UNIVERSITÄT BIELEFELD

BITS Bielefelder IT-Servicezentrum

Lets Encrypt DNS-Challenge (Alias Mode) mit dem acme.sh Client

Sergej Lang
Bielefelder IT-Servicezentrum
08.10.2020

Agenda

- Erklärung und Einschränkungen
- Lets Encrypt DNS Challange „händisch“
- Lets Encrypt DNS Challange „automatisiert“ (in der Uni Bielefeld)

Erklärung und Einschränkungen

- Der Vortrag gilt nur für den „acme.sh“ Client.
- Es wird nur die DNS-Challenge (mit „Alias Mode“) behandelt.
  - Es gibt noch viele andere Clients und Challenge Typen.
- **Beide vorgestellte DNS-Challenge Verfahren sind Prototypen (Testbetrieb in der Uni Bielefeld).**
- Bitte um Feedback im Betrieb.

Lets Encrypt DNS-Challenge „Händisch“:

Voraussetzung:

- Bluecat Schreibrecht für die DNS Zone der eigenen Einrichtung.

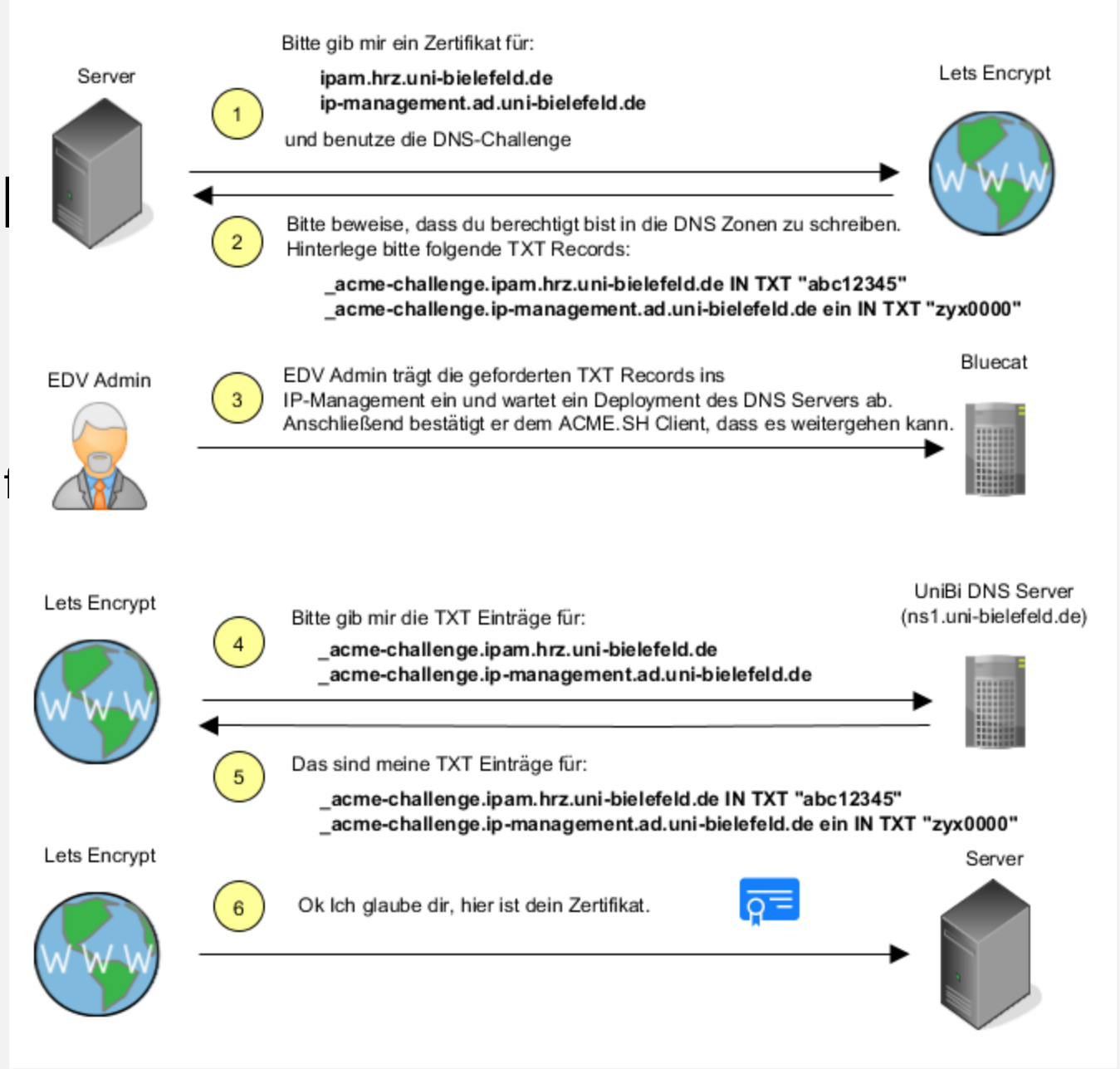
UNIVERSITÄT BIELEFELD

BITS Bielefelder IT-Servicezentrum

Lets Encrypt I

Voraussetzung:

- Bluecat Schreibrecht f



Lets Encrypt DNS-Challenge „automatisch“ (Vorarbeit):

Bluecat Admin (1x pro Einrichtung):

- Erstellt eine „ACME“ DNS Zone.
- Legt einen „External Host“ Eintrag an.
- Generiert und Verteilt den TSIG Key für DDNS Updates.

