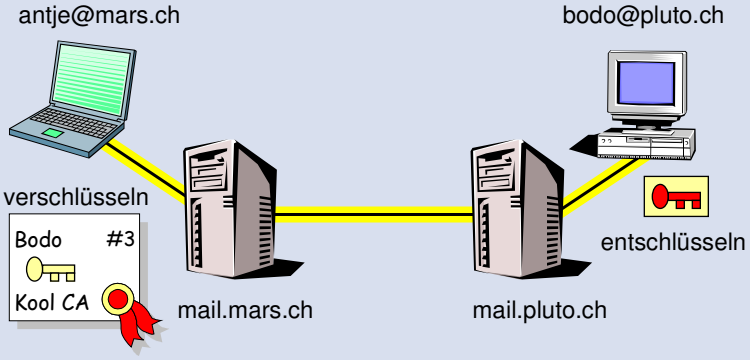
IT - Security Forum #3

Wie sicher reist meine E-Mail?

Prof. Dr. Andreas Steffen
Zürcher Hochschule Winterthur
andreas.steffen@zhwin.ch

IT - Security Forum #3

User-zu-User Email Sicherheit

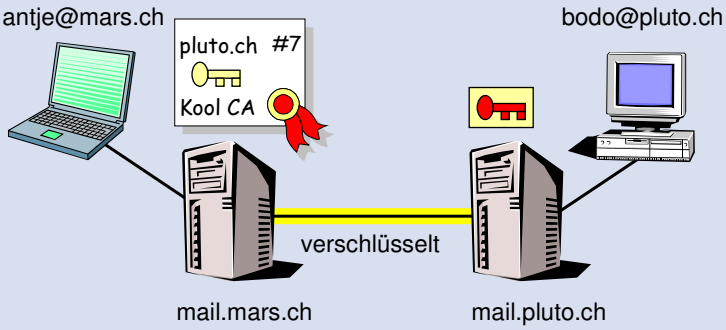


- **S/MIME User-zu-User Email Verschlüsselung bedingt, dass jeder User ein Zertifikat besitzen muss.**
- **Problem #1: Es gibt kein globales Zertifikatsverzeichnis für Email User.**
- **Problem #2: Private Key Recovery in Notfällen.**

2

IT - Security Forum #3

Server-zu-Server Email Sicherheit



- **SMTP Server-zu-Server Email Verschlüsselung auf der Basis von Transport Layer Security (SSL/TLS) bedingt, dass nur der Mailserver jeder Domain ein Zertifikat besitzen muss.**
- **Nachteil: Es muss den Mailservern in der Übertragungskette vertraut werden, obwohl diese überwacht werden könnten.**

3

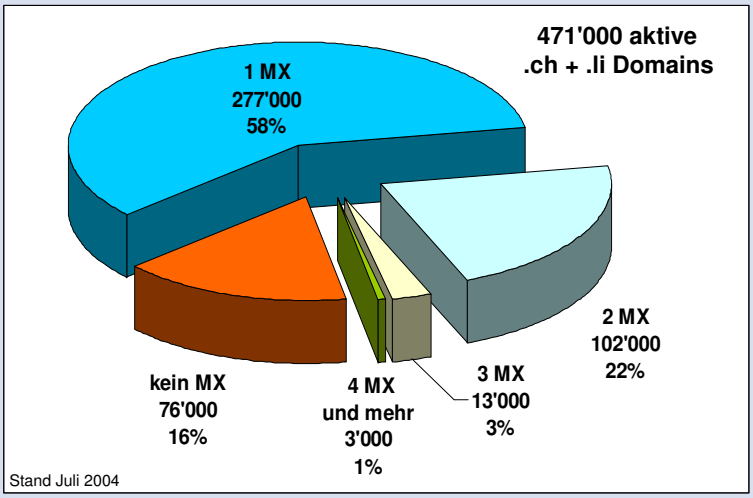
IT - Security Forum #3

Studie "TLS-fähige Mailserver in den .ch + .li Domains"

