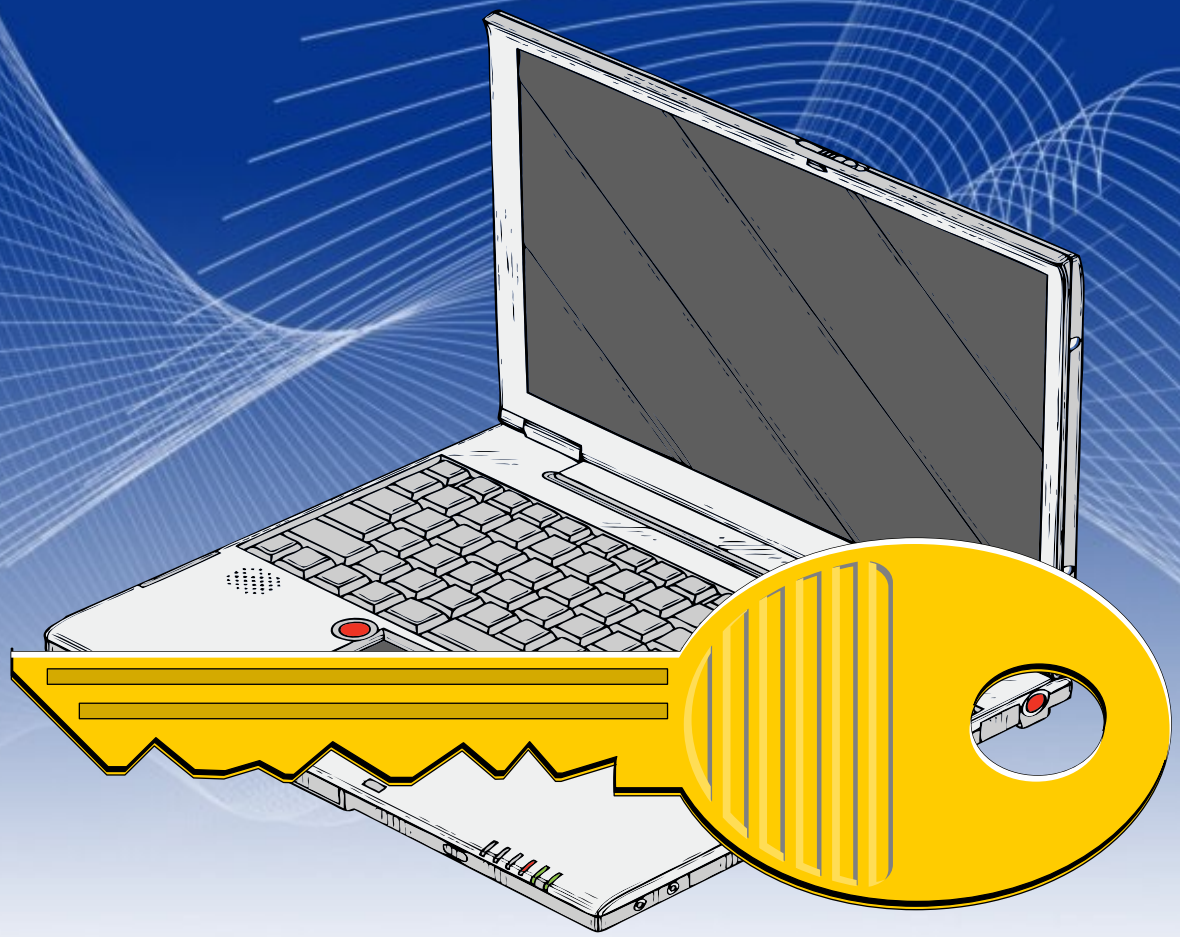
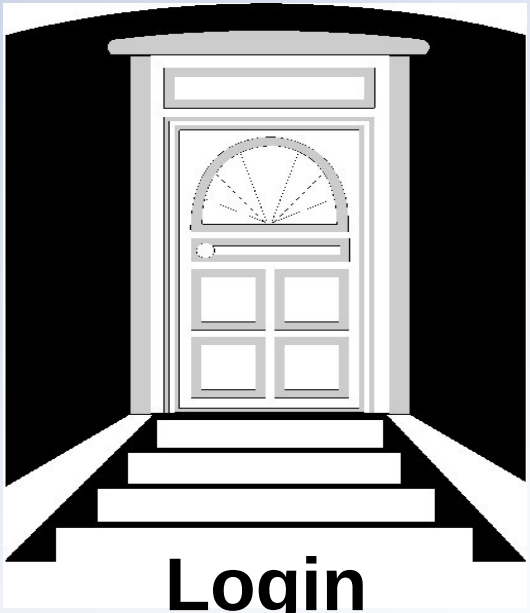


Kryptoschlüssel, Zertifikate und Smartcards in der Praxis

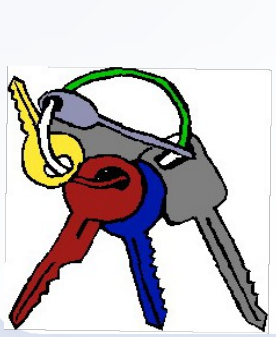
Rolf Wald
LUG-Balista Hamburg e.V.

