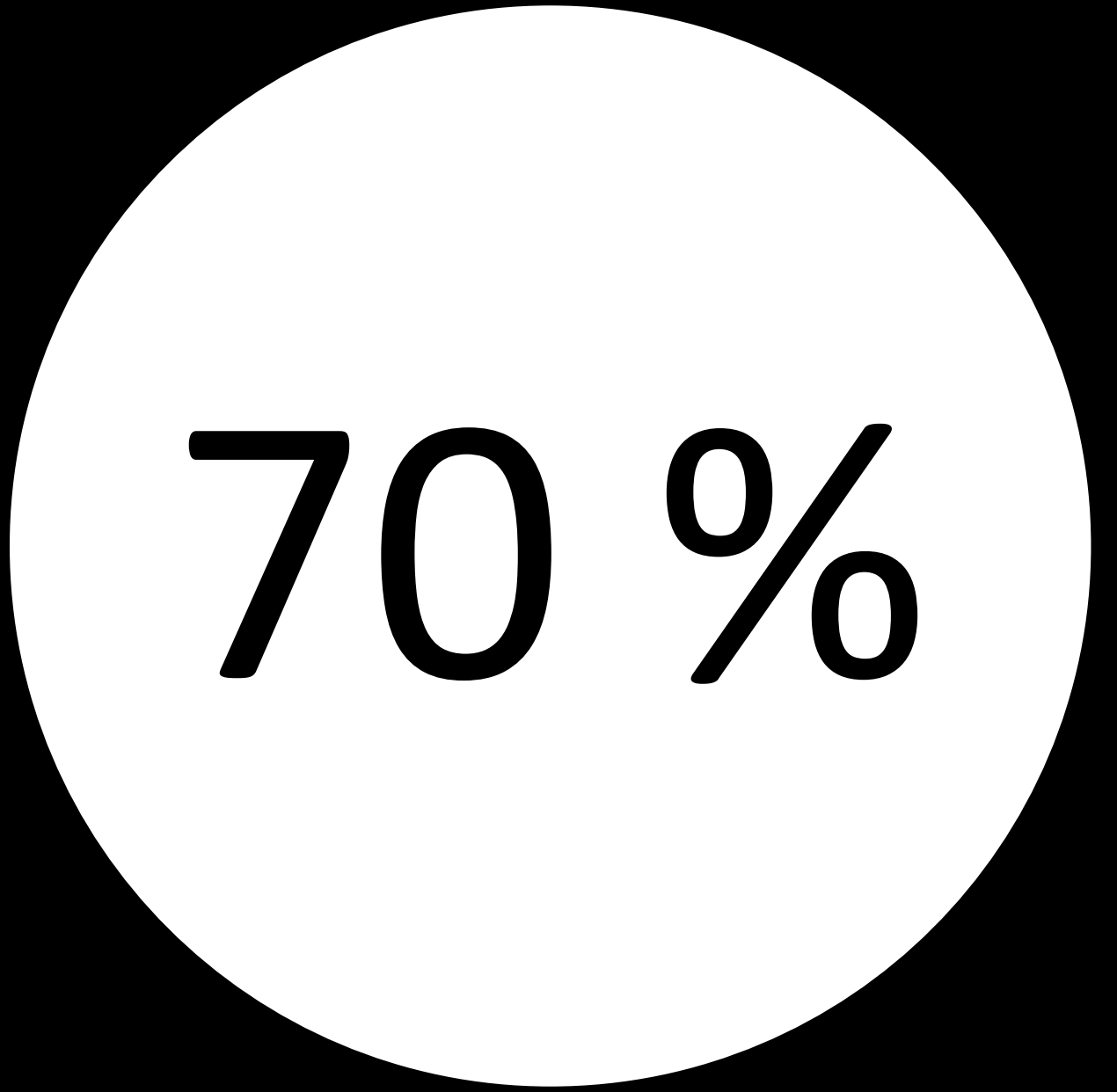
powered by Rachfahl IT-Solutions
CLOUD & DATACENTER CONFERENCE Germany

