



JWTs for CSRF & Microservices

Micah Silverman | Platform Specialist

September 30, 2017



Welcome!

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

The background is a solid blue color. On the right side, there are two overlapping circles. The circle in the foreground is a lighter shade of blue, while the one behind it is a darker shade. They are partially cut off by the right edge of the frame.

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!

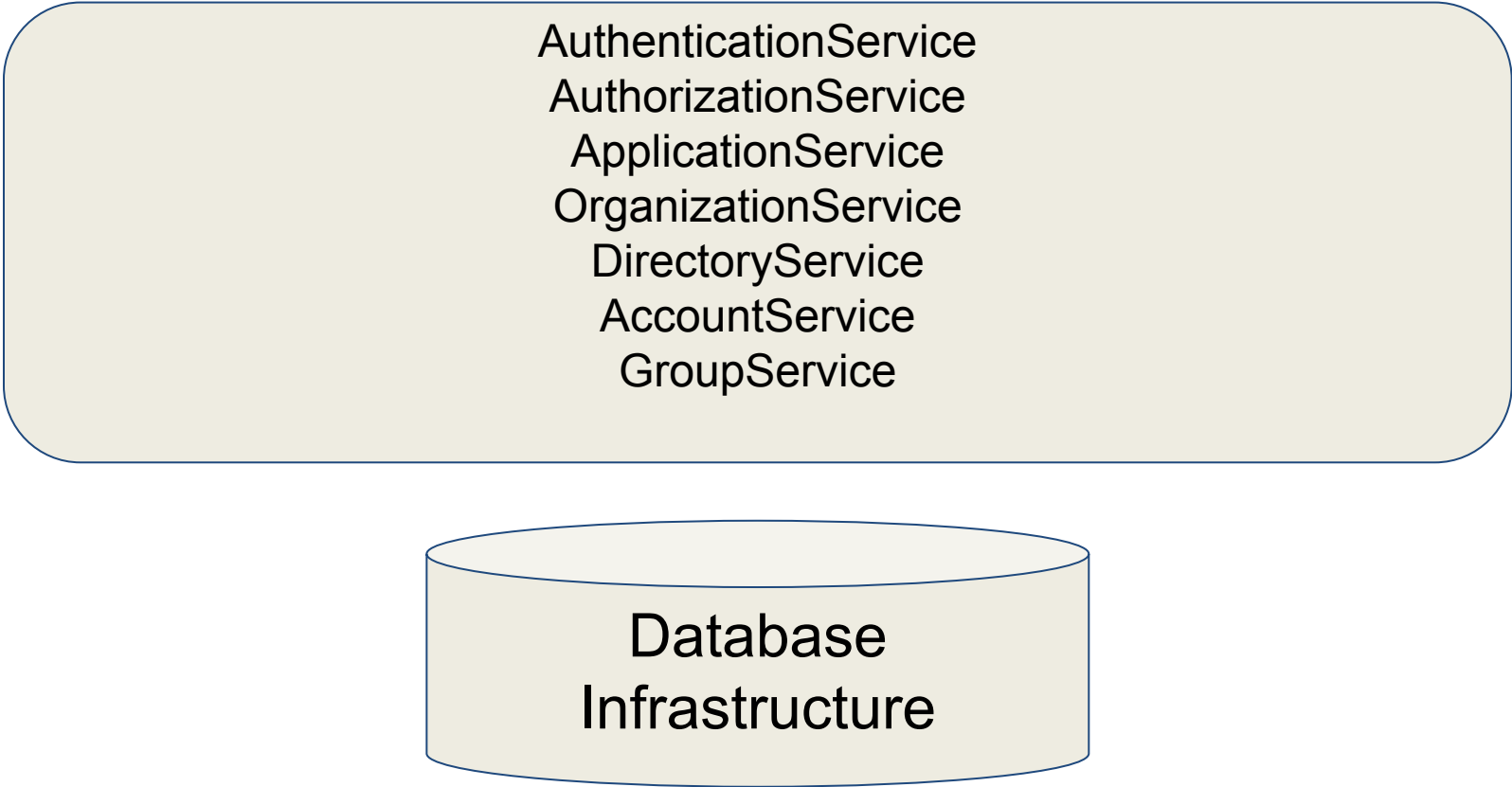
```
String b64EncodedSecret =  
    "Yn2kjibddFAWtnPJ2AF1L8WXmohJMCvigQggaEypa5E=";  
.signWith(  
    SignatureAlgorithm.HS512,  
    TextCodec.BASE64.decode(b64EncodedSecret)  
)
```



