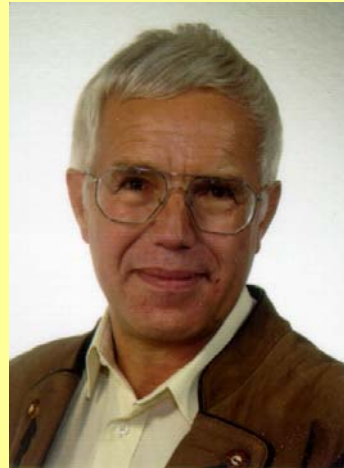




Referent

Reinhard Schmitt

Reinhard@ReinhardSchmitt.De



Referent

Das sichere https

20.06.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

Folie 1



https - Aufbau einer sicheren Verbindung über das Internet

- Anforderungen an eine sichere Verbindung
- Kryptographie (Verschlüsselung)
- https im OSI-Protokoll
- Verbindungsaufbau
- https - Verbindung beim Banking
- Zertifikate und Zertifikatsverwaltung
- Was sollte ich als Anwender beachten um die Sicherheit nicht zu gefährden
- Phishing

Thema

Das sichere https

20.06.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

Folie 2



Anforderungen an eine sichere Verbindung und Mittel dies zu erreichen.

- **Authentizität (Authentication) ...**
... des Kommunikationspartners? (Authentizität im engeren Sinn)
- **... Der Meldung:**
 - Wurde die Meldung von dem Kommunikationspartners abgeschickt?
(Originalität)
 - War die Meldung für den Empfänger bestimmt?
- **Schlüssel (Zertifikat)**
 - Informationen, die nur der Kommunikationspartner haben kann.
 - Beispiele: Password, Private Key, biometrische Merkmale
 - Zertifikate mit Public Key



- **Meldungsintegrität: (Integrity) Ist die Meldung unverändert?**
 - Schutz gegen beabsichtigte und unbeabsichtigte Veränderungen:
 - Einfügen, Löschen, Verändern der Reihenfolge von Paketen, Duplikation, Wiedereinspielen von Meldungen
 - Erkennen von Integritätsverletzungen vs. Korrekturmaßnahmen
- **Prüfziffer:**
 - Ein eindeutiger Wert („Fingerabdruck“), der aus der Meldung ermittelt wurde.
 - Beispiele: CRC, Message Digest Codes (Hashfunktionen MD5, SHA)



- **MD5** MD5 ist ein von Ron Rivest entwickelter Algorithmus, der einen 128-Bit Hashwert hervorbringt. Der MD5-Entwurf wurde für Intel-Prozessoren optimiert. Einige Elemente des Algorithmus wurden blossgestellt, wodurch seine Verwendung vermindert wird.
- **SHA-1** Wie auch der DAS-Algorithmus mit öffentlichen Schlüsseln wurde SHA-1 (Secure Hash Algorithm-1) von der NSA entwickelt und von NIST in den FIPS für das Hashing von Dateien integriert. Er bringt einen 160-Bit-Hashwert hervor. SHA-1 ist ein beliebiger unidirektionaler Algorithmus, der zum Erstellen digitaler Signaturen verwendet wird.

Quelle: Microsoft „Grundlagen der Kryptografie und der Infrastruktur öffentlicher Schlüssel (PKI)“



- **Vertraulichkeit (Confidentiality) ...**
 - ... des Inhalts: Konnte ein Dritter den Meldungsinhalt lesen?
 - ... des Akts der Kommunikation: Konnte ein Dritter erkennen, dass eine Kommunikation zwischen zwei Partnern stattgefunden hat?
- **Chiffrierung (Verschlüsselung, Kryptografie):**
 - Die Meldung wird vor dem Abschicken für einen Dritten unkenntlich gemacht und nach dem Empfang rückgewandelt.
 - Beispiele: Geheimschrift, Public Key Kryptografie, Stenographie



- **Verfügbarkeit**
 - „Denial of Service Attack“: Angreifer verhindern den berechtigten Zugriff auf Systemressourcen (z.B. Web-Server) z.B. dadurch, dass er den Server mit vielen kleinen Anfragen lahmlegt.
 - Service-Güte, Zusicherung der Verfügbarkeit
- **Hier muss der Serverbetreiber aufpassen**



Kryptografie bedeutet, Informationen so zu schreiben, dass sie für Dritte unlesbar sind.

Bereits seit Tausenden von Jahren werden Verschlüsselungssysteme eingesetzt, um Geheimnisse zu bewahren. Zu keiner Zeit waren die Systeme so zuverlässig, wie sie es heute sind. Dazu hat die moderne Computertechnik genauso beigetragen wie die durch Militär und E-Commerce vorangetriebene Forschung auf diesem Gebiet: Algorithmen sind gut dokumentiert und frei zugänglich. Das Buch *Applied Cryptography* von Bruce Schneier gilt als Standardwerk zum Thema.

In der modernen Kryptografie unterscheidet man Verschlüsselungsmethoden nach mehreren Kriterien - diese sagen jedoch nichts über Ihre Sicherheit aus. Das wichtigste Kriterium ist, ob es sich um ein symmetrisches (mit geheimen Schlüsseln) oder asymmetrisches System (mit öffentlichen Schlüsseln) handelt.

