikats.

## Die Hashfunktion

Die Hashfunktion (Bild 3) ist ein *nichtreziproker* Algorithmus, der aufgrund einer bestimmten Information beliebiger Länge einen *Hashwert (Kurzfassung/Komprimat)* fixer Länge herstellt. Er ist mit der Quersumme einer ganzen Zahl vergleichbar. Dabei ist die Länge der Meldung typischerweise um einiges grösser als der daraus berechnete Hashwert. So kann die Meldung beispielsweise mehrere Megabytes umfassen, wogegen der Hashwert nur

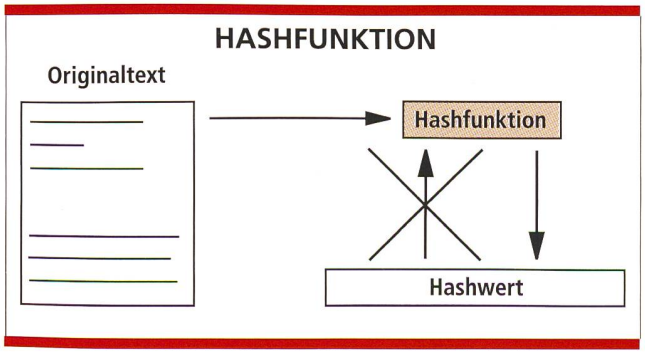


Bild 3. Hashfunktion.

[3] Unmöglich heisst hier, dass mit der heute mit Grossrechnern zur Verfügung stehenden Rechenleistung mehrere tausend Jahre benötigt werden, um den komplementären Schlüssel zu finden.



2

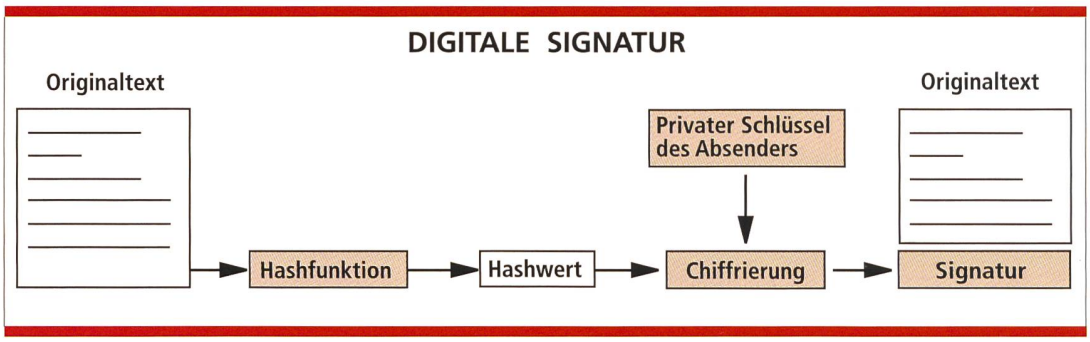


Bild 4. digitale Signatur.

128 bit lang ist. Es ist zu beachten, dass aufgrund des Hashwerts nicht auf die Originalinformation zurückgeschlossen werden kann (Nichtreziprokität) und dass es extrem schwierig ist, die Information so zu modifizieren, dass sie den gleichen Hashwert ergibt. Zweck einer solchen Funktion ist die Herstellung eines kurzen, für das jeweilige Dokument einzigartigen Codes. Dieser wird für die Herstellung der *digitalen Signatur* benutzt. Beispiele von Hashalgorithmen sind MD4 (Message Digest 4), MD5, RIPE-MD und SHA (Secure Hash Algorithm).

## Die digitale (elektronische) Signatur

Jeder Benutzer erhält einen privaten und einen öffentlichen Schlüssel. Um eine Meldung digital zu signieren, wird er *mit dem privaten Schlüssel des Absenders chiffriert.* Das Resultat ist die digitale Signatur (Bild 4). Da aber die so entstandene Signatur die gleiche Grösse wie die Originalmeldung aufweist (unter Umständen mehrere Megabytes), wird zuerst der Hashwert der Meldung berechnet. Wie schon erwähnt, hat der Hashwert eine fixe Länge, und er ist für eine bestimmte Meldung einzigartig. Statt der Originalmeldung wird nun deren Hashwert unterschrieben. Die so entstandene digitale Signatur wird dem Originaldokument beigefügt. Das Ganze wird dann an den Empfänger verschickt.

Da nur der Absender des Dokuments im Besitz seines privaten Schlüssels ist, kann nur er die digitale Signatur herstellen. Hier liegt denn auch die Analogie zu einer handschriftlichen Unterschrift. Die digitale Signatur besitzt aber gewisse Eigenschaften, die bei der handschriftlichen Unterschrift nicht vorhanden sind. So kann beispielsweise bei einem handschriftlich unterschriebenen Vertrag nicht ausgeschlossen werden, dass keine Information unbemerkt hinzugefügt oder gelöscht wurde, was bei der digitalen Signatur nicht möglich ist. Die digitale Signatur bietet also sogar eine noch bessere Sicherheit als die traditionelle handschriftliche Unterschrift.

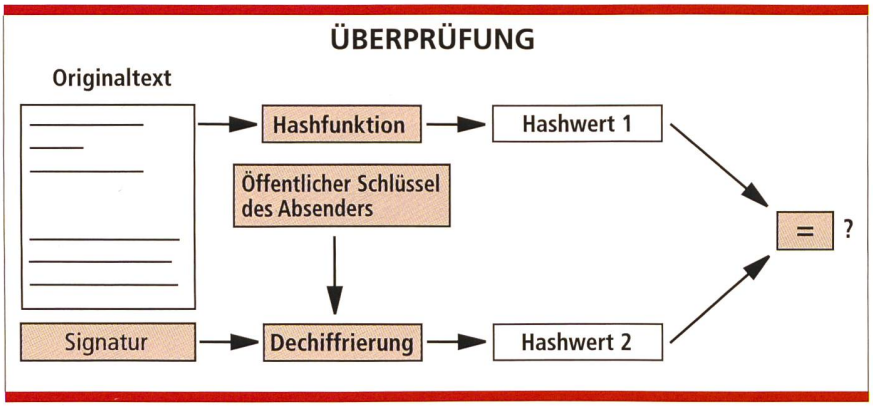


Bild 5. Überprüfung der digitalen Signatur.

