Ein Überblick über Security-Setups von E-Banking Websites

Stefan Huber
www.sthu.org

Linuxwochen Linz 2015
31. Mai 2015

Basierend auf Testergebnissen vom 28.03.2015 aus
https://www.sthu.org/blog/11-tls-dnssec-ebanking/

Motivation

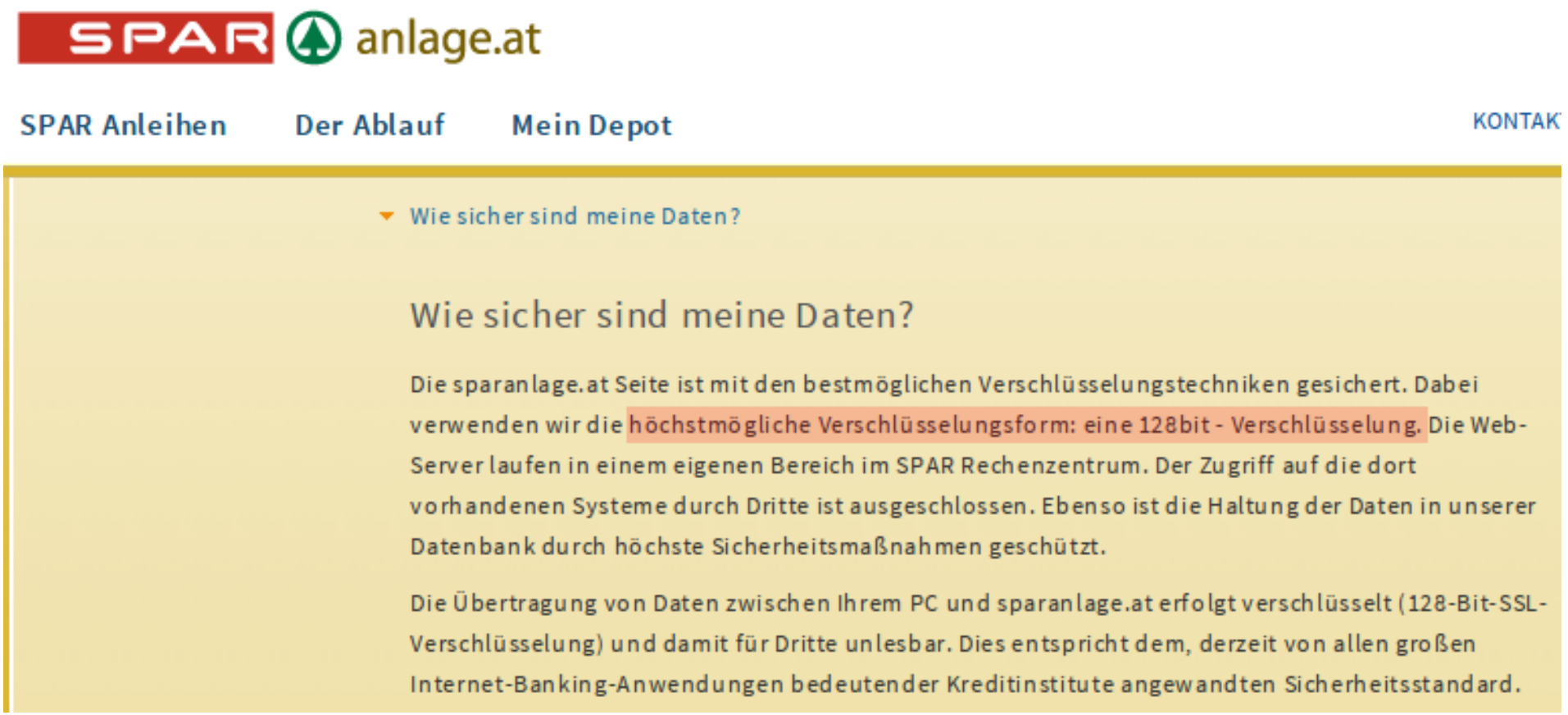


Abbildung: FAQ der sparanlage.at

Motivation

Sicherheit von Internet Banking

Mit Volksbank Internet Banking haben Sie eine sichere Verbindung zu Ihrem Konto!