Christian Brauchli, Jakob Furrer
Studiengang Kommunikation und Informatik
Zürcher Hochschule Winterthur
braucchr@zhwin.ch, furrejak@zhwin.ch

IT - Security Forum #3

Anzahl MX Records pro Domain

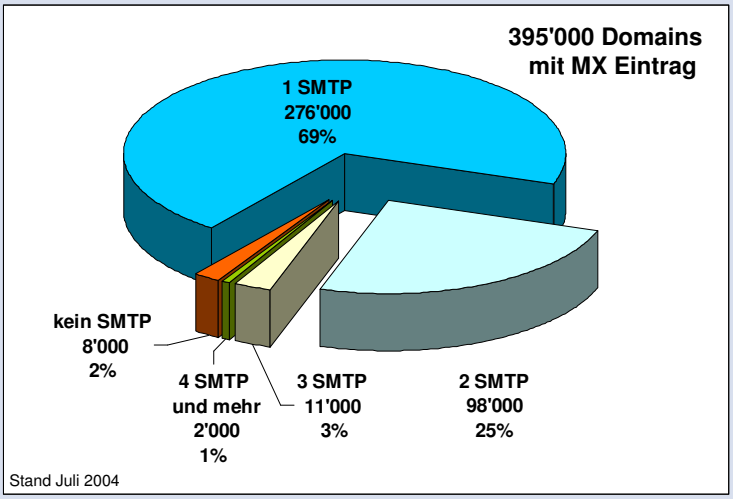


395'000 Domains mit MX Einträgen (84%)

5

IT - Security Forum #3

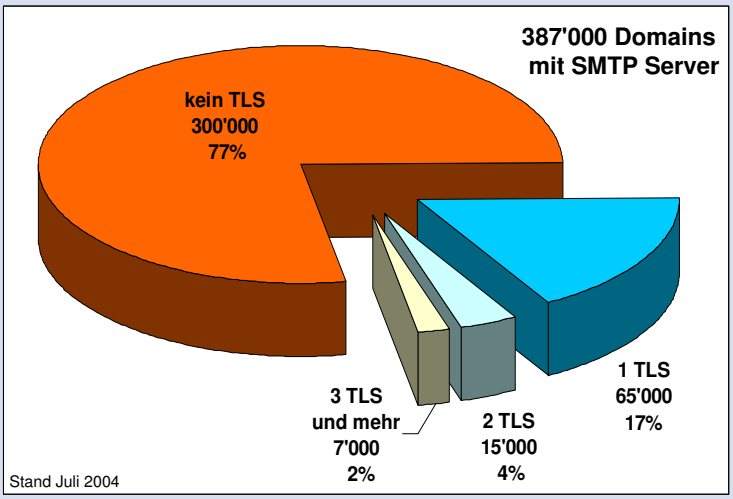
Domains mit SMTP Mailserver



387'000 Domains mit funktionierendem Mailserver (98%)

6

STARTTLS Support (SMTP Port 25)

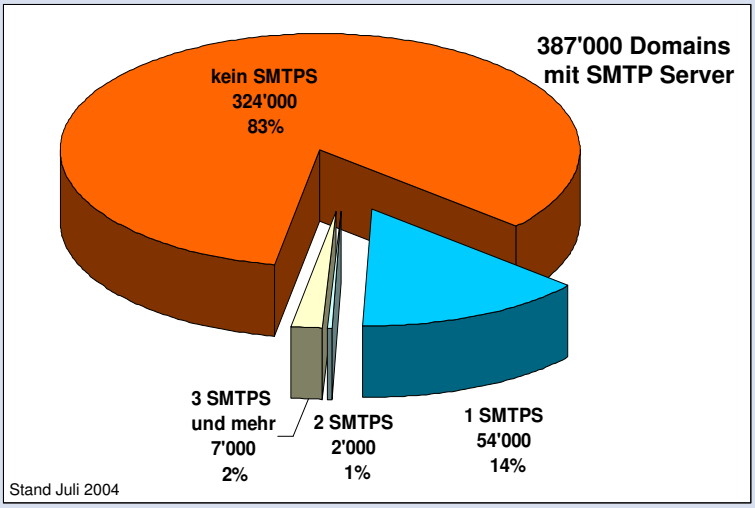


87'000 Domains mit STARTTLS Unterstützung (23%)
Bevorzugter Sicherheitsmechanismus