## Überprüfung der digitalen Signatur

Da der öffentliche Schlüssel an alle Benutzer verteilt wird und somit allgemein bekannt ist, kann jeder Empfänger die digitale Signatur überprüfen (Bild 5). Dazu dechiffriert er die digitale Signatur *mit dem öffentlichen Schlüssel des Absenders.* Das Resultat ist der *Hashwert* der Originalmeldung. Parallel dazu berechnet der Empfänger den Hashwert des Originaldokuments, das ja ebenfalls (zusammen mit der Signatur) an ihn übermittelt wurde. Diesen resultierenden zweiten Hashwert *vergleicht* der Empfänger nun mit dem aus der Signatur dechiffrierten Hashwert. Stimmen die beiden Hashwerte miteinander überein, so ist die digitale Signatur authentisch. Wenn nun die Originalmeldung während der Übermittlung verändert wird (ein Bit genügt), so wird sich auch deren Hashwert verändern. Somit würde der Empfänger feststellen, dass der Hashwert, den er aufgrund der Originalmeldung berechnet hat, nicht mit dem aus der Signatur dechiffrierten Hashwert übereinstimmt, was bedeutet, dass die Signatur nicht korrekt ist[4]. Folglich hat der Empfänger bei einer erfolgreichen Überprüfung der digitalen Signatur die Garantie, dass die Meldung nicht verändert wurde *(Integrität).*

Da nur der Hersteller einer Signatur im Besitz seines privaten Schlüssels ist, kann nur er die digitale Signatur herstellen. Dies bedeutet, dass der Empfänger, der die digitale Signatur besitzt, nachweisen kann, dass nur der Absender die Signatur herstellen

[4] Dies bedeutet, dass entweder die Information verändert wurde oder dass die digitale Signatur verändert wurde.

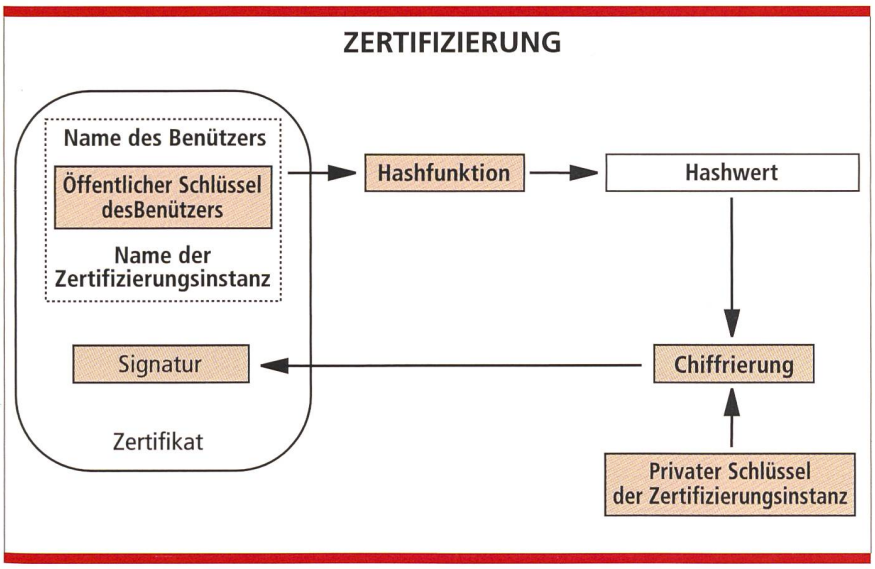


**Bild 6. Zertifizierung des öffentlichen Schlüssels durch die CA.**

konnte *(Nichtabstreitbarkeit des Informationsursprungs).*

## Zertifizierung des öffentlichen Schlüssels

Die digitale Signatur ermöglicht also die Nichtabstreitbarkeit des Ursprungs und die Integritätsgarantie einer Meldung. Nun bleibt aber noch ein Sicherheitsproblem, nämlich die *Echtheitsgarantie des öffentlichen Schlüssels des Absenders.* Bis jetzt hat nämlich der Empfänger keine Garantie, dass der öffentliche Schlüssel tatsächlich derjenige des Absenders ist. Die Signatur kann zwar gültig sein, der damit verbundene öffentliche Schlüssel könnte aber theoretisch von einem Betrüger stammen.

Nehmen wir an, ein Krimineller will jemanden zur Lieferung einer teuren Ware bewegen. Nichts hält ihn davon ab, selber einen öffentlichen und einen privaten Schlüssel zu generieren, die falsche Bestellung zu unterschreiben und die Bestellung mit der Signatur zu versenden. Dann sendet er die mit seinem eigenen Schlüssel unterschriebene Bestellung mit dem öffentlichen Schlüssel an den Empfänger, und zwar *unter einem falschen Namen.* Der Empfänger kann nicht feststellen, ob die Bestellung tatsächlich von der Person gesendet wurde, für die sie sich ausgibt. Die Signatur mag korrekt sein, aber der Empfänger hat keinen Anhaltspunkt dafür, dass der öffentliche Schlüssel, den er soeben erhalten hat, tatsächlich der richtigen Person gehört.

