



JWTs for CSRF & Microservices

Micah Silverman | API H@x0r

August 15, 2019



Welcome!

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

The background is a solid blue color. On the right side, there are two overlapping circles. The larger circle is a lighter shade of blue, and the smaller circle overlapping its right edge is a darker shade of blue.

Let's talk about CSRF!

Signature Computation Pseudo-code

```
encodedSecret =  
    "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 =  
    "Yn2kjibddFAWtnPJ2AF1L8WXmohJMCvigQggaEypa5E=";  
.  
signWith(  
    SignatureAlgorithm.HS256,  
    b64EncodedSecret.getBytes("UTF-8")  
)
```



Supersize that Secret!

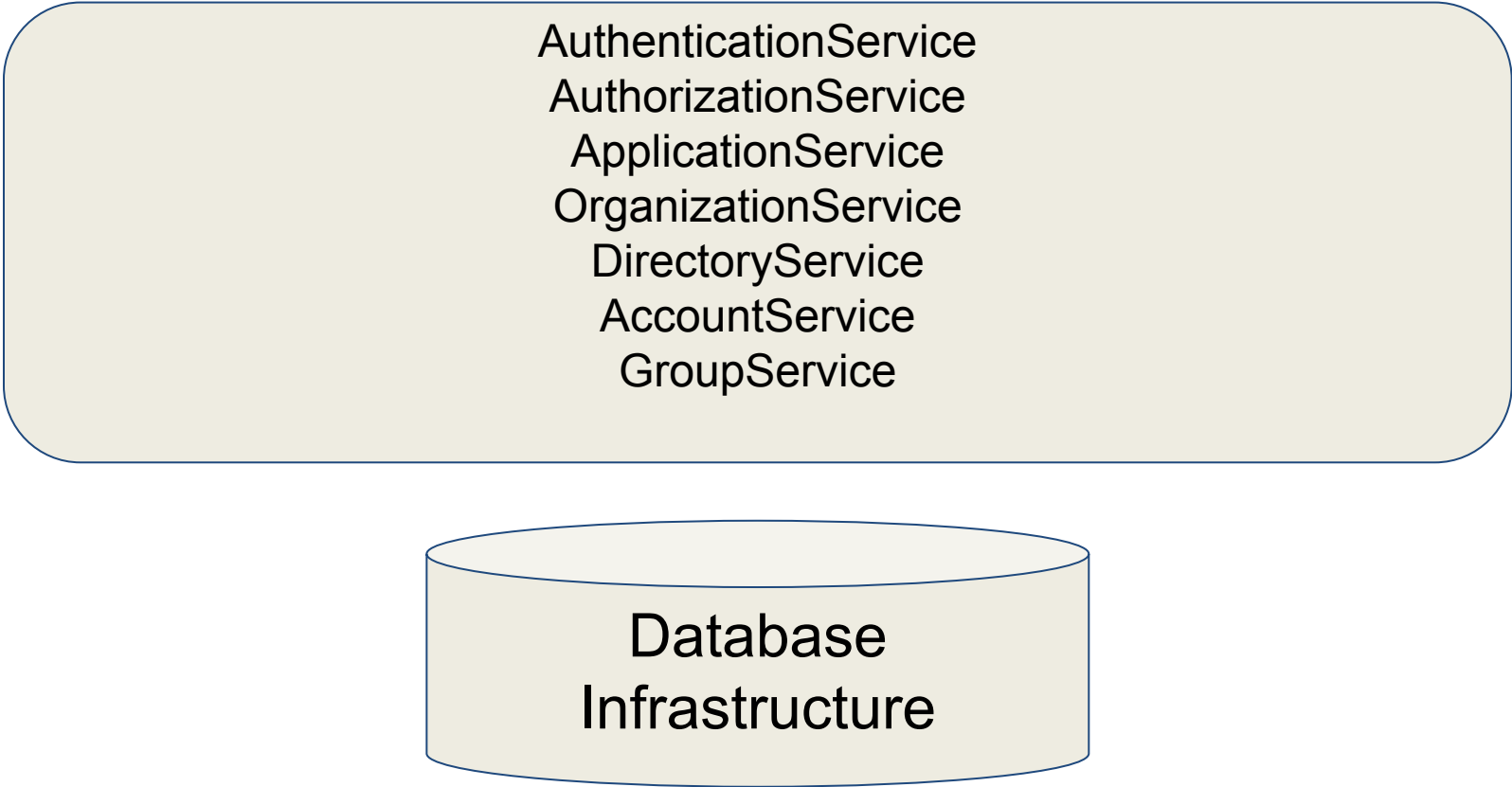
```
String b64EncodedSecret =  
    "Yn2kjibddFAWtnPJ2AF1L8WXmohJMCvigQggaEypa5E=";  
.signWith(  
    SignatureAlgorithm.HS512,  
    TextCodec.BASE64.decode(b64EncodedSecret)  
)
```