7

IT - Security Forum #3

TLS Support (SMTPS Port 465)

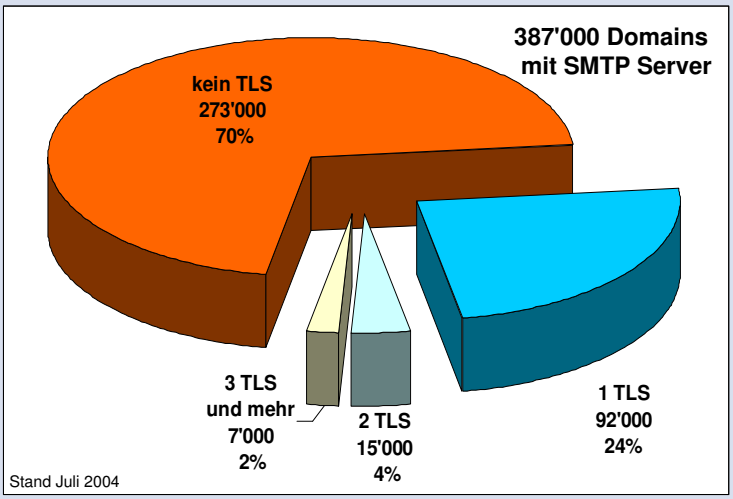


63'000 Domains mit SMTPS Unterstützung (17%)
Sollte nicht mehr verwendet werden

8

IT - Security Forum #3

STARTTLS und SMTPS kombiniert



114'000 Domains mit sicherem Mailserver (30%)

IT - Security Forum #3

9

Verschlüsselungsalgorithmen

- SSL_RSA_EXPORT_WITH_RC4_40_MD5 6 Verbindungen
- SSL_RSA_WITH_RC4_128_MD5 128'201 Verbindungen
- SSL_RSA_WITH_RC4_128_SHA 13'797 Verbindungen
- SSL_RSA_WITH_3DES_EDE_CBC_SHA 1'592 Verbindungen
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA 7 Verbindungen

☺ Schwache 40 Bit Verschlüsselung kommt fast nicht mehr vor.

Das Arbeitspferd ist immer noch RC4 mit 128 Bit Schlüssel.

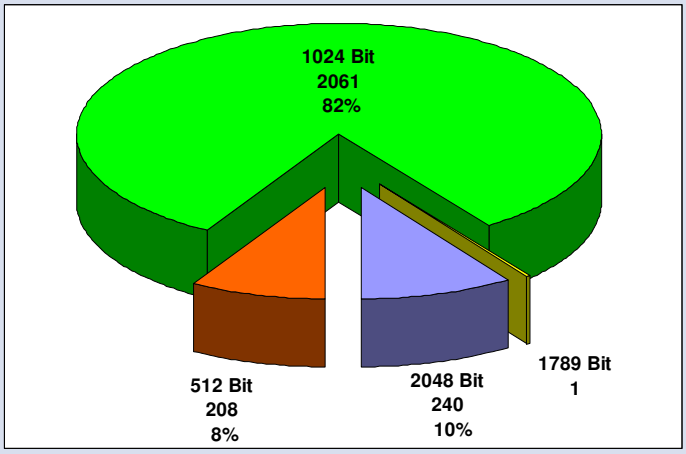
☹ Moderne AES Verschlüsselung wird noch kaum verwendet.

