SPNEGO-based Kerberos Authentication in SWITCH edu-ID

SWITCH edu-ID Team
eduid@switch.ch
01.12.2020

Inhalt

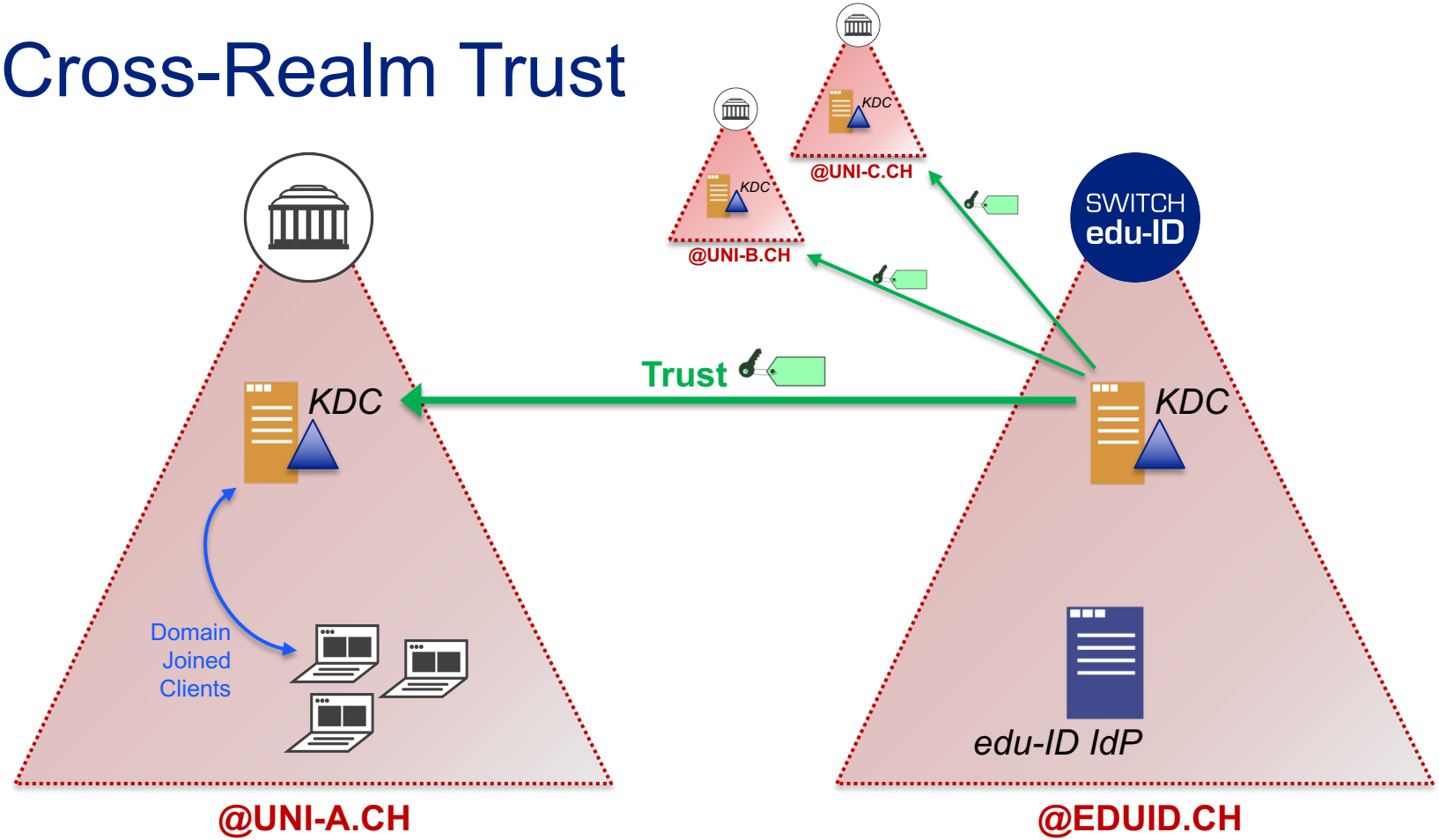
- Konzept
- Was muss eine Organisation bereitstellen und einrichten?
- Was muss SWITCH bereitstellen und einrichten?