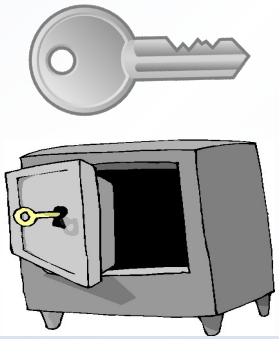
CLT 2014

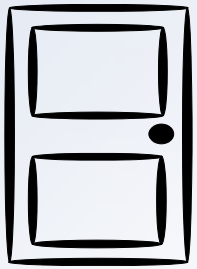
(Krypto-)Schlüssel in der Praxis



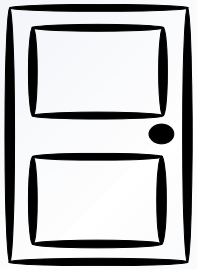
Login



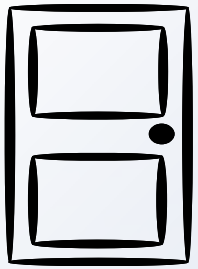




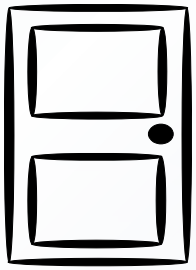
E-Mail
Signatur
Verschlüsselung



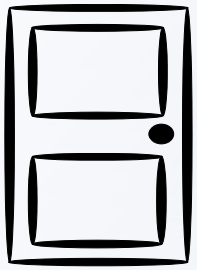
OpenVPN



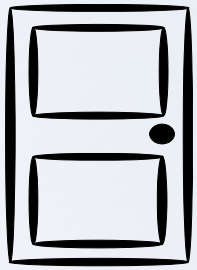
Authentifizierung
PAM-Module
ssh



Client-Auth
Webbrowser

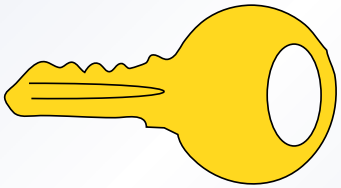


WPA Enterprise
Wlan
802.1X



Truecrypt
Key
Cryptsetup-
LUKS

(Krypto-)Schlüssel in der Praxis



Zertifikate einbinden

E-Mail/Client-Auth: Firefox, Thunderbird, Kmail, gpgsm, Chromium

Authentifizierung lokal und im Netzwerk, WPA Enterprise, OpenVPN

Smartcards Konfiguration

Basisinstallation, Firefox, Thunderbird

wpa_supplicant – wpa_gui, openvpn.conf

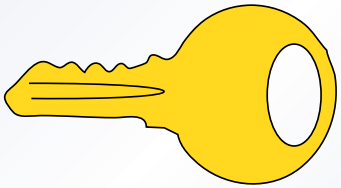
Authentifizierung über pam Module, Cryptsetup-LUKS, Truecrypt

Servereinstellungen

Apache-Webserver, Wordpress, Dokuwiki

Radius-Server, OpenVPN-Server

(Krypto-)Schlüssel in der Praxis



Zertifikate einbinden

- E-Mail/Client-Auth: Firefox, Thunderbird, Kmail, gpgsm, Chromium
- Authentifizierung lokal und im Netzwerk, WPA Enterprise, OpenVPN

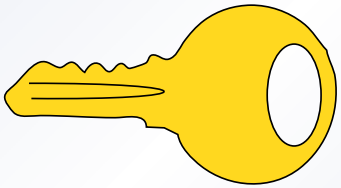
Smartcards Konfiguration

- Basisinstallation, Firefox, Thunderbird
- wpa_supplicant – wpa_gui, openvpn.conf
- Authentifizierung über pam Module, Cryptsetup-LUKS, Truecrypt

Servereinstellungen

- Apache-Webserver, Wordpress, Dokuwiki
- Radius-Server, OpenVPN-Server

(Krypto-)Schlüssel in der Praxis



Zertifikate einbinden

- E-Mail/Client-Auth: Firefox, Thunderbird, Kmail, gpgsm, Chromium
- Authentifizierung lokal und im Netzwerk, WPA Enterprise, OpenVPN

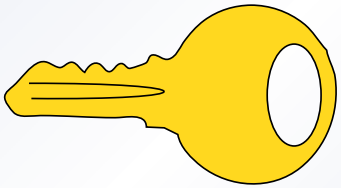
Smartcards Konfiguration

- Basisinstallation, Firefox, Thunderbird
- wpa_supplicant – wpa_gui, openvpn.conf
- Authentifizierung über pam Module, Cryptsetup-LUKS, Truecrypt