Design for Change:
Active Directory für das Cloud-Zeitalter

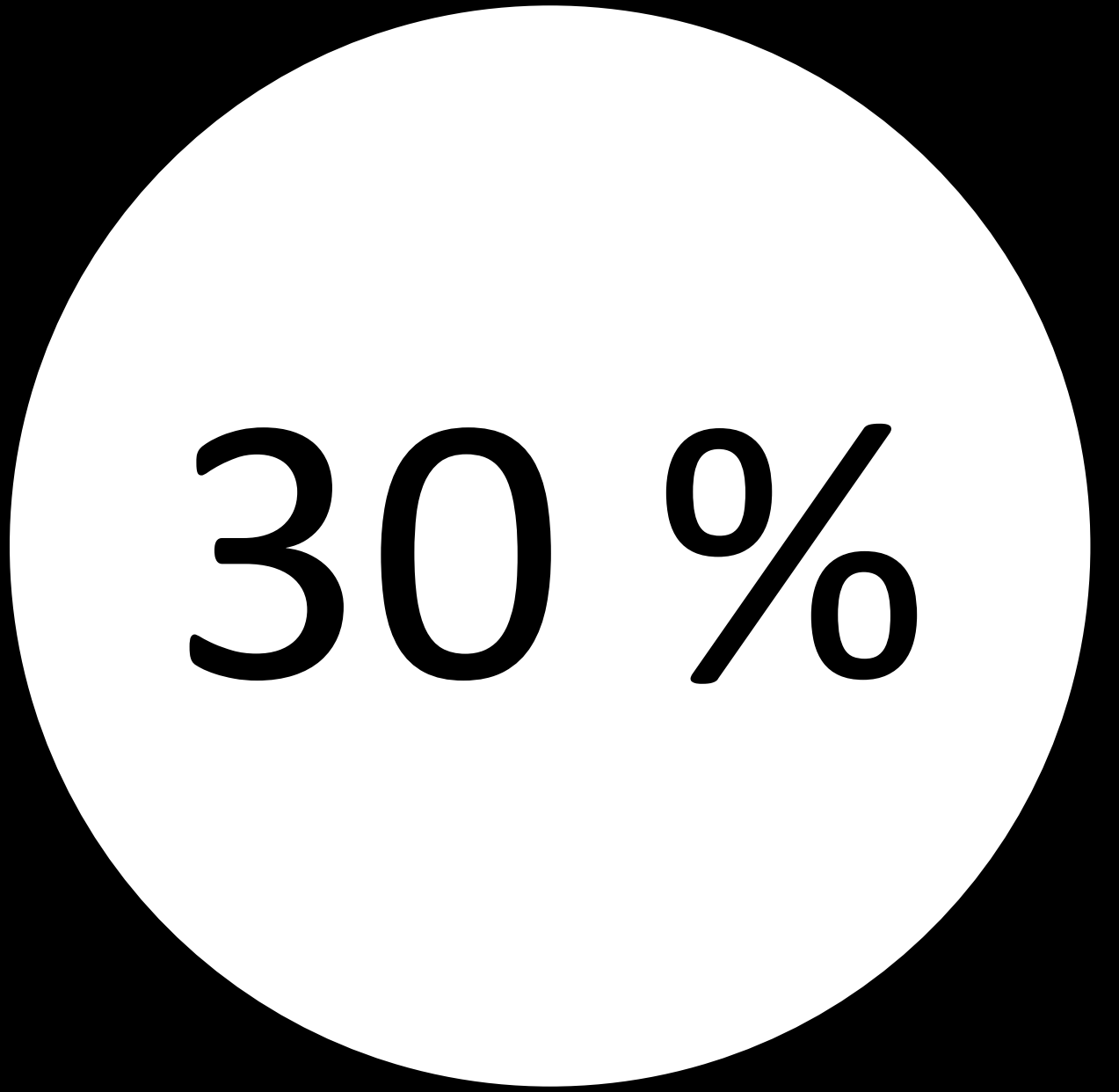
Nils Kaczenski


FaQ-o-maTiC.net
MVP
Microsoft®
Most Valuable
Professional

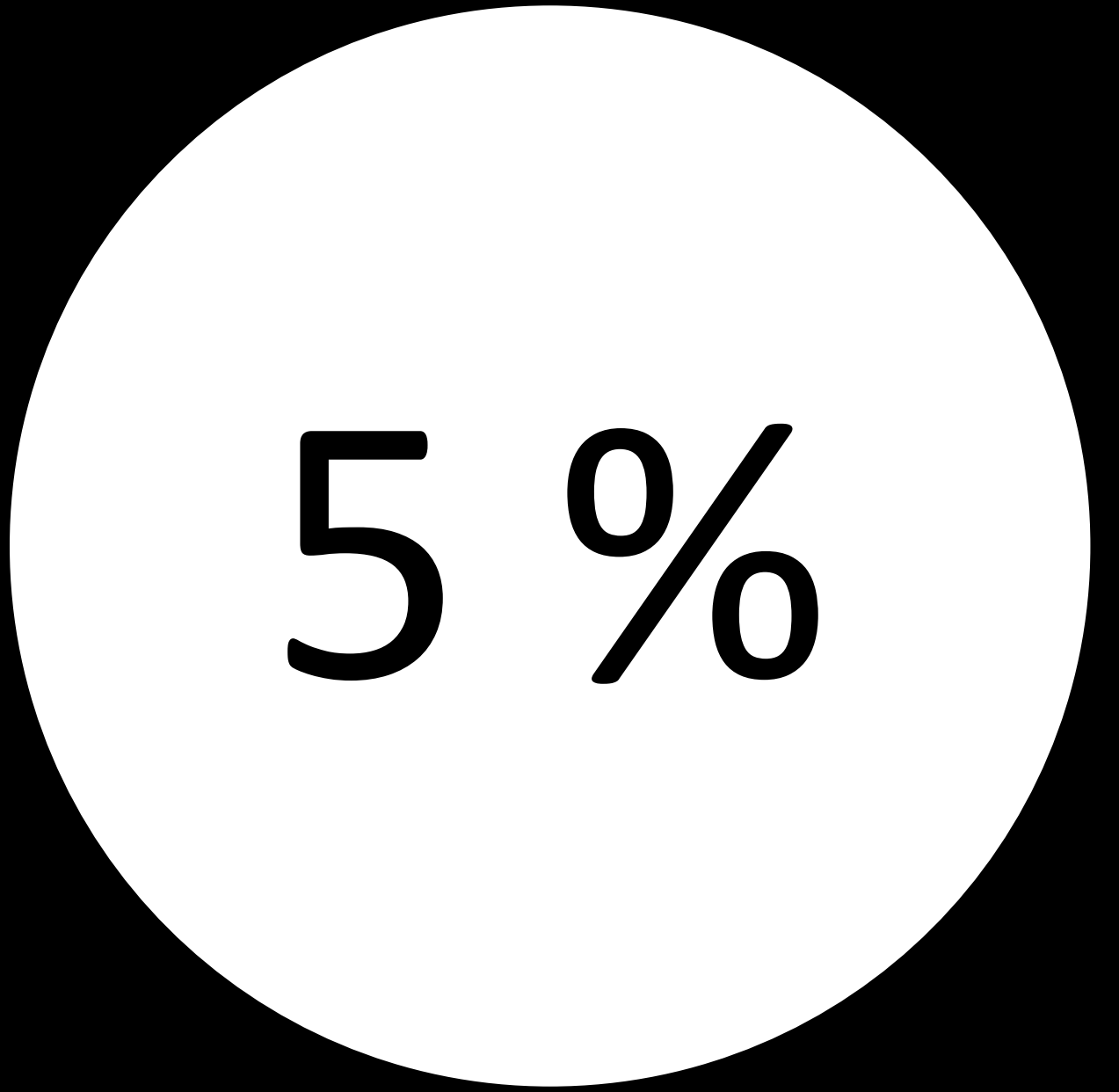
Kunden mit Interesse an „Cloud“



Kunden, die „Cloud“ produktiv nutzen



Kunden mit gutem AD-Design



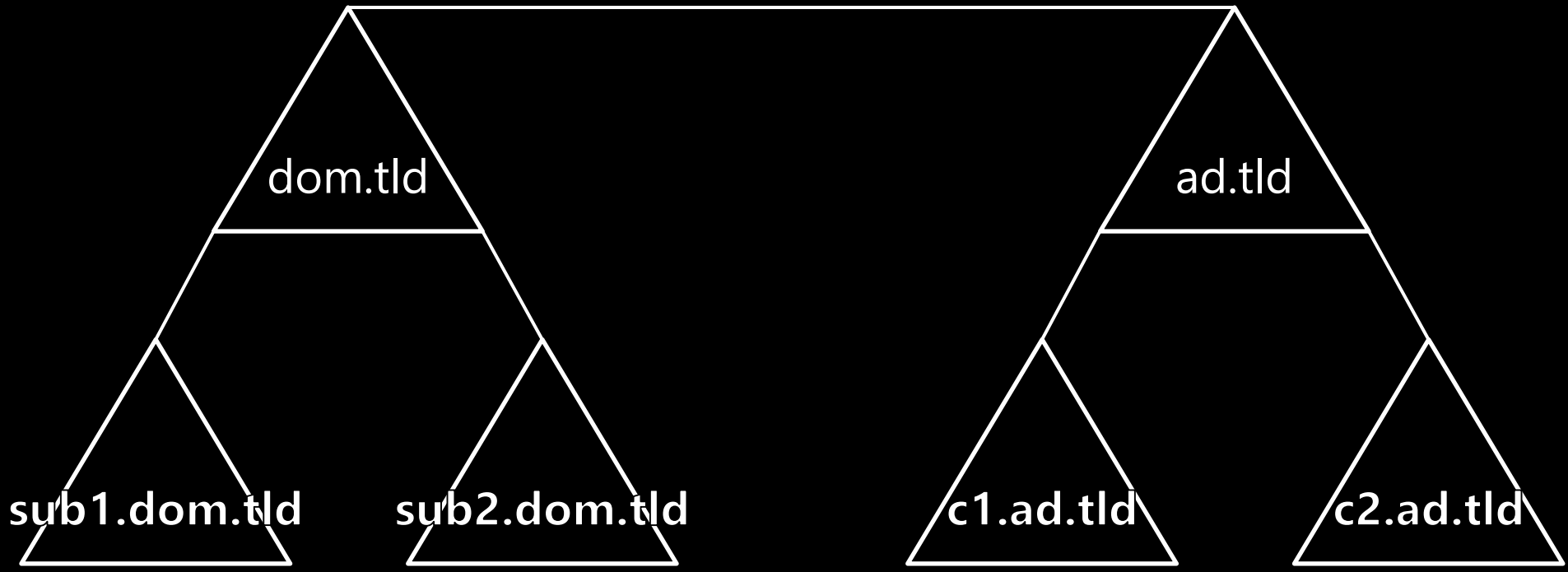
1

Design: Das Fundament für Identitäten

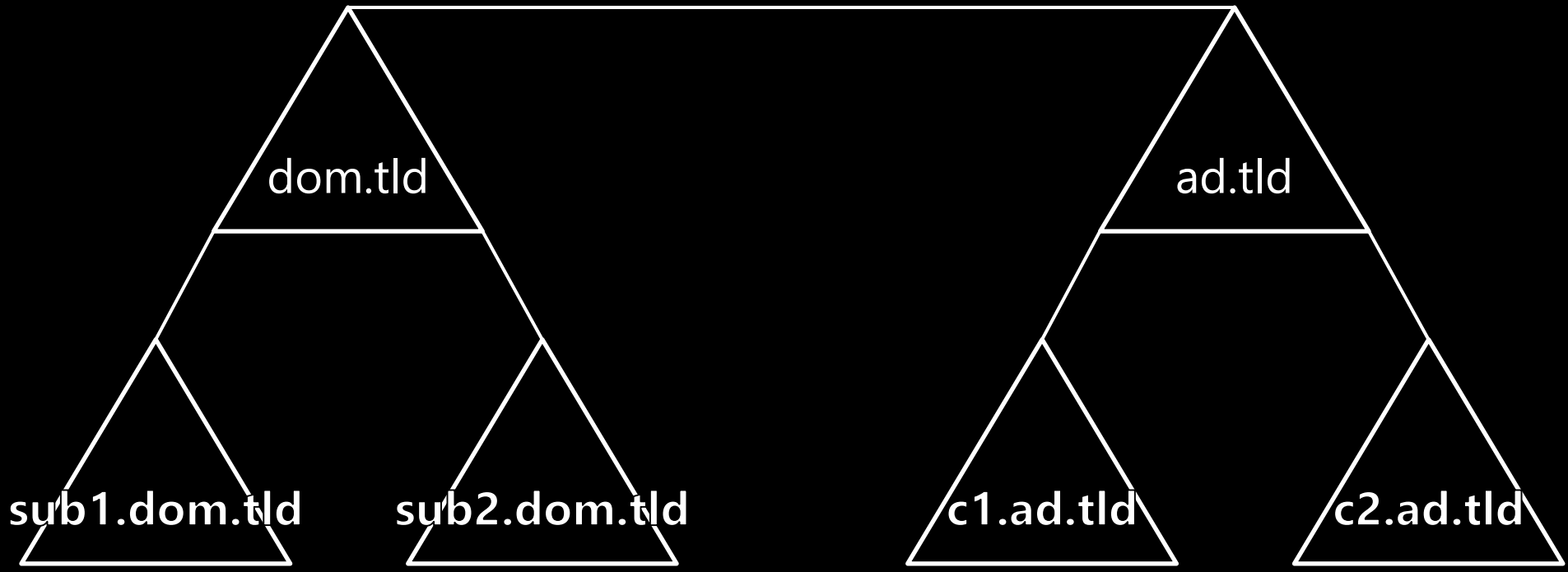
Name ist Schall und Rauch

abstrakt.org

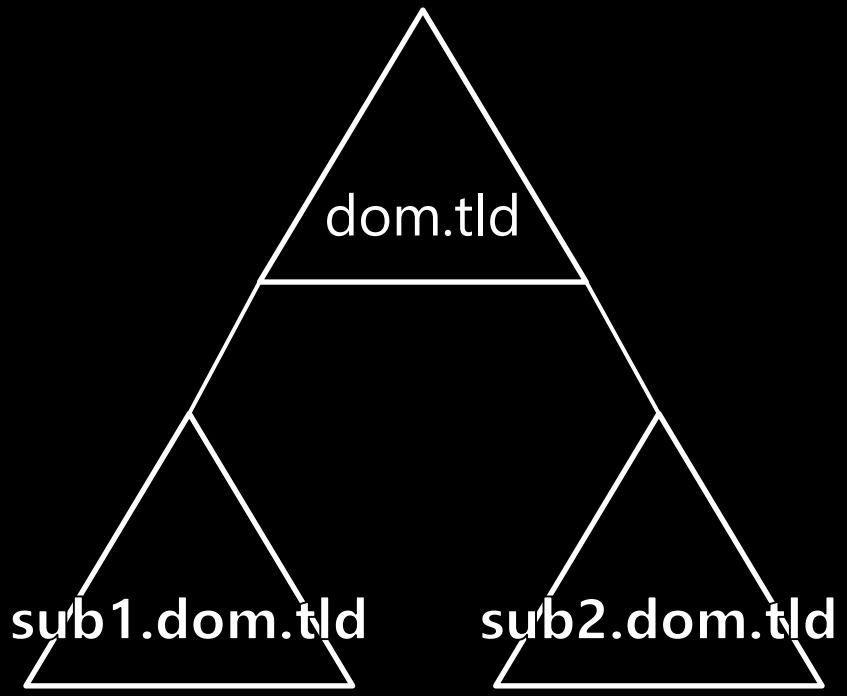
The Single Truth

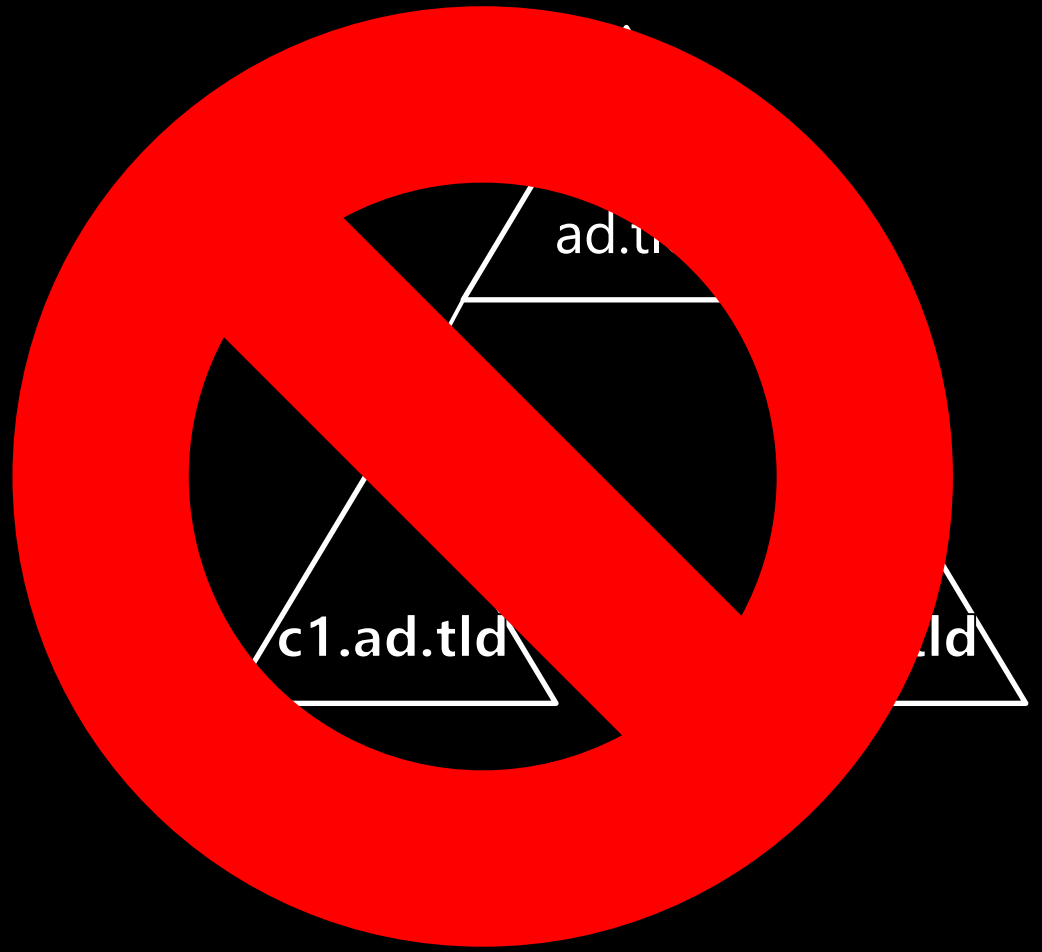


The Single Truth

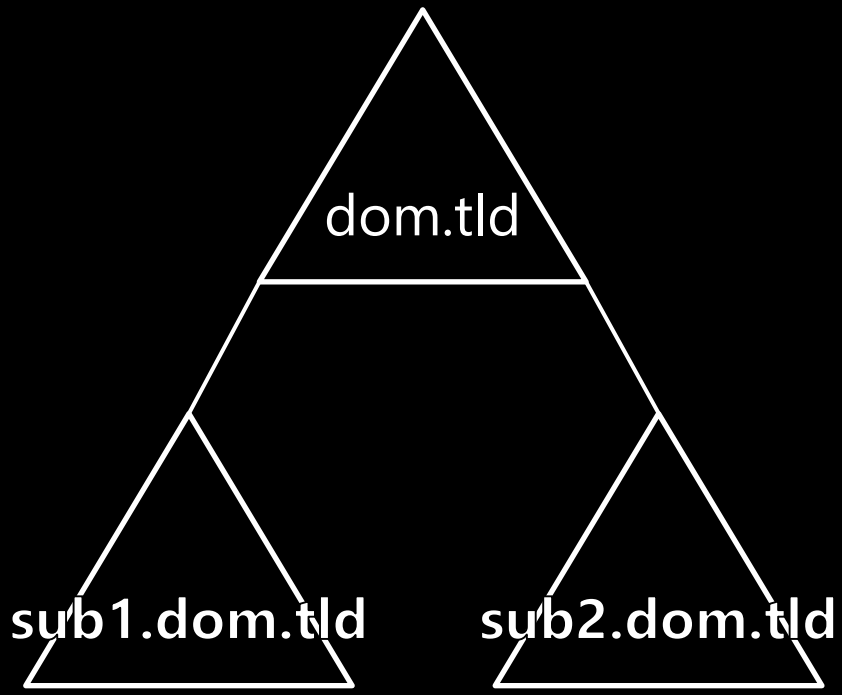