Verwendet man ein System mit geheimem Schlüssel, so muss man mit dem Kommunikationspartner ein Passwort vereinbaren. Programme, die auf asymmetrischer Verschlüsselung basieren, funktionieren anders. Ihre Funktionsweise kann man sich wie einen Briefkasten vorstellen: Jeder kann etwas einwerfen (verschlüsseln), aber nur der Besitzer des privaten Schlüssels kann es lesen (entschlüsseln).

Es folgt eine Auflistung der wichtigsten Verschlüsselungs-Algorithmen:

Algorithmus	Erfinder	Typ
Blowfish	Schneier	Symmetrisch
DES	IBM	Symmetrisch
Diffie-Hellman	Diffie, Hellman	Schlüsselaustausch
IDEA	Lai, Messey	Symmetrisch
AES	Daemen, Rijmen	Symmetrisch
RSA	RSA	Asymmetrisch
Skipjack	NSA	Symmetrisch

Bis heute geht man davon aus, dass es nur ein System gibt, das absolute Sicherheit bietet: Das sogenannte *one time pad* (nach seinem Erfinder auch Vernam-Verschlüsselung genannt). Bereits 1917 hat Gilbert S. Vernam, der zu diesem Zeitpunkt für AT&T arbeitete, dieses System entwickelt, um die Kommunikation von Fernschreibern zu sichern. Leider ist das Verfahren nicht praktikabel, da es voraussetzt, dass der Schlüssel mindestens so lang ist wie die geheimen Daten. Angeblich ist das berühmte 'rote Telefon' zwischen Washington und Moskau mit dem *one time pad* gesichert.



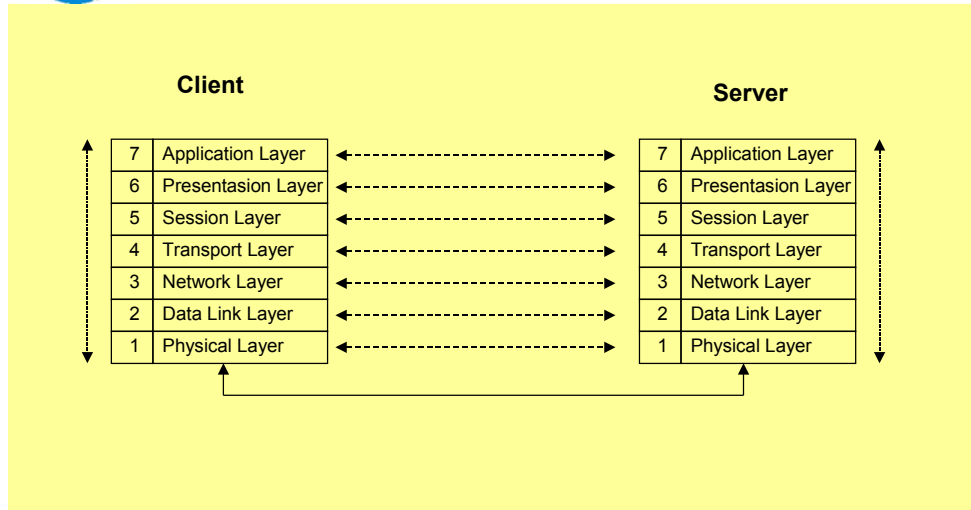
Verschlüsselung (Vertraulichkeit)

- **Symmetrische Verschlüsselung 1 Schlüssel**
 - Einfach (schnell)
 - Problem der Schlüsselaustausch
- **Asymmetrische Verschlüsselung 2 Schlüssel**
 - Public Key (wird veröffentlicht)
 - Privat Key (Kennt nur der Eigentümer, muss geheim bleiben)
 - Aufwendig (langsam)
- **Kombination**
 - Mit der Asymmetrischen Verschlüsselung (siehe Zertifikat) wird ein symmetrischer Schlüssel ausgetauscht.
 - Der eigentliche Datenaustausch erfolgt dann mit dem symmetrischen Schlüssel



Wo her kennen wir bisher die Verschlüsselung?

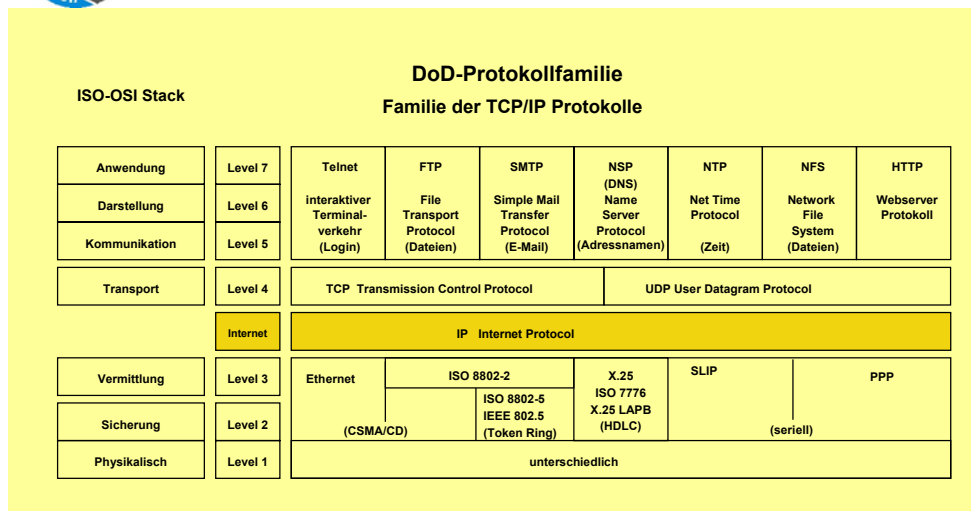
- **WLAN** symmetrisch möglich
- **Dateiverschlüsselung (Steganos)** symmetrisch möglich
- **E-Mail PGP** asymmetrische Verschlüsselung
- **https** asymmetrische & symmetrische Verschlüsselung
- **VPN (Virtual Privat Network)**