IT - Security Forum #3

10

IT - Security Forum #3

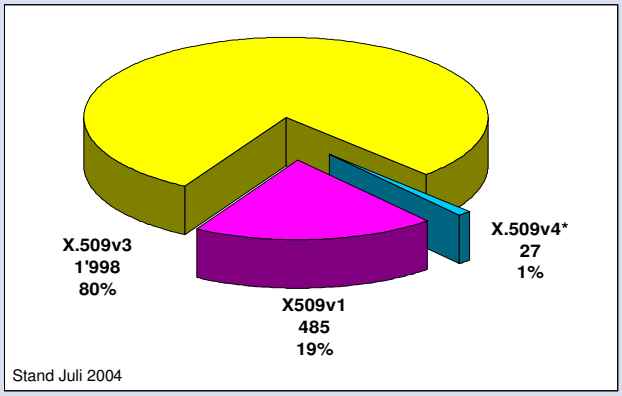
Länge der RSA Public Key Schlüssel



512 Bit RSA Schlüssel sind kryptografisch zu schwach und sollten nicht verwendet werden.

IT - Security Forum #3

TLS benötigt Mailserver-Zertifikate



2'510 X.509 Zertifikate auf 114'000 sichere Domains

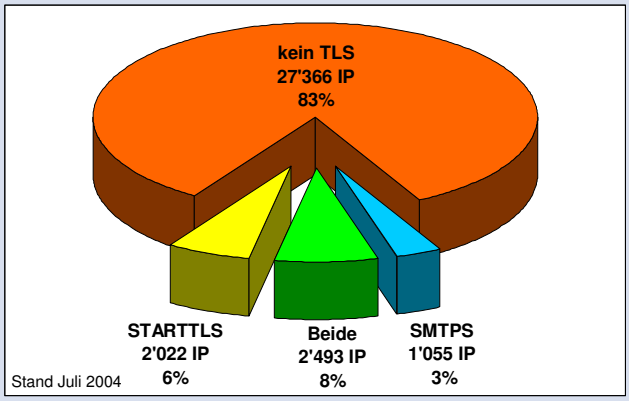
➔ 1 X.509 Zertifikat auf 45 sichere Domains !

Was ist der Grund ???

*Es gibt keine v4 Zertikate, sondern es wurde v3 falsch ASN.1 codiert (0x03 anstatt 0x02)

IT - Security Forum #3

Anzahl physikalischer Mailserver



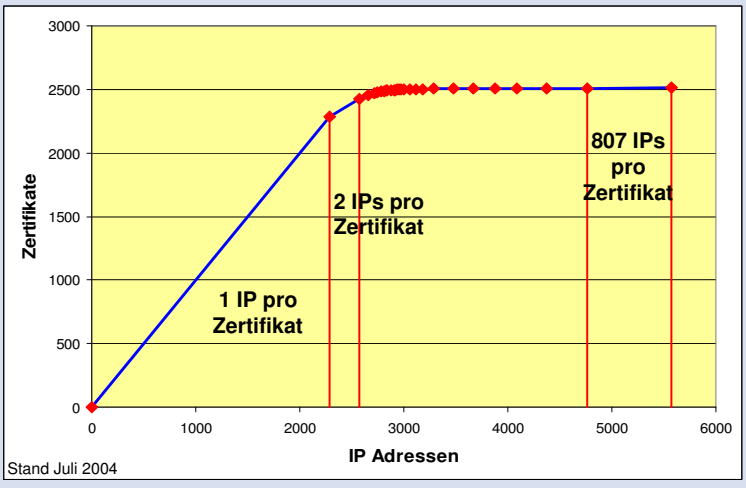
Die Maildienste von 387'000 CH + LI Domains werden auf nur 33'000 physikalischen Rechnern (identifiziert durch die IP Adresse) gehostet.

Davon unterstützen 5570 Server (17%) sichere Email (STARTTLS, SMTPS oder beide Ports).

