GISnet 2000
Geographische Informationssysteme
28.-30. März 2000, Messe Essen

Datensicherheit bei der Internet-basierten Vermarktung von Geodaten

Prof. Dr. Wolf-Fritz Riekert
Hochschule für Bibliotheks- und Informationswesen (HBI) Stuttgart

mailto:riekert@hbi-stuttgart.de
http://v.hbi-stuttgart.de/~riekert

Inhalt

- Das Internet als Marktplatz für Geodaten
- Fragestellungen
  - ⇨ Wie können meine Kunden sichere Bestellvorgänge im Internet tätigen?
  - ⇨ Inwieweit können wertvolle Geodaten sicher über das Internet übertragen werden?
  - ⇨ Wie können sich meine Kunden digital ausweisen?
  - ⇨ Wie können Daten und Dienste auf sichere Weise bezahlt werden?
- Ein kleiner Lehrgang
  - ⇨ Kryptographie (Verschlüsselungstechnologie)
  - ⇨ Digitale Zahlungssysteme
- Praktische Lösungsvorschläge

Das Internet als Marktplatz für Geodaten

Ziel: Alle wesentlichen Vorgänge des Erwerbs von Geodaten sollen rein digital vonstatten gehen:

- Anbieten der Geodaten
- Suchen nach geeigneten Geodaten
- Selektieren der Geodaten
- Preview (Vorschau) der Geodaten
- Prüfung der Berechtigung des Kunden zum Erwerb der Geodaten
- Kaufabschluss / Nutzungsvereinbarung
- Auslieferung der Geodaten
- Bezahlung der Geodaten

Internet-basierte Vermarktung von Geodaten: Wo liegt das Problem?

Naheliegende Lösung:

- Man nehme
  - ⇨ ein GIS,
  - ⇨ eine marktgängige Webshop-Software
- und kopple beide Komponenten.
- Fertig!

Leider funktioniert das nicht!

Die Internet-basierte Vermarktung von Geodaten stellt andere Anforderungen als der Internet-Auftritt eines Artikelversands.

Das Internet als Marktplatz: Versand von Artikeln vs. Vermarktung von Geodaten

	Versandartikel	Geodaten
Art der Ware	physisch (materiell)	digital (immateriell)
Herkunft	aus dem Regal	oft Einzelanfertigung
Auftragsdaten	Artikelnummer	räuml.-them. Selektion
Preview	dig. Photo/Video	oft identisch mit Ware
Preis	nach Katalog	oft erst nach Selektion ermittelbar
Auslieferung	per Postfracht o.ä.	per Internet
Identität des Kunden	wichtig für Bonität, Lieferadresse	wichtig für Bonität, Berechtigungsprüfung

Besondere Herausforderung für öffentliche Institutionen

Einerseits erwarten E-Commerce-Kunden eine Bearbeitung ihrer Bestellung in **Echtzeit.**

Andererseits sind öffentliche Institutionen (z.B. Vermessungsämter) durch den Gesetzgeber auf **komplizierte Regelungen** verpflichtet:

- Bürokratische Gebührenordnungen:
  - ⇨ Gebührenberechnung umständlich, oft erst nach Auftragsbearbeitung möglich, im Extremfall nicht automatisierbar.
  - ⇨ hoher Arbeitsaufwand beim Einzug insbesondere von kleinen Beträgen (Micropayment).
- Enggefasste Datenschutzrichtlinien
  - ⇨ komplizierte Abläufe bei der Berechtigungsprüfung.

Systeme zur Internet-basierten Vermarktung von Geodaten

Systeme zur Internet-basierten Vermarktung von Geodaten sind an vielen Orten am Entstehen:

- Marktgängige Webshops nur für klassischen Artikelversand (z.B. Landkarten, fertige CD-ROMS).
- **Dedizierte Lösungen für Geodaten**, hierfür gibt es noch keine Standardsoftware.
- Speziell für die Datensicherheit können gängige Techniken jedoch verwendet werden:
  - ⇨ **Sichere Datenübertragung durch Verschlüsselung**,
  - ⇨ **Digitale Bezahlsysteme**,
  - ⇨ **Digitale Signaturen zur Authentifizierung**.
- Diese Techniken sind das Hauptthema für den Rest des Vortrags.

Wie können meine Kunden sichere Bestellvorgänge im Internet tätigen?

- Bestellvorgänge im Internet werden in der Regel über ein Webformular getätigt.
- Beim Abschicken des Formulars werden im Normalfall die Formularinhalte (Bestelldaten, Adressdaten, Kreditkartennummern etc.) unverschlüsselt übertragen.
  - ⇨ Mangelhafter Schutz der Privatsphäre.
  - ⇨ Mangelhafter Schutz vor Kreditkartenbetrügern.
- Abhilfe: Verschlüsselung der Nachrichtenübertragung vom Kunden zum Geoinformationsanbieter durch
  - ⇨ **sichere, verschlüsselte Übertragungsprotokolle**,
  - ⇨ **moderne Browsertechnik**,
  - ⇨ **Sicherheitsinfrastruktur**.

Wie können wertvolle Geodaten sicher über das Internet übertragen werden?

Die Auslieferung der Geodaten erfolgt über das Internet.

