Zertifikat installieren unter Linux (ubuntu ab 14.04 LTS und Windows)

Zusatzknow how:  
Was sind die Prinzipien der Datensicherheit (Integrität, Authentizität, Vertraulichkeit, Verbindlichkeit, Verfügbarkeit), welche davon werden mit Zertifikaten abgedeckt?  
Was ist ein Zertifikat, wie ist es aufgebaut, welche Klassen gibt es, wozu dient es (siehe Kapitel 11 Webshops)

ACME automated certification managment environment  
zB LetsEncrypt: Man beantragt ein Zertifikat und der Anbieter wickelt die Überprüfung ob der Antragsteller berechtigt ist für den Rechner oder die Domäne ein Zertifikat zu erhalten und erstellt falls das in Ordnung ist das Zertifikat.

# Voraussetzungen

Mit ubuntu 12.04 ists offenbar nicht so einfach, weil trotz LTS ein dafür wichtiges repository nicht mehr verfügbar ist (Stand Feb 2017) und die Installation mit fehlenden libs scheitert.

Domäne muss existieren und erreichbar sein (IP Adresse reicht keinesfalls), man muss Besitzer der Domäne sein bzw. muss das script vom Rechner aus der Domäne ausgeführt werden (zumindest bei LetsEncrypt)

Man benötigt einen Benutzer mit root Rechten aber nicht den root selber.

sudo apt-get update … Repository Inhalte (Info welche SW Versionen aktuelle sind) aktualisieren

evtl sudo apt-get upgrade … SW wird aktualisiert

# Let’s Encrypt Client herunterladen

LetsEncrypt Klient in ein lokales Verezeichnis (zB usr/local/sbin) herunterladen und ausführbar machen  
  
cd /usr/local/sbin  
sudo wget <https://dl.eff.org/certbot-auto>  
sudo chmod a+x /usr/local/sbin/certbot-auto

# Einrichten des SSL Certificates

Es reicht den Befehl

certbot-auto --apache -d klio.htl-villach.at

auszuführen

Dann rennt die Installation und das Zertifikat wird genau für den Rechner installiert.  
Anders rennt das ab, wenn der Rechner mehrere Subdomains vergeben würde zB  
userspace1.domain.topleveldomain  
userspace2.domain.topleveldomain  
usw

dann übergibt man diese als zusätzliche Parameter. Der erste Parameter in der Liste ist die **base** domain, die Let’s Encrypt verwendet, um das Zertifikat zu erzeugen. Man übergibt also diese als erstes und die anderen bzw aliases als die restlichen jeweils mit dem Parameter –d subdomain zB:

certbot-auto --apache -d example.com -d www.example.com

Anschließend läuft die Zertifikatserzeugung, man wird dabei noch nach einer Email Adresse gefragt (email Domäne muss bei LetsEncrypt nicht eine Adresse der Domäne sein) und ob man den gesamten Datenverkehr auf https umleiten will oder nicht.

Nach Beendigung der Installation befindet sich das Zertifikat in /etc/letsencrypt/live.

Obs funktioniert, schaut man zB mit Mozilla und dann auf das Schlüsselsymbol klicken und Zertifikatinfos anzeigen lassen

Das Zertifikat ist 90 Tage gültig, dann muss es erneuert werden. Dafür gibt es den Befehl

certbot-auto renew

Falls nötig wird das Zertifikat dann erneuert, sonst passiert nichts. Am einfachsten ist es einen cron-job rennen zu lassen, der in regelmäßigen Abständen zb einmal wöchentlich das auto-renew aufruft.

Dazu sudo crontab –e aufrufen und in die cron – Tabelle zB folgendes eintragen

30 2 \* \* 1 /usr/local/sbin/certbot-auto renew >> /var/log/le-renew.log

(script jeden Montag um 2:30 starten Meldungen in der Datei le-renew.log protokollieren).

# Letsencrypt unter Windows:

Für den IIS ist das mittlerweile auch ganz einfach (getestet unter Server 2012 RS)

Man ladet letsencrypt-win-simple herunter, entpackt und startet es. Wenn ein IIS läft wird man gefragt, ob man für den ein Zertifikat erstellen will. Das wars. Es wird dabei sogar im TaskScheduler ein passender Eintrag erzeugt, um rechtzeitig ein neues Zertifikat zu holen;

Überprüfen mit schtasks.exe

Dann sollte es einen Eintrag der Art

Folder: \

TaskName Next Run Time Status  
======================================== ====================== ===============  
letsencrypt-win-simple httpsacme-v01.api 20.03.2017 09:00:00 Ready  
Optimize Start Menu Cache Files-S-1-5-21 N/A Ready

geben, der täglich die Gültigkeit des Zertifikats prüft.

# LDAP absichern

geht nicht weil lets encrypt nur Server Zertifikate vergibt

Für LDAPS reicht ein selber ausgestelltes Zertifikat. Vorgangsweise ab Server 2012 R2 sehr einfach (im Gegensatz zu 2008 und vorher):

mmc (Microsoft Management Console) aufrufen, certificate snapin hinzufügen, und dort auf personal/certificates rechte Maustaste -new certfificate request anfordern, wichtig ist dabei als intended purpose Client und ServerAuthentication anklicken.

Das Certifcate SnapIn ist verfügbar, wenn der Server Certification Authority ist (das legt man bei den Serverrollen fest ) oder man aktiviert es mittels mmc -> „snapin hinzufügen“ (das geht bei jedem Windows nicht nur bei den Serverversionen). Er ist dann natürlich keine allgemein gültige Authority, sondern nur lokal bzw in der Domäne und erzeugt sogenannte selbst signierte, root Zertifikate, die er selber ausstellt. Für LDAPs reicht das aber, wobei eine man in the middle attacke mit gefälscht eingeschleusten Zertifikaten dann trotzdem geht. Der Angreifer muss dann aber aus den eigenen Reihen kommen.

Testen kann man das dann mit einem einfachen vbs script in dem man den Port 636 (SSL) und SecureAuthetication beim Öffnen des LDAP Objektes verwendet (siehe Frage 1),oder es gibt dafür einfache freeware Test Tools, (ldp.exe ist bei den Windows Server Versionen sowieso dabei).

Unter linux gibt’s den Befehl ldapsearch mit allen möglichen Parametern

Erklären sie die wesentlichen Punkte der Abbildung im Beiblatt!

Wichtig ist vor allem, wo und wie findet man das?  
Was ist der Fingerabdruck?  
Was steht in den Details (der Public-key und die Signatur) ?