The Single Truth

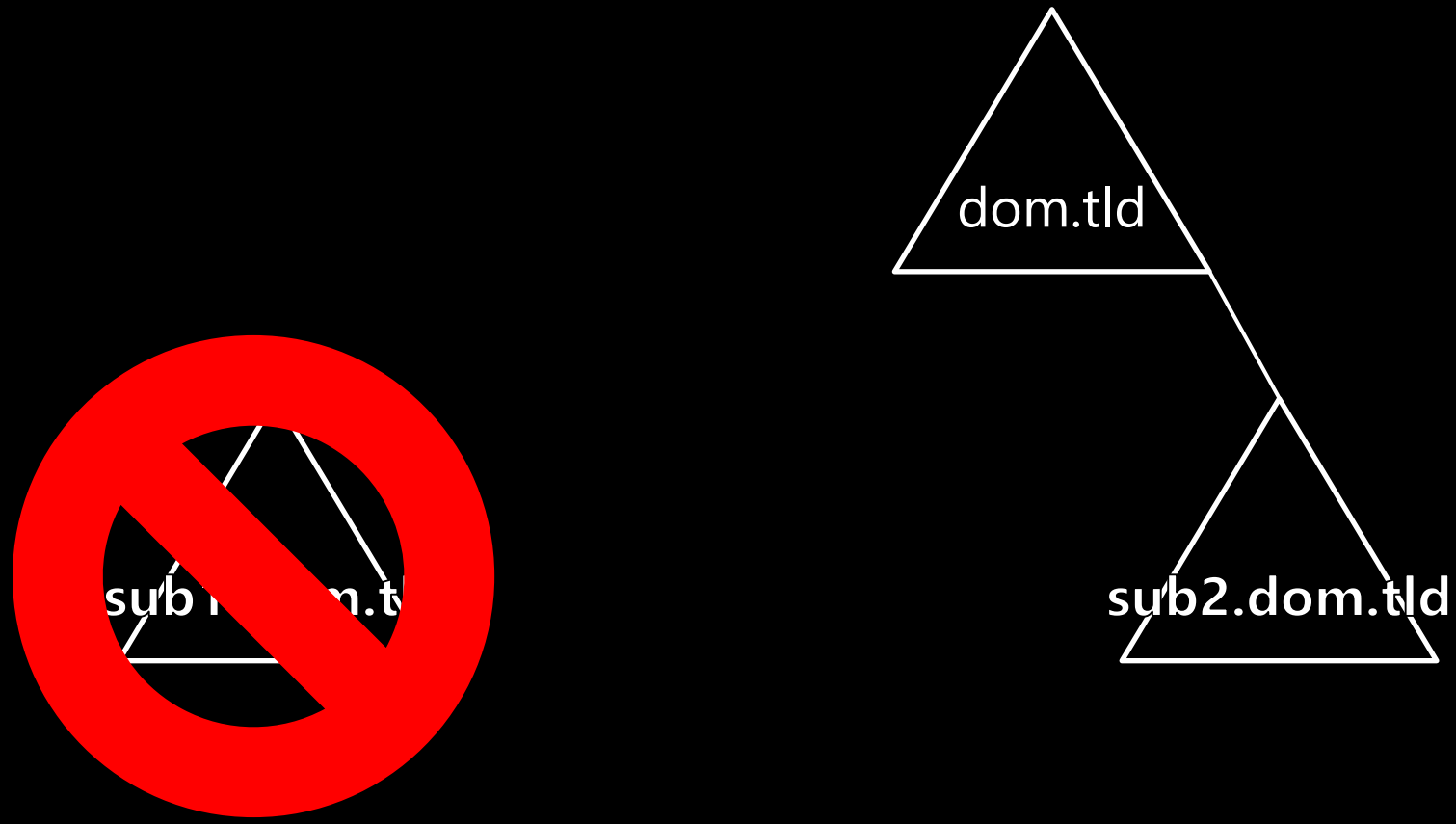




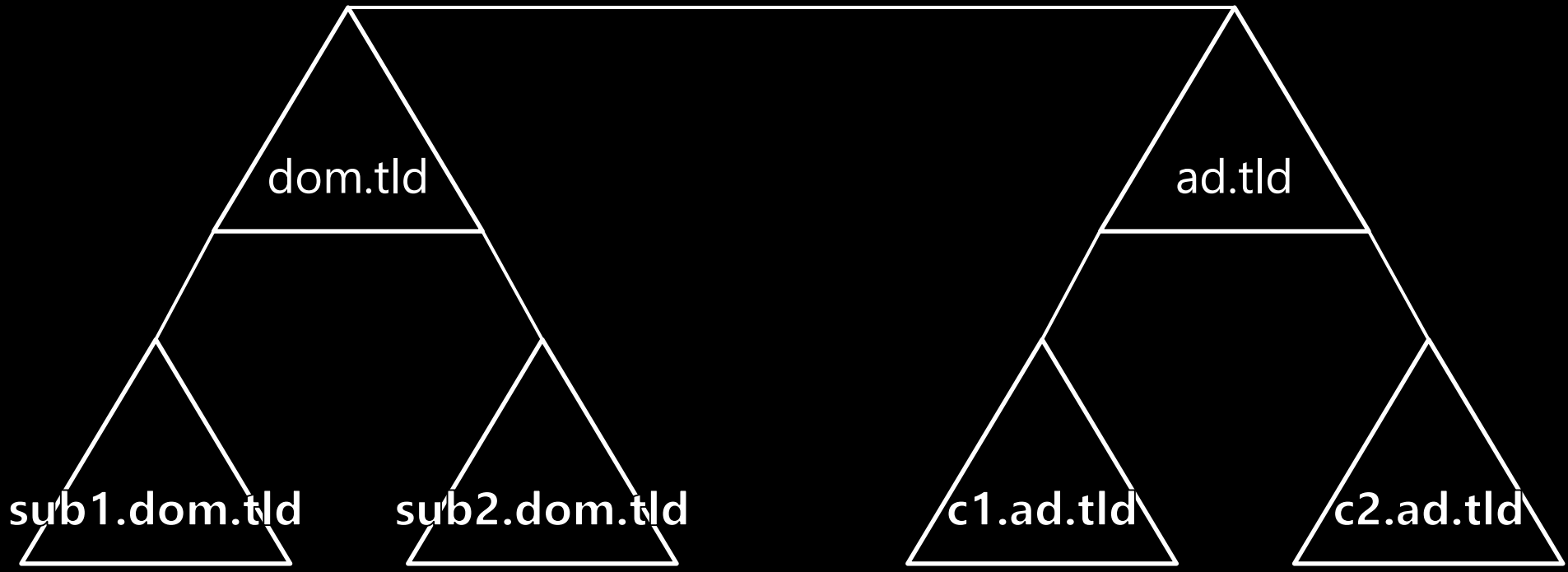
The Single Truth



The Single Truth

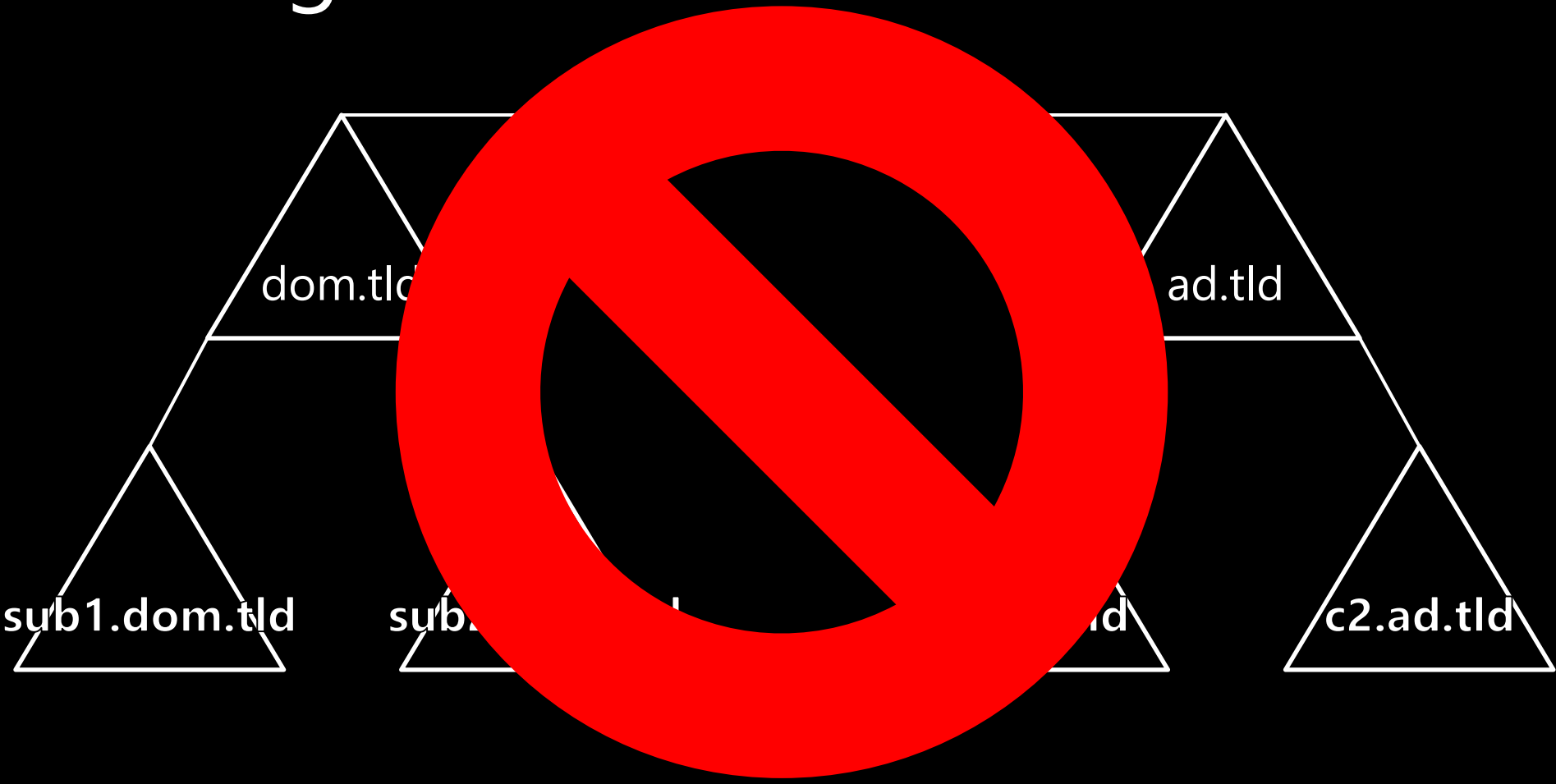


The Single Truth

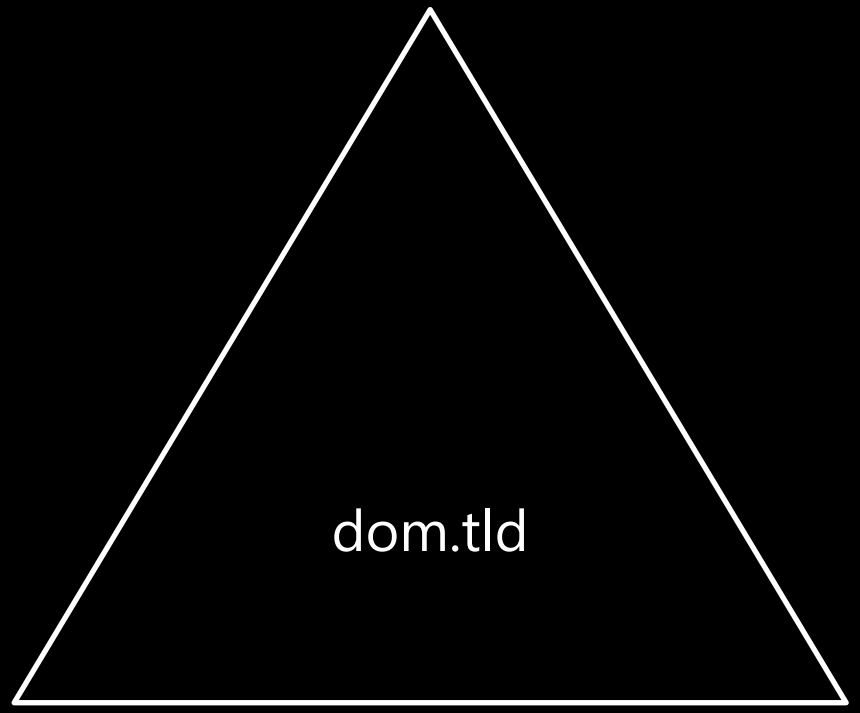


The Single Truth

The Single Truth



The Single Truth



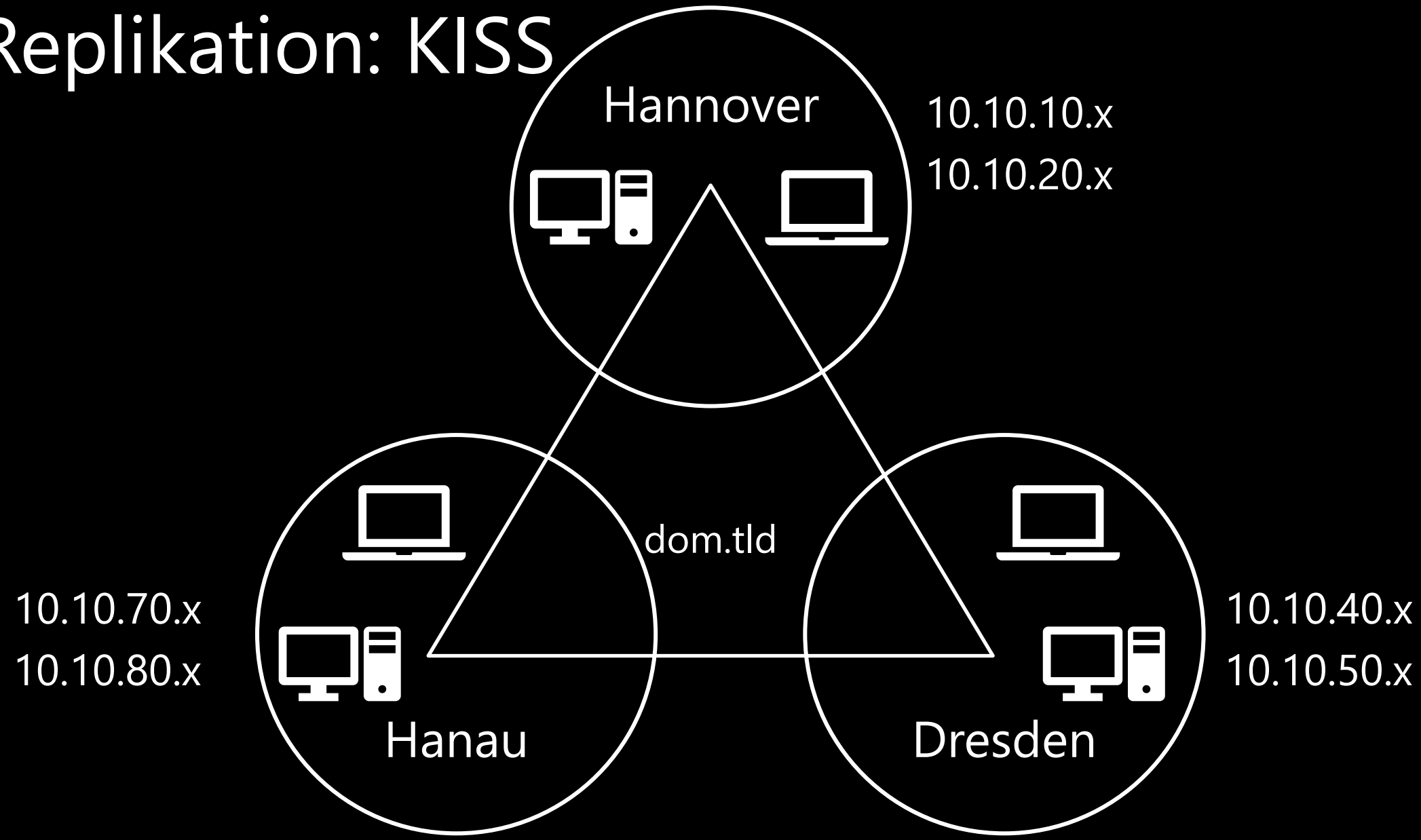
OU-Struktur ≠ Organigramm

- Administration
  - dezentral
  - zentral
- Service-Konten
  - dezentral
  - zentral
- Server
  - <Typ 1>
  - <Typ 2>
- Benutzer
  - <Typ 1>
  - <Typ 2>
- Gruppen
  - organisatorisch
  - Berechtigungen
- Clients
  - <Typ 1>
  - <Typ 2>