Der Empfänger einer Meldung braucht also die Gewissheit, dass der öffentliche Schlüssel des Absenders, in dessen Besitz er ist, tatsächlich dem richtigen Absender gehört. Diese Gewissheit kann er auf verschiedene Weise erlangen. Eine Möglichkeit ist, dass der Absender ihm den öffentlichen Schlüssel irgendwann einmal persönlich übergeben hat. Oder der Empfänger ruft den Absender an und vergleicht beispielsweise die ersten zehn Stellen des öffentlichen Schlüssels. Diese Methoden sind jedoch umständlich und bedingen, dass sich die Benutzer entweder schon kennen oder sich vorher getroffen haben. Dies ist aber oft nicht der Fall. Nehmen wir an, ein Schweizer will einem Schweden, den er vorher noch nie gesehen hat und dessen Stimme er nicht kennt, ein sicheres E-mail schicken. Der Schwede könnte nun dem Schweizer seinen öffentlichen Schlüssel per E-mail schicken, jedoch hat der Schweizer keine Möglichkeit, die Echtheit dieses öffentlichen Schlüssels mit der dafür nötigen Gewissheit festzustellen.

Eine bessere Lösung wäre es, wenn es eine Instanz gäbe, welche die Zugehörigkeit eines öffentlichen Schlüssels zu einer gewissen Person garantiert. Diese Instanz wird *Zertifizierungsinstanz (Certification Authority, CA)* genannt, und sie bürgt dafür, dass ein bestimmter öffentlicher Schlüssel einer bestimmten Person gehört[5]. Sie tut dies, indem sie ein sogenanntes Zertifikat des öffentlichen Schlüssels herstellt. Es besteht im wesentlichen aus dem öffentlichen Schlüssel und dem Namen des Besitzers. Das ganze wird dann von der Zertifizierungsinstanz signiert (Bild 6). Durch die Zertifizierung *bindet* die CA also einen öffentlichen Schlüssel an eine bestimmte Person (oder eine Maschine oder einen Prozess). Für alle Benutzer wird so von der CA ein Zertifikat des öffentlichen Schlüssels ausgestellt. *Diese Zertifikate sind für alle Benutzer zugänglich.*

Durch die Überprüfung der digitalen Signatur des Zertifikats des Absenders sowie der Signatur der Meldung selbst hat ein Empfänger den Beweis, dass die Meldung von demjenigen unterschrieben wurde, der sich als Absender ausgibt *(Authentifikation).*

Es ist zu beachten, dass die Schlüsselzertifikate nicht speziell geschützt werden müssen, da sie unfälschbar sind. Falls der Zertifikatsinhalt nämlich verändert wurde, merkt dies der Empfänger, da die Signatur nicht mehr korrekt ist. Und da niemand ausser der CA den privaten Schlüssel der CA hat, ist es niemandem möglich, die Signatur der CA zu fälschen.

Es gibt verschiedene Möglichkeiten, wie die Schlüsselzertifikate verbreitet werden können. Eine Möglichkeit ist, die Zertifikate mit jeder Meldung mitzuschicken (mit dem Nachteil, dass dadurch die übertragene Datenmenge unter Umständen stark anwachsen kann). Um jedoch jemandem eine vertrauliche, das heisst verschlüsselte Information zu übermitteln, *braucht der Absender das Zertifikat des Empfängers.* Falls er dieses nicht hat (z. B. bei der ersten Kontaktaufnahme), muss er es entweder direkt vom Empfänger verlangen, oder er holt es aus einem öffentlich zugänglichen Zertifikatsverzeichnis. Je nach Situation und Art der Benutzer (innerhalb der Firma, weltweit usw.) kann dieses Verzeichnis ein verteiltes Verzeichnis (X.500) oder ein Datenserver sein. Bei einer kleinen Anzahl von Benutzern können die Zertifikate auch in einer einzigen, an alle verteilten Datei enthalten sein. Verschiedene Kombinationen sind ebenfalls denkbar. Besonders in einem multinationalen offenen System von po-

[5] Damit bürgt sie gleichzeitig dafür, dass der dazugehörige private Schlüssel der Person gehört.

tentiell vielen Benutzern (Tausende bis Millionen) wird das Zertifikatsverzeichnis zu einer der wichtigsten Komponenten, da es die Schlüsselrolle bei der sicheren Kontaktaufnahme zweier Benutzer einnimmt.
Mit Hilfe der hier beschriebenen Techniken können also zwei einander unbekannte Personen, Maschinen oder Prozesse gegenseitig Informationen austauschen, und dies auf eine sichere Art und Weise. Möglich wird dies durch die CA. Die grundlegende Bedingung ist dabei, dass die CA *das Vertrauen aller Benutzer* geniesst. Theoretisch könnte die CA nämlich beispielsweise einen bestimmten öffentlichen Schlüssel unter einem falschen Namen zertifizieren (absichtlich oder durch Fahrlässigkeit). Dabei basiert das Vertrauen des Benutzers in eine CA nicht auf rein technischen Aspekten, sondern hängt vielmehr von der Art ab, wie die CA ihre Dienste anbietet,

