

AWS

S U M M I T



Large Scale Enterprise Account Management

Ronny Fauth, Daniel Woithe
DB Systel GmbH
18.05.2017, Berlin



Agenda

Introduction

Cloud adoption at Deutsche Bahn

Paradigm shifts in IT security

Basic security principles

Access security architecture

Why we are here

iX 5/2017

Im Gespräch: Gerald Hofer, Geschäftsführer Operations der DB Systel GmbH

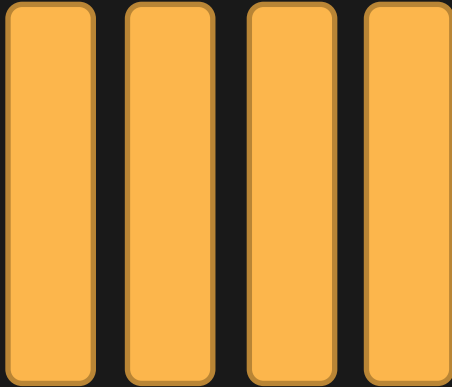
„Cloud ist ein Konzernziel“

Tilman Wittenhorst

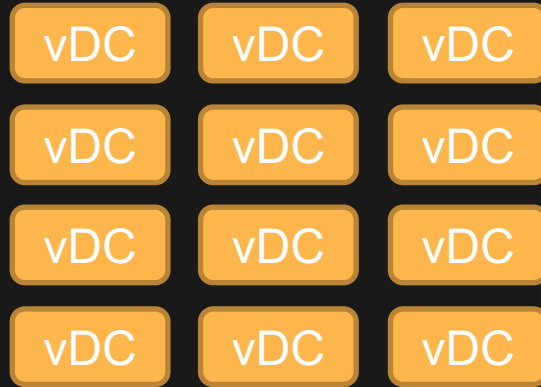
Der IT-Dienstleister der Deutschen Bahn, die DB Systel GmbH, verlagert ihr Rechenzentrum in die Amazon-Cloud. Bei diesem ehrgeizigen Projekt stellte sich nicht etwa die technische Umstellung als größte Hürde heraus, sondern der Wandel bei den Einstellungen der Mitarbeiter.

More than just a technical migration

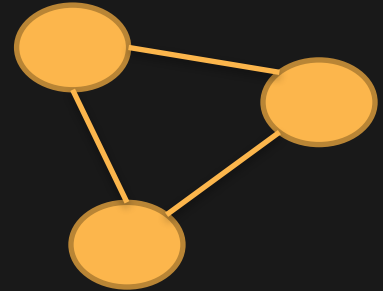
Vertical Operating Model



Distribution



Shared Responsibility



Security concepts need to adopt these changes.

