VPN & Zertifikate

Maturavorbereitung

Simon Modl, 5AHIT

Inhaltsverzeichnis

Was ist VPN

- VPN … virtual private Network

- VPN bietet eine gesicherte Verbindung von verschiedenen Punkten zu einem Ziel an

Arbeitsweise

- Client verbindet sich auf VPN-Server
  - Dort authentifiziert er sich; Verbindungsaufbau nur bei erfolgreicher Authentifizierung
- Server ist nun für Verbindung/ Datenaustausch/ Kommunikation zuständig
- Server baut Tunnel zum Ziel auf → Start der Kommunikation

Arten von VPN

- Point to Point (Verbindung zwischen 2 Endgeräten)
- Point to Site (Einwählen in ein Firmennetzwerk)
- Site to Site (Zusammenschalten 2er Netzwerke)
- Intranet VPN (Absichern interner Netzbereiche)
- Extranet VPN (Business Room)

Typen von VPN

- OpenSource VPN
- Proprietäres VPN

Anbieter von VPN

- NordVPN
- Cisco
- Surfshark
- ExpressVPN
- FortyClient

Vergleich von VPN zu SSH

- SSH … Secure Shell
- Verschlüsselte Tunnelverbindung zum Ziel
- Nicht für Weiterleitung von Netzwerkverkehr konzepiert

Vergleich von VPN zu WebDAV

- Prinzipiell nicht gesichert
- Verbindung nur dann gesichert, wenn HTTPS genutzt wird
- Weitere Möglichkeiten
  - User-Authentifizierung
  - Rechtesetzung, Rollen und Gruppen
- WebDAV stellt nur Dateien (Download und Upload)
- Keine Kommunikation, weitere Dienste, etc. möglich

Vergleich von VPN zu FTP

- FTP ist ungesichert
- Gesicherte Versionen sind sFTP und FTPS
- Rein für Datenübertragung

OpenVPN

- Open-Source commercial Software für VPN
- Verwendet SSL/TLS für Schlüsselaustausch
- Mehrere Sicherheitsmechanismen zur Verfügung
- Für viele OS verfügbar

Prinzip von Zertifikaten

- Anfrage an eine Stelle
- Stelle prüft Angefragten (Zertifikatsprüfung beim CA)
- CA untersucht Zertifikat auf Richtigkeit
- Bei Erfolg wird Datei/Anfrage/… zugelassen

Zertifikat erhalten

- Wenn öffentliches Zertifikat
- Muss beantragt werden
- Offizielle Dokumente müssen eingereicht werden
- Stelle verteilt Zertifikat wenn Prüfung abgeschlossen

Zertifikat erstellen

- Zertifikat-Details definieren
- CA verifiziert und verschlüsselt mit privatem Schlüssel
- CA speichert Zertifikat und hängt eigene Signatur dazu

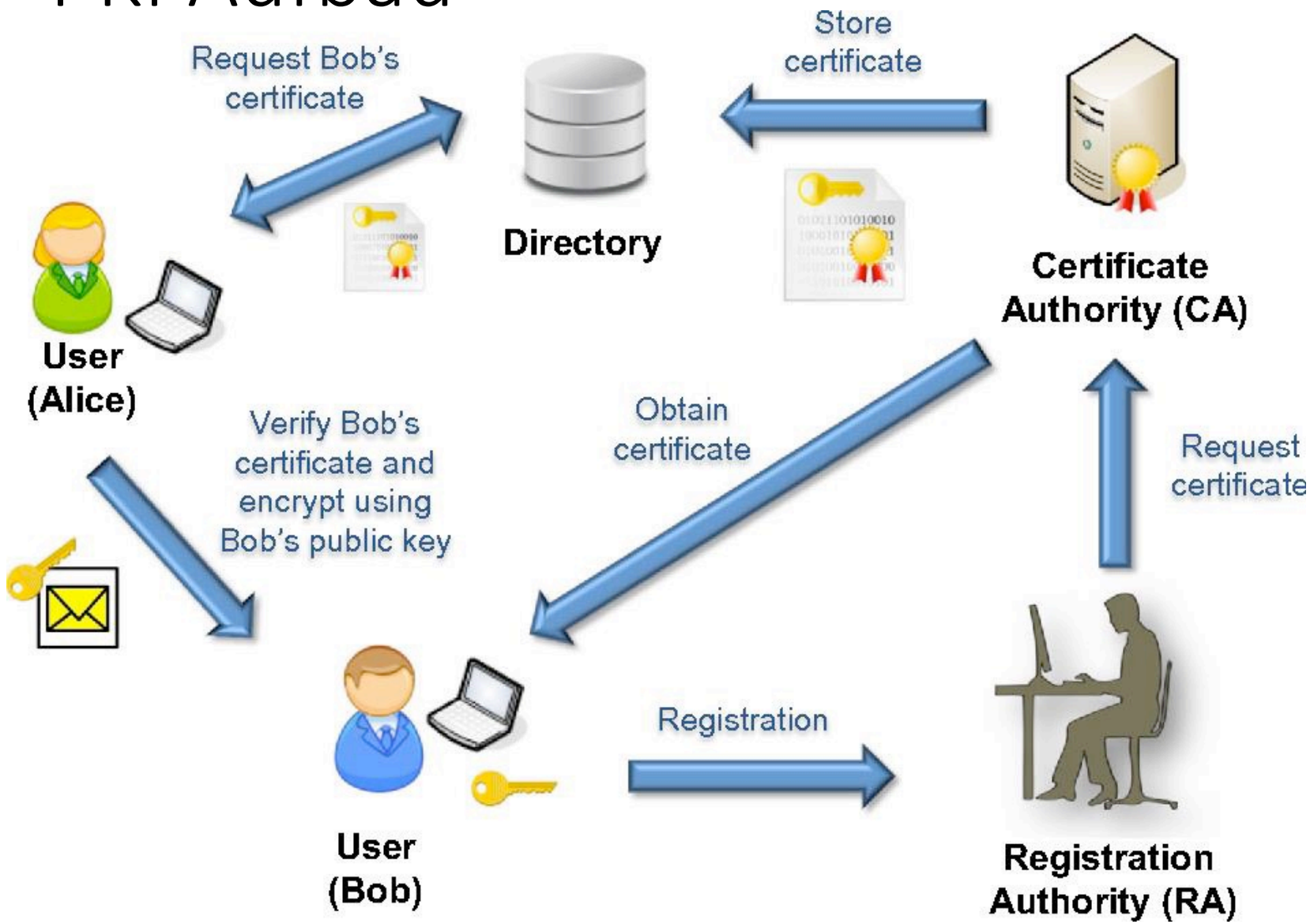
PKI Prinzip

- CA: Stelle, an welcher Zertifikate verwaltet werden
- RA: Stelle, an welcher man Zertifikate anmelden kann
- SSL Zertifikat: Behinhaltet Public Key und weitere Meta-Daten
- CMS: Verwaltet Zertifikate

Inhalt eines Zertifikats

- Erstell-Datum
- Verfahren
- Daten, wem das Zertifikat gehört
- Public Key
- Digitale Signatur des CA

PKI Aufbau


Request Bob's certificate
Store certificate
Directory
Certificate Authority (CA)
User (Alice)
Verify Bob's certificate and encrypt using Bob's public key
Obtain certificate
Request certificate
Registration
User (Bob)
Registration Authority (RA)