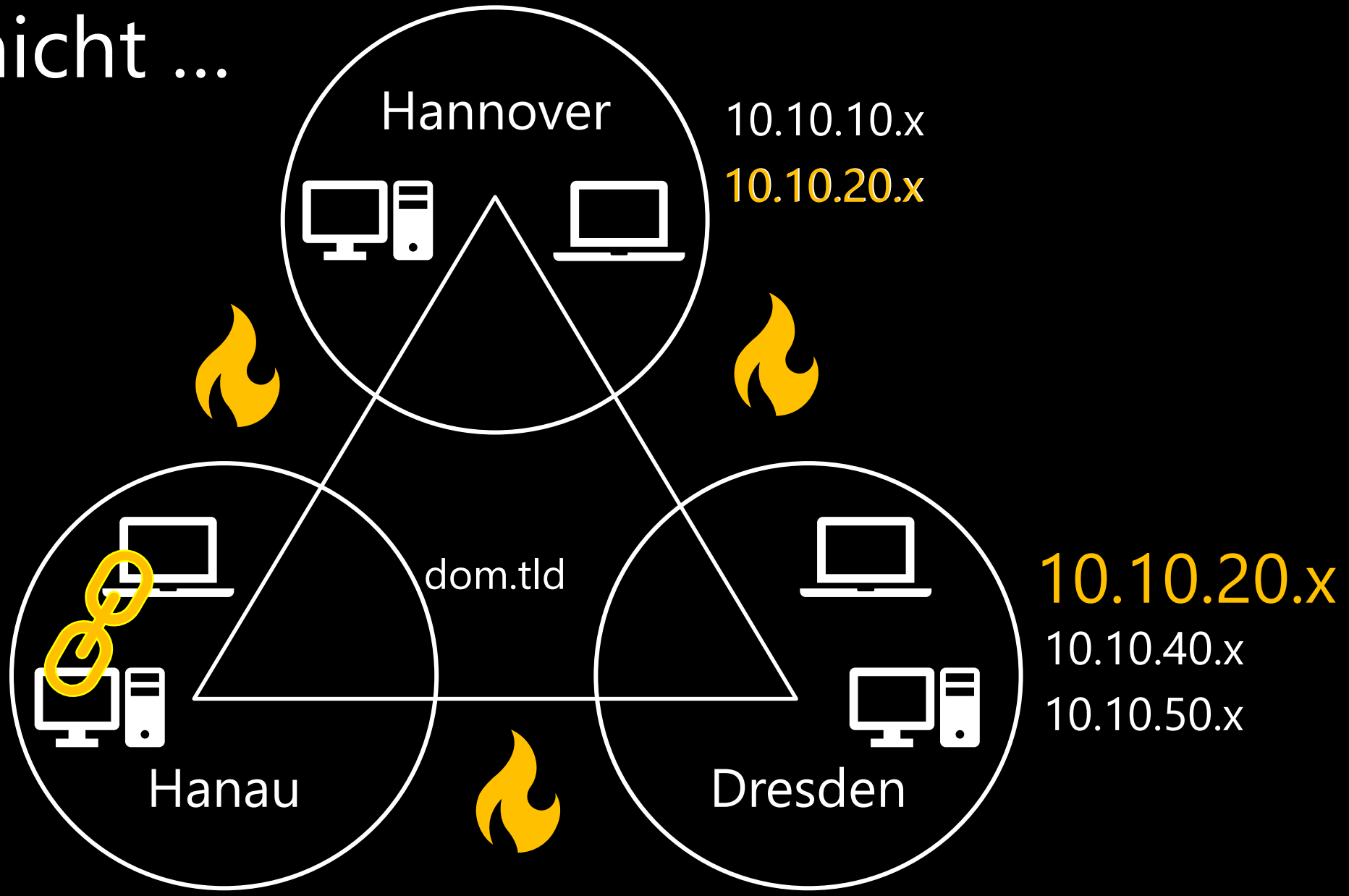
- Administration
  - dezentral
  - zentral
- Service-Konten
  - dezentral
  - zentral
- Server
  - <Typ 1>
  - <Typ 2>

- Benutzer
  - <Typ 1>
  - <Typ 2>
- Gruppen
  - organisatorisch
  - Berechtigungen
- Clients
  - <Typ 1>
  - <Typ 2>

Replikation: KISS



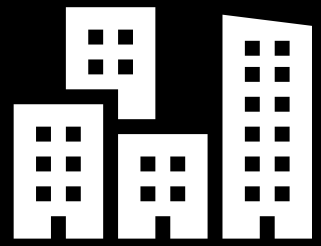
Lieber nicht …

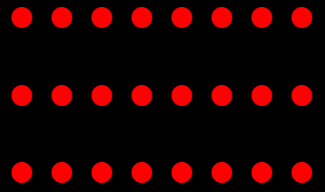


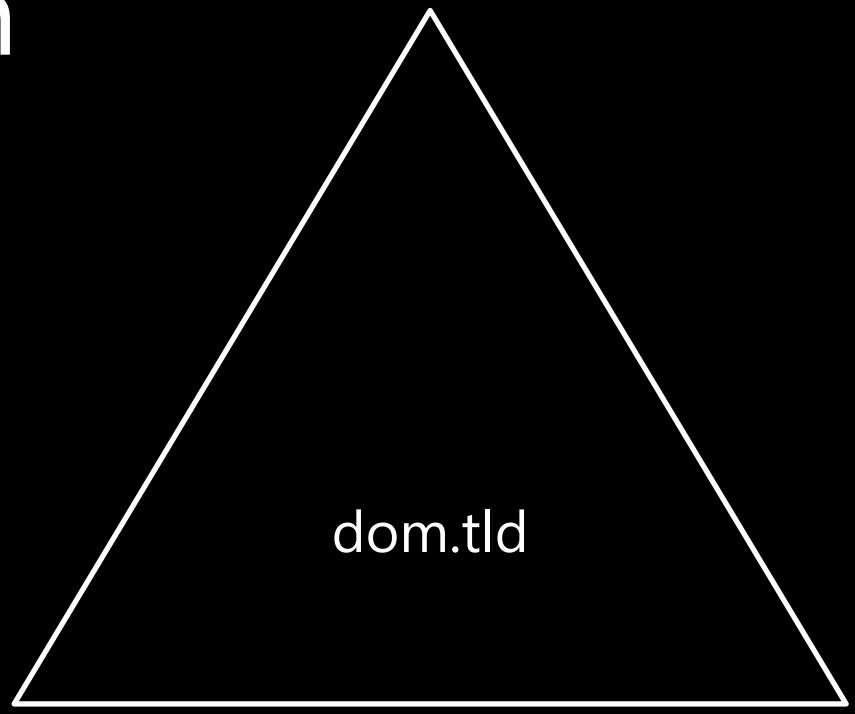
2

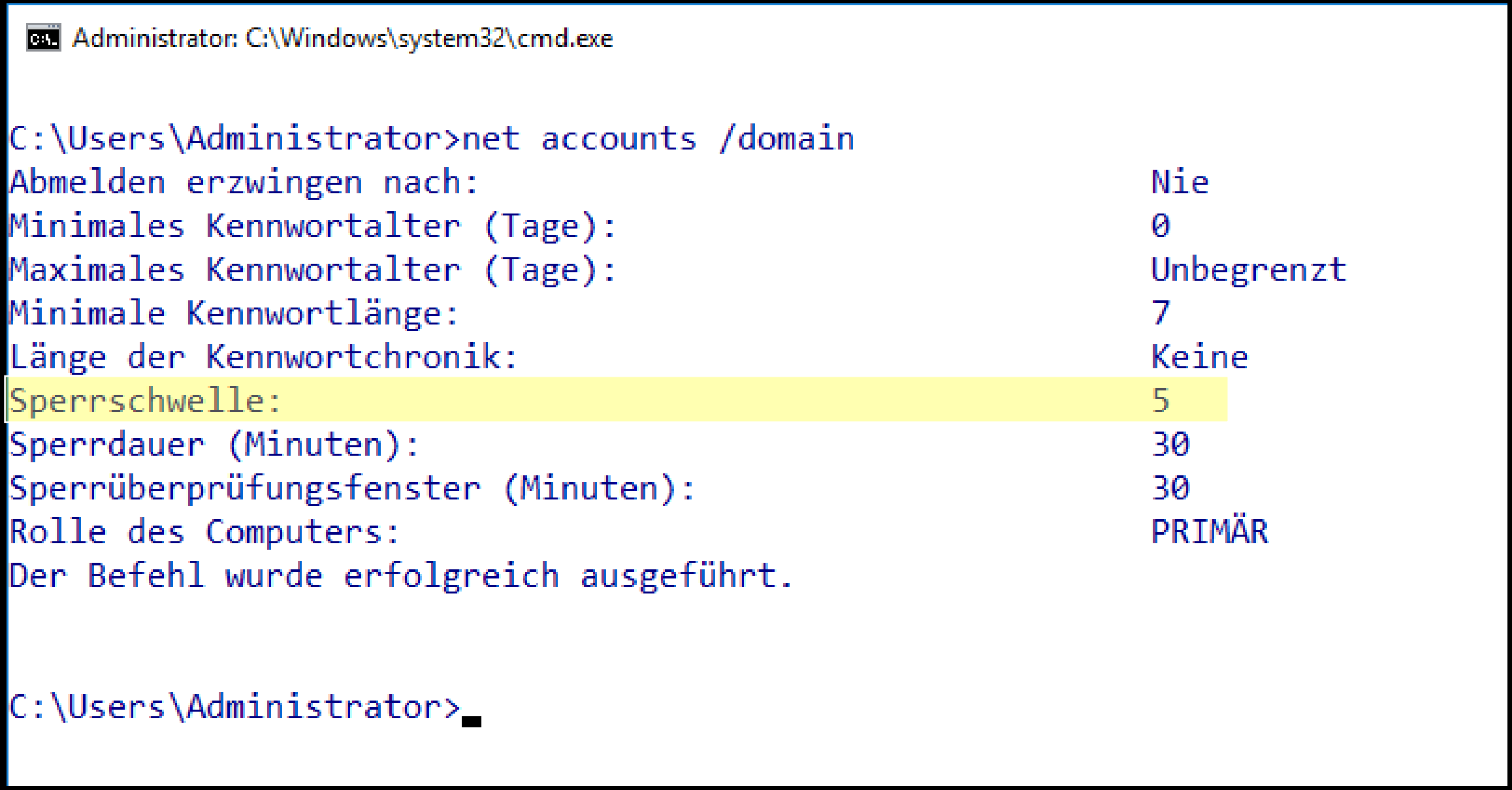
Sicherheit: Angriffe sind normal

Funktioniert seit 20 Jahren

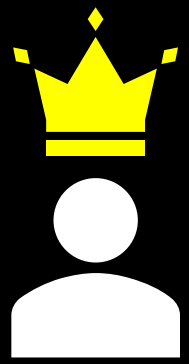




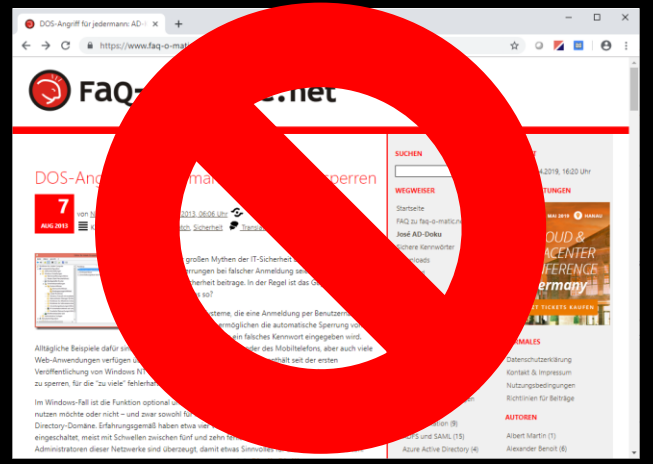



Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>net accounts /domain
Abmelden erzwingen nach: Nie
Minimales Kennwortalter (Tage): 0
Maximales Kennwortalter (Tage): Unbegrenzt
Minimale Kennwortlänge: 7
Länge der Kennwortchronik: Keine
Sperrschwelle: 5
Sperrdauer (Minuten): 30
Sperrüberprüfungsfenster (Minuten): 30
Rolle des Computers: PRIMÄR
Der Befehl wurde erfolgreich ausgeführt.
C:\Users\Administrator>