Schon beim Einstieg wird Ihr Konto von drei Sicherheitsmechanismen geschützt:

- **Verfügernummer:** Die Verfügernummer ist ein mehrstelliger Zahlencode, den Sie nach Anmeldung zum Internet Banking von Ihrer Volksbank bekommen.
- **Verfügername:** Der Verfügername dient als zusätzliches Sicherheitsmerkmal, welches beim Ersteinstieg von Ihnen festgelegt wird.
- **PIN**:Gemeinsam mit Verfügernummer und Verfügername ist die PIN Ihr „Schlüssel" zum Internet Banking. Eine Initial-PIN (Erst-PIN) erhalten Sie nach Anmeldung zum Internet Banking von Ihrer Volksbank. Ihre persönliche PIN legen Sie beim Ersteinstieg selbst fest. Die persönliche PIN hat aus mindestens 6 Zeichen, möglichst einer Zahlen/Buchstabenkombination zu bestehen und ist jener Teil der Identifikation, der unbedingt geheim zu halten ist.

Wir verwenden zur Datenübertragung die höchstmöglichen Sicherheits-Verschlüsselungen (**128-Bit SSL**) im Netz. Seiten, die das SSL-Protokoll verwenden, können an ihrer URL erkannt werden, da sie mit "**https://**" und nicht mit "http://" beginnen und ein Sicherheitsschloss aufweisen. Überprüfen Sie dies bitte immer bei der Verwendung Ihres Internet Bankings.
Wichtiger Hinweis: Die Internet Banking Anwendung funktioniert nur mit einem Internetbrowser, der die 128bit SSL-Verschlüsselung verwendet.

Wie funktioniert eine SSL-Verschlüsselung?

Nähere Informationen zur SSL-Verschlüsselung finden Sie auf der folgenden Webseite von Security Server Deutschland.

zu www.ssl.de

Abbildung: Volksbank

Oberbank eBanking Sicherheit

Sicherheit hat im Internet und speziell im Online-Banking für die Oberbank oberste Priorität. Zu Ihrer Sicherheit verwendet die Oberbank das Verschlüsselungsverfahren 128-Bit-SSL (secure socket layer).

So erkennen Sie die sichere Verbindung mit dem Internet:

- **Die vollständige eBanking Adresse lautet:**
  https://www.oberbank-banking.at/obk/tiles/start.action
  Sollte die angezeigte Adresse von der oben angeführten abweichen, wenden Sie sich bitte an die eBanking Hotline:
  Telefon: 43(0)732/7802-32128 oder e-Mail: eBanking@oberbank.at
- **https:** Das „s" steht für die sichere Verbindung über SSL (128-Bit).
- Ein **abgesperrtes Schloss in der Statusleiste** Ihres Browserfensters zeigt die sichere Verbindung zu unserem Server an.
- Das **Oberbank eBanking-Zertifikat** können Sie überprüfen, indem Sie auf das „Schloss"-Symbol doppelklicken. Vergleichen Sie am besten das angezeigte Zertifikat mit den Detailinformationen der Oberbank.

Abbildung: Oberbank

Motivation

1. Allgemeines:

Technische Anforderung:

- PC mit Internetanschluss
- Browser (Software zum Betrachten von Websites)

  MS Internet Explorer alle Version ab 6.0 in 100% Funktion und Layout

  Mozilla Firefox ab Version 1.5 in 100% Funktion und Layout

  Netscape - alle Versionen ab 7.0 in 100% Funktion und Layout

  Apple (Opera, Safari) - alle Versionen nur funktionell

  als Alternativ-Browser kann Firefox verwendet werden

Abbildung: Oberbank

EBANKING PER INTERNET

EINFACH BEQUEM

Erledigen Sie Ihre Bankgeschäfte einfach und bequem. Unabhängig von Banköffnungszeiten, rund um die Uhr. Mit einem Höchstmaß an Sicherheit und Flexibilität. Ganz selbstverständlich.

EINFACH SICHER

eBanking per Internet - Ihre direkte Verbindung zu uns. Damit Sie Ihre Bankgeschäfte bequem, sicher (mit 2048-Bit Verschlüsselungstechnik) und kostengünstig über das Internet durchführen können. Verfügen Sie uneingeschränkt - rund um die Uhr, 365 Tage im Jahr - und unabhängig von Banköffnungszeiten über Ihr Konto; zusätzlich können Sie auch Ihre Wertpapiergeschäfte ganz einfach online erledigen.