Das OSI-Referenzmodell

Das sichere https

20.06.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De
Folie 11



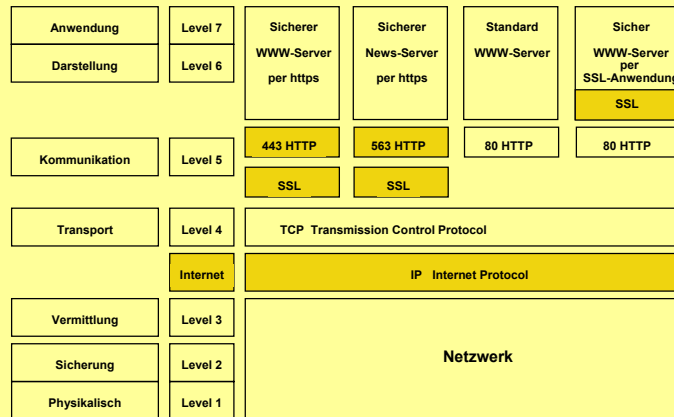
TCP-IP Protokoll-Familie

Das sichere https

20.06.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De
Folie 12



ISO-OSI Stack mit SSL



TCP-IP Absicherung auf der Transport-Schicht

Das sichere https

20.06.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De
Folie 13



- http Socket 80
- https SSL (Secure Socket Layer) & http Socket 443
- https SSL für News & http Socket 563
- S-http Socket 80 SSL auf Anwendungsebene

- Ausweise = Zertifikate

http / https

Das sichere https

20.06.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De
Folie 14



- Die Produktversion von SSL wurde 1996 von Netscape veröffentlicht.
- Bereits im Jahr 2001 waren etwa acht Prozent der Internet-Verkehrs verschlüsselt. Der Anteil an HTTPS-Verkehr in typischen Unternehmensnetzen hat stark zugenommen (2005).
- Viren können mit SSL verschlüsselt und damit für die Firewall unsichtbar gemacht werden.
- Das Schloss, das der Browser beim Aufruf einer HTTPS-Site anzeigt, vermittelt nur ein trügerisches Gefühl von Sicherheit.
- Der Internet Explorer wird mit über 100 vorinstallierten und von Microsoft-Entwicklern für vertrauenswürdig erklärten Certificate Authorities ausgeliefert.

Quelle: Webwasher SSL/HTTPS: Kontrolle des verschlüsselten Datenverkehrs
<http://www.webwasher.com>



Schlüsselaustausch-Protokoll



Setzen der Schlüssel



Asymmetrischer Schlüssel

Kanal zur Schlüsselaushandlung

Symmetrischer Schlüssel

Gesicherte Kommunikation

Schlüsselaustausch-Protokoll

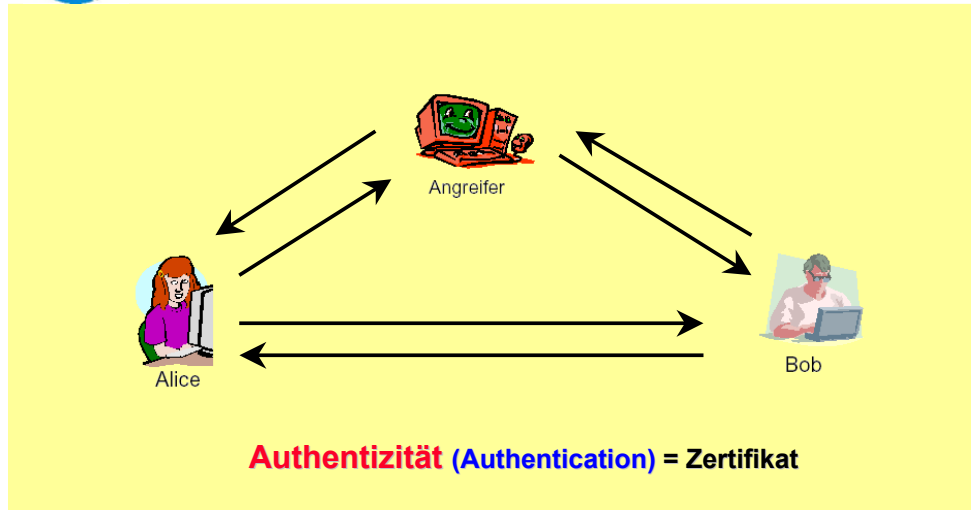


Setzen der Schlüssel



Schlüsselaustausch-Protokoll

1. Aushandlung der Austausch-/Sicherungsverfahren für den Kanal
2. Authentizitätsüberprüfung des Kommunikationspartners
3. Erzeugung des Schlüsselmaterials für den Kanal
4. Aushandlung der Sicherungsverfahren für Daten
5. Erzeugung des Schlüsselmaterials für die Datensicherung
6. Übergeben des Schlüsselmaterials an die Anwendung zur Datensicherung