13

IT - Security Forum #3

Zertifikate versus IP Adressen

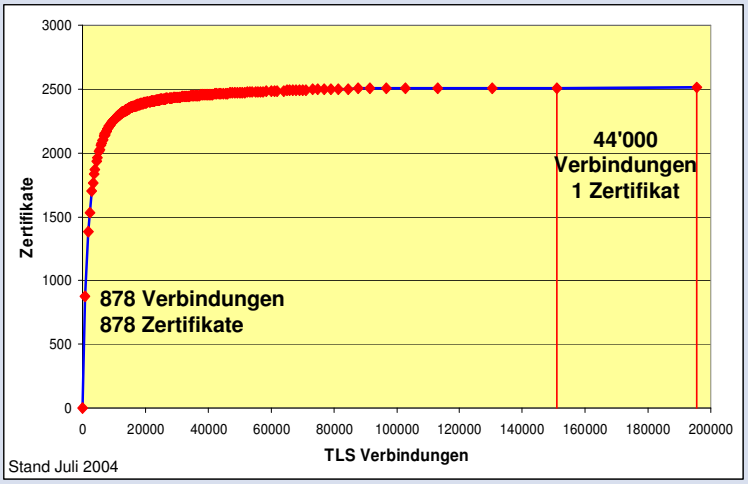


Zuordnung der 5570 physikalischen Mailhosts (IP Adressen) auf 2510 Zertifikate.

14

IT - Security Forum #3

Zertifikate vs TLS Verbindungen



Zuordnung der 195'000 getesteten TLS Verbindungen (STARTTLS und SMTPS) auf die 2510 Zertifikate.

15

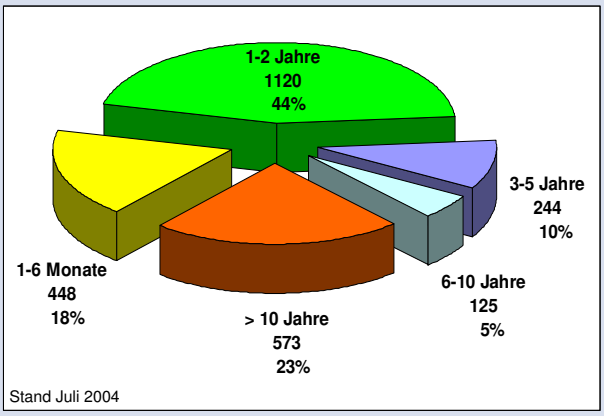
IT - Security Forum #3

Interpretation

- **Zertifikate versus IP Adressen**
  - 2293 von total 2510 Zertifikaten werden jeweils nur von einem Mailhost verwendet.
  - Die restlichen 217 Zertifikate werden auf mehreren Mailhosts eingesetzt.
  - Auf mehr als 1400 Mailhosts wird die Plesk Web Hosting Software mit einem Plesk Default-Zertifikat eingesetzt.
- **Zertifikate versus TLS Verbindungen**
  - Ca. 1500 Zertifikate werden jeweils nur von einem Domain verwendet.
  - In einem Fall wird ein Zertifikat von einem ISP verwendet, über den 44'000 TLS Verbindungen laufen.

16

Gültigkeitsdauer der Zertifikate

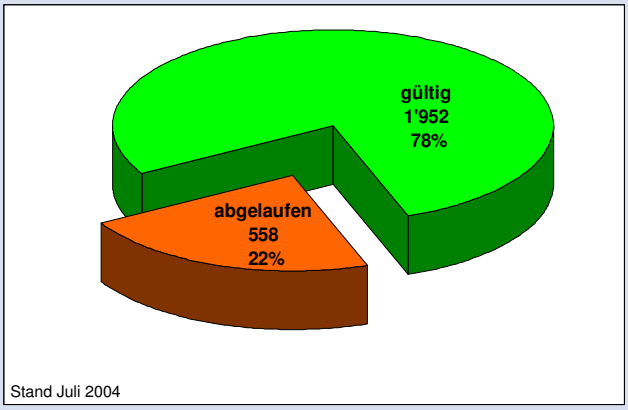


Stand Juli 2004

- Viele Demo-Zertifikate (1-6 Monate)
- Gültigkeitsdauer >10 Jahre bei 1024 Bit RSA Schlüsseln macht aus Sicherheitsgründen keinen Sinn.