- Die Übertragung kann durch Netzausfälle etc. scheitern.
  - ⇨ Wiederholbare Übertragung durch Bereithaltung der Geodaten auf dem Webserver des Datenanbieters.
- Es muss gewährleistet sein, dass nur der Käufer die Geodaten abrufen kann.
  - ⇨ Einsatz von **Authentifizierungstechniken** (digitale Techniken zur Überprüfung der Identität des Kunden).
- Die Übertragung der Geodaten vom Anbieter zum Kunden muss ablauschsicher sein.
  - ⇨ **Verschlüsselung** der Nachrichtenübertragung.
- Schutz des geistigen Eigentums des Anbieters
  - ⇨ Nutzungsvertrag mit **digitaler Unterschrift** des Kunden.

Wie können sich meine Kunden digital ausweisen?

- Die Identität der Kunden ist in vielen Fällen von Belang:
  - ⇨ Bestimmte Geodaten dürfen nur dazu Berechtigte erhalten.
  - ⇨ Nur der Käufer darf die erworbenen Daten abrufen.
  - ⇨ Viele digitale Zahlungssysteme erfordern eine Identitätsprüfung.
  - ⇨ Getätigte Bestellungen und abgeschlossene Nutzungsverträge sollen unabstreitbar sein.
- Es gibt Zertifikatbehörden (Certificate Authorities, auch **Trust Center** genannt), die mit **digitalen Zertifikaten** die Identität von Kunden und Datenanbietern beglaubigen.
  - ⇨ Die Zertifikate dienen als **digitale Ausweise.**
  - ⇨ Sie können für **digitale Signaturen** verwendet werden.

Wie können Daten und Dienste auf sichere Weise bezahlt werden?

- Wünschenswert sind **digitale Zahlungssysteme**, die den Einzug des Zahlungsbetrags in Echtzeit ermöglichen:
  - ⇨ Abbuchung von Kreditkarten oder anderen Konten,
  - ⇨ Bezahlung mit digitalem Geld (analog Geldkarte).
- Kunden möchten fremden Händlern ungern die Nummern ihrer Kreditkarten bekannt geben.
  - ⇨ Separate Verschlüsselung von Kartennummern und Bestelldaten;
  - ⇨ nur das Kreditinstitut kann die Kartennummer lesen,
  - ⇨ nur der Händler kann die Bestelldaten lesen.
- Alle diese Verfahren beruhen massiv auf **Kryptographie** (Verschlüsselungstechnologie).

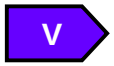
Kryptographie: Wichtige Begriffe

Chiffre	Verschlüsselungsverfahren für Nachrichten (einschließlich zugehörigem Entschlüsselungsverfahren)
Kryptographie	Entwerfen von Chiffren
Kryptoanalyse	Aufbrechen („Knacken“) von Chiffren
Kryptologie	Wissenschaft der Verschlüsselung, umfaßt Kryptographie und Kryptoanalyse
Klartext	zu verschlüsselnde Nachricht
Chiffretext	verschlüsselte Nachricht
Verschlüsselung	Umsetzung von Klartext in Chiffretext
Entschlüsselung	umgekehrter Vorgang

Übertragungssicherheit durch Kryptographie

Schutzgut	Maßnahme
Vertraulichkeit	digitale Verschlüsselung
Authentizität	digitale Zertifikate
Verbindlichkeit	digitale Signierung
Integrität	Message Digests (Prüfcodes)

Die „Cäsar-Chiffre“: Beispiel für ein einfaches Verschlüsselungsverfahren



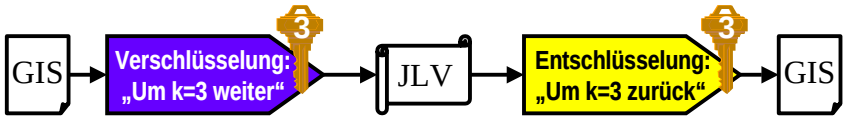
Verschlüsselungsverfahren:
„Gehe in alphabetischer Reihenfolge um k Buchstabenpositionen weiter!“

Schlüssel k = 3

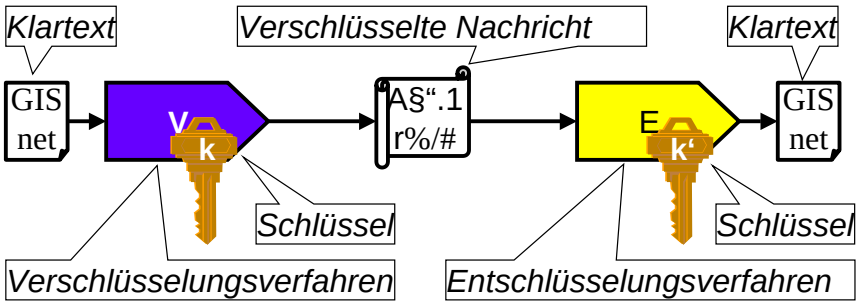
Entschlüsselungsverfahren:
„Gehe in alphabetischer Reihenfolge um k Buchstabenpositionen zurück!“

A	→ D
B	→ E
C	→ F
...	
W	→ Z
X	→ A
Y	→ B
Z	→ C

Für Verschlüsselung und Entschlüsselung wird hier derselbe Schlüssel k verwendet.
⇒ **Symmetrisches Verschlüsselungsverfahren.**



Verschlüsselung



Sender Übertragung Empfänger

Verschlüsselung

Eine **Verschlüsselung** $\mathbf{V_k}$ ist festgelegt durch zwei Vorgaben:

- ein allgemeines **Verschlüsselungsverfahren V** (auch Verschlüsselungsalgorithmus genannt, realisiert durch ein Programm),
- einen **Schlüssel** (Key) **k** (ein Zahlencode oder eine Zeichenkette), der das Verfahren einstellt (parametrisiert).