Nützen Sie als Online-Banking-Verfüger die Digitale Signatur und damit die zurzeit wohl sicherste Variante für die Durchführung elektronischer Transaktionen im Internet.

- keine zeitlichen Einschränkungen
- keine geografischen Einschränkungen (vorausgesetzt eine intakte Internetverbindung)
- keine sicherheitsbezogenen Einschränkungen

Optimieren Sie Ihr Finanzmanagement mit eBanking und wickeln Ihre Geldgeschäfte ganz einfach online ab!

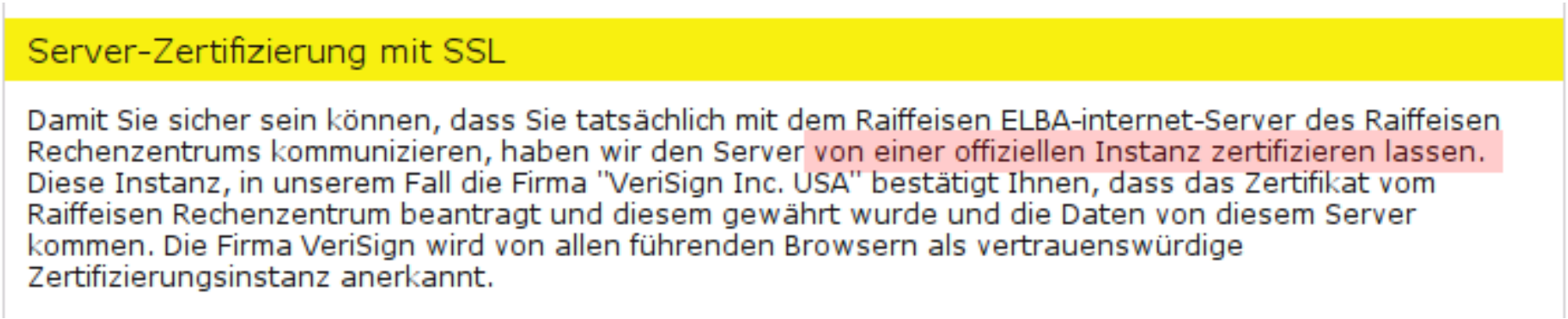
Abbildung: Bawag

Motivation

Sicherheit
Der Zugriff auf Ihr Konto ist durch Verfügernummer und PIN (Persönliche Identifikationsnummer) sowie TAN (Transaktionsnummer) immer gesichert. Durch die 2048-Bit-SSL Verschlüsselungstechnik genießen Sie ein Höchstmaß an Sicherheit. Die digitale Signatur, Ihre elektronische Unterschrift, bietet Sicherheit auf höchstem Niveau.

Abbildung: Easybank

Motivation



Server-Zertifizierung mit SSL

Damit Sie sicher sein können, dass Sie tatsächlich mit dem Raiffeisen ELBA-internet-Server des Raiffeisen Rechenzentrums kommunizieren, haben wir den Server von einer offiziellen Instanz zertifizieren lassen. Diese Instanz, in unserem Fall die Firma "VeriSign Inc. USA" bestätigt Ihnen, dass das Zertifikat vom Raiffeisen Rechenzentrum beantragt und diesem gewährt wurde und die Daten von diesem Server kommen. Die Firma VeriSign wird von allen führenden Browsern als vertrauenswürdige Zertifizierungsinstanz anerkannt.

Abbildung: Raiffeisen

Motivation

- Brechen Sie die Sitzung ab, wenn das Zertifikat auf etwas anderes hinweist als:
  This Certificate belongs to:
  banking.raiffeisen.at
  Terms of use at
  www.verisign.com/rpa (c)00
  Server Department
  Raiffeisen Informatik Zentrum
  Vienna, Vienna, AT
  This Certificate was issued by:
  www.verisign.com/CPS Incorp.by
  Ref. LIABILITY LTD.(c)97 VeriSign
  VeriSign International Server CA -
  Class 3
  VeriSign, Inc.
  VeriSign Trust Network

  oder für EPS2 Zahlungen:
  This Certificate belongs to:
  eps.raiffeisen.at
  Terms of use at
  www.verisign.com/rpa (c)00
  Server Department
  Raiffeisen Informatik Zentrum
  Vienna, Vienna, AT
  This Certificate was issued by:
  www.verisign.com/CPS Incorp.by
  Ref. LIABILITY LTD.(c)97 VeriSign
  VeriSign International Server CA -
  Class 3
  VeriSign, Inc.
  VeriSign Trust Network
  und informieren Sie umgehend Ihre Raiffeisenbank oder die ELBA-Hotline.