Man in the Middle

Das sichere https

20.06.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De
Folie 17

- **ID-Zertifikat (Authentication)**
 - Bindung eines öffentlichen Schlüssels an einen eindeutigen Namen (Identität)
 - Authentifizierung von öffentlichen Schlüsseln
- **Public Key Infrastructure (PKI)**
 - Management von ID-Zertifikaten
 - Ermöglicht die Authentifizierung von öffentlichen Schlüsseln
- **Vertrauen**
 - Erwartungsgemäßes Verhalten des Gegenübers
 - Transitivität von Vertrauen
- **Validierung von ID-Zertifikaten**
 - Vertrauensanker
 - Zertifizierungspfad
 - Widerrufmechanismen

ID – Zertifikat

Das sichere https

20.06.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De
Folie 18



Förderverein Bürgernetz München-Land e.V.

Zertifikatsinformationen



X.509-Zertifikatsinformationen

Das sichere https

20.06.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De
Folie 19



Förderverein Bürgernetz München-Land e.V.

The screenshot shows the Postbank website interface in Microsoft Internet Explorer. The browser title is "Postbank - Leistung ohne Umwege". The address bar shows "http://www.postbank.de/". The website content includes a navigation menu, a sidebar with "Produkte & Preise", "Online Services", and "Vermögensberatung", and a main content area with various financial offers and advertisements. A yellow box on the right side of the browser window contains the text "Kein Zeichen offene Verbindung" with an arrow pointing to the status bar area.

Login Postbank 1

Das sichere https

20.06.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De
Folie 20

Ein Schloss, d.h. Sichere https-Verbindung. Zertifikate sind ausgetauscht, ein Verfahren und ein Schlüssel sind vereinbart

Login Postbank 2 **Das sichere https**

20.06.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De
Folie 21

Es besteht eine sichere Verbindung, Nun kann ein Login erfolgen und Kontonummer und Pin eingegeben werden

Login Postbank 3 **Das sichere https**

20.06.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De
Folie 22



Förderverein Bürgernetz München-Land e.V.

Feld	Wert
Version	V3
Seriennummer	3CE0 D0B2 944F 8329 F40A 3F62 D0AE B48D
Signaturalgorithmus	sha1RSA
Aussteller	www.verisign.com/CPS Incorpor. by Ref. LIABILITY LTD.(c)97 VeriSign
Gültig ab	Montag, 30. August 2004 02:00:00
Gültig bis	Mittwoch, 31. August 2005 01:59:00
Antragsteller	banking.postbank.de, Terms of u...

PB Zertifikat

Das sichere https

20.06.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.de

Folie 23



Förderverein Bürgernetz München-Land e.V.

VeriSign Relying Party Agreement

YOU MUST READ THIS RELYING PARTY AGREEMENT ("AGREEMENT") BEFORE VALIDATING A VERISIGN TRUST NETWORKS DIGITAL CERTIFICATE ("CERTIFICATE"), USING VERISIGN'S ONLINE CERTIFICATE STATUS PROTOCOL ("OCSP") SERVICES, OR OTHERWISE ACCESSING OR USING A VERISIGN OR VERISIGN AFFILIATE DATABASE OF CERTIFICATE REVOCATIONS AND OTHER INFORMATION ("REPOSITORY") OR ANY CERTIFICATE REVOCATION LIST ISSUED BY VERISIGN, INC. ("VERISIGN CRL"). IF YOU DO NOT AGREE TO THE TERMS OF THIS AGREEMENT, DO NOT SUBMIT A QUERY AND DO NOT DOWNLOAD, ACCESS, OR USE ANY VERISIGN CRL BECAUSE YOU ARE NOT AUTHORIZED TO USE VERISIGN'S REPOSITORY OR ANY VERISIGN CRL. IN CONSIDERATION OF YOU AGREEING TO THE TERMS OF THIS RELYING PARTY AGREEMENT, YOU SHALL BE PERMITTED TO RELY ON CERTIFICATES ACCESSED BY YOU IN ACCORDANCE WITH THE TERMS OF THIS AGREEMENT.

1. **Background.** This Agreement becomes effective when you submit a query to search for a Certificate, or to verify a digital signature created with a private key corresponding to a public key contained in a Certificate, by downloading a VeriSign CRL, or when you otherwise use or rely upon any information or services provided by VeriSign's Repository, VeriSign's website, or any VeriSign CRL, or when you use VeriSign's OCSP services. Relying Party Agreements in force within VeriSign's subdomain of the VTN appear in the Repository at <http://www.verisign.com/repository>.

