
Zertifikate & Notes

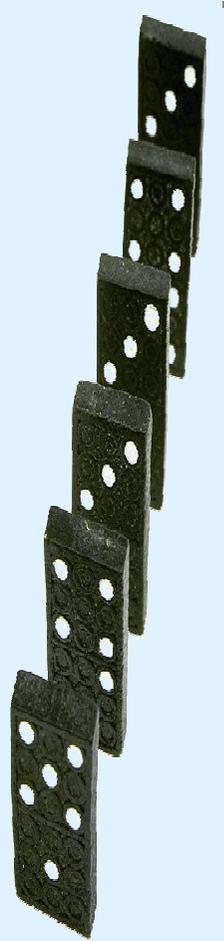
Bernhard Kolb

EBE-GmbH

www.ebe-edv.com



Zertifikate – wozu?

- 
- A vertical stack of several dominoes, showing different faces with dots, positioned on the left side of the slide.
- Nachweis meiner Identität
 - CN – Common Name
 - Organisation
 - Country
 - Email Adresse
 - Identität des Ausstellers

Wie geht das im Notes

- 
- A vertical stack of several dominoes, arranged in a slightly curved line, positioned on the left side of the slide.
- Cert.id bei erster Serverinstallation
 - Daraus User.id für jeden Benutzer
 - Public Key im Domino Directory

Wunderbar – alles klappt

- 
- A vertical stack of several dominoes, arranged in a slightly curved line. They are dark in color with white dots on their faces.
- Verschlüsselte mails
 - Signierte Mails
 - Nur innerhalb Notes....

...das andere Programm...

- 
- A vertical stack of several dominoes, arranged in a slightly curved line, positioned on the left side of the slide.
- Mails über das Internet (SMTP)
 - Outlook empfänger
 - X.509 Zertifikate !
 - -> kaufen (A-Trust, Verisign, ...) (*.p12)

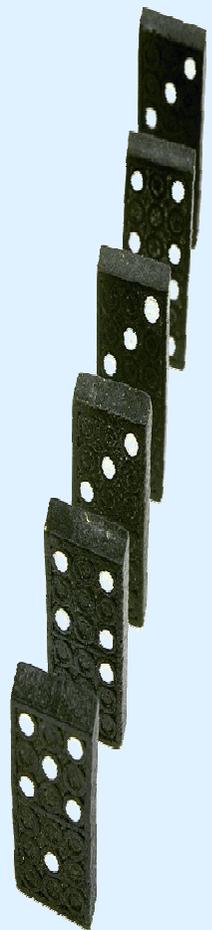
How to setup Self-Certified Certificates

- 
- A vertical stack of several dominoes, arranged in a slightly curved line, positioned on the left side of the slide.
- Certificate Authority (CA.nsf)
 - ACL -> CA Privileged User
 - Certificate erstellen
 - Certificate Properties definieren
 - Server Keyring erstellen

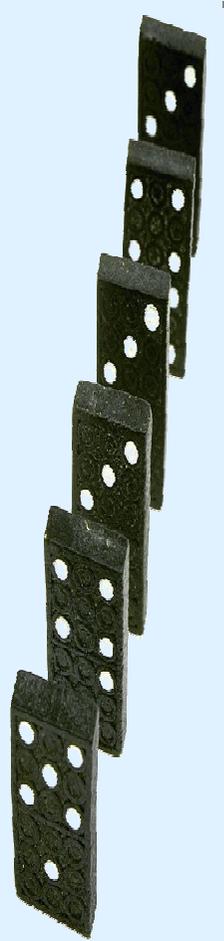
 - keyfile.kyr und keyfile.sth
ins Domino-Verzeichnis kopieren

 - Serverdokument:
Ports - Internet Ports - SSL aktivieren (http restart)