Servereinstellungen

- Apache-Webserver, Wordpress, Dokuwiki
- Radius-Server, OpenVPN-Server

(Krypto-)Schlüssel in der Praxis



Zertifikate einbinden

- E-Mail/Client-Auth: Firefox, Thunderbird, Kmail, gpgsm, Chromium
- Authentifizierung lokal und im Netzwerk, WPA Enterprise, OpenVPN

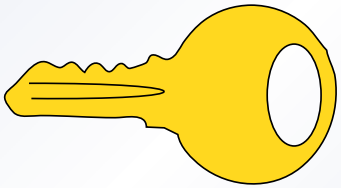
Smartcards Konfiguration

- Basisinstallation, Firefox, Thunderbird
- wpa_supplicant – wpa_gui, openvpn.conf
- Authentifizierung über pam Module, Cryptsetup-LUKS, Truecrypt

Servereinstellungen

- Apache-Webserver, Wordpress, Dokuwiki
- Radius-Server, OpenVPN-Server

(Krypto-)Schlüssel in der Praxis



Zertifikate einbinden

- E-Mail/Client-Auth: Firefox, Thunderbird, Kmail, gpgsm, Chromium
- Authentifizierung lokal und im Netzwerk, WPA Enterprise, OpenVPN

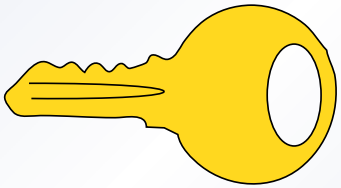
Smartcards Konfiguration

- Basisinstallation, Firefox, Thunderbird
- wpa_supplicant – wpa_gui, openvpn.conf
- Authentifizierung über pam Module, Cryptsetup-LUKS, Truecrypt

Servereinstellungen

- Apache-Webserver, Wordpress, Dokuwiki
- Radius-Server, OpenVPN-Server

(Krypto-)Schlüssel in der Praxis



Zertifikate einbinden

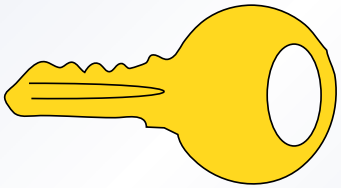
- E-Mail/Client-Auth: Firefox, Thunderbird, Kmail, gpgsm, Chromium
- Authentifizierung lokal und im Netzwerk, WPA Enterprise, OpenVPN

Smartcards Konfiguration

- Basisinstallation, Firefox, Thunderbird
- wpa_supplicant – wpa_gui, openvpn.conf
- Authentifizierung über pam Module, Cryptsetup-LUKS, Truecrypt

Servereinstellungen

- Apache-Webserver, Wordpress, Dokuwiki
- Radius-Server, OpenVPN-Server



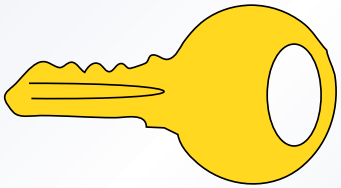
Welche Smartcard habe ich getestet?

Feitian PKI

Aventra MyEID

Athena ASECard Crypto

SmartCard-HSM



Welche Smartcardleser sind getestet?

- **SCM SCR 3500**
- **Gemalto ID Bridge**
- **SPR532 Chipdrive pinpad pro**
- **Gemalto PC Pinpad Reader**
- **ACR 83 pineasy**

Wo ist der Haken?

Kosten der Smartcard Lösung

Nicht jede Smartcard und nicht jeder Smartcardleser funktioniert unter OpenSource Software.

Smartcards und Leser arbeiten nicht beliebig miteinander.

Firefox und Thunderbird müssen bei jeder Änderung des Smartcardlesers neu gestartet werden.

Einige Programme sind fehlerhaft und müssen manuell repariert werden.

Kenntnisse der Kommandozeile sind notwendig.

Wenn Sie noch Fragen haben

- Beantorten wir sie gerne auf unserem Stand
- Werden Artikel darüber auf unseren Webseiten und unserem Wiki nach der Veranstaltung veröffentlicht. (www.lug-hh.de und wiki.lug-balista.de)
- Die ausführliche Anleitung gibt es bereits auf unserem Wiki zum Nachlesen und Ausprobieren: http://wiki.lug-balista.de/doku.php/balista:projekte
- Eine Auswahl an Artikeln zu diesem Thema gibt es auf der CLT Seite
  http://chemnitzer.linux-tage.de/2014/vortraege/shortpaper/257-kryptoschluessel.pdf

Vielen Dank für Ihre Aufmerksamkeit