2. **Definitions.** The capitalized terms used in this Agreement shall have the following meanings unless otherwise specified:

- "Certificate" shall mean a digitally signed message that contains a Subscriber's public key and associates it with information authenticated by VeriSign or a VeriSign-authorized entity
- "Certificate Applicant" shall mean an individual or organization that requests the issuance of a Certificate by a Certification Authority.
- "Certificate Chain" shall mean an ordered list of Certificates containing an end-user Subscriber Certificate and CA Certificates, which terminates in a root Certificate.
- "Certification Authority" ("CA") shall mean an entity authorized to issue, manage, revoke, and

PB Zertifikat

Das sichere https


20.06.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.de


Folie 24





Förderverein Bürgernetz München-Land e.V.

Sicherheitshinweis ✕

 Informationen, die Sie mit dieser Site austauschen, können von anderen weder angesehen noch verändert werden. Das Sicherheitszertifikat der Site ist jedoch fehlerhaft.

 Das Sicherheitszertifikat wurde von einer Firma ausgestellt, die Sie als nicht vertrauenswürdig eingestuft haben. Überprüfen Sie das Zertifikat, um festzustellen, ob Sie der ausstellenden Institution vertrauen möchten.

 Das Datum des Sicherheitszertifikates ist gültig.

 Der auf dem Sicherheitszertifikat angegebene Name ist gültig und stimmt mit dem Namen der gewünschten Site überein.

Soll der Vorgang fortgesetzt werden?

Sicherheitshinweis

Das sichere https

20.06.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De
Folie 25



Förderverein Bürgernetz München-Land e.V.

- **Version** V3
- **Seriennummer** 3CE0 D0B2 944F 8329 F40A 3F62 D0AE B48D
- **Signaturalgorithmus** sha1RSA
- **Austeller** OU = www.verisign.com/CPS Incomp.by Ref. LIABILITY LTD.(c)97 VeriSign
OU = VeriSign International Server CA - Class 3
OU = VeriSign, Inc.
O = VeriSign Trust Network
- **Gültig ab** Montag, 30. August 2004 02:00:00
- **Gültig bis** Mittwoch, 31. August 2005 01:59:59
- **Antragsteller** CN = banking.postbank.de
OU = Terms of use at www.verisign.com/rpa (c)00
OU = Postbank Systems AG
O = Deutsche Postbank AG
L = Bonn
S = NRW
C = DE
- **Öffentlicher Schlüssel** 3081 8902 8181 00B8 0464 0A3C 1F74 F883 7039 2830 BE42 CF9F 4A7E
4758 51E5 BDDA 5618 A647 C5BE B4D2 71E9 5262 25D7 5232 74DD 831B FF9B 31C5 F932 0C2D 16AC B047
1003 445E 3E02 8705 D94D 4474 38FE 5B39 8368 680C A3A9 E5BA FB60 85C0 BEF0 D42E C5C5 C83A EBD0
F14A D8AA E152 9320 9609 FF92 09F8 9796 C4F2 EAF0 476A E5E8 05A9 63AB 1776 C6C5 2502 0301 0001
- **Basiseinschränkungen** Typ des Antragstellers=Entity beenden
Einschränkung der Pfadlänge=Keine
- **Schlüsselverwendung** Digitale Signatur, Schlüsselverschlüsselung(A0)
- **CRL-Verteilungspunkt** [1]Verteilungspunkt der Zertifikatssperlliste
Name des Verteilungspunktes:
Vollst. Name:
URL=http://crl.verisign.com/Class3InternationalServer.crl

Inhalt eines Zertifikates 1

Das sichere https

20.06.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De
Folie 26



Förderverein Bürgernetz München-Land e.V.

● **Zertifikatsrichtlinien** [1]Zertifikatsrichtlinie:
Richtlinien-ID=2.16.840.1.113733.1.7.23.3
[1,1]Richtlinienqualifizierinfos:
ID des Richtlinien-Qualifiers=1.3.6.1.5.5.7.2.1
Qualifier=161C 6874 7470 733A 2F2F 7777 772E 7665 7269 7369 676E
2E63 6F6D 2F72 7061

● **Erweiterte Schlüsselverwendung** Unbekannte Schlüsselverwendung(2.16.840.1.113730.4.1)
Serverauthentifizierung(1.3.6.1.5.5.7.3.1)
Clientauthentifizierung(1.3.6.1.5.5.7.3.2)

● **Zugriff auf Zertifizierungsstelleninformationen** [1]Stelleninformationszugriff
Zugriffsmethode=Onlinestatusprotokoll des Zertifikats(1.3.6.1.5.5.7.48.1)
Alternativer Name:
URL=http://ocsp.verisign.com

● **1.3.6.1.5.5.7.1.12** 30 5F A1 5D A0 5B 30 59 0 . . . [OY
30 57 30 55 16 09 69 6D 0WOU..im
61 67 65 2F 67 69 66 30 age/gif0
21 30 1F 30 07 06 05 2B !0.0...+
0E 03 02 1A 04 14 8F E5
D3 1A 86 AC 8D 8E 6B C3k.
CF 80 6A D4 48 18 2C 7B ..j.H.,{
19 2E 30 25 16 23 68 74 ..0%.#ht
74 70 3A 2F 2F 6C 6F 67 tp://log
6F 2E 76 65 72 69 73 69 o.verisi
67 6E 2E 63 6F 6D 2F 76 gn.com/v
73 6C 6F 67 6F 2E 67 69 slogo.gi
66 f

● **Fingerabdruckalgorithmus** sha1
Fingerabdruck AA2F 4573 238B 58F4 EAB2 2F2D 7436 D0C1 09CF 8FC9

Inhalt eines Zertifikates 2

Das sichere https

20.06.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De
Folie 27



Förderverein Bürgernetz München-Land e.V.