Konzept

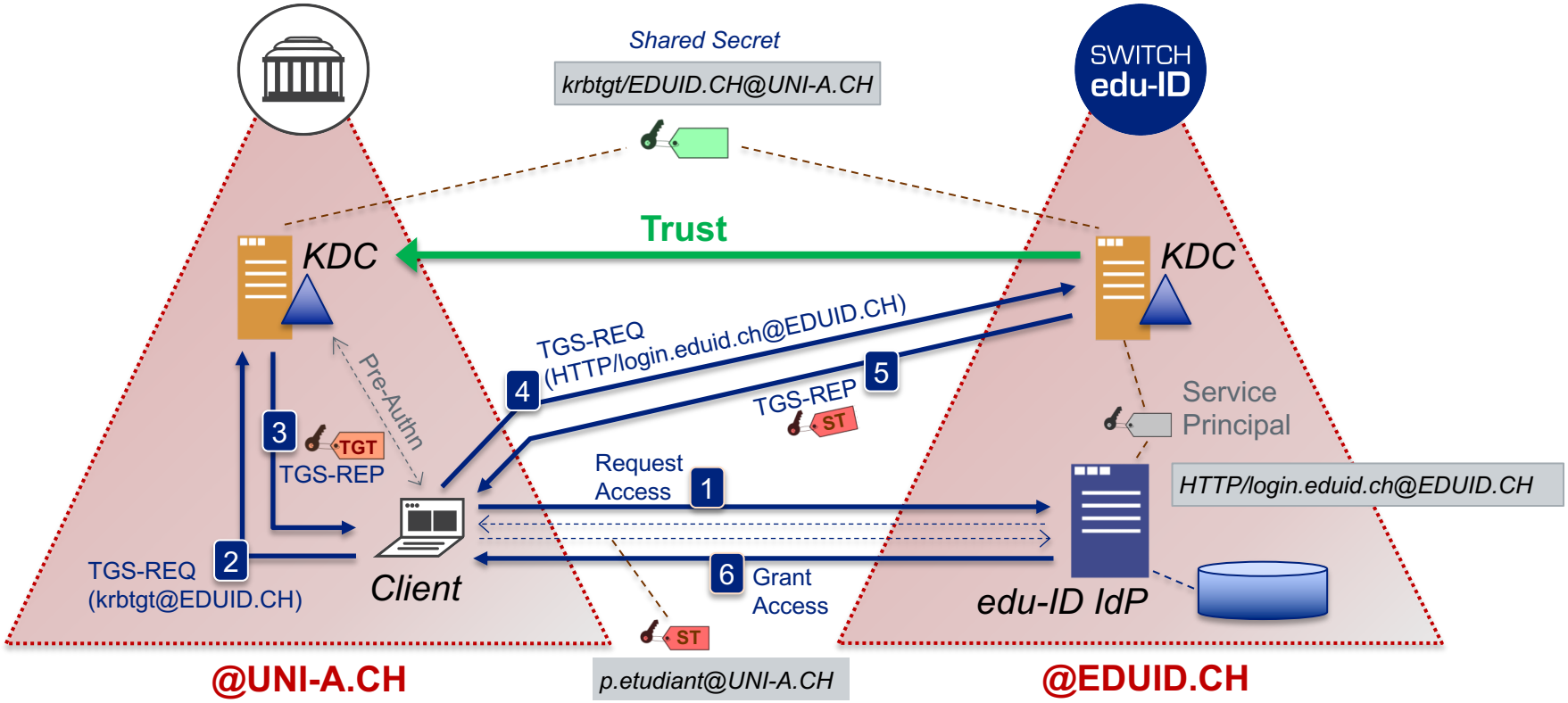
Key Feature: Kerberos Cross-Realm Authentication

- edu-ID betreibt eigenen Kerberos KDC Service
  Realm: @EDUID.CH
- edu-ID Realm vertraut den Realms der Organisationen zur Authentisierung von Benutzern (einseitiges Vertrauen reicht aus)
- Anbindung mehrerer Organisationen möglich

Cross-Realm Trust



Cross-Realm Authentication



Cross-Realm Authentication

1. **Der Benutzer (Client) gelangt während eines edu-ID Logins auf den edu-ID IdP.**
   Der IdP bietet SPNEGO an (Activation Condition ist erfüllt).
2. **Der Client fordert beim eigenen Windows KDC *(@UNI-A.CH)* ein *Ticket Granting Ticket (TGT)* an, damit er beim edu-ID KDC *(@EDUID.CH)* ein *Service Ticket (ST)* für den IdP beziehen kann.**
   Der Client muss entsprechend konfiguriert sein, z. B. via GPO.
3. **Der Windows KDC liefert das gewünschte *TGT* Ticket zurück.**
   Die für den edu-ID KDC bestimmten Daten im Ticket sind für diesen verschlüsselt (mit Shared Secret).

Cross-Realm Authentication

4. **Der Client fordert mittels *TGT* beim edu-ID KDC *(@EDUID.CH)* ein *Service Ticket (ST)* für den Zugriff auf den IdP (https://login.eduid.ch) an.**
5. **Der edu-ID KDC *(@EDUID.CH)* liefert das gewünschte *ST* Ticket zurück, da er dem Windows KDC vertraut (*Cross-Domain Trust*).**
   Die für den IdP bestimmten Daten im ST Ticket sind für diesen verschlüsselt (mit Service Principal Password).
6. **Der IdP gewährt Zugriff, da er das Service Ticket erfolgreich entschlüsseln und validieren kann.**
   Er erhält die Identität des Benutzers (Kerberos Principal Name), zum Beispiel p.etudiant@UNI-A.CH.

Was muss eine Organisation tun?

- **Für alle edu-ID Affiliationen bzw. AD-Konten, für die SPNEGO verfügbar sein soll: Synchronisation vom Kerberos Principal Name *<sAMAccountName>@<DOMAIN>* zur edu-ID (via „Push“ oder „Pull“)**
  Vorgesehenes edu-ID Attribut: *extKerberosPrincipalName*
- **Konfiguration Trust mit edu-ID Kerberos Realm *(Shared Secret)***
- **Konfiguration edu-ID Kerberos Realm für Clients via GPO**
- **Konfiguration der Browser auf Clients, für die SPNEGO verfügbar sein soll**
- **Spezifikation *Activation Condition* (z. B. Identifier in User Agent String, IP-Adress-Range, etc.)**

Was muss SWITCH tun?

- **Konfiguration Trust mit Kerberos Realm der Organisation *(Shared Secret)***
- **Aktivierung SPNEGO in IdP-Konfiguration für die Organisation (*Activation Condition*)**

SWITCH

Working for a better digital world