Zertifikate anfordern

- 
- A vertical stack of several dominoes, arranged in a slightly curved line, positioned on the left side of the slide.
- <http://server/ca.nsf> - request Client Certificate
 - Admin muß manuell freigeben
 - Dem Link im email folgen
 - „Accept Certificate“ im IE
 - Extras – Internetoptionen – Inhalte – Zertifikate exportieren.... -> myCert.p12

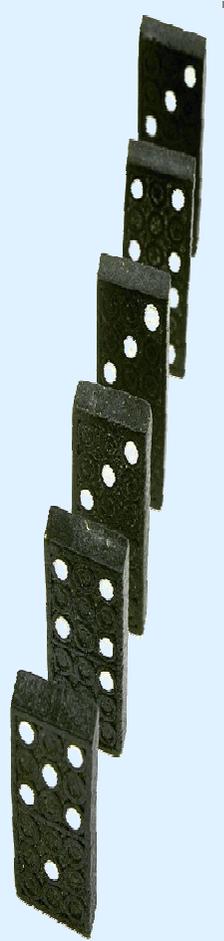
Erhaltenes pk12 File im Notes importieren

- 
- File-user security – Your Identity – Your Certificates – Your Internet Certificates
 - Voilá wir können signierte Nachrichten senden..
 - Beim Erhalt der ersten signierten email aus dem internet muß der Empfänger ins lokale Adreßbuch hinzugefügt werden (Cross certificate)
 - Voilá wir können verschlüsselte Nachrichten senden..

Erhaltenes pk12 im Outlook importieren

- 
- A vertical stack of several dominoes, arranged in a slightly curved line, positioned on the left side of the slide.
- Extras – Optionen – Sicherheit – importieren
Angabe des .pk12 Files samt Kennwort
 - Oder Import im IE
 - Wichtig: die email-adresse muss übereinstimmen!

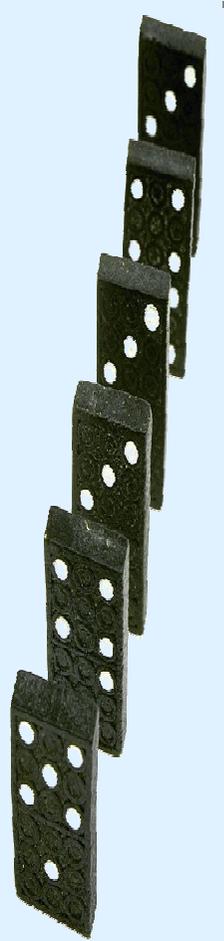
Summary

- 
- A vertical stack of several dominoes on the left side of the slide, arranged in a slightly curved line.
- Pk12 Files organisieren
 - Bei Verisign etc. Kaufen
 - Oder cca50.ntf verwenden
 - Im Mail Client importieren
 - Einmal signierte Nachrichten austauschen

Domino Web-Authentication

- 
- A vertical stack of several dominoes, showing different faces with dots, positioned on the left side of the slide.
- Im Serverdokument
Ports – Internet Ports – Web – Authentication
Options: Clientcertificate: **Yes**
 - **Keine Passworteingabe nötig!**

Https

- 
- A vertical stack of several dominoes on the left side of the slide, arranged in a slightly curved line.
- Keyfile.kyr und keyfile.sth im Domino-Data Verzeichnis
 - Serverdokument: SSL aktivieren (http restart)
 - Clients erhalten beim ersten Zugriff eine Warnung (falls self-certified)
im IE: Zertifikat anzeigen – installieren
Zertifizierungspfad – root – Zertifikat anzeigen – installieren (Fingerprint)!!
 - Der Client ist damit sicher, dass der Server der ist, der er vorgibt zu sein....

Grundlagen ...



Zertifikate – wozu also?

- 
- A vertical stack of several dominoes, arranged in a slightly curved line, positioned on the left side of the slide.
- Verschlüsselte SMTP Mails
 - Signierte SMTP Mails
 - Https
 - Client (Web) Authentication