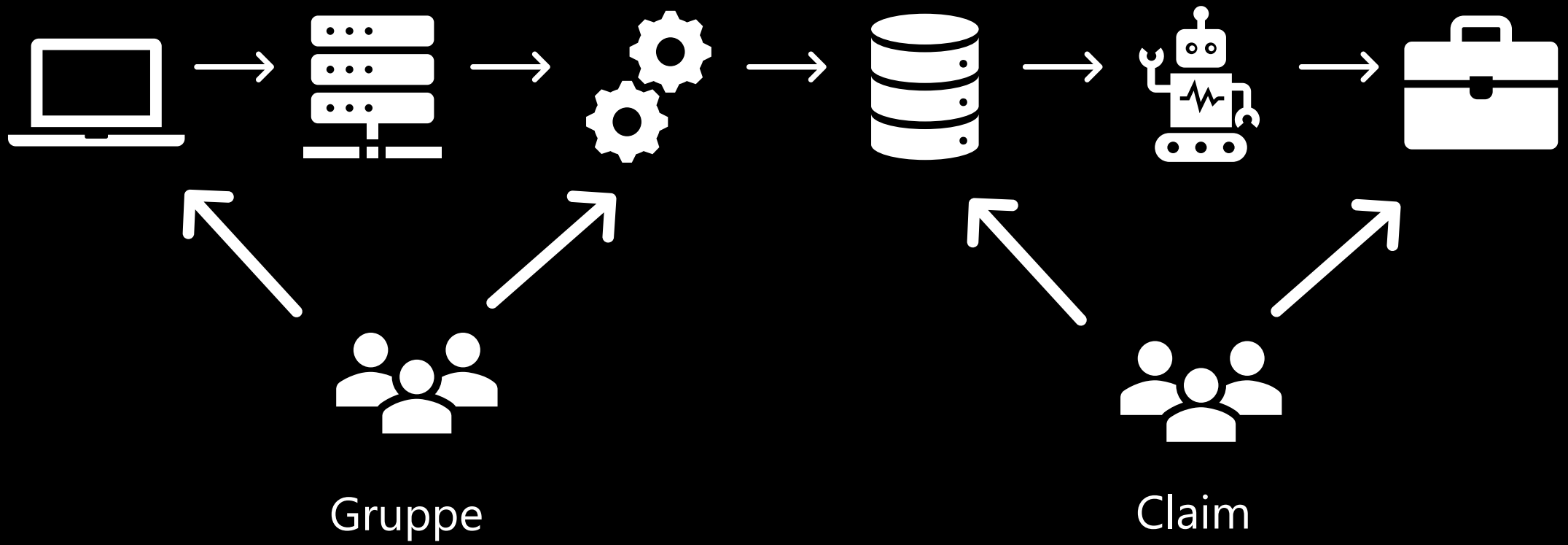
Rollen trennen



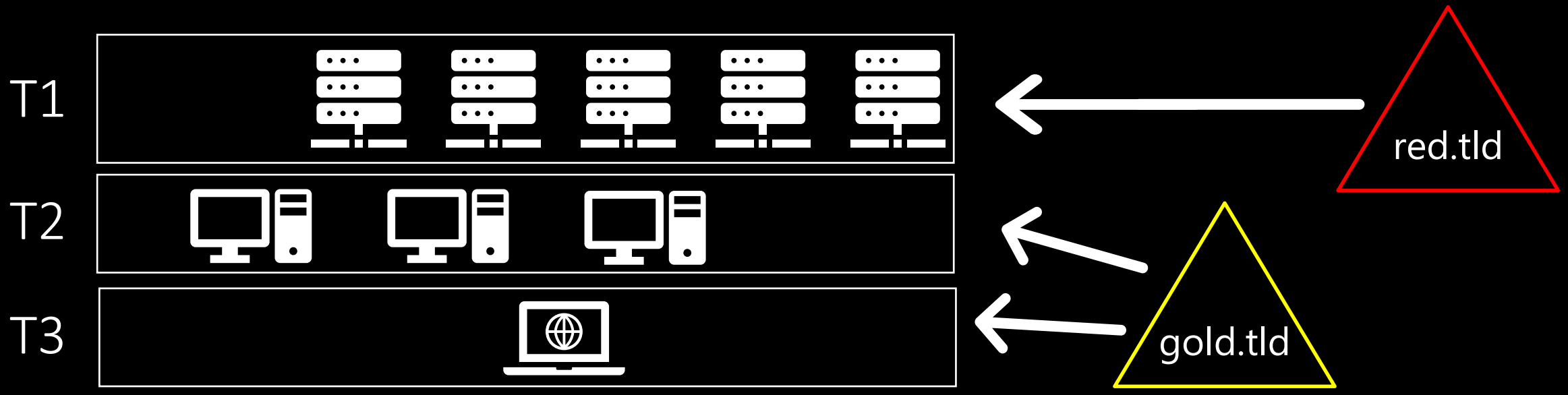
Rollen trennen



Rollen definieren



Admin Tiering: Rollen ernst gemeint



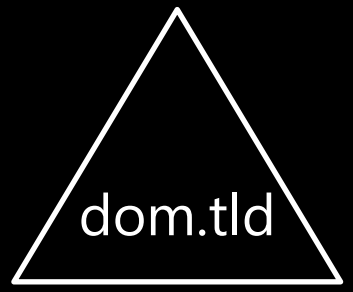
Suchbegriff: ESAE

3

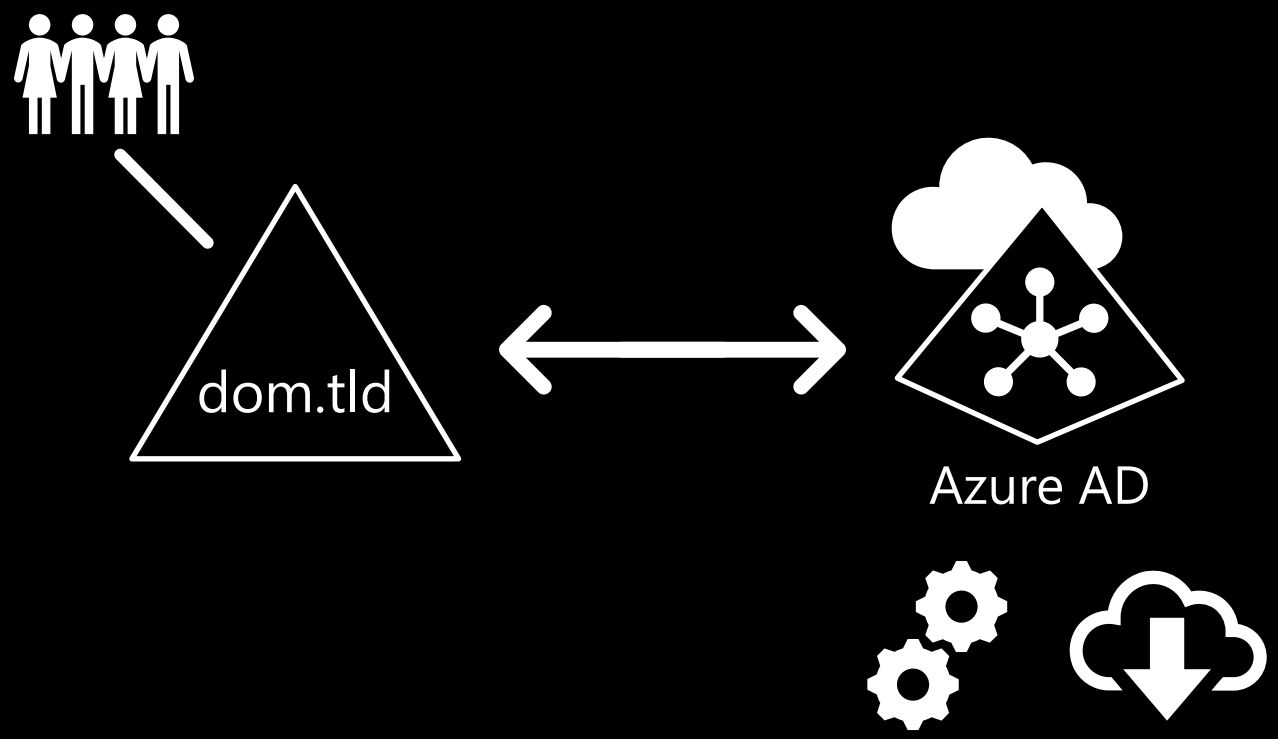
Hybrid-Design: Cloud und lokal

Identity is the new perimeter

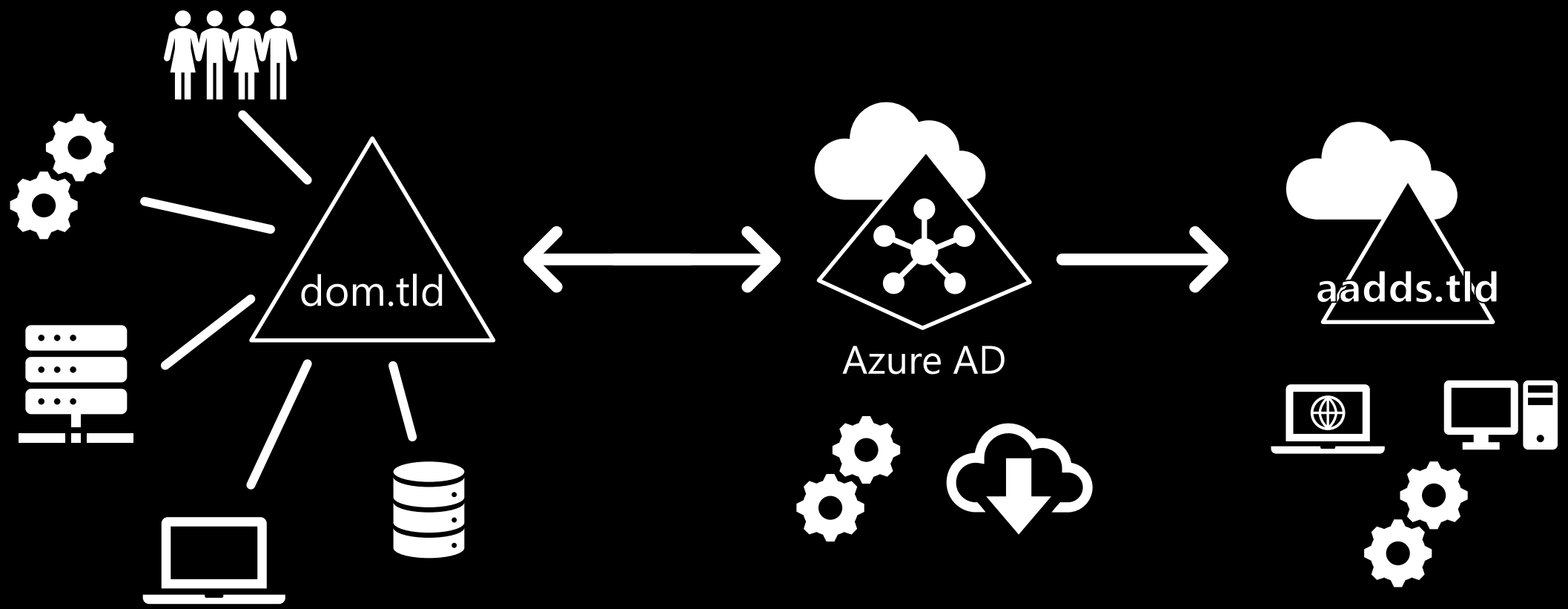
AD als lokaler Anker



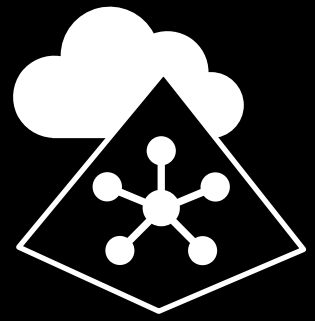
AD als lokaler Anker



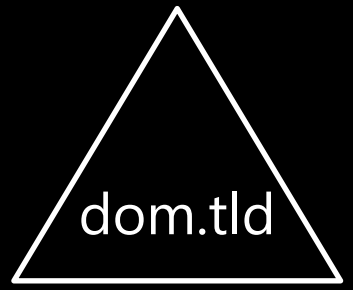
AD als lokaler Anker

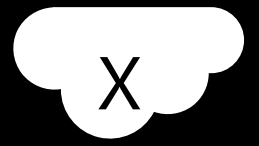


Federation

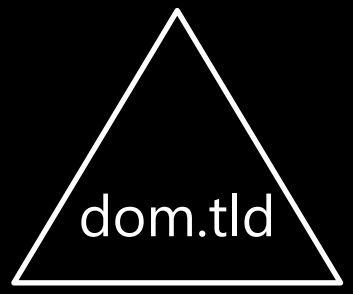


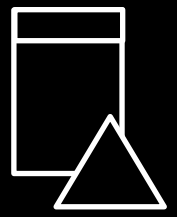
Azure AD

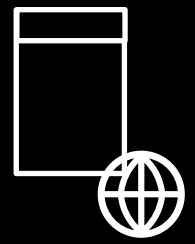