Google-Suche: x509 - Microsoft Internet Explorer bereitgeste

Internetoptionen

Verbindungen Allgemein Sicherheit Programme Datenschutz Erweitert Inhalte

Startseite
Sie können die Seite ändern, die als Startseite angezeigt wird.
Adresse: about:blank
Aktuelle Seite Standardseite Leere Seite

Temporäre Internetdateien
Seiten, die Sie im Internet besucht haben, werden in einem speziellen Ordner gespeichert, um sie später schneller anzeigen zu können.
Cookies löschen... Dateien löschen... Einstellungen...

Verlauf
Der Ordner "Verlauf" enthält Links zu Seiten, die Sie besucht haben, um einen schnellen Zugang zu kürzlich besuchten Seiten zu ermöglichen.
Tage, die die Seiten in "Verlauf" aufbewahrt werden: 20
"Verlauf" leeren

Farben... Schriftarten... Sprachen... Eingabehilfen...

OK Abbrechen Übernehmen

Zertifikatsmanagement

Das sichere https

20.06.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De
Folie 28



Förderverein Bürgernetz München-Land e.V.

The screenshot shows two overlapping dialog boxes. The 'Internetoptionen' dialog is on the left, with the 'Zertifikate' tab selected. A red arrow points from the 'Zertifikate...' button in this dialog to the 'Zertifikatsverwaltung' dialog on the right. The 'Zertifikatsverwaltung' dialog is open to the 'Eigene Zertifikate' tab, which is currently empty. A red arrow points from the 'Zertifikate...' button in the 'Internetoptionen' dialog to the 'Eigene Zertifikate' tab in the 'Zertifikatsverwaltung' dialog.

Zertifikatsmanagement

Das sichere https

20.06.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

Folie 29



Förderverein Bürgernetz München-Land e.V.

The screenshot shows the 'Zertifikatsverwaltung' dialog box with the 'Eigene Zertifikate' tab selected. The dialog displays a list of certificates with the following columns: 'Ausgestellt für', 'Ausgestellt von', 'Gültig bis', and 'Angezeigte'. The list contains the following entries:

Ausgestellt für	Ausgestellt von	Gültig bis	Angezeigte
control-center.de	Thawte Server CA	31.07.02	<Keine>
www.britishairways.c...	www.verisign.com/CP...	03.09.04	<Keine>
www.britishairways.c...	www.verisign.com/CP...	21.08.04	<Keine>
www.sternberg.de	Thawte Server CA	07.11.04	<Keine>

Below the list, there are buttons for 'Importieren...', 'Exportieren...', and 'Entfernen'. At the bottom, there is a section for 'Beabsichtigte Zwecke des Zertifikats' with an 'Anzeigen' button and a 'Schließen' button at the very bottom.

Zertifikatsmanagement

Das sichere https

20.06.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

Folie 30



Förderverein Bürgernetz München-Land e.V.

Ausgestellt für	Ausgestellt von	Gültig bis	Angezeigter Name
A-Trust-Qual-01	A-Trust-Qual-01	07.02.05	A-Trust Qual-01
ABA.ECOM Root CA	ABA.ECOM Root CA	09.07.09	DST (ABA.ECOM...
America Online Root...	America Online Root C...	19.11.37	America Online R...
America Online Root...	America Online Root C...	29.09.37	America Online R...
Arge Daten Oesterrei...	Arge Daten Oesterreic...	12.02.09	Austrian Society f...
Autoridad Certificado...	Autoridad Certificadora...	28.06.09	Autoridad Certific...
Autoridad Certificado...	Autoridad Certificadora...	29.06.09	Autoridad Certific...
Autoridad de Certific...	Autoridad de Certificaci...	25.10.13	Autoridad de Certi...
Autoridade Certificad...	Autoridade Certificador...	01.12.11	Autoridade Certifi...

Zertifikatsmanagement

Das sichere https

20.06.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

Folie 31



Förderverein Bürgernetz München-Land e.V.