- Um ganz sicher zu gehen, können Sie auch **VeriSign RSA Secure Server CA** in der Liste der akzeptierten Zertifizierungsinstanzen in Ihrem Browser deaktivieren. Dadurch wird Sie Ihr Browser bei jeder neuen Verbindung auf die Prüfung des Zertifikats aufmerksam machen.

Section 2

TLS

Übersicht TLS/SSL

TLS ist ein Protokoll, kein Verschlüsselungsalgorithmus:

- Transport Layer Security
- Unsichere Application Layer Protokolle innerhalb TLS eingekapselt:
  - Application Layer: HTTP/SMTP/FTP/etc.
  - TLS
  - Transport Layer: TCP
  - Internet Layer: IPv4, IPv6

Das soll geleistet werden:

- Confidentiality
- Integrity & Authenticity

Versionen:

- SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3 (draft)

Bestandteile von TLS

Authenticity:

- Ein digitales Zertifikat (X.509 Zertifikat) zertifiziert die Echtheit des Servers.
- Signatur Algorithmus, z.B. RSA + SHA1

Confidentiality:

- Verschlüsselung des Datenstroms über symmetrischen Cipher.
  - Z.B. RC4, 3DES CBC, oder AES GCM
- Die Schlüssel werden über einen Key Exchange Algorithmus ausgetauscht.
  - Z.B. RSA, DH, oder ECDHE

Integrity:

- MAC (Message Authentication Codes)
- Z.B. HMAC via MD5 oder SHA1

→ Cipher Suite: Key exchange Alg. + Cipher + MAC

TLS Versionsgeschichte

- SSL 2.0: 1995
- SSL 3.0: 1996
  - Gilt seit vielen Jahren als unsicher.
  - POODLE Attacke verlieh endgültigen Todesstoß. Oberbank ist noch immer anfällig!
  - Sparanlage unterstützt noch immer SSL3, ist aber wegen dem RC4 Cipher nicht auf POODLE anfällig.
- TLS 1.0: 1999
  - Veraltet.
  - Unterstützt kein Secure Renegotiation, ermöglicht gewisse MITM Attacken.
  - Denizbank unterstützt nur TLS 1.0.
- TLS 1.1: 2006
  - Gegenmaßnahmen für einige Attacken gegen CBC Cipher Modus, z.B. BEAST.
- TLS 1.2: 2008
  - Aktueller Goldstandard.
  - Unterstützung für AES-GCM Cipher.

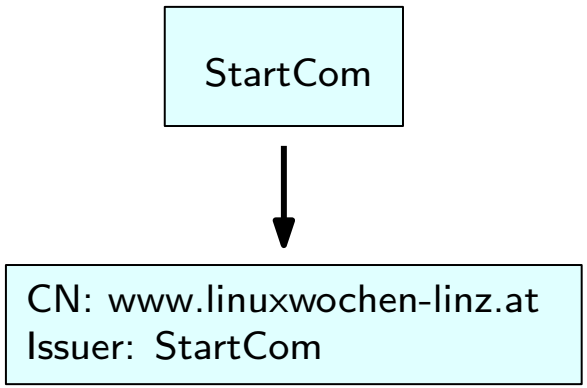
X.509 Zertifikate: Prinzip

Digitales Zertifikat:

- Signature Algorithmus (Public Key Crypto) + Hash Algorithmus
  - Z.B., RSA + SHA1, RSA + SHA256
- An einen Domain Namen gebunden.
- Gültigkeitszeitraum

Certificate Chain:

- Server Zertifikat wird durch Zertifikat einer Certificate Authority signiert, welcher man vertraut.