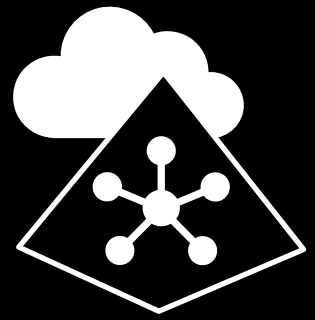
Federation





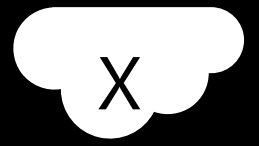


ADFS

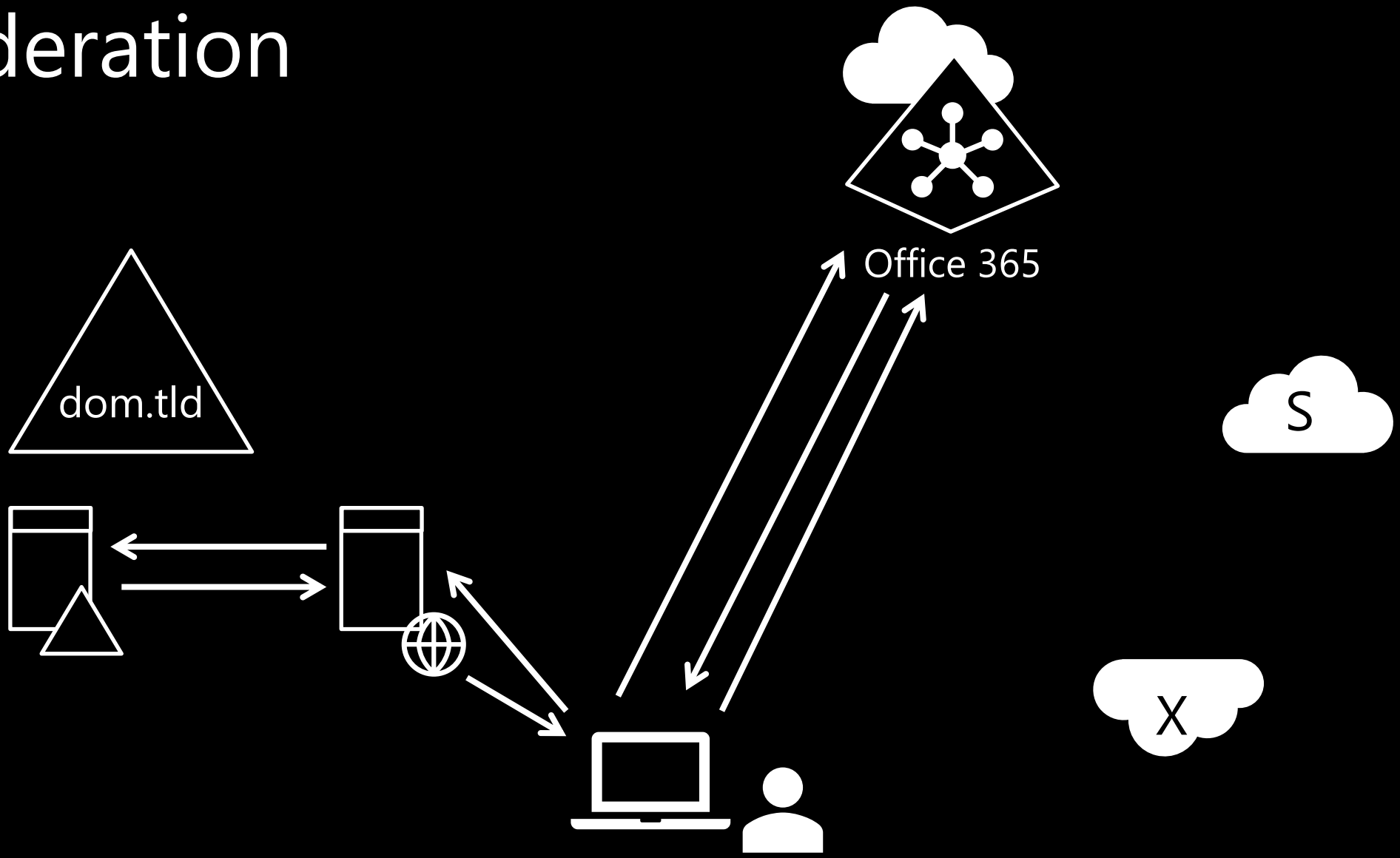


Azure AD

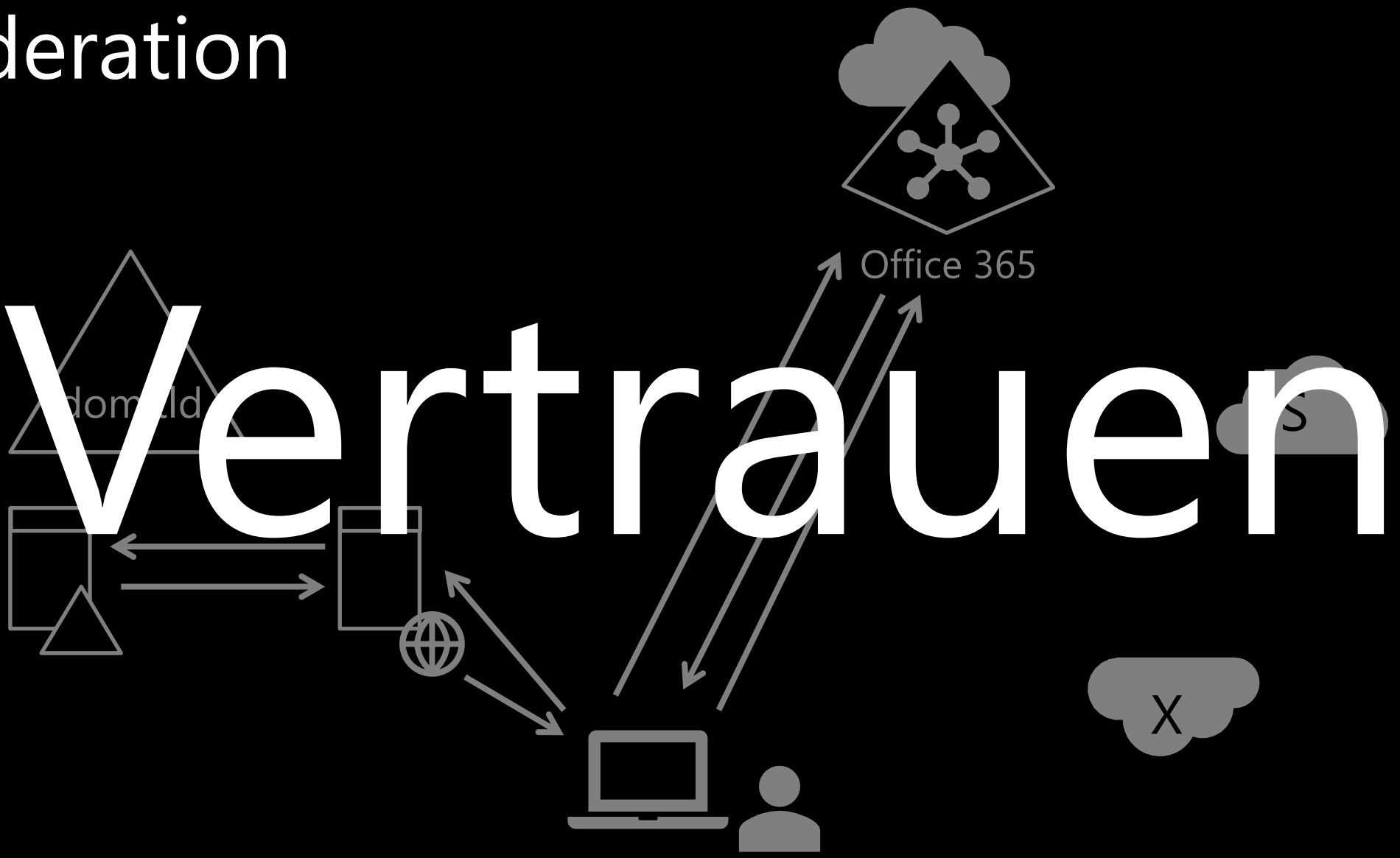
SAML
OAuth
OpenID



Federation

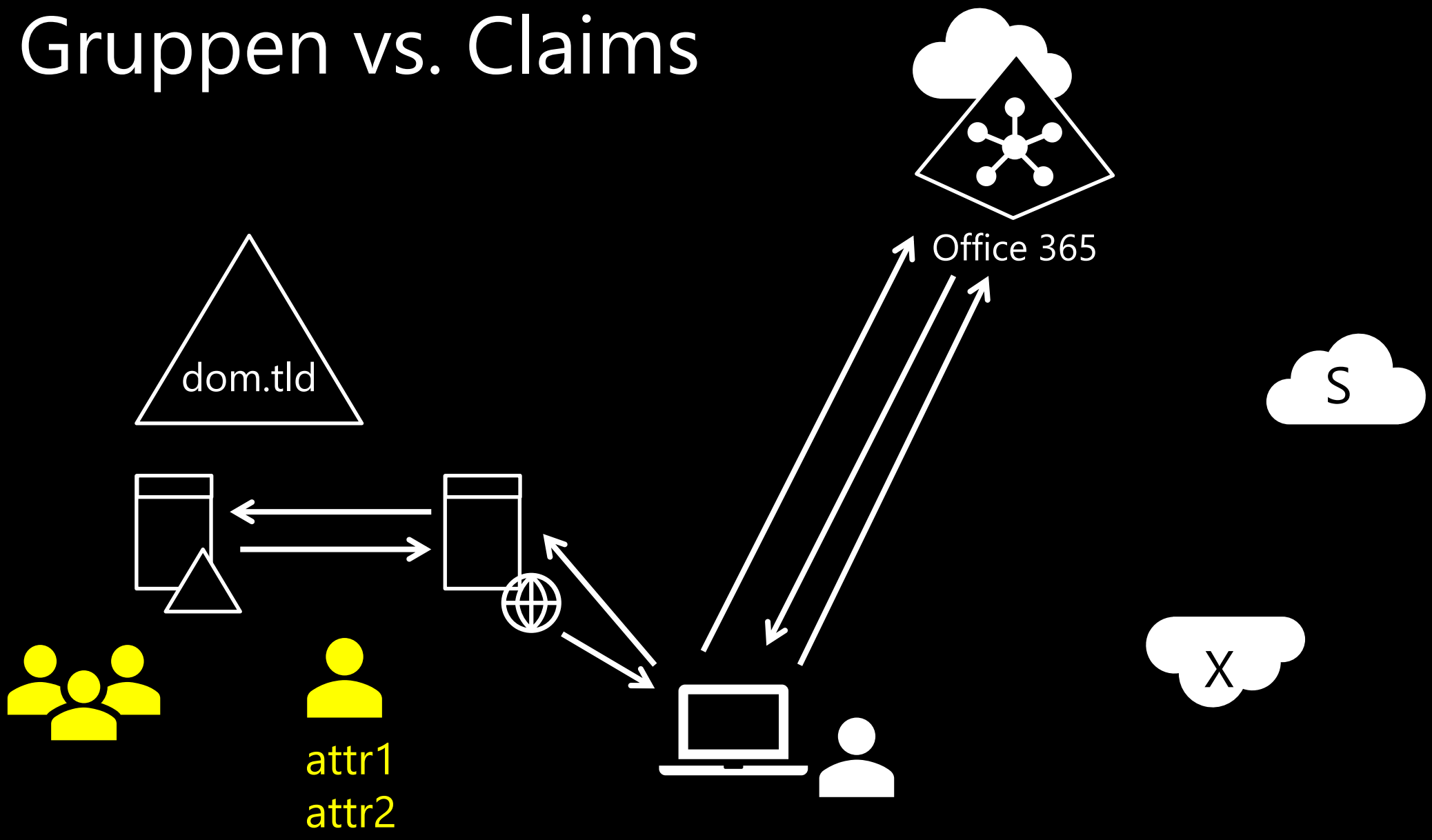


Federation



Vertrauen

Gruppen vs. Claims



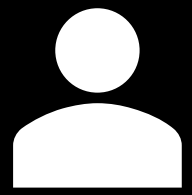
Design for change

Special: UPN für Azure-Auth

userPrincipalName

Benutzer EllenBogen@mydomain.org

Kennwort ••••••••••••••



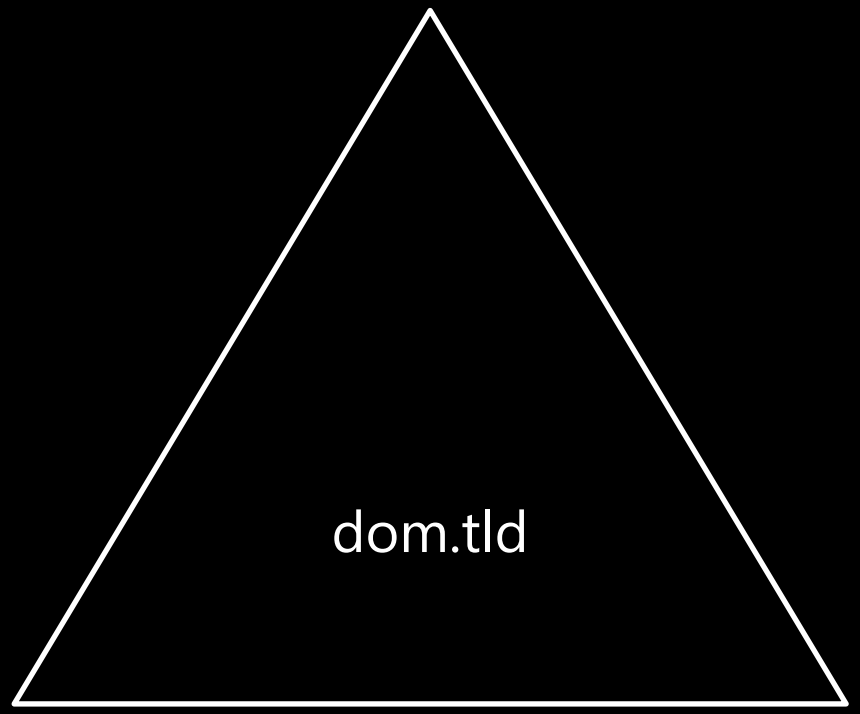
dom\EllenB

EllenB@dom.local

EllenBogen@mydomain.org

4

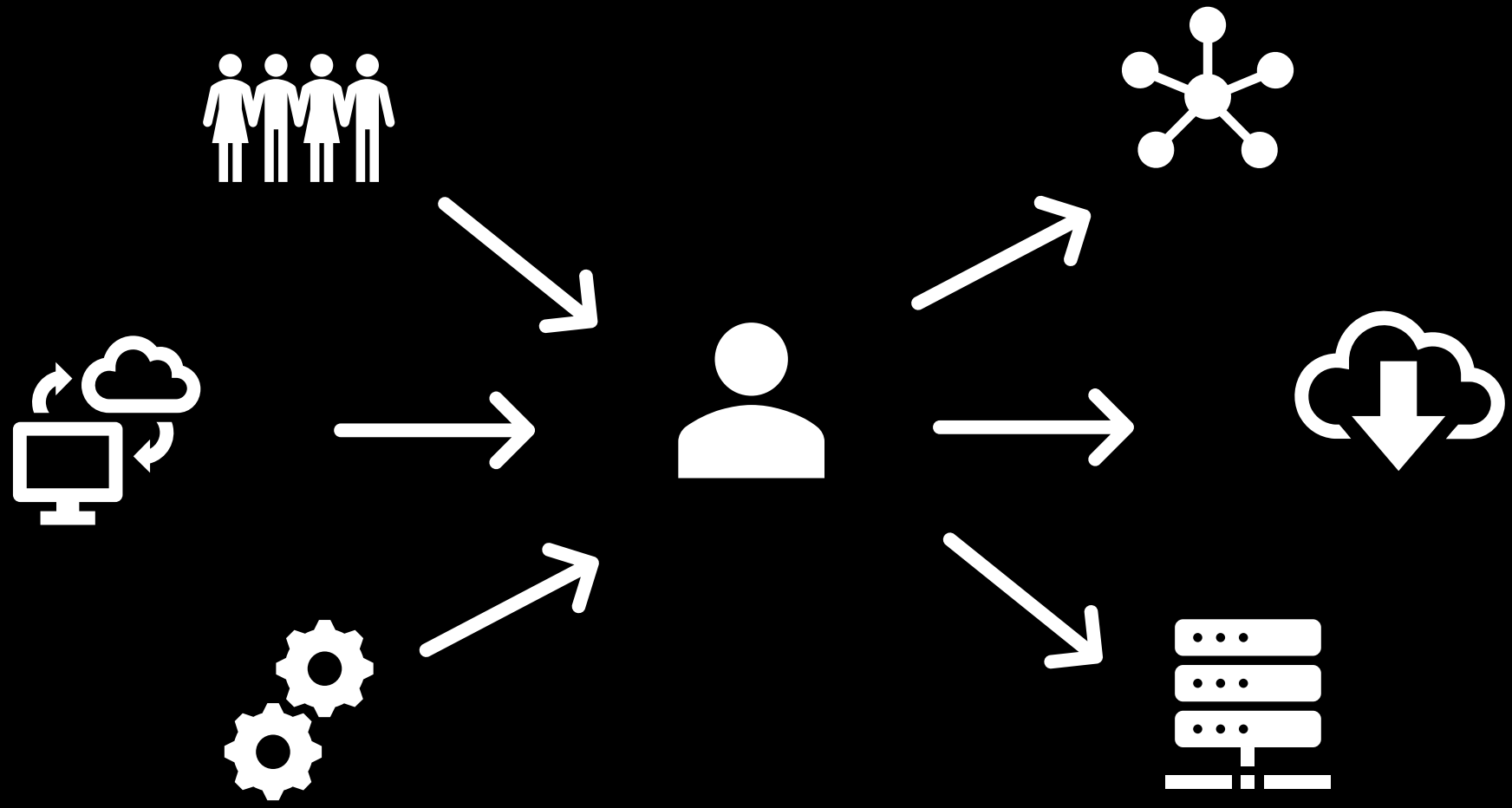
Datenpool: Teile und herrsche



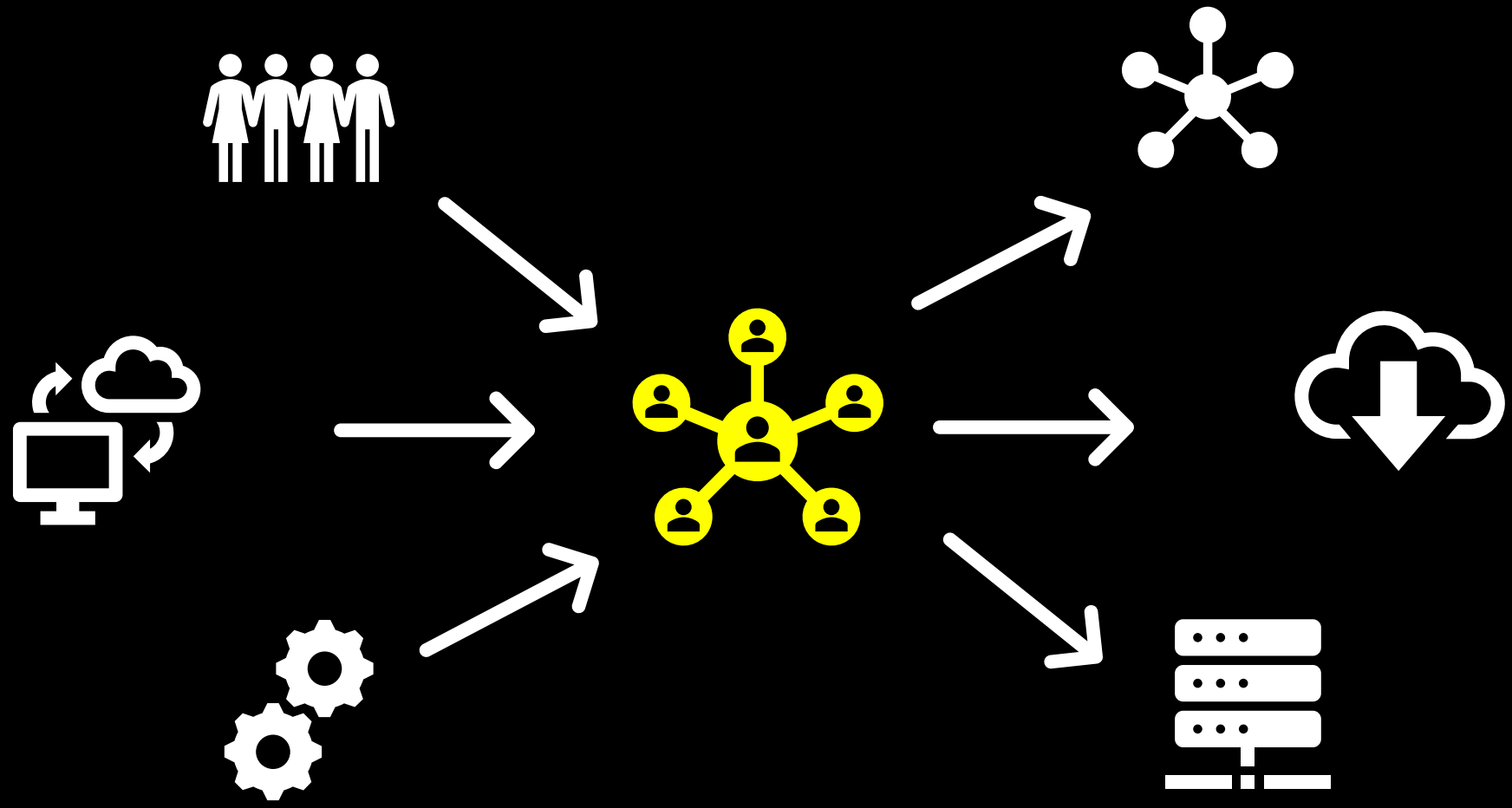