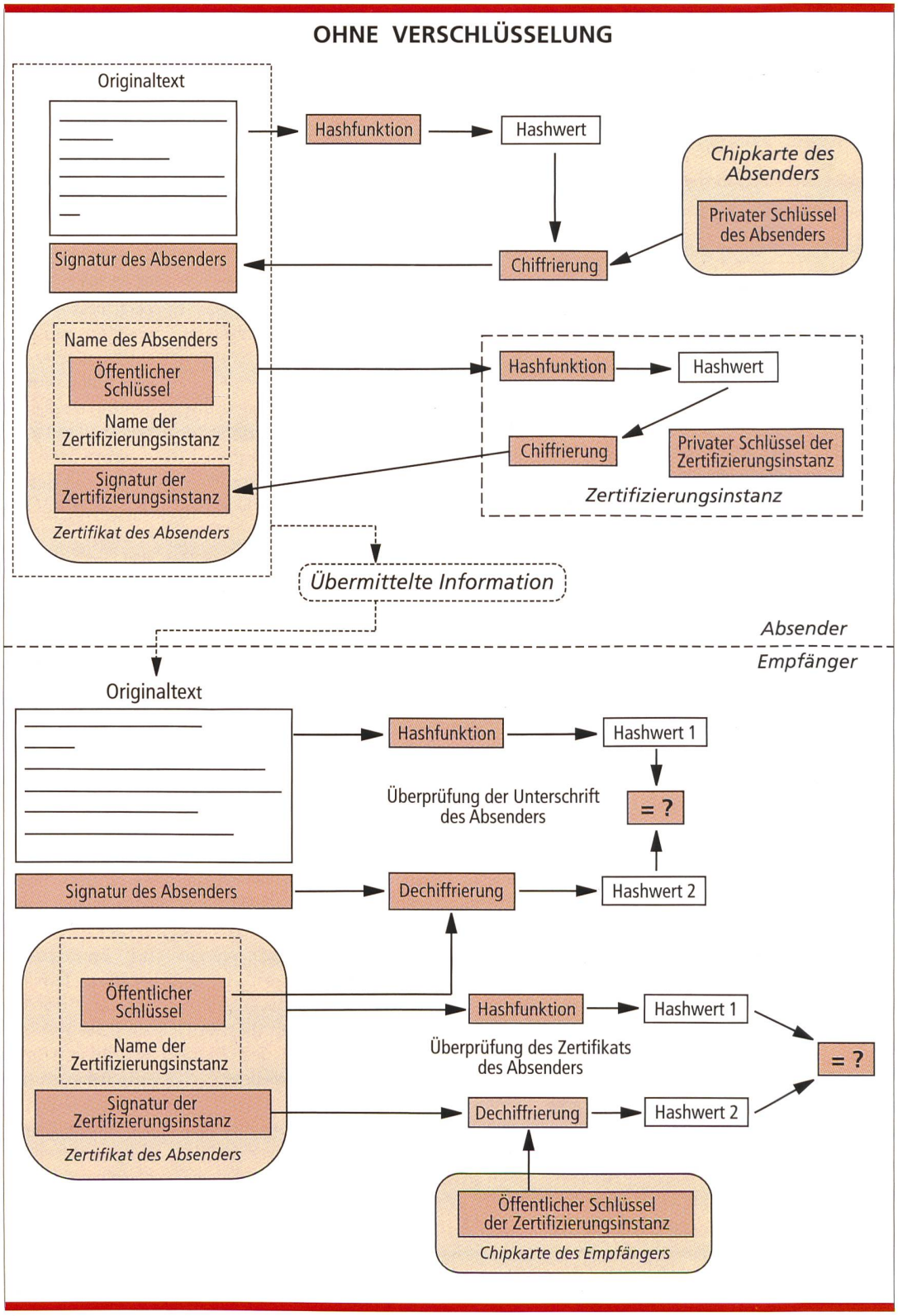


**Bild 7. digitale Signatur ohne Verschlüsselung.**

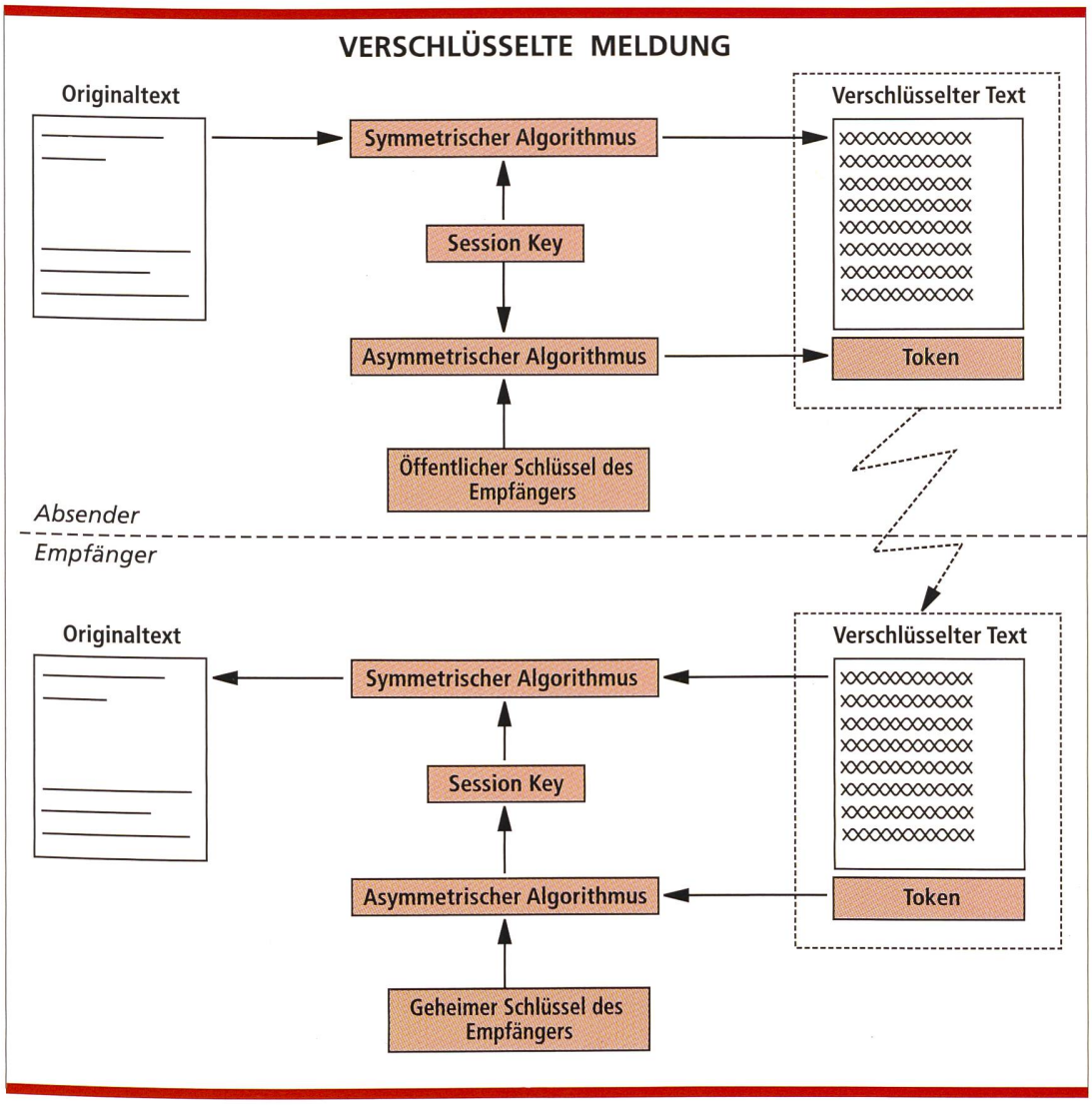


**Bild 8. Übermittlung einer verschlüsselten Meldung (ohne Unterschrift).**

wie seriös sie die Benutzer identifiziert, wie sicher ihre physikalische Arbeitsumgebung ist, welche Sicherheitsmassnahmen sie intern trifft usw.

## Verteilung des öffentlichen Schlüssels der Zertifizierungsinstanz

Nun bleibt noch ein letztes Problem. Wie im vorhergehenden Kapitel beschrieben, überprüft der Empfänger einer Meldung das Zertifikat des Absenders. Dazu benötigt er den öffentlichen Schlüssel der Zertifizierungsinstatz. Die CA könnte nun zwar ihren eigenen öffentlichen Schlüssel zertifizieren; dies macht aber wenig Sinn, da es ja jedem möglich ist, selber ein Schlüsselpaar zu generieren und selbst ein CA-Zertifikat (mit dem entsprechenden Namen der CA) herzustellen. Für den öffentlichen Schlüssel der CA gibt es also *kein eigentliches Zertifikat.* Diese Tatsache erlaubt theoretisch einem Kriminellen, sich als Zertifizierungsinstanz auszugeben und so falsche Schlüsselpaare und Zertifikate herzustellen und zu verteilen. Darum muss der öffentliche Schlüssel der Zertifizierungsinstanz *auf einem sicheren Weg zum Benutzer gelangen.* Der Benutzer muss *überzeugt* sein, den richtigen Schlüssel der CA zu besitzen.

Eine Lösung, die sich sofort anbietet, ist, den öffentlichen Schlüssel der Zertifizierungsinstanz *in der Chipkarte des Benutzers* zu speichern. Jener kann zwar (im Gegensatz zum privaten Schlüssel des Benutzers) gelesen, aber nicht überschrieben oder gelöscht werden. Dies wird durch die spezielle Architektur des Chips erreicht.

Falls keine Chipkarten eingesetzt werden, muss der Schlüssel auf einem anderen sicheren Kanal zum Benutzer gelangen (z. B. auf Diskette mit eingeschriebenem Brief).

Es ist ausserdem denkbar, dass der öffentliche Schlüssel der CA (oder Teile davon) so häufig publiziert, veröffentlicht und vervielfältigt wird (z. B. Telefonbücher, Telefonserver, Plakate, Verzeichnisdienste usw.), dass ein Krimineller gar nicht die Möglichkeit hat, seinen falschen Schlüssel in gleichem Masse zu publizieren. In diesem Fall wird die Sicherheit durch die starke Publikation des öffentlichen Schlüssels der CA erreicht.

| | |
|---|---|
| Verschlüsselung/ Chiffrierung | Umwandlung einer bestimmten Information (Bitsequenz) in einen unleserlichen Zustand mit einem kryptographischen Schlüssel |
| Entschlüsselung/ Dechiffrierung | Zurückwandlung einer verschlüsselten Information mit einem kryptographischen Schlüssel |