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

- Les Hazlewood

Monolithic SOA



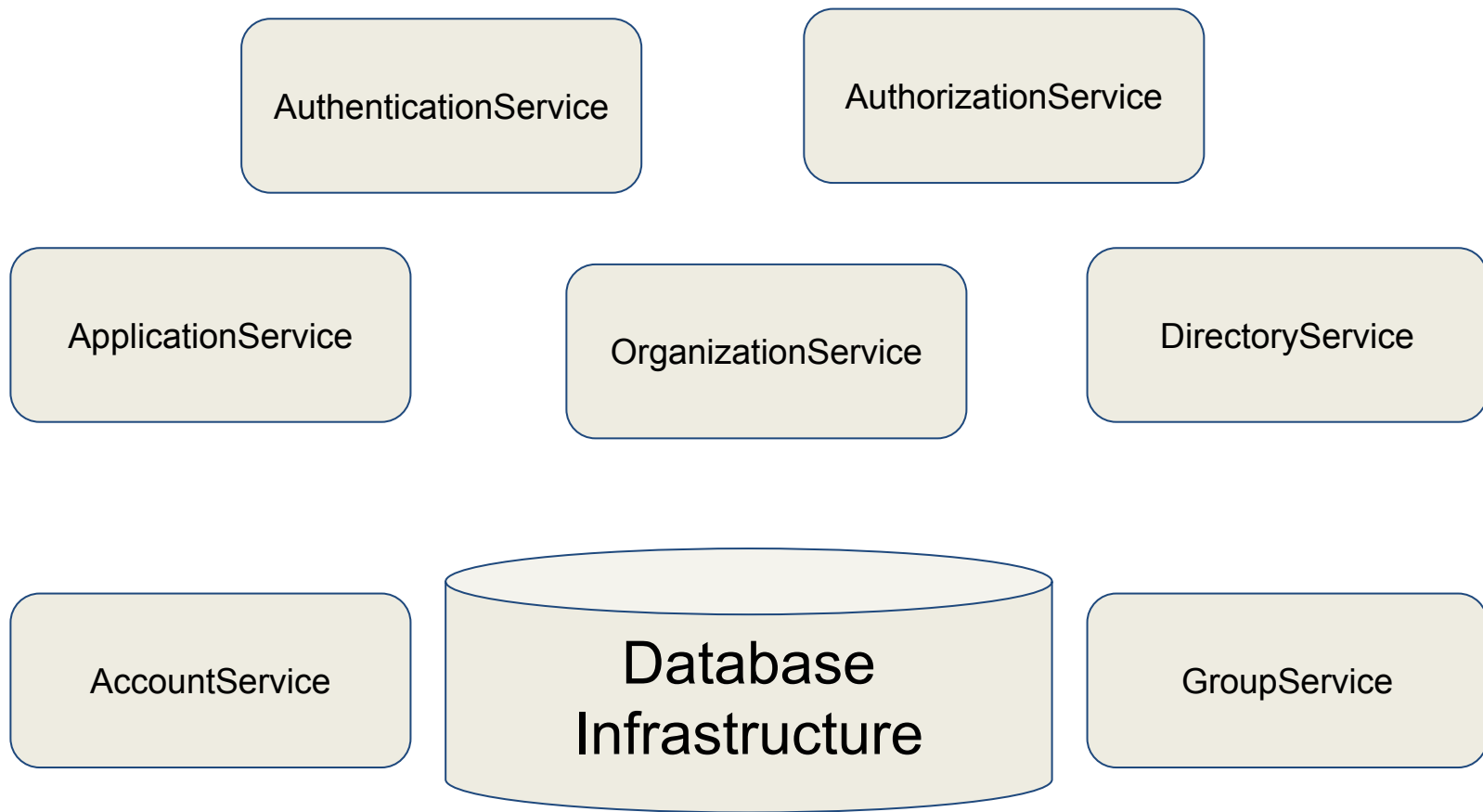
The diagram illustrates a Monolithic SOA architecture. It features a large, light-beige rounded rectangle at the top containing a list of services: AuthenticationService, AuthorizationService, ApplicationService, OrganizationService, DirectoryService, AccountService, and GroupService. Below this rectangle is a light-beige cylinder representing the Database Infrastructure. The entire diagram is set against a white background.