Für die **Entschlüsselung** $\mathbf{E_{k'}}$ gilt Entsprechendes, diese ist festgelegt durch:

- ein allgemeines **Entschlüsselungsverfahren E,**
- einen **Schlüssel k‘**, der das Verfahren einstellt (parametrisiert).

Symmetrische und asymmetrische Verschlüsselung

- **Symmetrische Verschlüsselung:**
  Für Entschlüsselung und Verschlüsselung wird derselbe Schlüssel k verwendet.
  - ⇨ Problem: Für jedes Paar von Kommunikationspartnern wird ein eigener Schlüssel benötigt.

- **Asymmetrische Verschlüsselung:**
  Für Entschlüsselung und Verschlüsselung werden unterschiedliche Schlüssel k und k‘ verwendet.
  - ⇨ Es gibt asymmetrische Verschlüsselungsmethoden, bei denen der Entschlüsselungsschlüssel k‘ praktisch nicht aus dem Verschlüsselungsschlüssel k abgeleitet werden kann.
  - ⇨ Mögliche Verwendung: sogenannte öffentliche Verschlüsselungsverfahren.

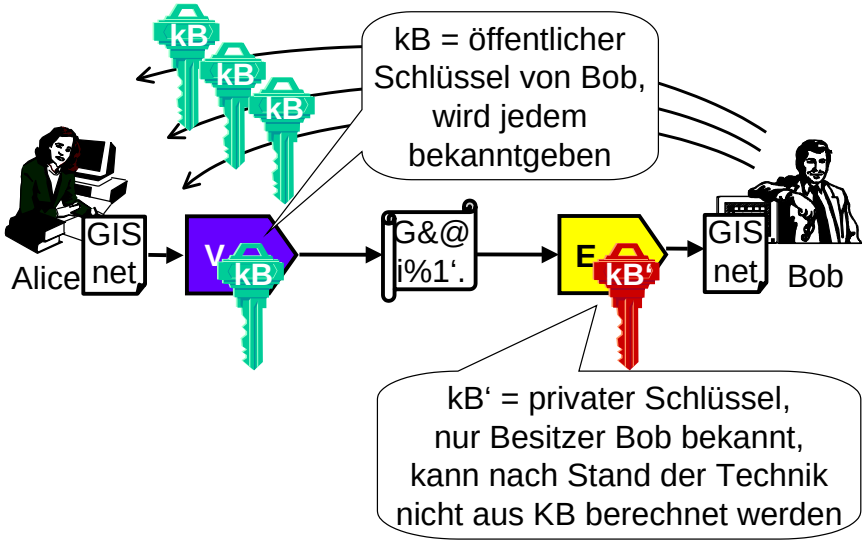
Öffentliche Verschlüsselungsverfahren

Asymmetrische Verschlüsselungsverfahren ermöglichen sogenannte öffentliche Verschlüsselungsverfahren:

- die **Verschlüsselung** erfolgt mit einem öffentlich bekannten Schlüssel k (dem **öffentlichen Schlüssel**).

- die **Entschlüsselung** mit einem nur dem Besitzer bekannten **privaten Schlüssel** k‘.
- Es ist in der Praxis **unmöglich, k‘ aus k abzuleiten**. Ein solcher Versuch würde bei guten asymmetrischen Verschlüsselungsverfahren viele Jahre bis zum Erfolg benötigen, selbst wenn ein Supercomputer benutzt wird.

Verschlüsselung mit öffentlichen und privaten Schlüsseln



Kombination asymmetrischer und symmetrischer Verschlüsselung

- Um vertrauliche Nachrichten an Bob senden zu können, genügt ein öffentlicher Schlüssel für alle Absender.
- Nachteil: Asymmetrische Verschlüsselungsverfahren sind sehr aufwendig (erfordern viel Rechenleistung bzw. -zeit).
- Abhilfe: **Kombination mit symmetrischem Verschlüsselungsverfahren**. Alice erzeugt als erstes einen Schlüssel **ks** für ein symmetrisches Verfahren, verschlüsselt diesen mit Bobs öffentlichen Schlüssel **kB**, und schickt ihn in dieser Form auf sichere Weise an Bob.
- Mit dem symmetrischen Schlüssel **ks** können Bob und Alice vertrauliche Nachrichten in beide Richtungen austauschen! Mit dem öffentlichen Schlüssel **kB** wäre das nur in Richtung Bob möglich gewesen!

RSA & Co. - Gängige asymmetrische Verschlüsselungsverfahren

RSA = Bedeutendste asymmetrische Chiffre, wird in den meisten Verfahren mit öffentlichen und privaten Schlüsseln verwendet.