Zertifikatshierarchie

Das sichere https

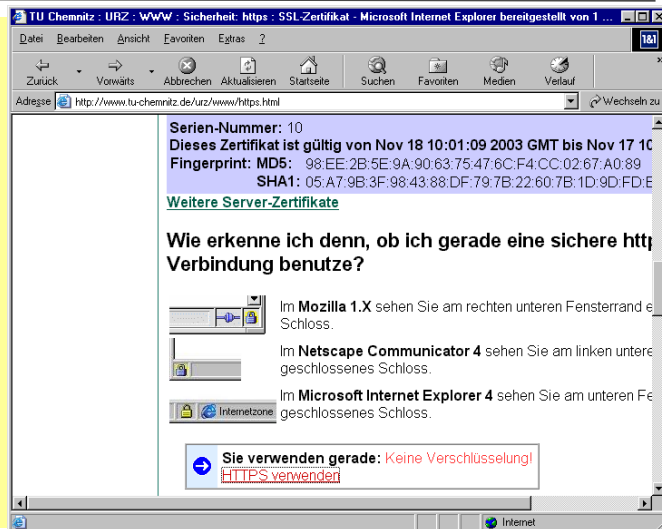
20.06.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

Folie 32

Anwendungen von https

- **Banking**
- **Austausch von vertraulichen Daten**
 - Login
 - Visa-Card Nummer bei Geschäften
 - Angabe von privaten Informationen
- **Achtung! Über https können Viren eingeschleust werden, da die verschlüsselten Daten nicht vom Virens scanner gescannt werden können.**

Was sollte ich als Anwender beachten um die Sicherheit nicht zu gefährden





Förderverein Bürgernetz München-Land e.V.

- **https statt http**
- **Ist das Schloss vorhanden**
- **Prüfen des Zertifikates**
 - Gültigkeitszeitraum ggf. alte entfernen
 - Stammzertifizierungsstelle
- **Vorsicht beim Installieren bzw. Übernehmen von neuen Zertifikaten**
- **Auf richtige Schreibweise achten!**
Z.B Poslbank statt Postbank
- **Browser auf dem letzten Standhalten, damit auch die neuesten Algorithmen zur Verfügung stehen.**
- **Mit dem Thema beschäftigen, die Zeit steht nicht still und Angreifer werden auch das „sicher“ „unsicher“ machen**

Sicherheit beachten

Das sichere https

20.06.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

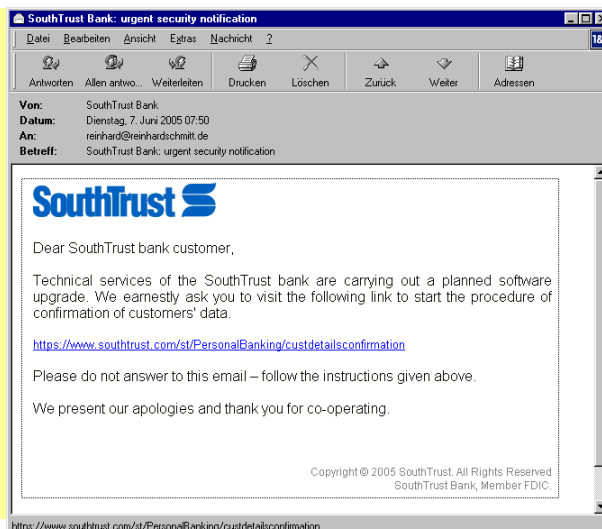
Folie 35



Förderverein Bürgernetz München-Land e.V.

Die Bezeichnung **Phishing** leitet sich vom **Fischen** (engl.: **fishing**) nach persönlichen Daten ab. Die Ersetzung von **F** durch **Ph** ist dabei eine im Insider-Jargon (**Leetspeak**) häufig verwendete Verfremdung. Es könnte unter Umständen sein, dass der Ausdruck auch auf password harvesting fishing zurückführbar ist.

Quelle:Wikipedia



Phishing

Das sichere https

20.06.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

Folie 36

Förderverein Bürgernetz München-Land e.V.

Phishing 2

Das sichere https

20.06.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De
Folie 37

Förderverein Bürgernetz München-Land e.V.

Phishing erkannt!

Das sichere https

20.06.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De
Folie 38



08.06.2005 14:48 Uhr

Adresse http://www.sueddeutsche.de/computer/artikel/575/5452

11.06.2005 15:14

sueddeutsche.de

Betrugsprävention

Erkennen Sie die Phishing-Mails?

Mit einem Quiz wird getestet, wie gut die Teilnehmer Phishing- von echten Mails unterscheiden können

Frank Ziemann

Das Unternehmen Mail-Frontier bietet ein so genannten Phishing-IQ-Test an. Jeder kann anonym daran teilnehmen und versuchen, ob er Phishing-Mails und echte Mails von Banken und anderen Unternehmen auseinander halten kann. Es werden jeweils zehn Mails angezeigt und die Teilnehmer sollen angeben, ob sie diese für echt oder betrügerisch halten. Dann können sie sich ihr Ergebnis anzeigen lassen und erhalten zu jeder Test-Mail eine Erklärung, woran man hätte erkennen können, dass sie echt oder eine Fälschung ist.

Seit einiger Zeit wird eine Fassung mit amerikanischen Mails angeboten, unter anderem von Amazon, MSN und Paypal. Später hinzugekommen ist auch eine Version mit britischen Mails, darunter solche von Visa, Ebay und MSN.