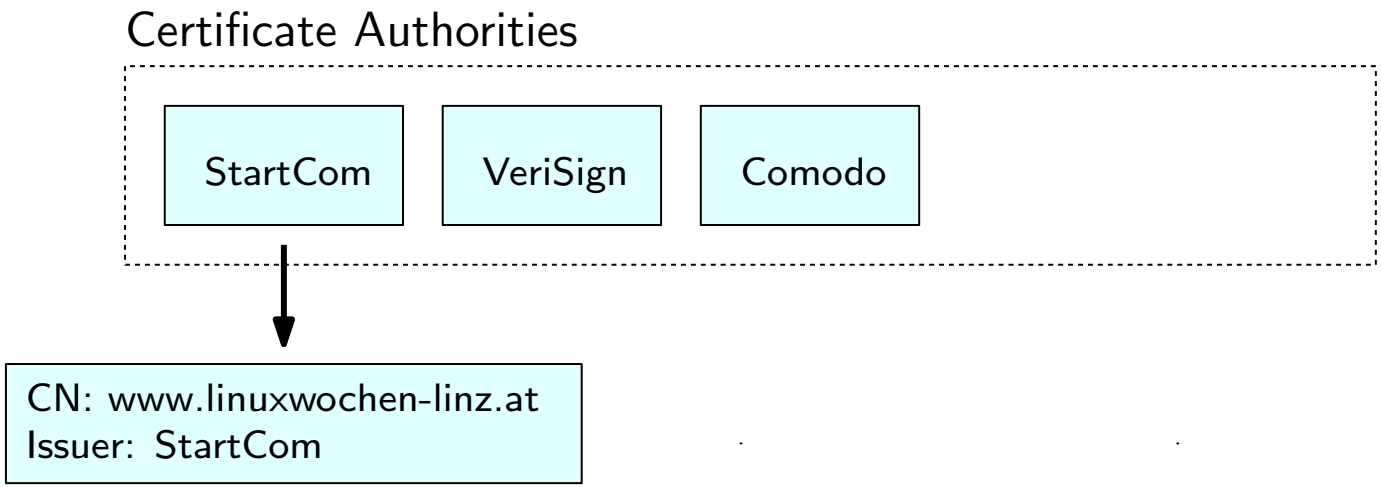
X.509 Zertifikate: Prinzip

Digitales Zertifikat:

- Signature Algorithmus (Public Key Crypto) + Hash Algorithmus
  - Z.B., RSA + SHA1, RSA + SHA256
- An einen Domain Namen gebunden.
- Gültigkeitszeitraum

Certificate Chain:

- Server Zertifikat wird durch Zertifikat einer Certificate Authority signiert, welcher man vertraut.
- Firefox kommt mit einer Liste von ca. 200 CAs, denen vertraut wird.



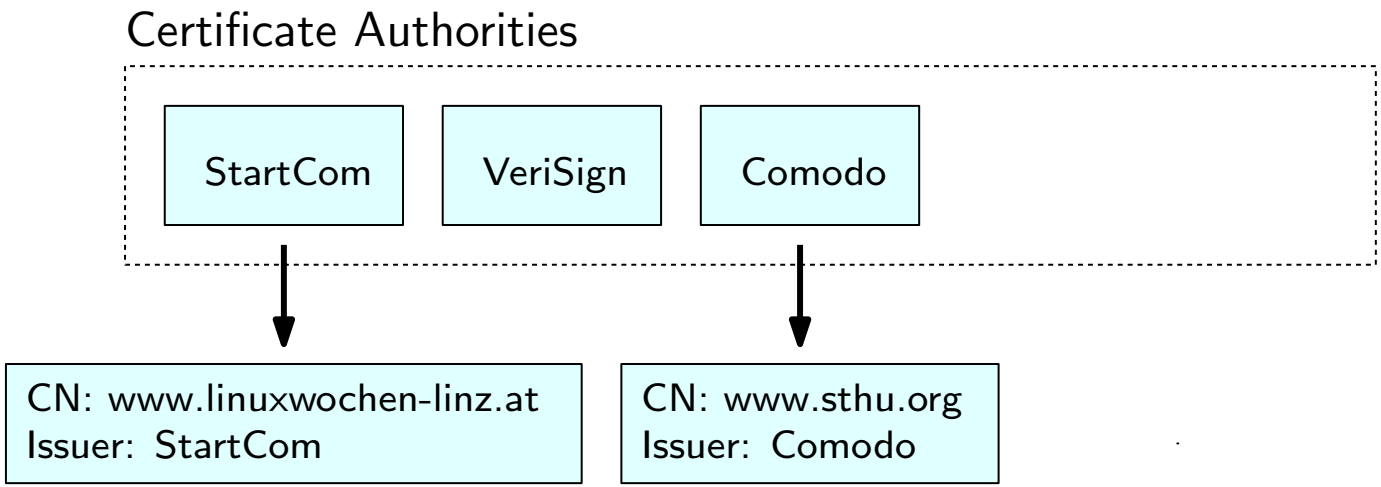
X.509 Zertifikate: Prinzip

Digitales Zertifikat:

- Signature Algorithmus (Public Key Crypto) + Hash Algorithmus
  - Z.B., RSA + SHA1, RSA + SHA256
- An einen Domain Namen gebunden.
- Gültigkeitszeitraum

Certificate Chain:

- Server Zertifikat wird durch Zertifikat einer Certificate Authority signiert, welcher man vertraut.
- Firefox kommt mit einer Liste von ca. 200 CAs, denen vertraut wird.



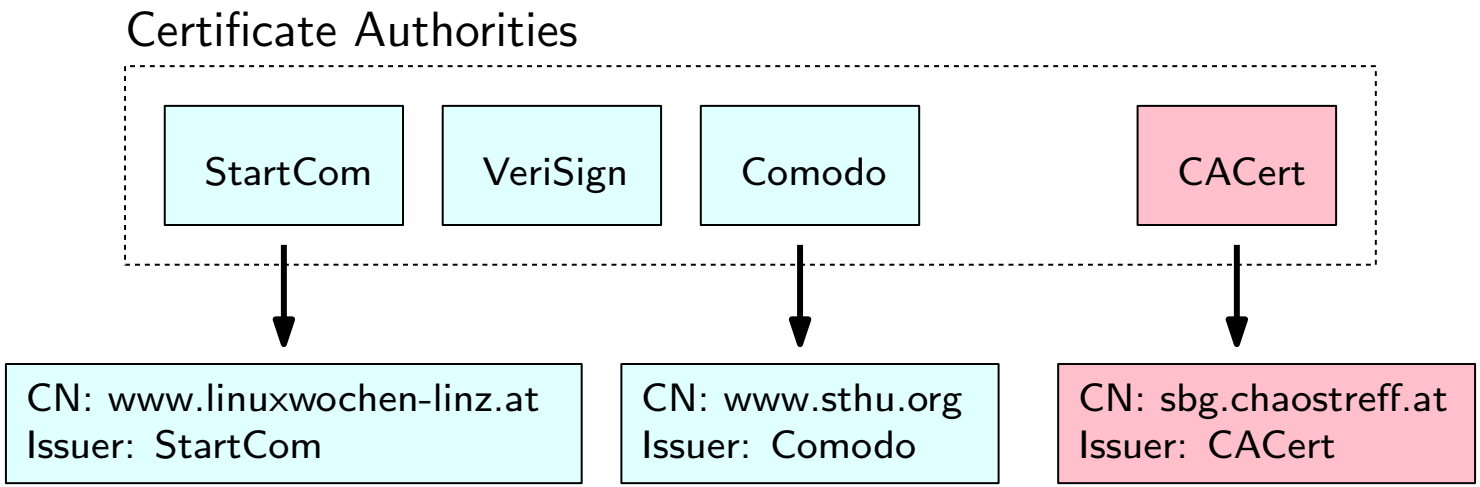
X.509 Zertifikate: Prinzip

Digitales Zertifikat:

- Signature Algorithmus (Public Key Crypto) + Hash Algorithmus
  - Z.B., RSA + SHA1, RSA + SHA256
- An einen Domain Namen gebunden.
- Gültigkeitszeitraum

Certificate Chain:

- Server Zertifikat wird durch Zertifikat einer Certificate Authority signiert, welcher man vertraut.
- Firefox kommt mit einer Liste von ca. 200 CAs, denen vertraut wird.



X.509 Zertifikate: Algorithmen

Signatur Algorithmus:

- Typischerweise RSA.
- Zumindest 2048 Bit empfohlen.
  - Alle getesten Institute verwenden 2048 Bit Zertifikate.
- „2048 Bit Verschlüsselungstechnik“ der Bawag und Easybank?

Hash Algorithmus:

- SHA-2 (SHA-256, SHA-384, etc.) ist der Goldstandard.
- SHA-1 sollte in absehbarer Zeit getauscht werden.
  - Google Chrome warnt in einer aktuellen Version.
  - Betrifft Easybank, Raiffeisen, Volksbank.
- MD5 ist tot.
  - Erzeugung falscher Zertifikate seit 2008 (25C3).
  - Selbst MS blockiert seit 2013 MD5 Zertifikate.

