okta

JWTs for CSRF & Microservices

Micah Silverman | Platform Specialist

August 3, 2017

1515
YAMAHA
YAMAHA

Welcome!

- Agenda
    - JWT with CSRF & Microservices (40 mins)
    - Okta 101 (5 mins)
    - Q&A (15 mins)

Let’s talk about CSRF!

Signature Computation Pseudo-code

```
encodeSecret =
    "4pE8z3PBoHjnV1AhvGk+e8h2p+ShZpOnpr8cwHmMh1w="
computeHMACSHA256(
    header + "." + payload,
    base64DecodeToByteArray(encodedSecret)
)
```

JWT Secret Anti-Patterns

Short but not Sweet

```
.signWith(
    SignatureAlgorithm.HS256,
   "secret".getBytes("UTF-8")
)
```

You’re Doing it Wrong

```
String b64EncodedSecret =
    "Yn2kjibddFAWtnPJ2AFlL8WXmohJMCvigQggaEypa5E=";
.signWith(
  SignatureAlgorithm.HS256,
   b64EncodedSecret.getBytes("UTF-8")
)
```

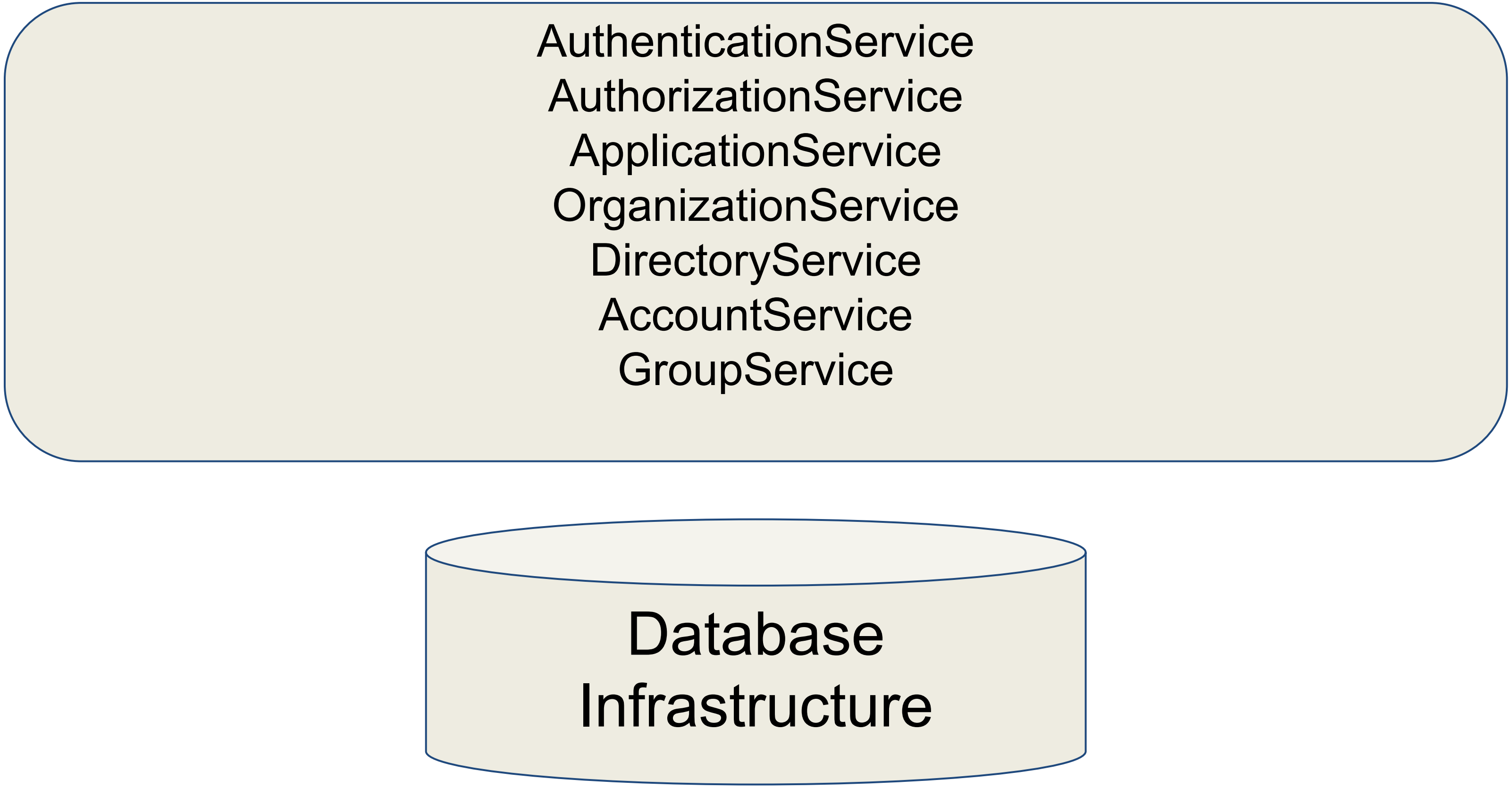
Supersize that Secret!

```
String b64EncodedSecret =
    "Yn2kjibddFAWtnPJ2AFlL8WXmohJMCvigQggaEypa5E=";
.signWith(
   SignatureAlgorithm.HS512,
   TextCodec.BASE64.decode(b64EncodedSecret)
)
```