RSA = Anfangsbuchstaben der Nachnamen von Ronald **R**ivest, Adi **S**hamir und Leonard **A**dleman. Dies sind die Erfinder des Verfahrens und jetzt Professoren am Massachussetts Institute of Technology (MIT).

RSA Data Security: Firma für Kryptographie-Technologie, vertreibt RSA und andere Verschlüsselungsverfahren.

Alternative asymmetrische Chiffren mit ähnlichen Eigenschaften, aber geringerer Bedeutung: **Diffie-Hellman Key Exchange**, **ElGamal**, **DSS** (Digital Signature Standard).

Gängige symmetrische Verschlüsselungsverfahren

DES (Data Encryption Standard): genormt durch ANSI, 56-Bit-Schlüssel, heute innerhalb weniger Stunden knackbar.

Triple-DES: Dreifache Anwendung von DES, ist doppelt so sicher wie DES (d.h. entspricht 112-Bit), gilt als sicher.

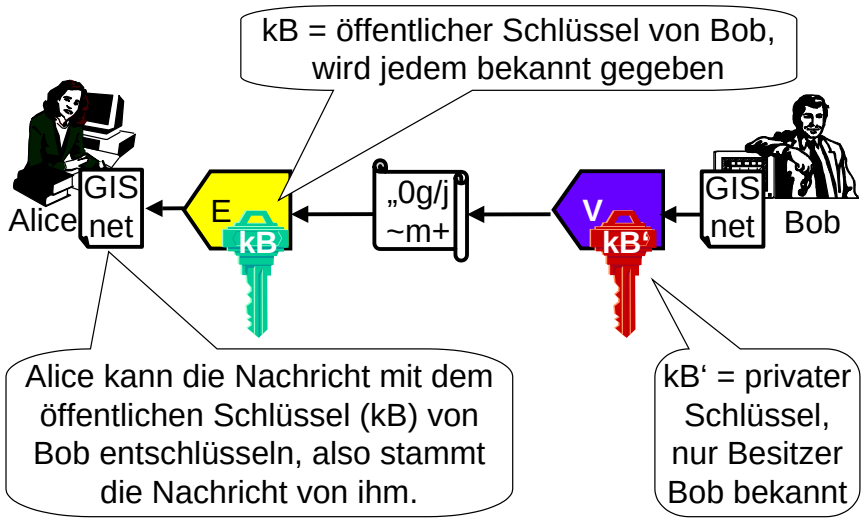
IDEA (International Data Encryption Algorithm): benutzt 128-Bit-Schlüssel, gilt als sehr sicher, in Schweiz entwickelt.

RC2 (verschlüsselt Datenblöcke) und **RC4** (verschlüsselt Datenströme) erlauben Schlüssel zwischen 1 und 2048 Bits. Entwickelt und patentiert von RSA Data Security. Netscape verwendet in USA RC4 mit 128 Bit, in Export-Ausführungen werden bisher wegen US-Ausfuhrbeschränkungen 88 Bit aufgedeckt (Ausnahme: Bankanwendungen). Lockerung der US-Ausfuhrbeschränkungen im Januar 2000 beschlossen!

Verschlüsselung mit privatem Schlüssel ermöglicht Signierung (dig. Unterschrift)

- Das asymmetrische Verschlüsselungsverfahren RSA (wie auch vergleichbare Verfahren) kann auch in umgekehrter Richtung betrieben werden.
- D.h., es wird eine Nachricht mit dem privaten Schlüssel verschlüsselt und mit dem öffentlichen Schlüssel entschlüsselt.
- Die Entschlüsselbarkeit mit dem öffentlichen Schlüssel ist der Beweis, dass die Nachricht vom betreffenden Absender stammt.
  - ⇨ Technische Grundlage für die **digitale Signierung** (**digitale Unterschrift**).

Digitale Unterschrift mit öffentlichen und privaten Schlüsseln



Öffentliche und private Schlüssel für Verschlüsselung und digitale Unterschrift

- **Verschlüsselung**:
  - ⇨ Sender verwendet öffentlichen Schlüssel des Empfängers zur Verschlüsselung der Nachricht.
  - ⇨ Empfänger verwendet eigenen privaten Schlüssel zur Entschlüsselung der Nachricht.
- **Digitale Unterschrift (Signierung)**:
  - ⇨ Die zu unterschreibende Nachricht wird mit dem privaten Schlüssel des Senders verschlüsselt. Das Ergebnis ist die unterschriebene Nachricht.
  - ⇨ Empfänger verwendet öffentlichen Schlüssel des Senders zur Entschlüsselung der Nachricht. Wenn diese Entschlüsselung gelingt, ist die „Unterschrift“ echt.