„Offizielle Zertifizierung“ der Raiffeisen?

TLS: Handshake

Sehr stark vereinfacht:

1. Browser verbindet sich zu Server und sendet:
   - Höchste unterstützte TLS Version.
   - Liste von unterstützten Cipher Suites.
2. Server antwortet:
   - Wählt TLS Version.
   - Wählt Cipher Suite.
   - Schickt Zertifikat.

Cipher Suites: Key Exchange

Algorithmen:

- RSA
- DH + RSA
- ECDH + RSA
- DHE + RSA
- ECDHE + RSA

Forward Secrecy:

- Ephemeral Diffie-Hellman (DHE, ECDHE) erzeugen neue Schlüssel bei jeder Session.
- Ist das Schlüsselmaterial auf dem Server kompromittiert, so kann alter aufgezeichneter Traffic nicht entschlüsselt werden. (April 2014: Heartbleed Attacke.)
- Bank Austria, Paypal, Denizbank, Sparanlage, Oberbank unterstützen kein Forward Secrecy.

Cipher Suites: Symmetric Encryption

Algorithmen:

- RC4
  - Hat eine lange Liste bekannter Angriffe seit den 90ern.
  - RFC7525 verbietet RC4.
  - Sparanlage verwendet 128-Bit RC4.
- 3DES
  - Schwacher Algorithmus.
  - Volksbank mit Firefox als Browser wählt 3DES CBC.
- AES
  - Der AES Algorithmus gilt prinzipiell als sicher.
  - CBC Modus:
    - Notorische Anfälligkeit auf Padding Attacken: BEAST, Lucky Thirteen, POODLE.
    - TLS-1.1 schafft großteils Abhilfe, bei TLS-1.0 muss der Browser Attacken verhindern.
    - Paylife (Firefox), Raiffeisen, Volksbank, Bank Austria, Paypal, Denizbank, und Oberbank verwenden AES im CBC-Modus.
  - GCM Modus:
    - Aktueller Goldstandard.
    - Sparkasse, Bawag, Easybank, Paylife (Chrome).

Cipher Suites: Message Authentication Codes

Algorithmen:

- MD5:
  - Unsicher, praktische Attacken.
  - RFC 5246 verbietet MD5.
  - Sparanlage verwendet MD5.
- SHA-1:
  - Gilt trotz theoretischer Fortschritte noch als sicher.
  - Sollte in naher Zukunft durch SHA-2 (SHA-256, SHA-384, SHA-512) ersetzt werden.
- SHA-256:
  - Aktueller Goldstandard.
  - Sparkasse, Bawag, Easybank, Paylife.

TLS: 128-Bit Verschlüsselung?

Was heißt jetzt „SSL (128-Bit)“ oder „höchstmöglichen Sicherheits-Verschlüsselung (128-Bit SSL)“?

Crypto Wars:

- U.S. Export Regulierung von „starker“ Kryptographie in den 90ern.
- 128-Bit Verschlüsselung (RC4, 3DES) konnte nicht aus den USA exportiert werden.
  - „128-Bit SSL“

HSTS

HTTP Strict Transport Security

- Beim ersten Besuch via HTTPS wird Browser angewiesen in Zukunft nur via HTTPS zuzugreifen.
- Schützt for MITM Attacken.
- Einfach umzusetzen.
- Paylife, Denizbank, Sparanlage, Oberbank machen das nicht.

Section 3

DNSSEC

DNSSEC: Überblick

Status quo:

- DNS ist ein zentraler Service im Internet.
- DNS ist nicht authentifiziert.
- DNS cache poisoning, DNS hijacking Attacken.

DNSSEC:

- Kryptographische Signaturen um DNS Records zu signieren.
- Auch um Nicht-Existenz von DNS Records zu beweisen.

DANE:

- DNS-based Authentication of Named Entities
- X.509 Zertifikate via DNS ausliefern.
- Alternative zu CAs.

DNSSEC: Status Quo

- Kein Finanzinstitut unterstützt DNSSEC.
  - Paypal.com unterstützt DNSSEC, aber www.paypal.com ist ein CNAME auf e6166.a.akamaiedge.net, und hierfür gibt es keinen DNSSEC Support.
- 2013 habe ich per Mail die meisten Institute kontaktiert:
  - Oberbank: Nameserver durch Telekom betrieben. Hätten gerne DNSSEC bis Q1/2014, spätestens Q2/2014.
  - Paylife: Es wird 6–12 Monate dauern bis DNSSEC läuft.
  - BAWAG: Sie müssen das mit den Admins besprechen.
  - Alle anderen: Keine Antwort.