EDV Admin

- Brauch ein Schreibrecht für seine DNS Zone im Bluecat IPAM.
- Legt für jede Domain* einen CNAME zur eigenen „ACME“ Zone an.

  *nur für die mit einem Lets Encrypt Zertifikat.

Lets Er
(Vorarb

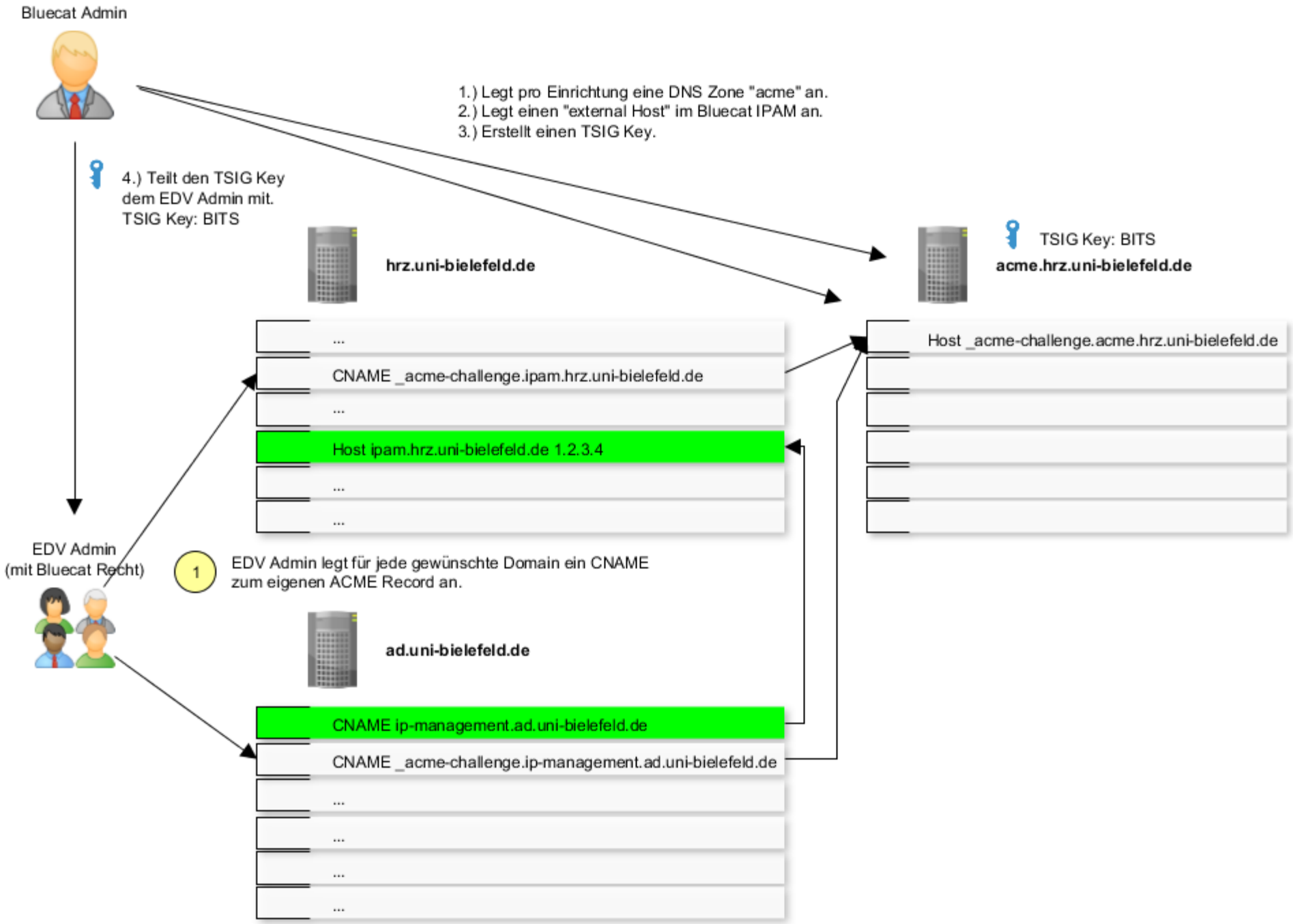
Bluecat

- Erstellt e
- Legt eine
- Generier

EDV Adı

- Brauch e
- Legt für j

*nur für



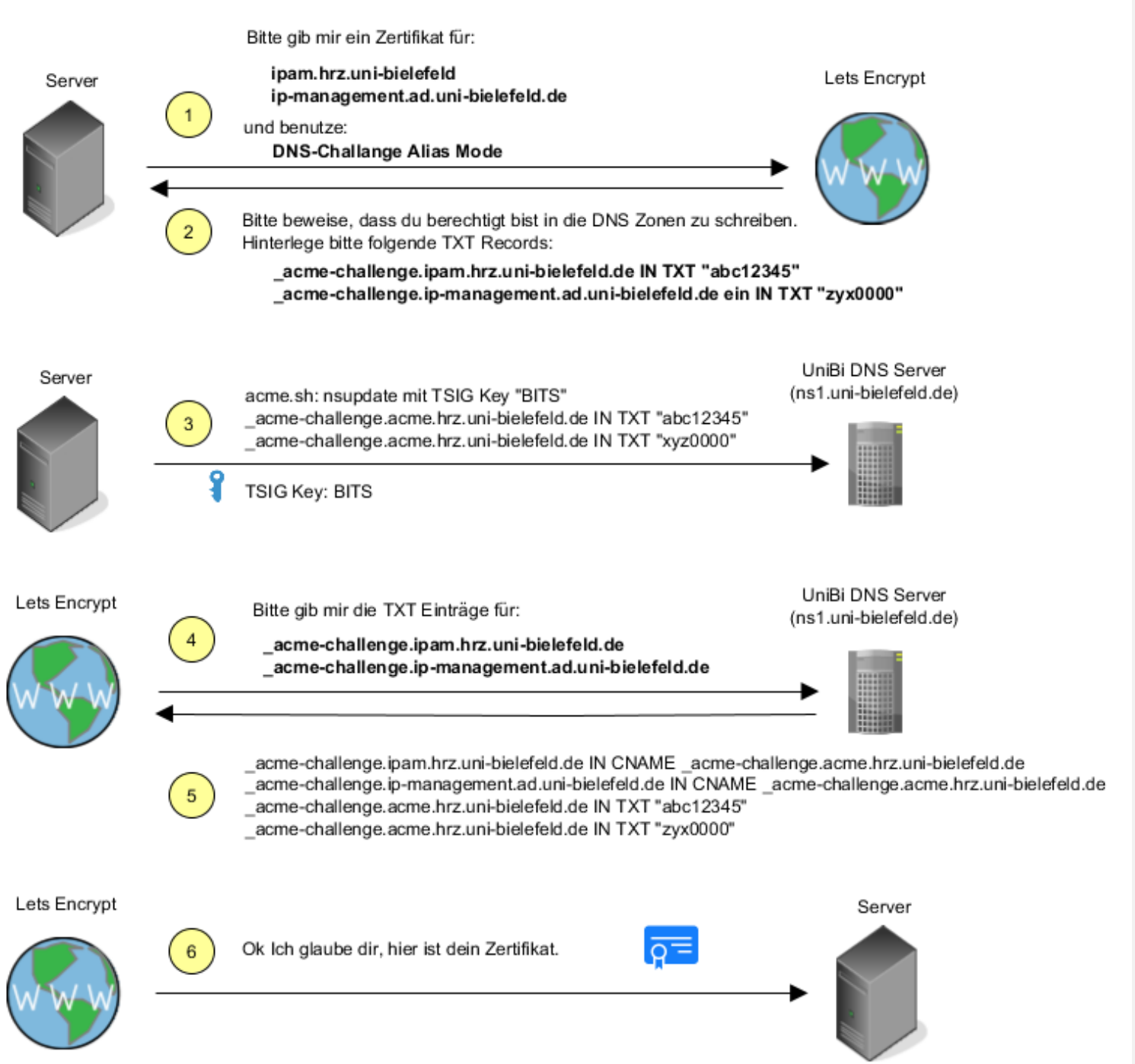
Lets Enrypt DNS-Challenge „automatisch“

```
cat ~/.nsupdate.key
key "BITS" {
algorithm hmac-sha512;
secret "SuperGeheimllllelf==";
};

export NSUPDATE_SERVER="ns1.uni-bielefeld.de"
export NSUPDATE_KEY="/path/to/your/nsupdate.key"

acme.sh --issue --dns dns_nsupdate --challenge-alias acme.hrz.uni-bielefeld.de \
    -d ipam.hrz.uni-bielefeld.de \
    -d ip-management.ad.uni-bielefeld.de
```

UNIVERSITÄT BIELEFELD

BITS Bielefelder IT-Servicezentrum

Lets Enrypt D
„automatisch



Fragen?

Weitere Infomationen:

https://github.com/acmesh-official/acme.sh/wiki/DNS-alias-mode

https://letsencrypt.org/de/docs/challenge-types/

So sieht ein TSIG Key File aus:

```
key BITS {
    algorithm hmac-sha512;
    secret "+Cdjlkef9ZTSeixERZ433Q==";
};
```