| (Kryptographischer) Schlüssel | Bitsequenz, mit dessen Hilfe eine bestimmte Information ver- oder entschlüsselt wird |
| Symmetrischer Algorithmus | Kryptographischer Verschlüsselungsalgorithmus, bei dem der Schlüssel für die Ver- und Entschlüsselung der gleiche ist |
| Asymmetrischer Algorithmus | Kryptographischer Verschlüsselungsalgorithmus, bei dem die Schlüssel für die Verschlüsselung und die Entschlüsselung verschieden sind |
| Geheimer Schlüssel | Symmetrischer Schlüssel, der nur dem Absender und dem Empfänger einer Information bekannt ist |
| Privater Schlüssel | Asymmetrischer Schlüssel, der nur einem einzigen Benutzer bekannt ist und nur von diesem verwendet werden kann |
| Öffentlicher Schlüssel | Asymmetrischer, zum privaten Schlüssel komplementärer Schlüssel, der allen Benutzern zugänglich ist und der veröffentlicht wird |
| Schlüsselpaar | Privater und öffentlicher Schlüssel |
| Digitale Signatur (elektronische Unterschrift) | Bitsequenz als Resultat aus einer asymmetrischen Verschlüsselung mit einem privaten Schlüssel |
| Zertifizierungsinstanz/ Certification Authority (CA) | Unabhängige Instanz, die für die Zugehörigkeit eines öffentlichen Schlüssels zu einer bestimmten Person garantiert |
| Schlüsselzertifikat/ Public Key Certificate | Es bindet einen öffentlichen Schlüssel an einen Namen eines Benutzers.<br>Es enthält im wesentlichen:<br>• eine Seriennummer<br>• den öffentlichen Schlüssel eines Benutzers<br>• den Namen des Benützers<br>• den Namen der Zertifizierungsinstanz<br>• eine Gültigkeitsperiode<br>Dieser Information wird die digitale Signatur der Zertifizierungsinstanz hinzugefügt. |
| Certificate Revocation List | Von der Zertifizierungsinstanz erstellte Liste der für ungültig erklärten Zertifikate. Ein Eintrag in der Liste enthält:<br>• die Seriennummer des Zertifikats<br>• das Datum, an dem das Zertfikat für ungültig erklärt wurde<br>Die Liste wird von der Zertifizierungsinstanz digital signiert. |
| Querzertifikat/Cross Certificate | Zertifikat einer anderen CA |

**Tabelle 1. Begriffe.**

## Übermittlung einer digital signierten Meldung ohne Chiffrierung

- Der Absender unterschreibt die Meldung mit seinem privaten Schlüssel, um dessen Ursprung zu bestätigen.
- Die Originalmeldung wird zusammen mit der Signatur und dem Zertifikat des Absenders an den Empfänger gesendet.
- Der Empfänger überprüft die digitale Signatur des Dokuments mit Hilfe des im Zertifikat des Absenders mitgeschickten öffentlichen Schlüssels des Absenders.
- Ausserdem versichert er sich der Echtheit des öffentlichen Schlüssels des Absenders, indem er die digitale Signatur des Zertifikats überprüft.