Paradigm shifts in IT security

Decentralization changes security models



Physical security controls are obsolete



Basic security principles

Security by Default – Four security principles

Identity Federation

Multi Factor Authentication

Short Living Credentials

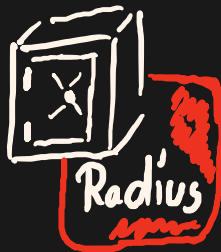
Access Control & Isolation

Access security architecture

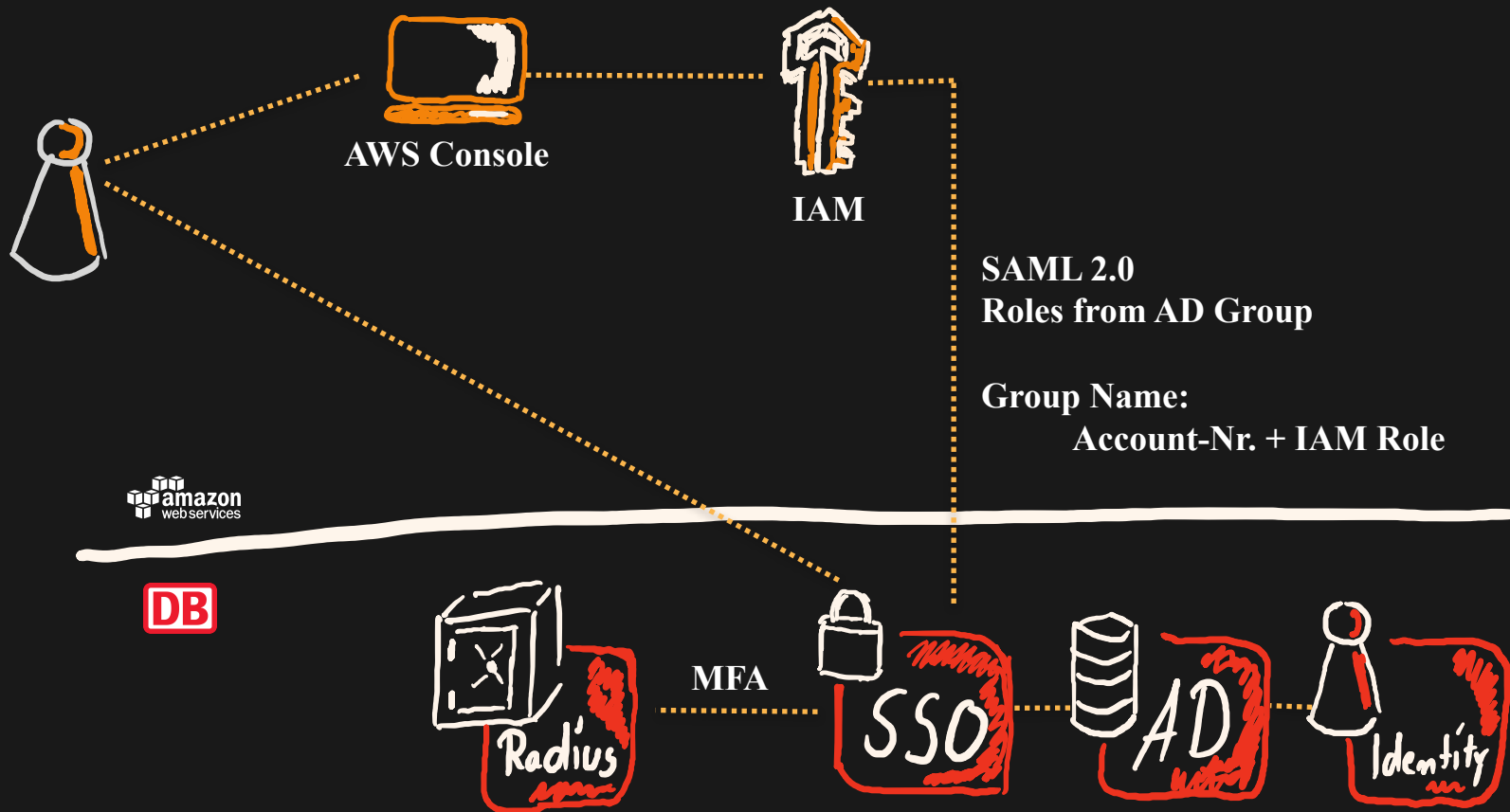
Access Security Architecture