Die Auswertung der Ergebnisse von 300.000 Teilnehmern an der US-Version zeigt, dass 96 Prozent mindestens eine der gezeigten Mails falsch zuordnet. Im Durchschnitt erkennen sie sieben von zehn Mails richtig. Ferner fällt auf, dass die Teilnehmer in den letzten Monaten beim Erkennen von Phishing-Mails besser geworden sind, jedoch misstrauischer bei den echten. Für die Fassung mit britischen Mails wurden bislang noch keine Ergebnisauswertungen veröffentlicht.

http://survey.mailfrontier.com/survey/quiztest.html

20.06.2005 Reinhard Schmitt Reinhard@ReinhardSchmitt.De

Folie 39

Phishing 3

Das sichere https



Adresse http://www.antiphishing.org/



Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud

register

http://www.antiphishing.org/

report phishing - click here
vendor solutions directory

Website Hosting Courtesy GeoTrust

Members' Notice: Consumer Education Campaign at the Phish.Fry Summit on June 13 in San Francisco

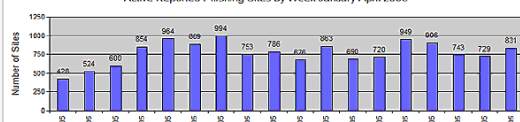
Report Phishing

Report phishing emails, phishing sites and malicious spyware to the Anti-Phishing Working Group and do your part to stomp out this insidious threat to our payment systems and e-commerce infrastructure. Click the top left "Report Phishing" link for instructions.

What is Phishing and Pharming?

Phishing attacks use both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Social-engineering schemes use "spoofed" e-mails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers. Hijacking brand names of banks, e-retailers and credit card companies, phishers often convince recipients to respond. Technical subterfuge schemes plant crimeware onto PCs to steal credentials directly, often using Trojan keylogger spyware. Pharming crimeware misdirects users to fraudulent sites or proxy servers, typically through DNS hijacking or poisoning.

Active Reported Phishing Sites by Week January-April 2005



20.06.2005 Reinhard Schmitt Reinhard@ReinhardSchmitt.De

Folie 40

Phishing 4

Das sichere https



Förderverein Bürgernetz München-Land e.V.

- Handout Uni-Essen 14.12.2003
- **keine URL mehr gefunden**
- **Netzicherheit:Architektur und Protokolle** <http://www.tm.uka.de>
- **Webwasher** <http://www.webwasher.com>
- **HTTPS-Die sichere Verbindung** <http://www.drweb.de/webmaster/https.shtml>
- **TU Chemnitz (https-Test)** <http://www.tu-chemnitz.de/urz/https.html>
- **AES Advanced Encryption Standard** <http://www.korelstar.de/aes.php>
- **Kryptologie** <http://www.regenechsen.de/krypto/Vorwort.php>
- **SSL Secure Sockets Layer** <http://www.webopedia.com/TERM/S/SSL.html>
- **SSL Secure Sockets Layer** <http://home.netscape.com/security/techbriefs/ssl.html>
- **TLS Transport Layer Security** <http://www.ietf.org/html.charters/tls-charter.html>
- **S-HTTP** <http://www.ietf.org/rfc/rfc2660.txt>
- **Apache-Server (SSL)** <http://www.apache-ssl.org>
- **Open Source Server-Implementierung** <http://www.openssl.org>

- **Phishing IQ Test II** <http://survey.mailfrontier.com/survey/quiztest.html>

Links zu Informationsquellen

Das sichere https

20.06.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De
Folie 41



Förderverein Bürgernetz München-Land e.V.

- **Bundesamt für Sicherheit in der Informationstechnik**
www.bsi.de
www.bsi.bund.de
- **Sichern aber Wie?**
www.bsi-fuer-buerger.de/druck/kap_07.pdf
- **Ins Internet - Mit Sicherheit**
www.bsi-fuer-buerger.de
- **Advanced Encryption Standard (AES)**
www.korelstar.de/aes.php
www.computerbase.de/lexikon/Advanced_Encryption_Standard
- **10 Gebote für Passwörter**
www.hirschbeutel.de/password.html

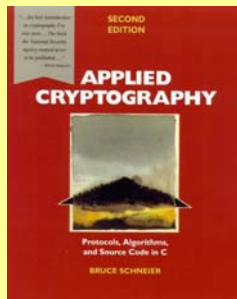
Links

Das sichere https

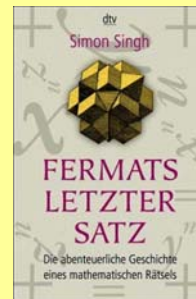
20.06.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De
Folie 42



ISBN 3-423-33071-6
Deutsch 12,50 €
Amazon ab 7,99 €



ISBN
Englisch 50,40 €
Amazon ab 38,59 €



ISBN 3-446-19313-8
Deutsch 10,00 €
Amazon ab 7,35 €

Literatur

Das sichere https

20.06.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

Folie 43

Weitere mögliche Vortragsthemen (bei Interesse).

- CD – DVD Normen
CD & DVD-Authoring (Diashows, Filme, Aufbau)
- Registry – das Gehirn von Windows
- IT-Security: Wie schütze ich meinen PC?
- Digitale Bilder fürs Web-Album aufbereiten

Vertiefung des Wissens

Das sichere https

20.06.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

Folie 44



Förderverein Bürgernetz München-Land e.V.



Fragen und Diskussion

Diskussion

Das sichere https

20.06.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

Folie 45



Förderverein Bürgernetz München-Land e.V.

XX

Das sichere https

20.06.2005 Reinhard Schmitt
Reinhard@ReinhardSchmitt.De

Folie 46