Zentraler Datenspeicher

Zentra eicher

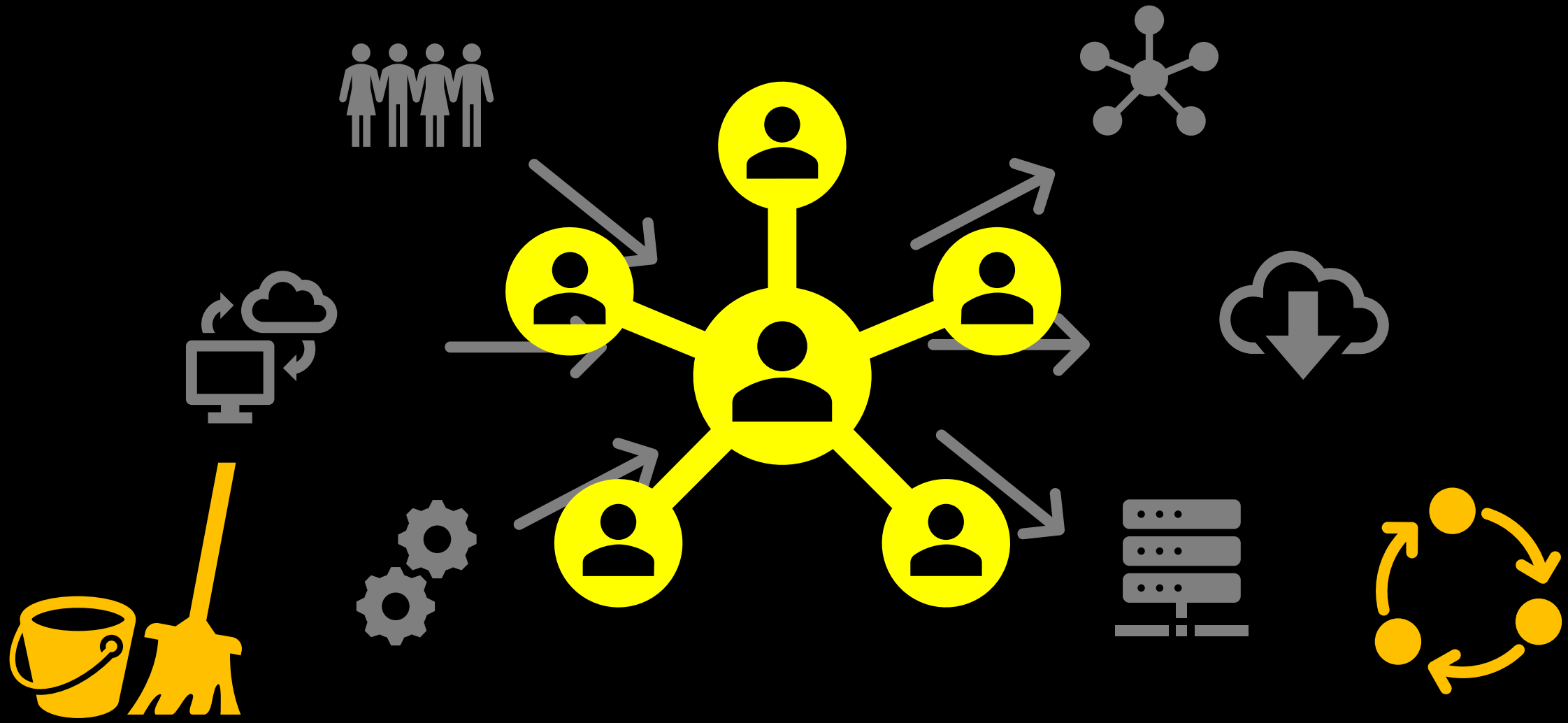
Identitätsdaten



Daten-Drehscheibe

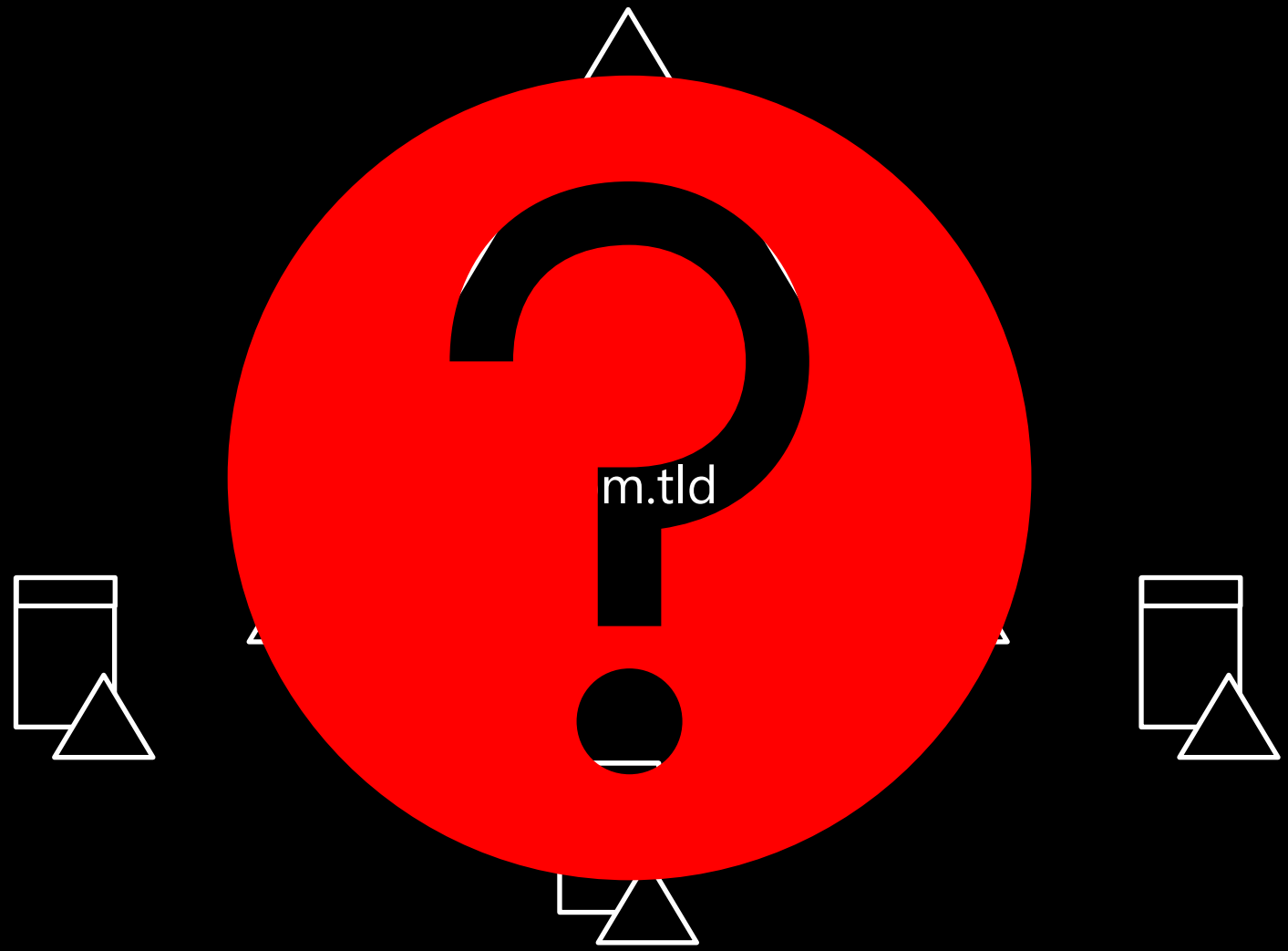


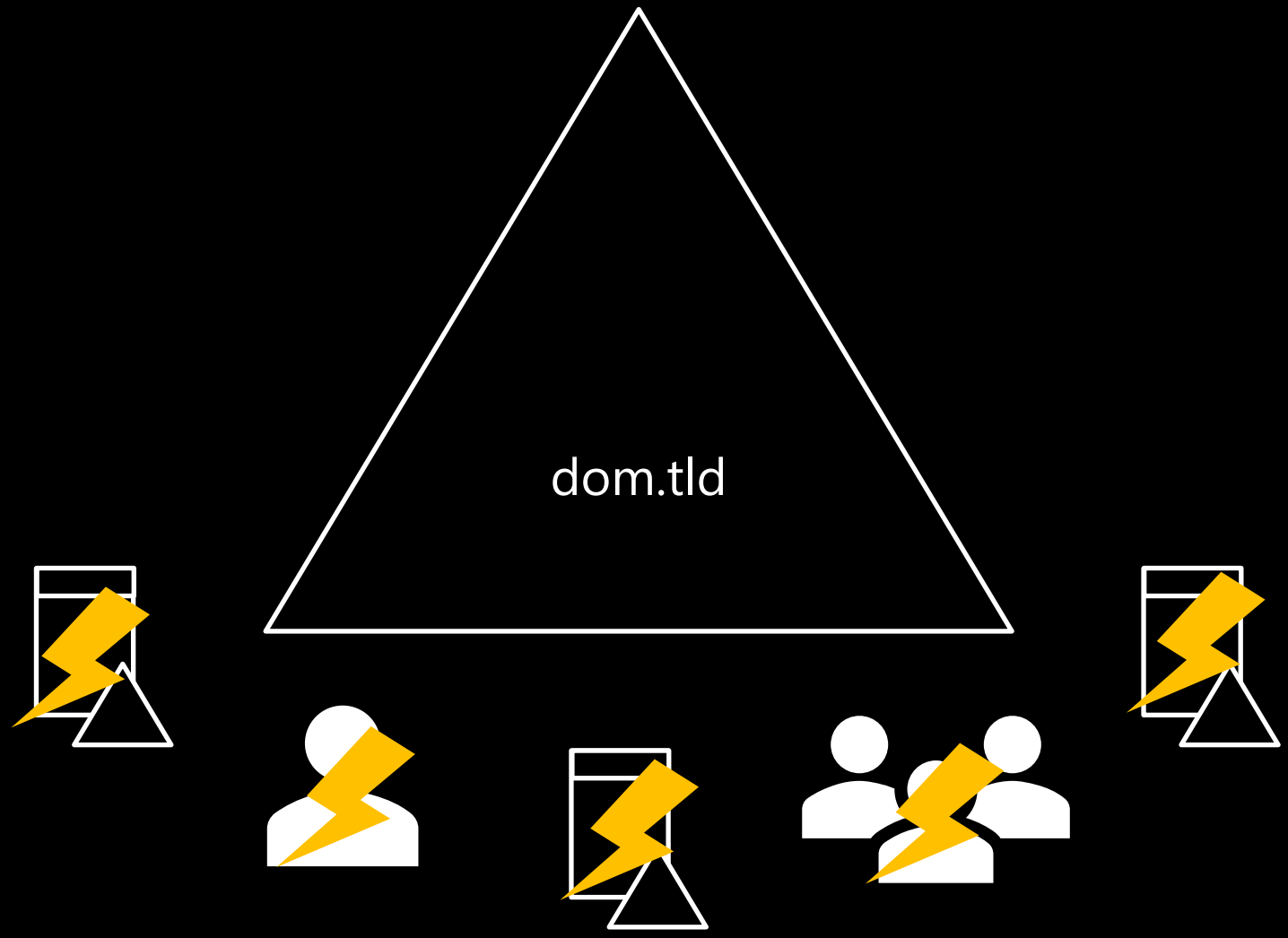
Daten-Drehscheibe



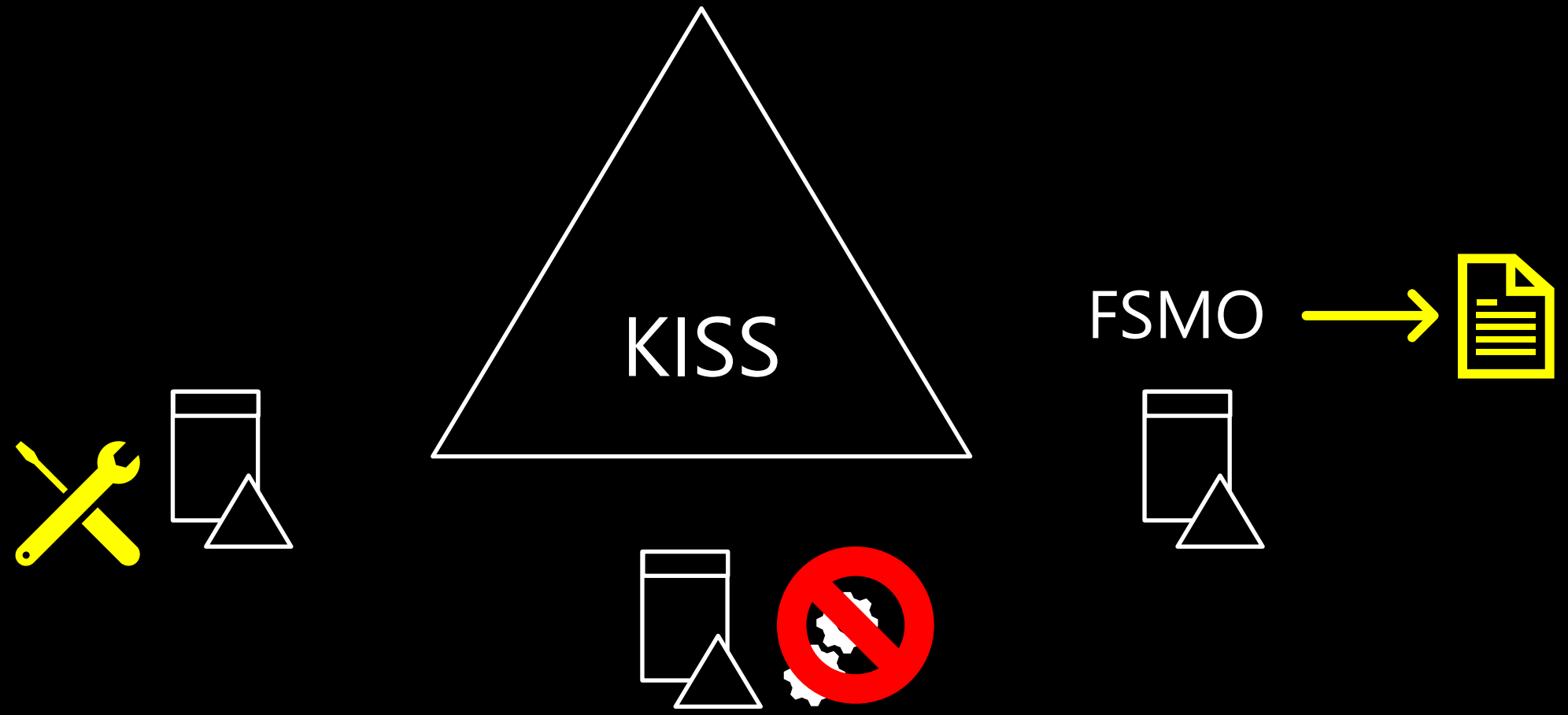
5

Notfall: Von hinten gedacht

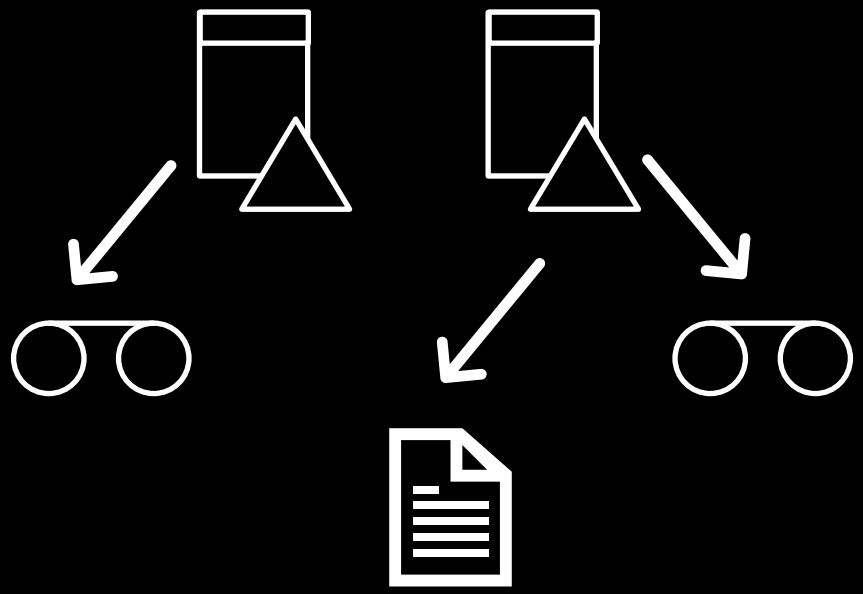

m.tld

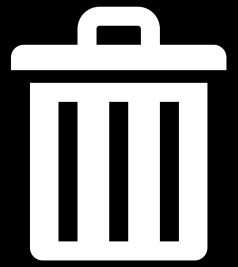

dom.tld

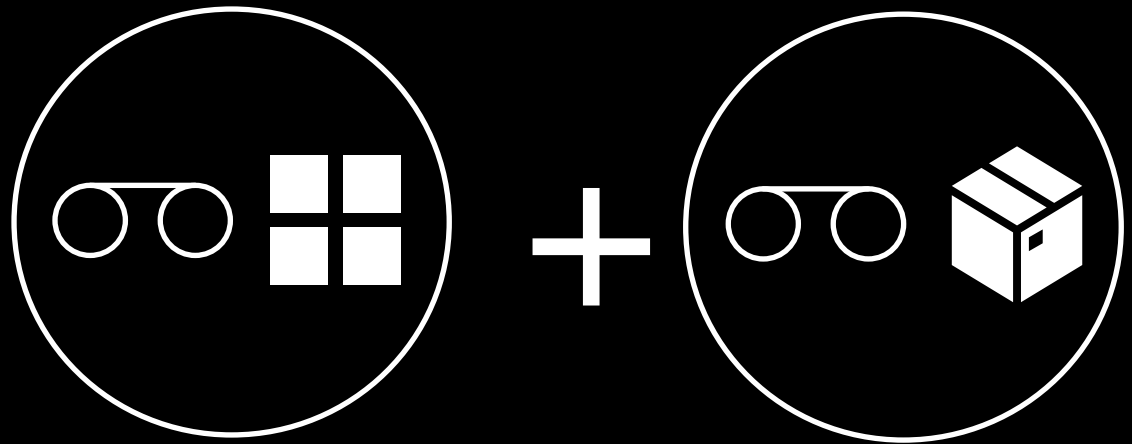
Das Design verhindert den Notfall



Cheat Sheet: AD-Backup



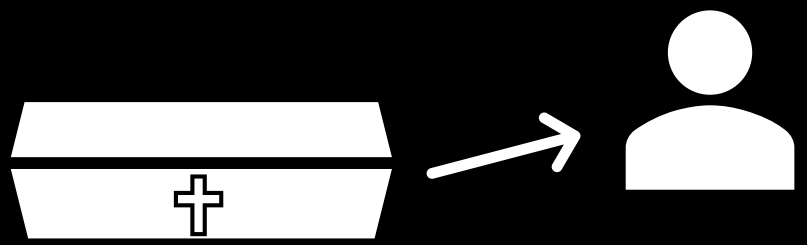


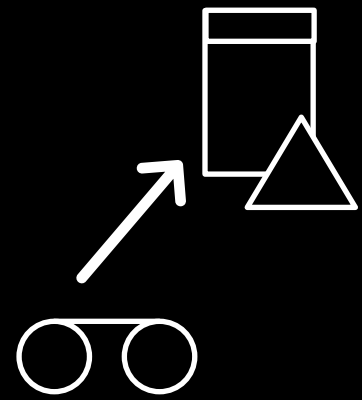


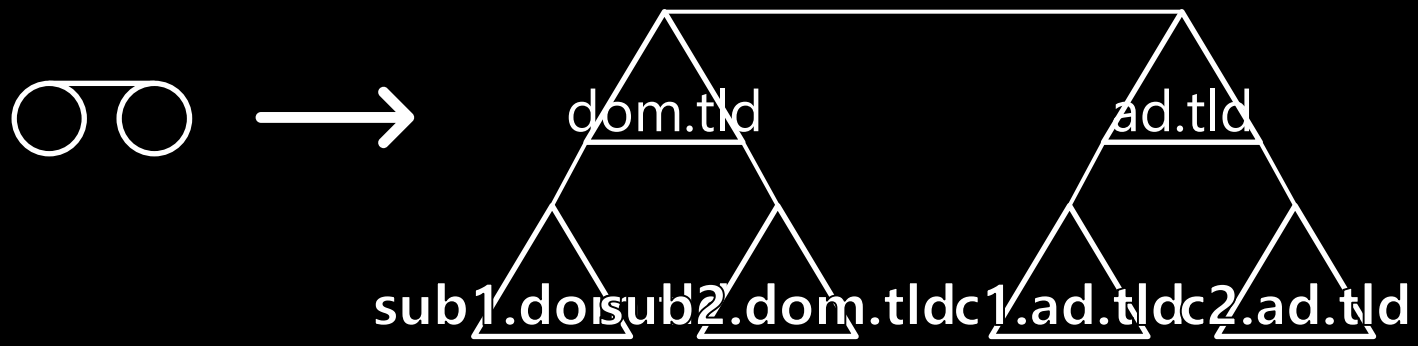
Cheat Sheet Cheat Sheet

- min. 2 DCs pro Domäne sichern
- Textexport aller Objekte bei jedem Backup
  - csvde -f C:\AD\exp.txt -u -l sAMAccountName,objectClass,description
- AD-Papierkorb aktivieren
- min. 1 Backup mit Windows Server Backup (Systemstate)
- Andere Produkte nur als Ergänzung

Üben. Ernsthaft.







Zum Mitnehmen

- 1 Design: Fundament für Identitäten
  - AD-Design prüfen: Einfach genug?
  - Objektorientiert aufbauen
- 2 Sicherheit: Angriffe sind normal
  - Rollen trennen
  - Red Forest Design
- 3 Hybrid-Design: Cloud und lokal
  - AD ist der Identitäts-Anker
  - Namensräume planen
- 4 Datenpool: Teile und herrsche
  - Alle Daten an ihrem Platz
  - Datenverteilung steuern
- 5 Notfall: Von hinten gedacht
  - Das Design verhindert den Notfall
  - Recovery üben