AuthenticationService
AuthorizationService
ApplicationService
OrganizationService
DirectoryService
AccountService
GroupService

Database
Infrastructure



Microservices



Okta Enables Companies to Do Both IT & API

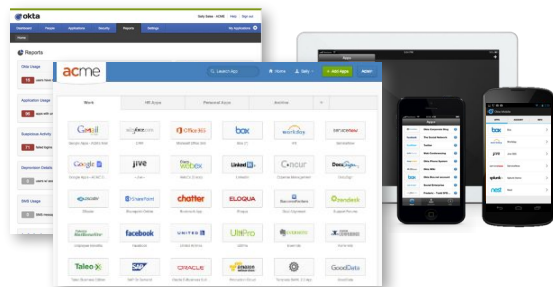


Employees,
Contractors



Identity & Mobility Service:

Identity Management
Mobility Management
Strong Authentication

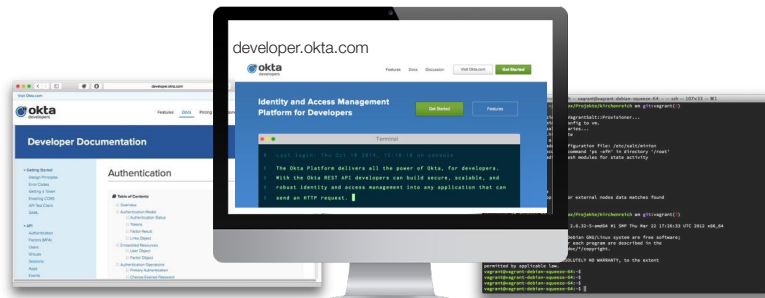


Partners,
Customers



Identity API Products:

Identity API for Any App
Developer Tools
and Community



Resources

- Repos used in today's preso:
 - github.com/jwtk/jjwt
 - github.com/dogearred/JavaRoadShow
- JWT Guest Post on Baeldung - bit.ly/29ZPZAd
- OIDC Playground - okta-oidc-fun.herokuapp.com
- JWT Inspector - jsonwebtoken.io
- HTTPie - github.com/jkbrzt/httpie
- What are Microservices?
 - martinfowler.com/articles/microservices.html
- @afitnerd @OktaDev



The image features a blue background with a radial burst pattern of light streaks emanating from the center. Overlaid on this are several semi-transparent blue circles, each containing a white dot in the center, arranged in a grid-like pattern. The Okta logo is centered in the upper half of the image.

okta

Thank You