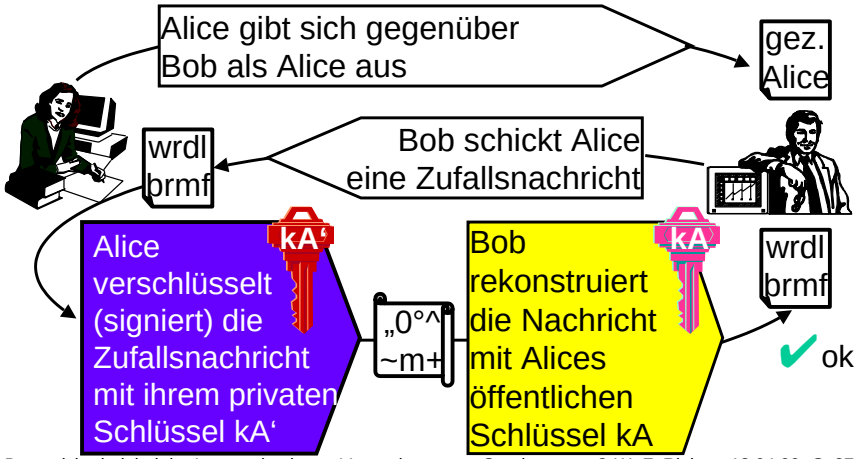
Verschlüsselung mit öffentlichem Schlüssel und Signierung: Folgerungen

Signierung und Verschlüsselung sind voneinander unabhängig möglich:

- Mit öffentlichen Schlüsseln verschlüsselte Nachrichten haben nicht notwendig eine Unterschrift. Sie können von jedermann stammen.
- Mit privaten Schlüsseln signierte Nachrichten sind nicht vertraulich. Sie können mit Hilfe des passenden öffentlichen Schlüssels von jedermann entschlüsselt werden.
- Verschlüsselung und Signierung können aber auch kombiniert werden. Hierzu verschlüsselt der Sender zunächst die Nachricht mit dem eigenen privaten Schlüssel (= Signierung) und dann mit dem öffentlichen Schlüssel des Empfängers (= Verschlüsselung).

Authentifizierung

Mit Hilfe der Technik der Signierung können sich Kommunikationspartner ausweisen (authentifizieren):



Integrität der Nachrichten durch Signierung von Message Digests

Signierung kann zur Gewährleistung der Integrität (Unverfälschtheit) von Nachrichten genutzt werden.

- Bob will Alice eine unverfälschbare Nachricht senden.
- Dazu bestimmt er aus der Nachricht einen Prüfcode, den sogenannten **Message Digest**.
- Bob signiert den Message Digest, d.h. er verschlüsselt ihn mit seinem privaten Schlüssel.
- Alice verifiziert Bobs Unterschrift, d.h. sie entschlüsselt den Message Digest mit Bobs öffentlichem Schlüssel.
- Alice berechnet den Message Digest aus der Nachricht und vergleicht ihn mit dem entschlüsselten Message Digest. Wenn beide gleich sind, ist die Integrität der Nachricht gesichert.

Message Digests

Eigenschaften guter Verfahren zur Berechnung von Message Digests:

- Jedes Bit des Message Digests wird von jedem Bit der Nachricht beeinflusst.
- Wenn irgendein Bit der Nachricht verändert wird, kann sich jedes Bit des Message Digest mit 50% Wahrscheinlichkeit ändern.
- Wenn eine Nachricht und ihr Message Digest vorgelegt wird, sollte es mit heutigen technischen Mitteln unmöglich sein, eine zweite Nachricht mit demselben Message Digest zu erzeugen.

In der Praxis werden meist nur die Message Digests signiert und nicht die eigentlichen Nachrichten.

Kryptographie-Infrastruktur für öffentliche Verschlüsselungsverfahren

Problem:

- Wie erfährt Alice den öffentlichen Schlüssel ihres Gesprächspartners, wenn sie zu ihm keine persönliche Verbindung hat?
- Wenn Sie den öffentlichen Schlüssel kennt, welche Gewissheit hat sie über die Identität des Gesprächspartners?

Abhilfe:

- Aufbau einer sog. „**Kryptographie-Infrastruktur**“.
- D.h.: Einrichtung von Zertifikatbehörden, sog. **Certificate Authorities** (CA) oder **Trustcenters**, die die Identität von Personen / Einrichtungen prüfen und deren öffentliche Schlüssel beglaubigen.
- Diese Beglaubigung erfolgt mit sog. **digitalen Zertifikaten**.

Digitale Zertifikate

Zertifikate sind digitale Dokumente, die folgende Informationen enthalten:

- Angaben zur **Identität der Person/Institution** (Name, ggf. Adressangaben)
- **Öffentlicher Schlüssel** der Person/Institution
- **Ausgabedatum, Verfallsdatum**
- **Seriennummer**
- **Digitale Unterschrift des Trustcenters**
  - ⇨ kann mit öffentlichem Schlüssel des Trustcenters verifiziert werden.

Die derzeit gängige Norm für Zertifikate trägt die Bezeichnung **X.509 v3**

Sichere Übertragung auf der Basis von Zertifikaten nach X.509 v3

- Es gibt auf der Basis von Zertifikaten nach X.509 v3 verschiedene sichere Protokolle, die die Signierung und Verschlüsselung von Nachrichten erlauben:
  - ⇨ **SSL v3**: für allgemeine Datenübertragung,
  - ⇨ **https:** sichere Übertragung von Webseiten und Formularinhalten (aufbauend auf SSL v3),
  - ⇨ **S/MIME:** Sichere Email-Übertragung.
- Alle modernen **Internet-Browser** (Netscape Navigator, Internet Explorer) verstehen diese Protokolle und haben die öffentlichen Schlüssel der wichtigsten Trustcenter vorinstalliert, so dass sie deren Zertifikate nutzen können.
- **Webserver** mit SSL-Unterstützung gibt es in der Regel gegen Aufpreis.