"Microservices are awesome, but they're not free."

- Les Hazlewood

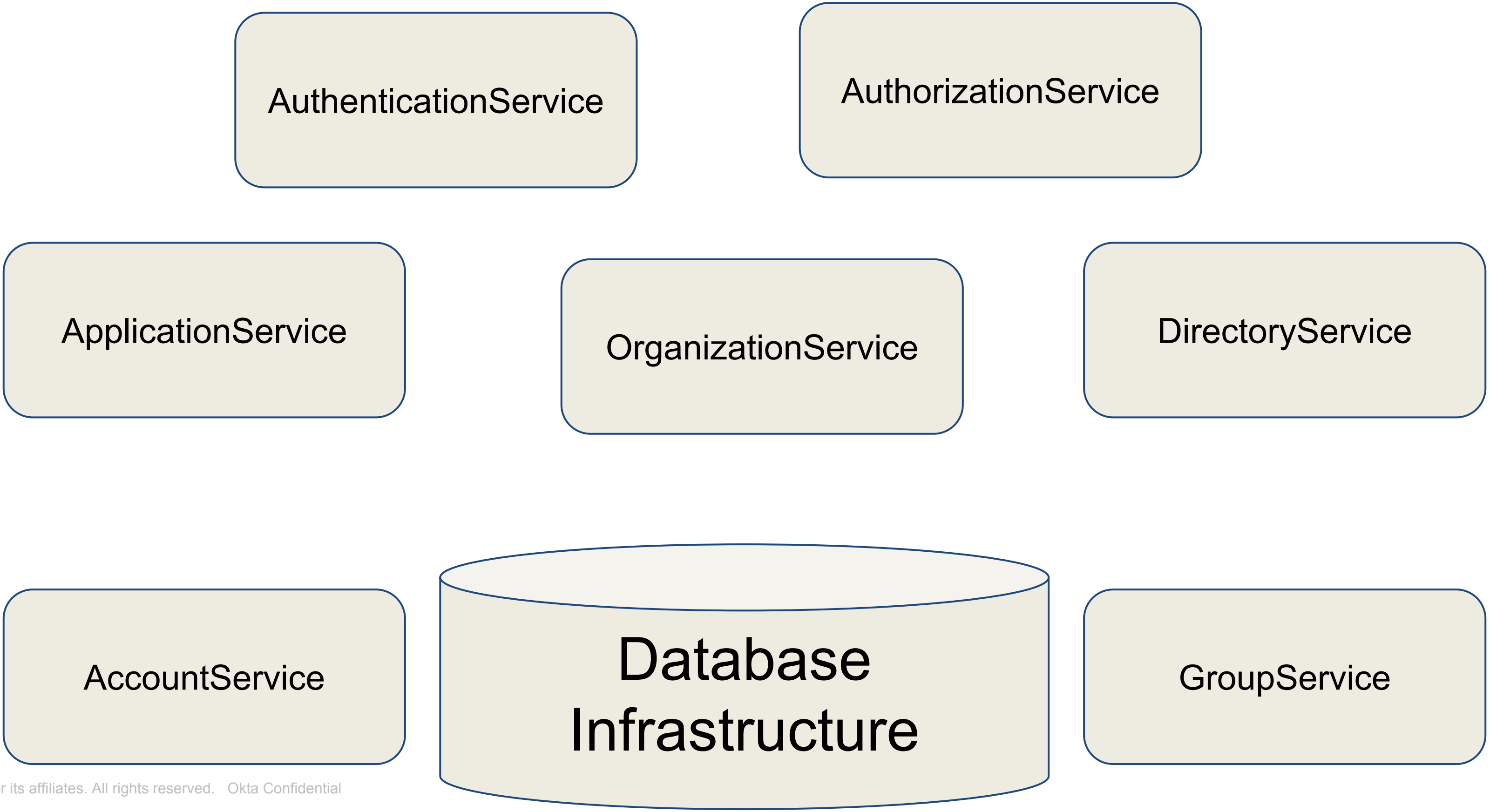
Monolithic SOA



AuthenticationService
AuthorizationService
ApplicationService
OrganizationService
DirectoryService
AccountService
GroupService

Database Infrastructure

Microservices



AuthenticationService

AuthorizationService

ApplicationService

OrganizationService

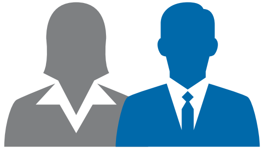
DirectoryService

AccountService

Database Infrastructure

GroupService

Okta Enables Companies to Do Both IT & API

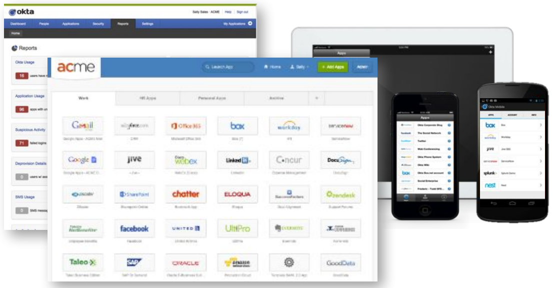


Employees,
Contractors

okta

Identity & Mobility Service:

Identity Management
Mobility Management
Strong Authentication

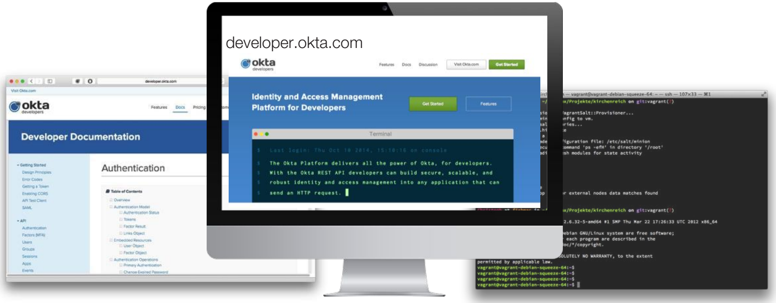


Partners,
Customers

okta

Identity Platform:

Identity API for Any App
Developer Tools
and Community



developer.okta.com

Identity and Access Management Platform for Developers

```
Terminal
$  Last login: Thu Oct 10 2014, 15:10:16 on console
$  The Okta Platform delivers all the power of Okta, for developers.
$  With the Okta REST API developers can build secure, scalable, and
$  robust identity and access management into any application that can
$  send an HTTP request.
```

Resources

- Repos used in today’s preso:
  - github.com/jwtk/jjwt
  - github.com/dogeared/JavaRoadStorm2016
- https://afitnerd.com/JavaRoadStorm2016/
- JJWT Guest Post on Baeldung - bit.ly/29ZPZAd
- Stormpath Microservices Screencast - bit.ly/29Wi6iw
- JWT Inspector - jwtinspector.io
- HTTPie - github.com/jkbrzt/httpie
- What are Microservices?
  - martinfowler.com/articles/microservices.html
- @afitnerd @OktaDev

okta

Thank You