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

- Les Hazlewood

Monolithic SOA



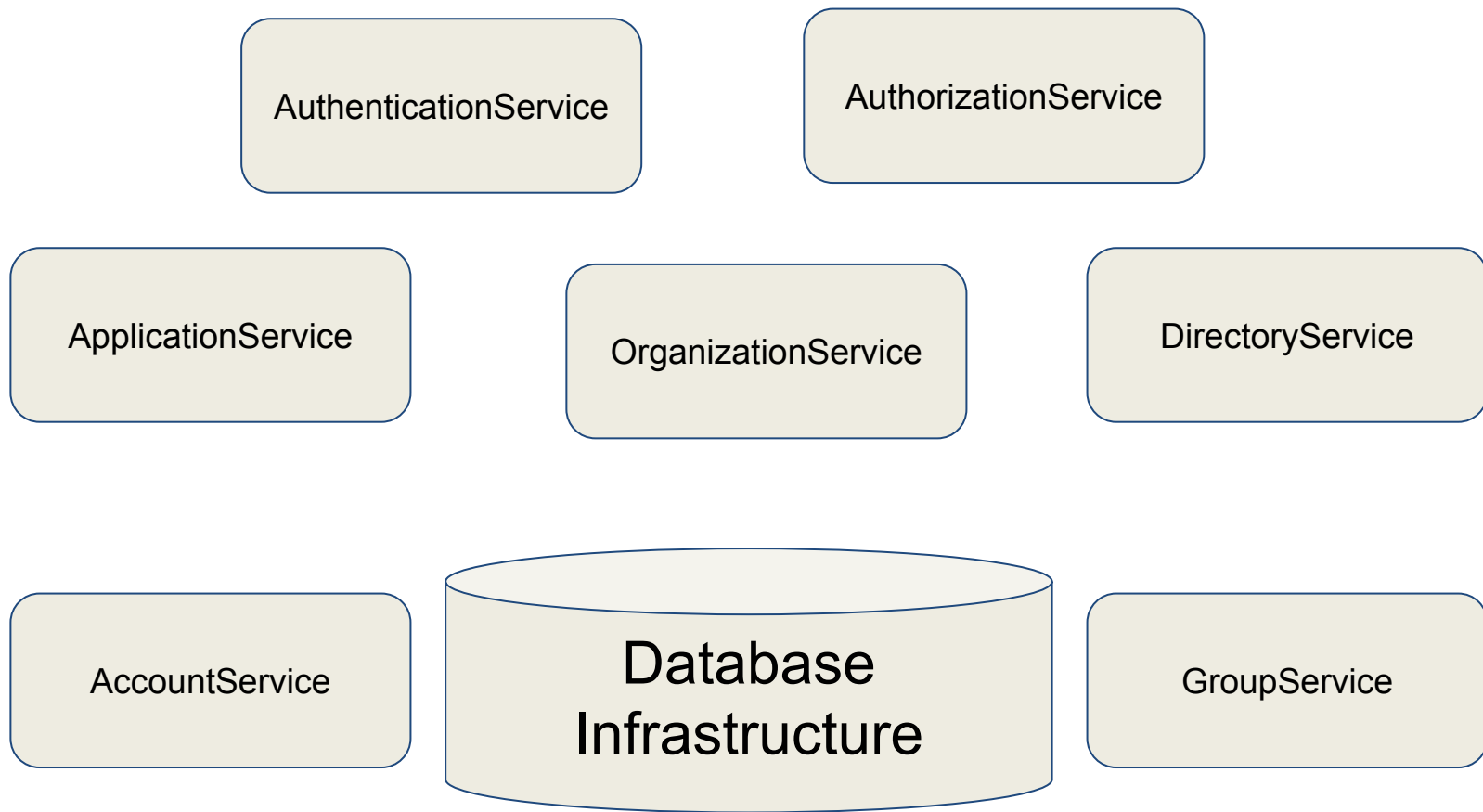
The diagram illustrates a Monolithic SOA architecture. It features a large, light beige rounded rectangle at the top containing a list of services: AuthenticationService, AuthorizationService, ApplicationService, OrganizationService, DirectoryService, AccountService, and GroupService. Below this rectangle 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

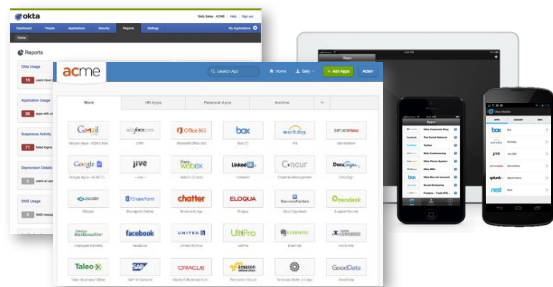


Employees,
Contractors



Identity & Mobility Service:

Identity Management
Mobility Management
Strong Authentication

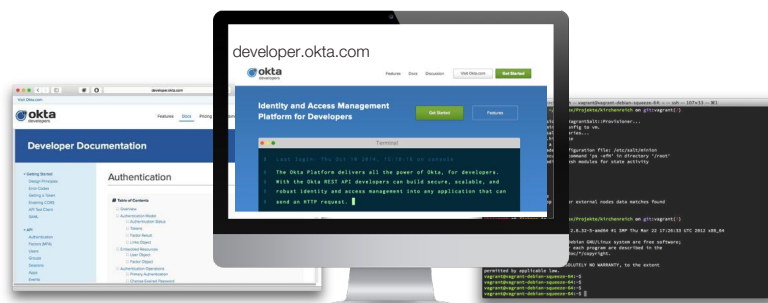


Partners,
Customers



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/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



The image features a blue background with a radial blur effect, creating a sense of motion. Scattered across the background are several semi-transparent circular patterns, each consisting of two concentric circles. In the center, the word "okta" is written in a white, lowercase, sans-serif font.

okta

Thank You