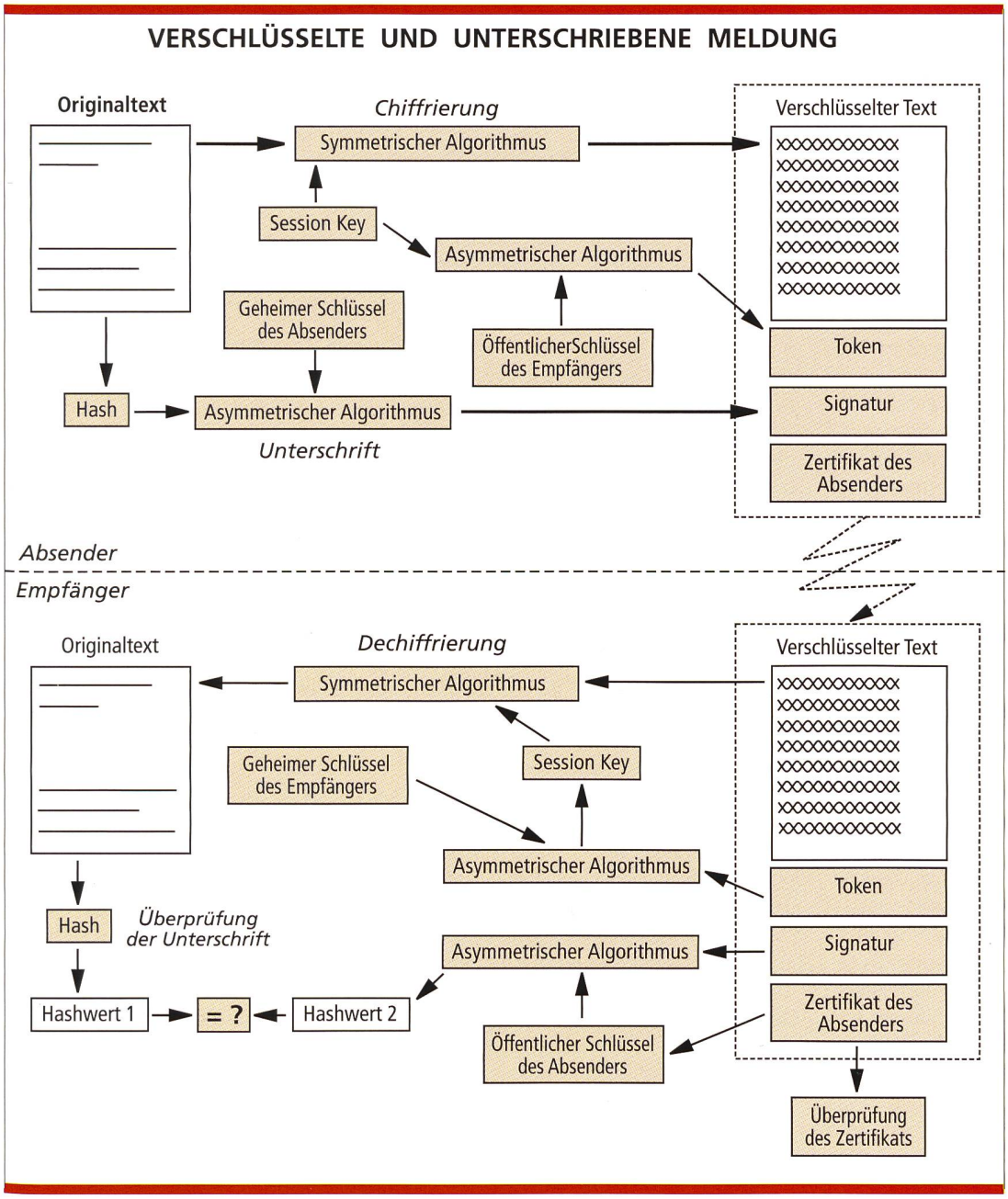


**Bild 9. Übermittlung einer verschlüsselten und unterschriebenen Meldung.**

Dazu verwendet er den öffentlichen Schlüssel der Zertifizierungsinstanz (Bild 7).

## Chiffrierung der Meldung

Wenn die *Vertraulichkeit* einer Übermittlung, das heisst der Schutz vor der Einsichtnahme durch Unbefugte, gewährleistet sein soll, muss die Meldung verschlüsselt (chiffriert) werden. Dafür gibt es theoretisch zwei Möglichkeiten. Man könnte die Meldung mit dem öffentlichen Schlüssel des Empfängers verschlüsseln. Da nur der Empfänger im Besitz des dazugehörigen privaten Schlüssels ist, kann folglich nur er die Meldung entschlüsseln. Nun ist es aber so, dass die asymmetrischen Chiffrieralgorithmen im Vergleich zu den symmetrischen *sehr langsam* sind. Wenn man sich vorstellt, dass die Meldung unter Umständen mehrere Megabytes umfassen kann, spielt dieser Zeitaufwand eine entscheidende Rolle. (Die Chiffrierung mehrerer Megabytes mit einem asymmetrischen Algorithmus benötigt je nach Rechenleistung Minuten bis Stunden.)