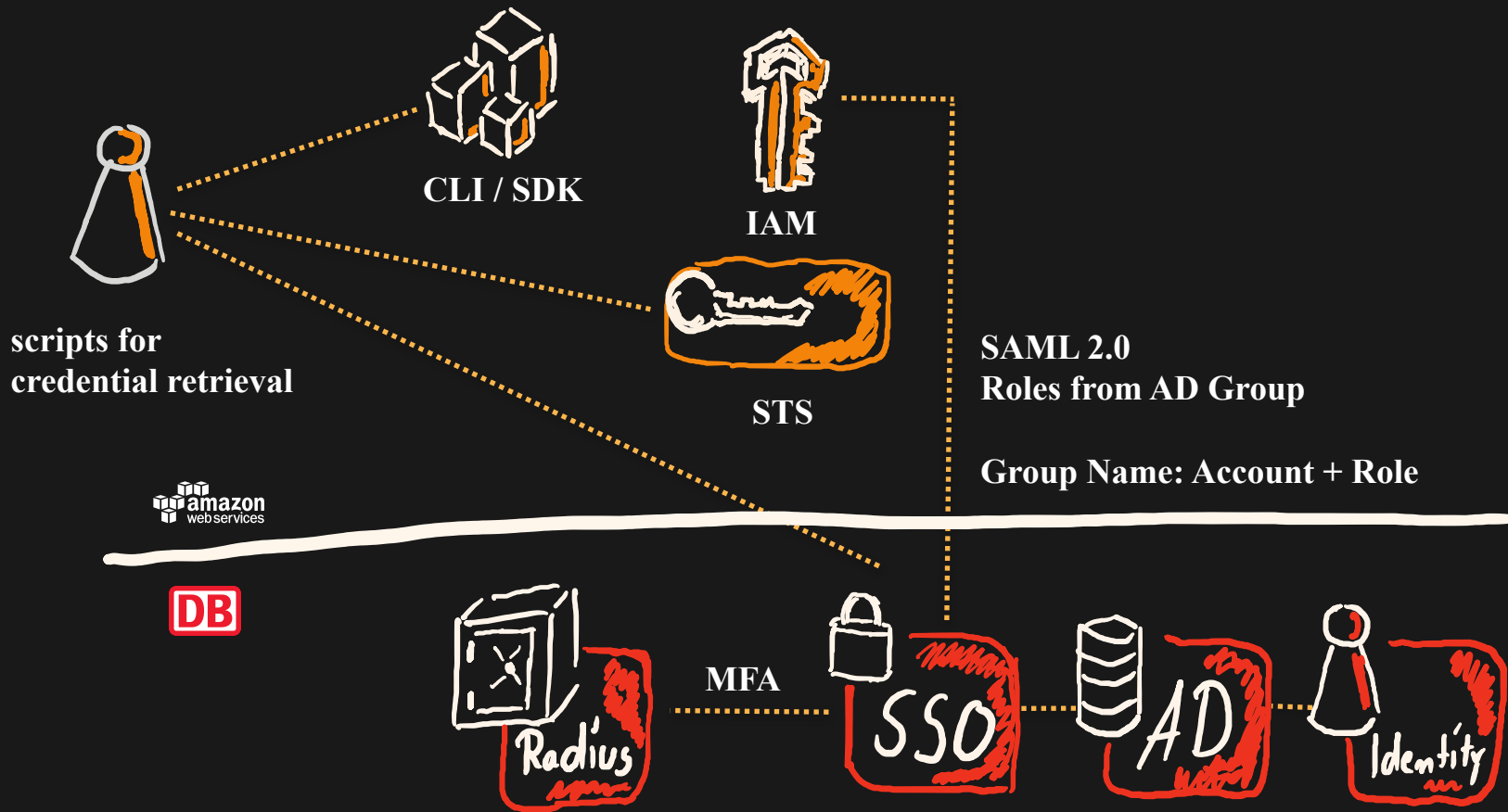
DB



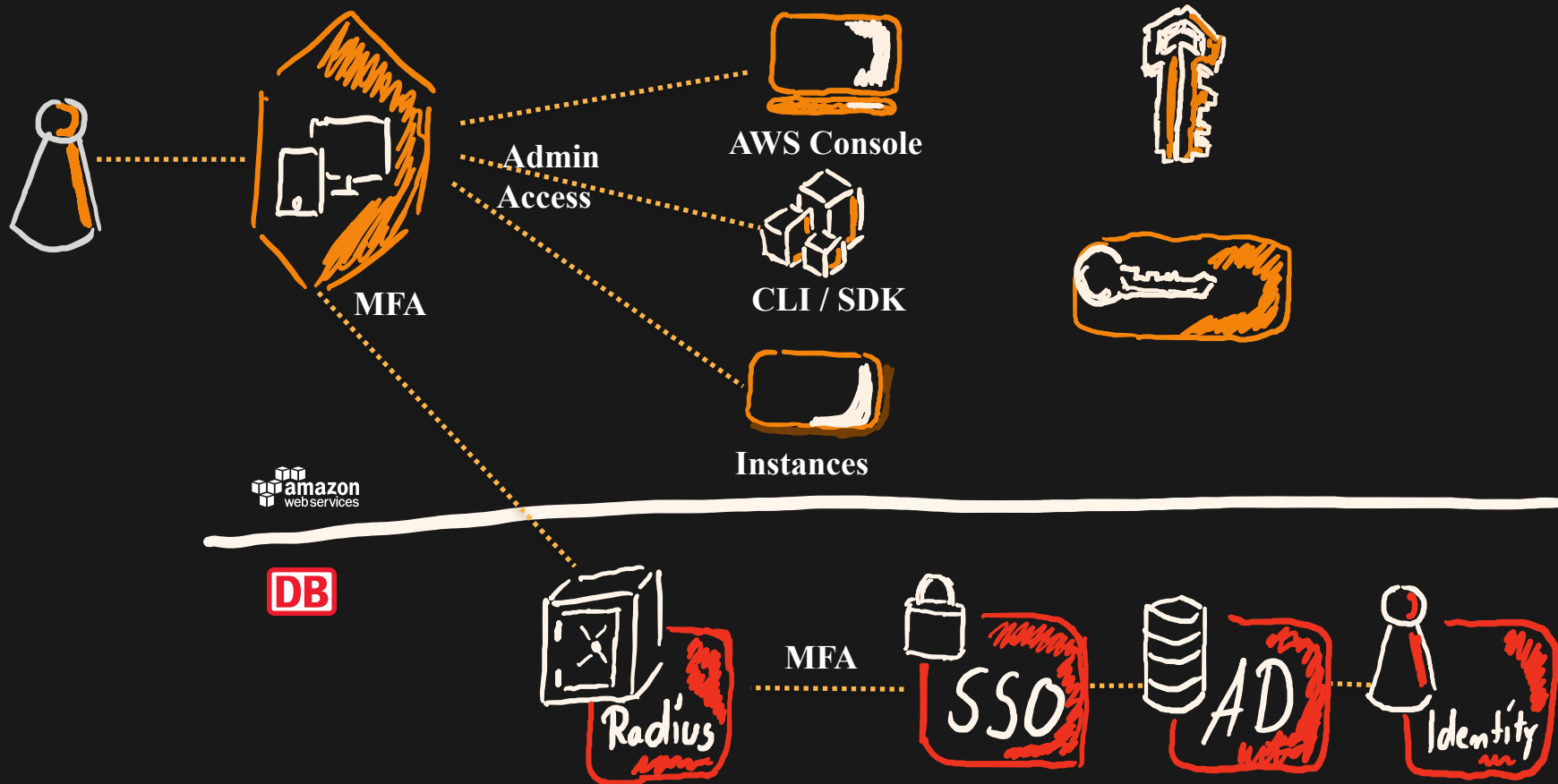
Identity Federation



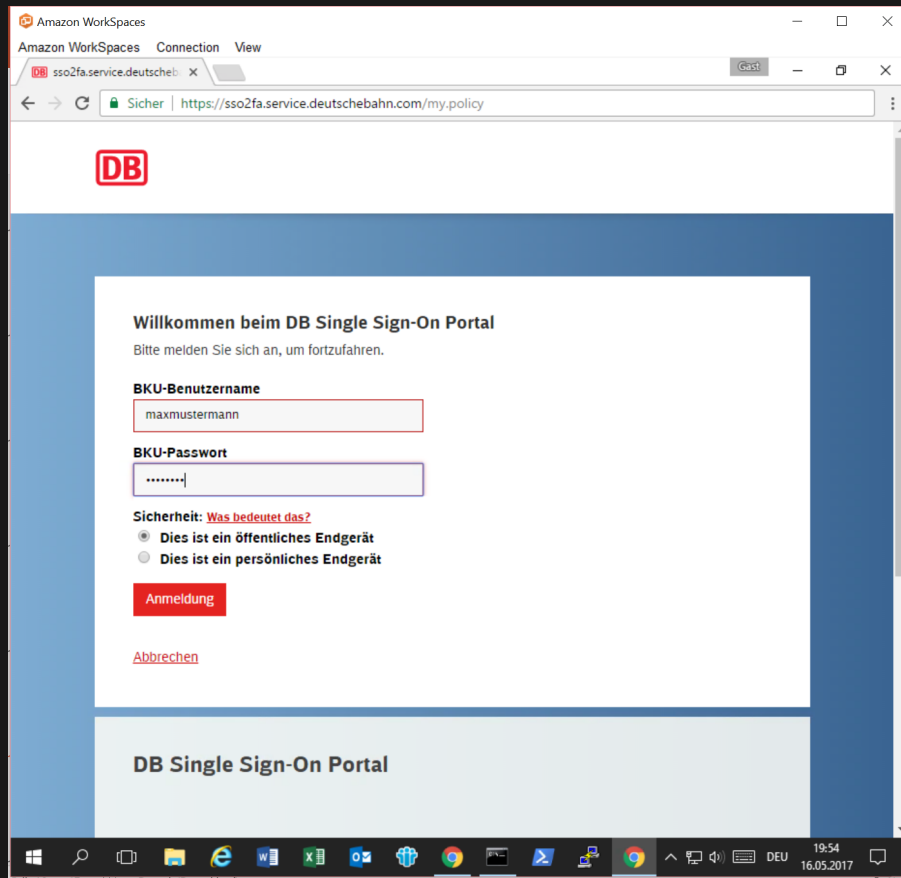
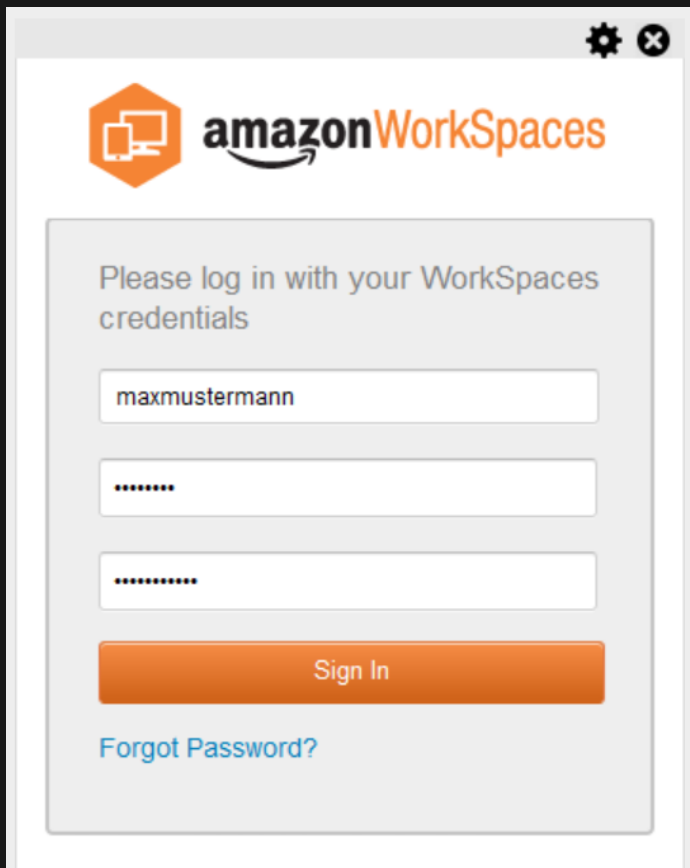
Short Living Credentials



Access Control & Isolation



Demo




```
D:\Users\maxmustermann>token
Please provide BKU credentials to login.
BKU-Username: maxmustermann
BKU-Passwort:
```

```
Please choose the role you would like to assume:
[ 0 ]: arn:aws:iam::123456789012:role/NetworkAdmin
[ 1 ]: arn:aws:iam::123456789012:role/BasisTeam
Selection:
1
```

Your new access key pair has been stored in the AWS configuration file {0} under the saml profile.

After this time you may safely rerun this script to refresh your access key pair.
To use this credential call the AWS CLI with the --profile option (e.g. aws --profile saml ec2 describe-instances).

```
credentials x
1 [saml]
2 output = json
3 region = eu-central-1
4 aws_access_key_id = AKIAIOSFODNN7EXAMPLE
5 aws_secret_access_key = wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY
6 aws_session_token = FQoDYXdzEBsaDjczmHX3A0yCuld8vyKrAkTpkLJfSzV6WDHN4cu0Rapn9zN5tmcOOZXLW2FJoN1ha4
7
8 [lab]
9 region = eu-central-1
10 output = json
11 role_arn = arn:aws:iam::987654321012:role/ServiceTeam
12 source_profile = saml
13
```

AWS

S U M M I T

Thank you!