Arten von Zertifikaten

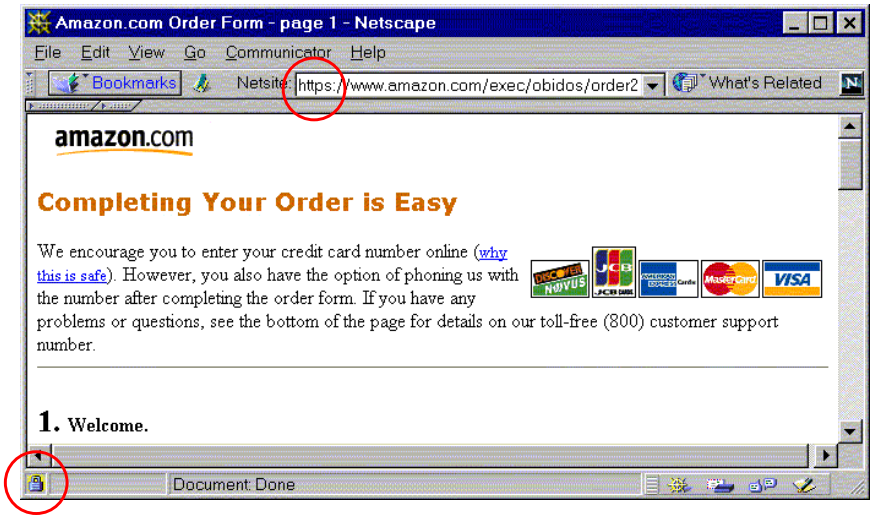
Trustcenter unterscheiden **Zertifikate nach Einsatz**

- im Mailsystem: Verschlüsselung und Signierung (S/MIME)
- im Web-Server: Signierung von Webseiten, Initiierung einer sicheren Web-Verbindung (hhtps)
- im Internet-Browser: Authentifizierung von Benutzern

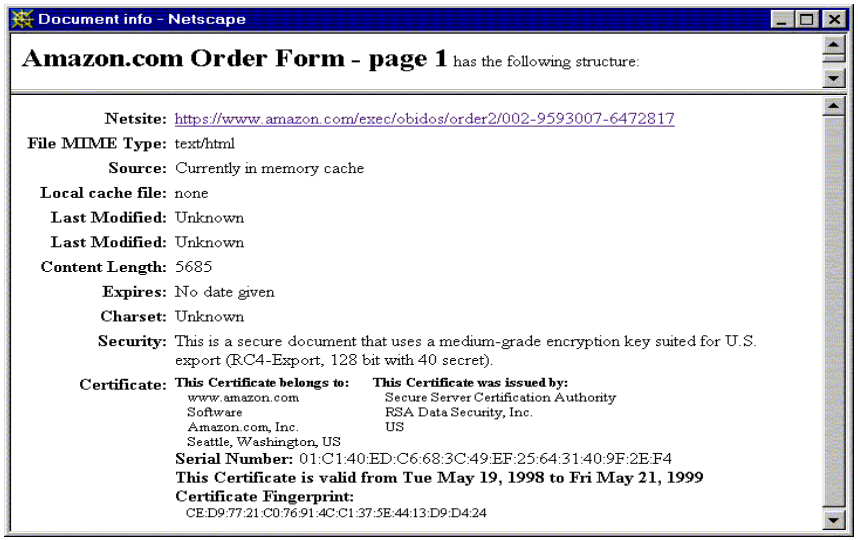
Es werden Zertifikate in verschiedenen **Klassen** ausgegeben.

- Im einfachsten Fall: Legitimierung durch gültige Email-Adresse (nur für Privatpersonen, Zertifikat wird umgehend per Email zugeschickt).
- Für hohe Sicherheit: Legitimierung durch Personalausweis oder Reisepass und persönliches Erscheinen bei einer Behörde oder Agentur.

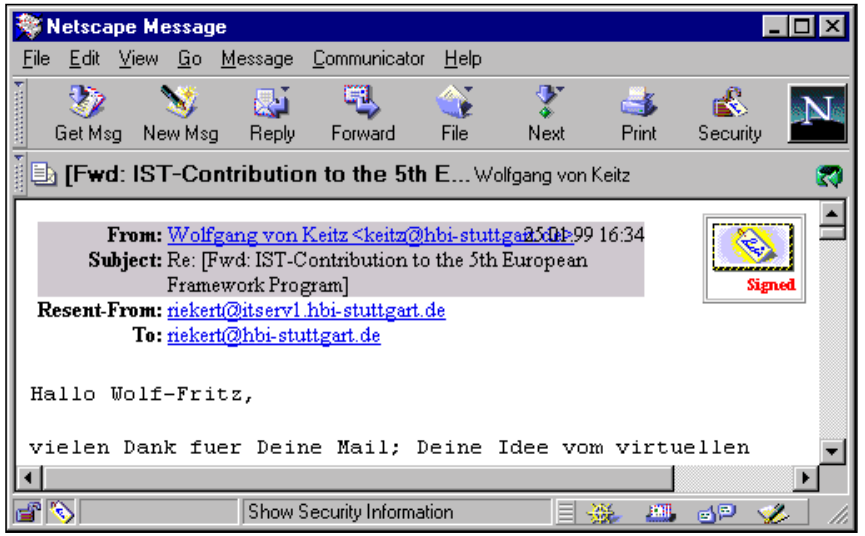
Verschlüsselte Kommunikation mit https und ssl am Beispiel eines Buchversands