Darum weicht man in der Regel auf einen *symmetrischen Algorithmus* für die Chiffrierung der Meldung aus. Der Absender einer Meldung *generiert einen symmetrischen Schlüssel,* mit dessen Hilfe er die Meldung verschlüsselt. Diese symmetrische Verschlüsselung nimmt nur einen Bruchteil der Zeit in Anspruch, die bei der Verwendung eines asymmetrischen Algorithmus benötigt würde. (Sie beträgt typischerweise ein paar Sekunden.) Dies bedeutet aber, dass der Empfänger *denselben symmetrischen Schlüssel* kennen muss. Er muss ihm also übermittelt werden, und zwar *verschlüsselt,* da sonst ein Betrüger den Schlüssel bei der Übertragung mitlesen und die Meldung entschlüsseln könnte.

Darum wird der symmetrische Schlüssel, der sogenannte *Session Key,* mit dem *öffentlichen Schlüssel des Empfängers* verschlüsselt. Der so entstandene verschlüsselte Session Key wird auch *Token* genannt. Der Token enthält also den für die Chiffrierung der Meldung benützten symmetrischen Schlüssel, verschlüsselt mit dem öffentlichen (asymmetrischen) Schlüssel des Empfängers. Der Token wird zusammen mit der verschlüsselten Meldung, der Signatur und dem Zertifikat übermittelt (Bild 8).
Der Empfänger entschlüsselt den Token mit seinem privaten Schlüssel. So erhält er den für das Entschlüsseln der Meldung benötigten symmetrischen Schlüssel. Da nur er den privaten Schlüssel hat, kann nur er den Token entschlüsseln und somit die Meldung dechiffrieren *(Vertraulichkeit).*

## Übermittlung einer digital signierten Meldung mit Chiffrierung

*Absender:*
- Der Absender unterschreibt die Meldung mit seinem privaten Schlüssel (Session key). Dann verschlüsselt er die Meldung mit einem von ihm generierten symmetrischen Schlüssel.
- Diesen symmetrischen Schlüssel verschlüsselt er dann mit dem öffentlichen Schlüssel des Empfängers. Daraus entsteht der Token.
- Die Originalmeldung wird dann zusammen mit der Signatur, dem Token und dem Zertifikat an den Empfänger gesendet.

*Empfänger:*
- Der Empfänger entschlüsselt zunächst den Token mit seinem privaten Schlüssel.
- Mit dem daraus gewonnenen symmetrischen Schlüssel entschlüsselt er die Meldung.
- Nun überprüft er die digitale Signatur des Dokuments mit Hilfe des im Zertifikat des Absenders enthaltenen öffentlichen Schlüssels.
- Ausserdem versichert er sich der Echtheit des öffentlichen Schlüssels des Absenders, indem er die digitale Signatur des Zertifikats durch die Zertifizierungsinstanz überprüft. Dazu verwendet er den öffentlichen Schlüssel der Zertifizierungsinstanz (Bild 9).

## Revocation List/ Ungültigkeitserklärung von Zertifikaten

Nehmen wir an, einem Benutzer wird die Smart Card, welche seinen privaten Schlüssel enthält, mitsamt dem PIN-Code gestohlen. Der Einbrecher kann nun diesen privaten Schlüssel einsetzen und sich für den Bestohlenen ausgeben, ohne dass dies der Empfänger merkt. Darum braucht es einen Mechanismus, um allen Benutzern mitzuteilen, dass das zum gestohlenen privaten Schlüssel gehörige Zertifikat nicht mehr gültig ist. Dies geschieht mit einer sogenannten Liste von ungültigen Zertifikaten, einer *Certificate Revocation List (CRL).* Sie wird von der CA digital signiert und veröffentlicht, das heisst, sie wird allen Benutzern zugänglich gemacht (entweder mit einem Verzeichnis oder mittels Zusendung der Liste an alle Benutzer). Jeder Empfänger einer Meldung muss nun also zusätzlich zu der Überprüfung der Signatur und des Zertifikats des Absenders kontrollieren, ob letzteres sich nicht in der Revocation List befindet, das heisst, ob es nicht ungültig ist. Falls dies aber der Fall ist, sollte der Empfänger der Signatur nicht trauen und sich bewusst sein, dass ein anderer als der angegebene Absender die Signatur geleistet haben könnte.
Damit die Revocation List nicht zu gross wird, wird statt des ganzen Zertifikats nur die Seriennummer sowie das Datum, an dem das Zertifikat für ungültig erklärt wurde, eingefügt. Die Liste besteht also aus Seriennummern und Ungültigkeitserklärungsdaten, welche am Schluss von der CA digital signiert wird. Vorhanden sind ebenfalls das Veröffentlichkeitsdatum der Liste und der Name der CA.

## Das Trust Center und Trusted-Third-Party-Dienste

Wie wir gesehen haben, braucht es in einem offenen und verteilten System von vielen Benutzern, in dem zwei Benutzer, die über kein gemeinsames Vertrauensverhältnis verfügen, sicher miteinander kommunizieren wollen, eine dritte Stelle, die diesen Benutzern gewisse Sicherheitsdienste zur Verfügung stellt, da nämlich sonst für die Benutzer der Aufwand zu gross wird, selber die notwendigen Schlüssel auszutauschen und zu verwalten. Diese Stelle wird *Trust Center* oder *Trusted Third Party (TTP)* genannt, und die Dienste, die sie anbietet, werden als *TTP-Dienste* bezeichnet. Die CA ist beispielsweise ein solcher Dienst. Die TTP übernimmt die Schlüsselverwaltungsaufgaben für die Benutzer und geniesst darum deren Vertrauen. TTP-Dienste dienen also zur Sicherung von diversen Applikationen und Protokollen. Da die Sicherheitsmechanismen