17

Gültigkeit der Zertifikate



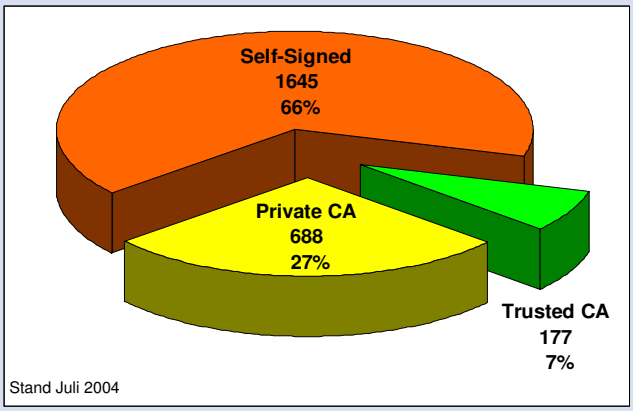
Stand Juli 2004

- Viele abgelaufene Demo-Zertifikate

18

IT - Security Forum #3

Vertrauenswürdige Zertifikate

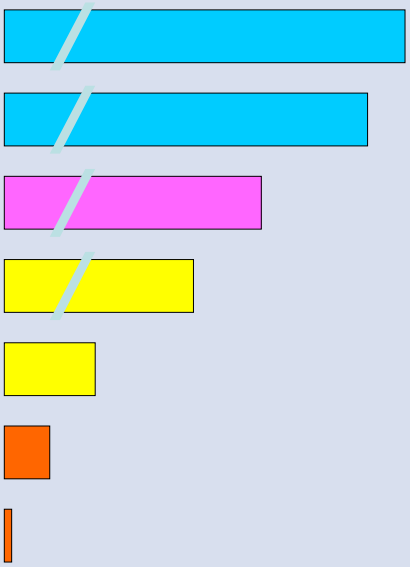


- **Self-Signed Zertifikaten kann nicht vertraut werden.**
- **Private Root CA Zertifikate sind meist nicht lokalisierbar.**
- **Trusted CAs (Thawte, Equifax, Comodo, TrustCenter, Verisign, etc.) werden nur vereinzelt eingesetzt.**

19

IT - Security Forum #3

Fazit



471'000 aktive Domains

387'000 Domains mit Mailserver

114'000 TLS-fähige Domains

33'000 physikalische Mailhosts

5'570 TLS-fähige Mailhosts

2'510 Server-Zertifikate

177 vertrauenswürdige Zertifikate

20

IT - Security Forum #3

Fazit

- 30% aller Domains unterstützen zumindest empfangsseitig die verschlüsselte Übertragung von Emails.
- Erfreulicherweise wird fast ausschliesslich starke 128 Bit Verschlüsselung eingesetzt.
- Es sind 2510 X.509 Zertifikate im Gebrauch, die höchst ungleich auf die Domains verteilt sind, da ein grosser Teil der Domains durch ein paar wenige ISPs gehostet wird.
- Die Zertifikate beeinhalten meist 1024 Bit Public Keys. 60% davon sind 1-10 Jahre gültig, der Rest ist entweder schon abgelaufen oder eindeutig zu lange gültig.
- Nur 7% aller Zertifikate sind von einer offiziellen CA signiert. Eine verlässliche Authentisierung des Mailservers ist deshalb meist nicht möglich.
- Damit TLS zur SPAM-Bekämpfung eingesetzt werden könnte, müsste der Prozentsatz vertrauenswürdiger Zertifikate stark vergrössert werden.

21