TeleTrusT-EBCA "PKI-Workshop" 2020

Berlin, 01.10.2020

"Private CA mit ACME Server und SSH-CA für die Absicherung von internen Systemen"

Kay Scholz, ANMATHO

Vorstellung

ANMATHO AG

Willkommen!

Kay Scholz

Systemadministrator @ ANMATHO AG

20 Jahre in der IT als

System / Netzwerk Administrator

Agenda

1. Vorstellung step-ca
2. Kernfunktionen
   - Zertifizierungsstelle
   - ACME 2.0 Unterstützung
   - SSH-CA
3. SSH
4. Nachteile

Fragen?

1. Vorstellung step-ca

- Open Source Projekt (Apache License, Version 2.0)
- Firma Smallstep
- Source Code einsehbar bei Github
- geschrieben in Go
- Zwei Komponenten
  - step-ca: Server
    - Verfügbar für Linux und MacOS
  - step: Kommandoclient (CLI-Tool)
    - Verfügbar für Linux, MacOS und Windows

2. Kernfunktion / Zertifizierungsstelle

Features (step-ca)

- Schnelle, einfache, flexible und stabile private Zertifizierungsstelle
  - Schlüsseltypen: RSA, ECDSA, EdDSA
  - Vorlagen pro Provisioner
  - OAUTH mit OpenID
  - Automatische Rollout, Erneuerung und passiver Wiederruf der Zertifikate
  - Datenbank Backends: Badger, BoltDB, MySql
  - Hochverfügbarkeit (HA) möglich
  - Zwischenzertifizierungsstelle bei einer vorhanden Stammzertifizierungsstelle fungieren

2. Kernfunktion / ACME 2. Unterstützung

- Komplete Unterstützung von ACMEv2 (RFC8555)
- Rollout der Zertifikate über jeden ACME-Client möglich
- Zertifikatslebensdauer einstellbar
- Lösung Let´s Encrypt vorgestellt

2. Kernfunktion / SSH-CA

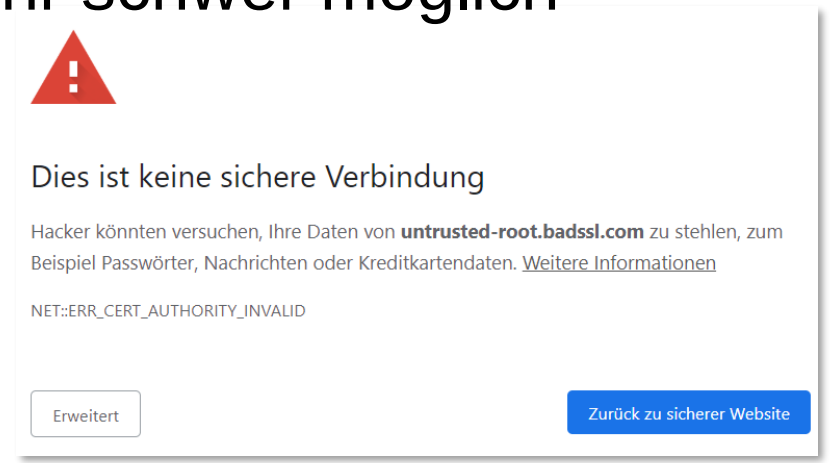
- Generiert SSH Benutzer- und Host- Schlüsselpaare
- Zertifikatslebensdauer einstellbar
- Hinzufügen und entfernen von Zertifikaten aus dem SSH-Agenten
- Überprüfen von SSH-Zertifikate
- Integration SSO für die einmalige Anmeldung per SSH

3. SSH

Probleme:

- Benutzerfreundlich, Bedienbarkeit und Sicherheit
- Betrieb von SSH in großen Maßstab ist eine Katastrophe
- SSH fördert schlechte Sicherheitspraktiken
- Neuinstallationen mit gleichen Hostname sehr schwer möglich (know_hosts)

```
$ ssh ubuntu@prod01
The authenticity of host prod01 can't be established.
ECDSA key fingerprint is SHA256:4Lih01wP5lW35gci0zcfh
Are you sure you want to continue connecting (yes/no)?
```



3. SSH

Lösungen:

- Zertifizierungsstelle-SSH
  - seit einen Jahrzehnt verfügbar (openSSH 5.4)
- Host können immer authentifizieren
  - TOFU-Warnungen verschwinden (Trust on first use)
- Auf allen Systemen ist nur noch ein Eintrag in der (know-hosts) nötigt
  - Global Know-Hosts: (@cert-authority *.example.com ecdsa-sha2-nistp25...)
- Keine statischen Schlüssel für „~/.ssh/authorized_keys“ bei Verwendung von OAUTHv2
  - Ein idealer SSH-Flow beim Identitätsanbieter Ihres Unternehmens (intern/extern)

4. Nachteile

- Putty / WinSCP / Filezilla (Windows)
  - Keine Unterstützung Cert-Keys
  - seit April 2016 auf der Wishlist
- Windows Integration schwieriger
  - Software-Deployment
  - Active Directory (LDAPS)
  - Exchange Server
  - IIS

Vielen Dank für Ihre Aufmerksamkeit!

Haben Sie Fragen?