Section 4

Konklusion

Übersicht: Februar 2014

Hostname	TLS	Key exch.	Encryption	Msg. auth.
netbanking.sparkasse.at	1.2	ECDHE_RSA	AES_128_GCM	SHA384
ebanking.bawagpsk.com	1.2	DHE_RSA	AES_128_GCM	SHA384
ebanking.easybank.at	1.2	DHE_RSA	AES_128_GCM	SHA384
www.kreditkarte.at (PayLife)	1.0	DHE_RSA	AES_256_CBC	SHA1
online.bankaustria.at	1.2	RSA	AES_256_CBC	SHA1
www.paypal.com	1.2	RSA	AES_256_CBC	SHA1
www.sparanlage.at (new)	1.2	RSA	AES_256_CBC	SHA1
banking.hypo.at	1.1	RSA	AES_256_CBC	SHA1
banking.raiffeisen.at	1.1	RSA	AES_256_CBC	SHA1
www.banking.co.at (Volksbank)	1.0	RSA	AES_256_CBC	SHA1
www.oberbank-banking.at	1.0	RSA	AES_256_CBC	SHA1
www.sparanlage.at (old)	1.0	RSA	RC4_128	MD5

Übersicht: März 2015

Hostname		TLS	Sign. Alg.	Cipher suite			HSTS	DNS-SEC
				Key exch.	Encryption	MAC		
netbanking.sparkasse.at	A+	TLS 1.0-1.2	SHA256	ECDHE_RSA	AES_128_GCM	SHA256	Y	N
ebanking.bawagpsk.com	A	TLS 1.0-1.2	SHA256	ECDHE_RSA	AES_128_GCM	SHA256	Y	N
ebanking.easybank.at	A	TLS 1.0-1.2	SHA1	ECDHE_RSA	AES_128_GCM	SHA256	Y	N
my.paylife.at	A	TLS 1.0-1.2	SHA256	DHE_RSA	AES_128_GCM	SHA256	N	N
				ECDHE_RSA	AES_256_CBC	SHA		
banking.raiffeisen.at	A-	TLS 1.0-1.2	SHA1	DHE_RSA	AES_256_CBC	SHA	Y	N
www.banking.co.at (Volksbank)	A-	TLS 1.0-1.2	SHA1	ECDHE_RSA	AES_128_CBC	SHA	Y	N
					3DES_EDE_CBC			
online.bankaustria.at	A-	TLS 1.0-1.2	SHA256	RSA	AES_256_CBC	SHA	Y	N
www.paypal.com	B	TLS 1.0-1.2	SHA256	RSA	AES_256_CBC	SHA	Y	Y/N
ebanking.denizbank.at	B	TLS 1.0	SHA256	RSA	AES_128_CBC	SHA	N	N
www.sparanlage.at	B	SSL3, TLS 1.0, TLS 1.2	SHA256	RSA	RC4_128	MD5	N	N
www.oberbank-banking.at	C	SSL3 – TLS 1.2	SHA256	RSA	AES_256_CBC	SHA	N	N

- Sparanlage: „Höchstmögliche Verschlüsselung“
- Volksbank: „Höchstmögliche Sicherheits-Verschlüsselung“
- Oberbank: „Sichere Verbindung über SSL (128-Bit)“

Tools

TLS:

- sslyze[1]: `https://github.com/nabla-c0d3/sslyze`
- Qualsys SSL Labs ssltest: `https://www.ssllabs.com/ssltest/`
- `openssl s_client -connect www.sthu.org:https -showcerts`
- Der Browser der Wahl.

DNSSEC:

- `dig +dnssec sthu.org`
- `whois sthu.org | grep DNSSEC`
- `http://dnsviz.net/d/www.sthu.org/dnssec/`

[1] Dank an Florian Preinstorfer für den Hinweis.

Anleitungen

TLS:

- RFC 7525 (Mai 2015): Recommendations for Secure Use of Transport Layer Security (TLS) and Datagram Transport Layer Security (DTLS)
- Better Crypto: `https://bettercrypto.org/`