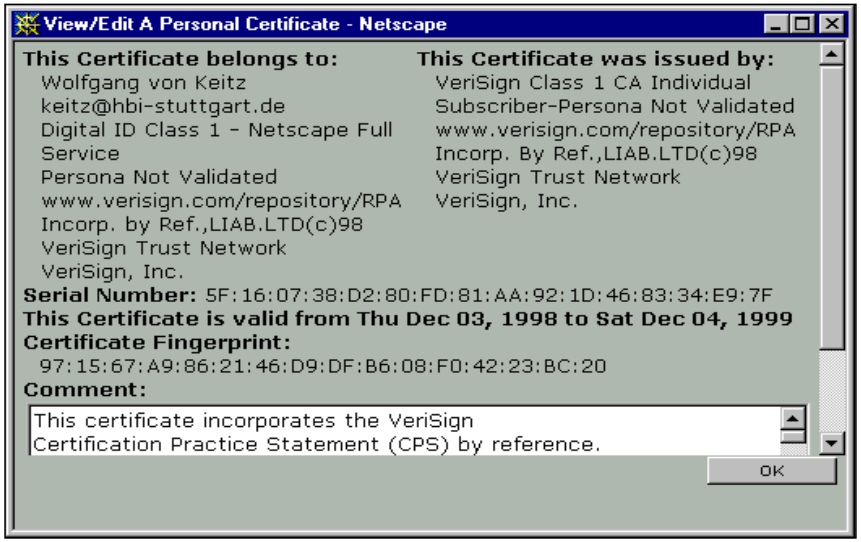
Dokumenteninformation zu einer sicheren Webseite



Signierte Emails mit S/MIME



Ein Zertifikat, das durch ein Trust Center ausgestellt wurde



Vom Netscape-Browser akzeptierte Trust Center (Certificate Authorities)

Digitale Zahlungssysteme

- Meistverbreitetes digitales Zahlungssystem im Internet ist die **Kreditkarte**.
  - ⇨ Kartennummer wird i.d.R. mit SSL verschlüsselt.
  - ⇨ Die eigentliche Transaktion erfolgt wie bei der klassischen Kreditkartennutzung.
  - ⇨ Dabei wird die Kartennummer dem Händler bekannt.
- **Neue Internet-basierte Zahlungssysteme** zielen auf verschiedene Verbesserungen ab:
  - ⇨ Verringerte Transaktionskosten für Kleinstbeträge,
  - ⇨ Geheimhaltung der Bankverbindung des Kunden gegenüber Händler
  - ⇨ oder gar völlige Anonymität des Kunden,
  - ⇨ Benutzbarkeit auch ohne Kreditkarte, z.B. durch Lastschrift vom Girokonto oder „digitale Münzen“.

Neue Internet-basierte Zahlungssysteme

Es lassen sich zwei Arten neuer Internet-basierter Zahlungssysteme unterscheiden:

- **Private Zahlungssysteme**: Nur der Betreiber des Zahlungssystems braucht die Identität des Kunden zu erfahren, der Händler nur, wenn der Kunde das möchte (z.B. wegen Lieferadresse). Die Kaufdaten wiederum erfährt nur der Händler.
- **Anonyme Zahlungssysteme**: Weder der Betreiber des Zahlungssystems noch der Händler erfahren etwas über die Identität des Kunden bei einer Transaktion

Die Wallet (digitale Brieftasche)

Für die meisten neuen Internetbasierten Zahlungssysteme benötigt der Kunde eine **Wallet**, das ist eine Art „digitale Brieftasche“.

- Die Wallet ist eine Anwendung, die mit dem Internet-Browser kooperiert, wenn ein Kauf im Internet stattfindet.
- Die Wallet erhält man i.d.R. per Download vom Betreiber des Zahlungssystems.
- Die Wallet enthält alle für Transaktionen wichtigen Informationen, z.B. Zertifikate, private und öffentliche Schlüssel sowie ggf. auch Guthabenstände.
- Um sich vor dem Zahlungssystembetreiber sicher ausweisen zu können, muss der Kunde ein geeignetes **Zertifikat** erwerben und auf seiner Wallet installieren.

Private Zahlungssysteme

Typische Eigenschaften:

- Alle Teilnehmer (Kunde, Händler, Betreiber des Zahlungssystems) authentifizieren sich mit Zertifikaten.
- Alle Daten werden verschlüsselt übertragen.
- Die übertragenen Daten zerfallen in zwei Teile, die mit öffentlichen Schlüsseln von Händler bzw. Zahlungssystembetreiber verschlüsselt werden:
  - ⇨ Kaufdaten erhält nur der Händler.
  - ⇨ Die Identität und die Bankverbindung des Kunden erfährt nur der Zahlungssystembetreiber.
- Abbuchung von einem Konto des Kunden.