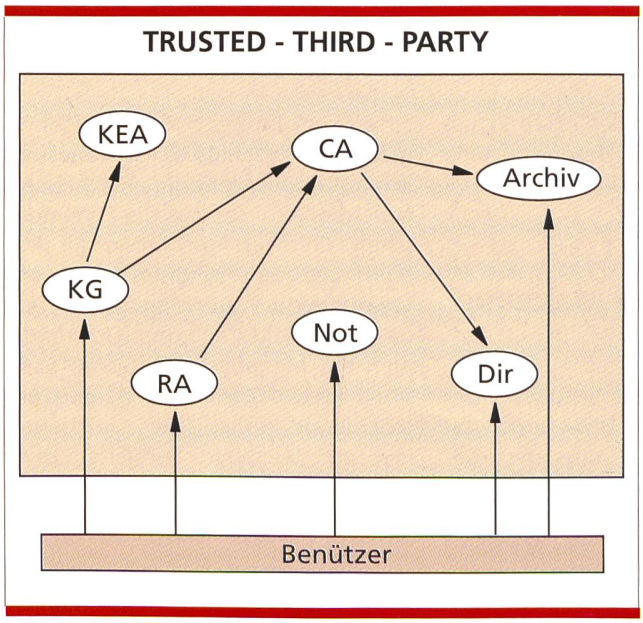


**Bild 10. Trusted Third Party. CA = Certification Authority/Zertifizierungsinstanz, RA = Registration Authority/Registrierungsinstanz, KG = Key Generation/Schlüsselgenerierungsstelle, KEA = Key Escrow Agency/Schlüsselhinterlegungsstelle, Dir = Directory/Verzeichnisdienst, Not = Notary/Notariatsdienste, Archiv = Archivierungsdienst für Zertifikate.**

immer die gleichen sind, kann ein Kunde denselben TTP-Dienst für diverse Applikationen und Netzwerkprotokolle beanspruchen.

Die Bestandteile einer TTP sind:
- *Registrierungsinstanz (RA):* Sie identifiziert die Benutzer, nimmt ihre Daten auf und leitet sie an die Zertifizierungsinstanz weiter. Die Identifikation der Benutzer ist nötig, da ja die CA dafür garantiert, dass ein bestimmter öffentlicher Schlüssel einer bestimmten Person gehört. Dafür muss sich diese Person aber zuerst identifizieren.
- *Zertifizierungsinstanz (CA):* Sie stellt die Schlüsselzertifikate und Revocation Lists her. Diese werden anschliessend zur Veröffentlichung in ein Verzeichnis abgelegt oder direkt den Benutzern zugesandt.
- *Schlüsselgenerierungsdienst:* Er generiert die Schlüssel für die Benutzer. Der private Schlüssel wird auf einem sicheren Kanal dem Benutzer übergeben, der öffentliche Schlüssel wird an die CA gesendet zwecks Zertifizierung.
- *Schlüsselpersonalisierungsdienst:* Er legt die privaten Schlüssel in einem Modul (z. B. einer Chipkarte) ab, um sie vor unbefugtem Zugriff zu schützen.
- *Schlüsselhinterlegungsdienst (Key Escrow):* Er speichert eine Kopie der verwendeten Schlüssel (zwecks Rückerstattung im Falle eines Verlusts oder zwecks «Abhören» der Polizei aus Staatsschutz- oder Verbrechensbekämpfungsgründen).
- *Archivierungsdienst:* Er archiviert die Schlüsselzertifikate (zwecks langfristiger Garantie der Überprüfbarkeit von digitalen Signaturen)
- *Verzeichnisdienst:* Er stellt den Benutzern Schlüsselzertifikate und Revocation Lists zur Verfügung.
- *Notariatsdienste* für
  Sende- und Empfangsbeweis
  Zeitstempel
  Beglaubigung der inhaltlichen Korrektheit (analog zu bestehenden Notariatsdiensten)

Der hier verwendete Begriff «Benutzer» beschränkt sich nicht nur auf eine Person, sondern es kann damit auch eine Maschine, ein Hardwaremodul oder sogar ein einzelner Prozess gemeint sein.
TTP ist also ein Oberbegriff, unter dem diverse TTP-Dienste gemeint sind. Eine TTP kann entweder alle in Bild 10 beschriebenen Dienste anbieten oder nur eine Untermenge davon.

## Transparenz der Sicherheitsabläufe für den Endbenutzer

In den bereits geschilderten Abläufen steht häufig geschrieben «Der Empfänger überprüft die Signatur» oder «Der Absender verschlüsselt die Meldung». Natürlich muss der Benutzer all diese Funktionen im Normalfall nicht explizit selber ausführen, sondern das System macht das für ihn automatisch. Dabei sind diese Aktionen für den Benutzer mehr oder weniger transparent, das heisst, die Funktionen laufen zum Teil im Hintergrund ab. Der Benutzer erfährt nur das Endresultat der verschiedenen Aktionen. Der Grad der Transparenz hängt von der jeweiligen Implementierung sowie von der unterstützten Applikation ab. Wichtig ist allerdings, dass bei der Generierung der digitalen Signatur der Benutzer explizit darauf hingewiesen wird, dass er nun im Begriff ist, eine solche zu tätigen. 9.4


## SUMMARY

**Encryption, symmetric and asymmetric cryptographic algorithms, private and public keys, digital signatures, public key certificates, certification authorities, revocation lists and Trusted Third Parties are terms which are of more and more importance when solving security problems in today's information technology systems. This paper explains the underlying technology and the services that are needed to support security in IT-systems.**

**Peter M. Keller** schloss sein Studium 1994 an der ETH Lausanne mit dem Diplom eines Elektroingenieurs ETH, Fachrichtung Telekommunikation, ab. Seitdem arbeitet er in der Direktion Forschung und Entwicklung der Telecom PTT, Gruppe für Sicherheitsdienste. Er befasst sich mit sicheren Informationsverarbeitungs-Systemen und -Applikationen sowie mit Trusted-Third-Party-Sicherheitsdiensten.