Private Zahlungssysteme: Beispiele

Beispiele privater Zahlungssysteme:

- **SET** (entwickelt von den Kreditkartenunternehmen Visa und Mastercard, weitere sind beteiligt):
  - ⇨ Abbuchung nur von Kreditkartenkonto.
- **CyberCash** (Partner einer Reihe großer Geldinstitute):
  - ⇨ Abbuchung von Kreditkartenkonto, von Girokonto oder von einem einfachen wiederaufladbaren Verrechnungskonto für Kleinstbeträge (**CyberCoin**).
- Marktdurchdringung beider Verfahren ist noch gering (Stand 19.03.2000):
  - ⇨ Der deutsche Mastercard-Partner www.eurocard.de führt 34 Vertragshändler auf, die SET akzeptieren, www.cybercash.de listet 51 Händler auf.

Anonyme Zahlungssysteme

Anonyme Zahlungssysteme funktionieren mit Hilfe digitaler Geldstücke (**Coins**).

- Der Kunde kann solche Coins von einer digitalen Münze (Mint) erwerben. Die entsprechende Summe wird dann von seinem Bank- oder Kreditkartenkonto abgebucht.
- Jedes Coin besteht aus einer eindeutigen Zeichenfolge und ist von der ausgebenden Mint signiert.
- Bezahlt wird durch Übersenden des Coins, d.h. der signierten Zeichenfolge an den Händler.
- Coins dürfen nur einmal ausgegeben werden. Der Händler tauscht die Coins sofort bei der Mint ein. Doppeltes Ausgeben eines Coins würde dabei als Betrug erkannt.
- Bekanntestes System: **Digicash**, früher E-Cash genannt.

Bewertung der neuen Internet-basierten Zahlungssysteme

Die neuen Internet-basierten Zahlungssysteme haben sich allesamt noch **nicht richtig auf dem Markt durchgesetzt**.

Gründe:

- Anlaufkosten bei den Händlern.
- Arbeitsaufwand beim Kunden: Installation von Software, Erwerb von Zertifikaten.
- Da Marktdurchdringung noch gering, Anreiz gering für neue Teilnehmer (Händler und Kunden) am Verfahren.

Konsequenz:

- **Kreditkarten mit SSL-abgesicherter Übertragung von Kartennummern werden noch auf lange Sicht das Standard-Bezahlungssystem im Internet darstellen.**

Praktischer Lösungsvorschlag: Sichere Bestellvorgänge

Wie können meine Kunden sichere Bestellvorgänge im Internet tätigen?

Lösung:

- Absicherung der Kommunikation mit dem sicheren Webprotokoll **https**. Dies erfordert:
  - ⇨ Verwendung eines **SSL**-fähigen Webservers,
  - ⇨ Erwerb eines **Server-Zertifikats** von einem (den Standardbrowsern) bekannten Trustcenter,

Praktischer Lösungsvorschlag: Sichere Übertragung der Geodaten

Inwieweit können wertvolle Geodaten sicher über das Internet übertragen werden?

Lösung:

- Absicherung der Kommunikation mit dem sicheren Web-Protokoll **https** (siehe oben).

Alternative Lösung (weniger Rechenaufwand, aber auch nicht ganz so sicher):

- Bereitstellung der Geodaten in einem verschlüsselten Archiv auf dem Webserver (z.B. symmetrisch verschlüsselt in einer Winzip-Datei).
- Nur der Schlüssel wird mit https verschlüsselt übertragen.
- Das (verschlüsselte) Archiv wird mit dem Standardprotokoll http übertragen.

Praktischer Lösungsvorschlag: Authentifizierung der Kunden

Wie können sich meine Kunden digital ausweisen?

Lösung:

- Normale Kunden brauchen sich beim Händler nicht besonders auszuweisen, dies übernimmt das **Zahlungssystem**.
- Falls Berechtigungsprüfung und/oder Nutzungsvereinbarung erforderlich ist:
  - ⇨ Verwaltung von registrierten Kunden und deren Berechtigungen in einer Datenbank, Vergabe von **Passwörtern**, die SSL-gesichert übertragen werden
  - ⇨ Alternativ: **Authentifizierung der Kunden** mit Hilfe von Client-Zertifikaten und einem (öffentlichen oder organisationseigenen) Trustcenter. Allerdings erfordert dies Mühe auf Seiten der Kunden und wird deshalb derzeit nur ungern akzeptiert.

Praktischer Lösungsvorschlag: Sichere Bezahlung

Wie können Daten und Dienste auf sichere Weise bezahlt werden?

Standardlösung:

- Abbuchung der Entgelte in Echtzeit mit Hilfe SSL-gesicherter Übermittlung von **Kreditkarten**nummern.

Alternativ:

- Verwendung eines neuen **Internet-basierten Zahlungssystems** wie SET oder CyberCash.
  - ⇨ Allerdings derzeit noch geringe Akzeptanz.

Nur bei registrierten Kunden:

- Lieferung gegen **Rechnung oder Bankeinzug**.

Ergebnisse

- Alle Sicherheitsfragen der Internet-basierten Vermarktung von Geodaten sind mit den **vorhandenen Techniken** lösbar:
  - ⇨ symmetrische und asymmetrische Verschlüsselungsverfahren,
  - ⇨ digitale Zertifikate,
  - ⇨ digitale Zahlungssysteme.
- Vorhandene Webshops verfügen über solche Techniken, sind aber für Geodaten nicht geeignet!
- **Spezialentwicklungen** sind erforderlich, die derzeit im Entstehen sind.