KONFERENZ + AUSSTELLUNG

Oracle Apex: Authentifizierung aus architektonischer Sicht

Mittwoch, 20. November 2024 (16:30 - 17:15)

Robert Marz
DATABEE
Die IT-Architekten

ANWENDERKONFERENZ.DOAG.ORG

Robert Marz – Independent Consultant

Primary Role

Senior Technical Architect
with database centric view of the world

DOAG
(German Oracle User Group)

Active Member of Database Community
Responsible for Cloud Topics

DATABEE
Die IT-Architekten

Databees.

SYM42

Oracle ACE Pro

@RobbieDatabee

https://robbie.databee.org

robert.marz@databee.org

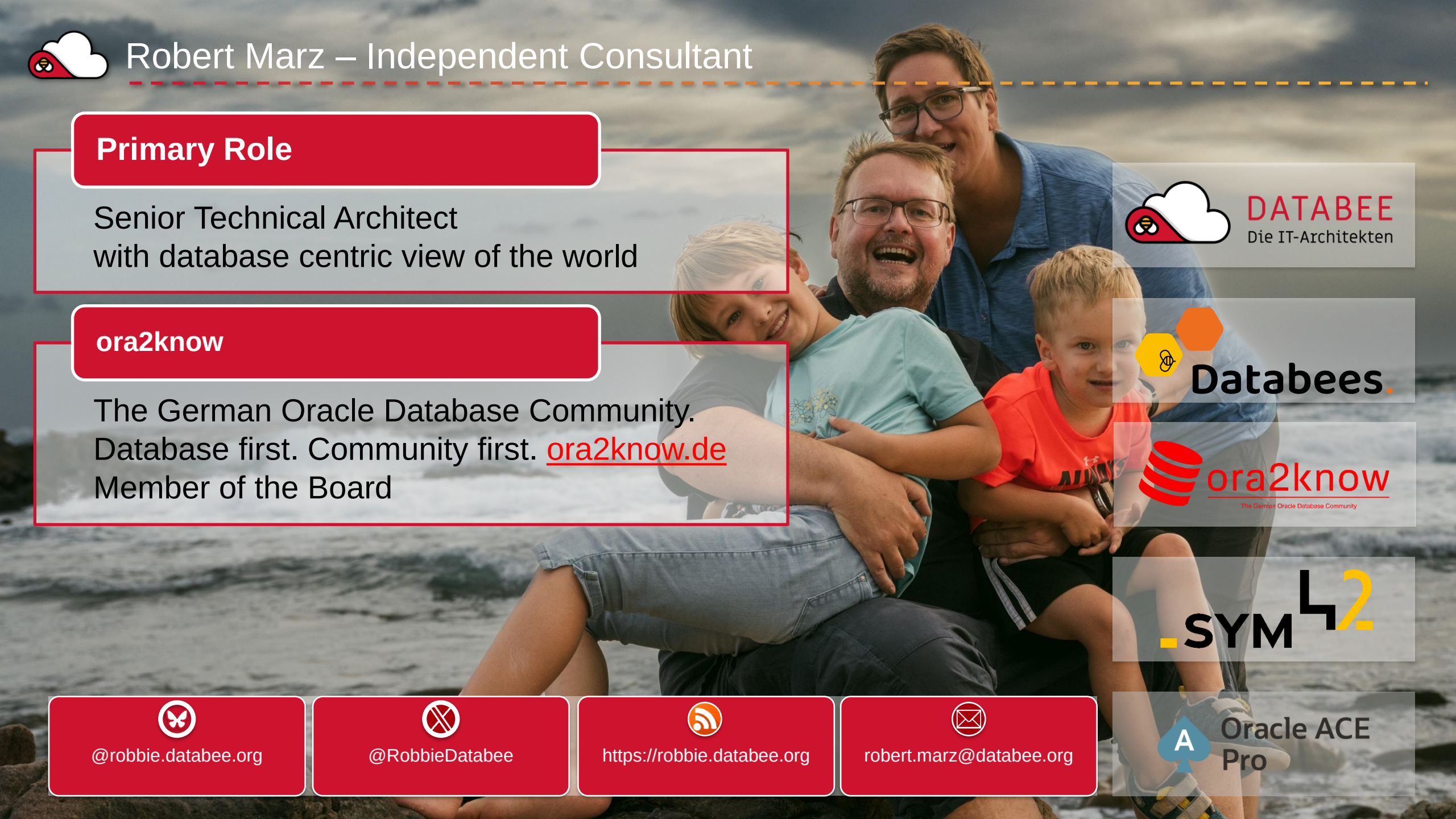
Robert Marz – Independent Consultant

Primary Role

Senior Technical Architect
with database centric view of the world

ora2know

The German Oracle Database Community.
Database first. Community first. ora2know.de
Member of the Board



DATABEE
Die IT-Architekten

Databees.

ora2know
The German Oracle Database Community

SYMLINK

Oracle ACE Pro

@robbie.databee.org

@RobbieDatabee

https://robbie.databee.org

robert.marz@databee.org

Eine starke Community für Oracle Datenbank Benutzer

Ziele: Wissensvermittlung für Entwickler und DBAs

Angebote: MeetUps, Podcasts, Live Events

Projekte: Veranstaltung zum Kennenlernen

Kontakt: info@ora2know.de

ora2know

The German Oracle Database Community

Oracle ACE

The Oracle ACE Program

400+ technical experts helping peers globally

- The Oracle ACE Program recognizes and rewards community members for their technical and community contributions to the Oracle community
- 3 membership levels: Director, Pro, and Associate
- Nominate yourself or a colleague at ace.oracle.com/nominate
- Learn more at ace.oracle.com

aceprogram_ww@oracle.com
Facebook.com/OracleACEs
@oracleace
Oracle ACE Program Group

.SYMPOSIUM 42

Created by the community, to support the community

Sharing of reliable knowledge
Supporting the various user groups and individuals

@sym_42

https://sym42.org/


Oracle APEX Authentication

Oracle APEX Authentication vs Authorization

Authentication

Who are you

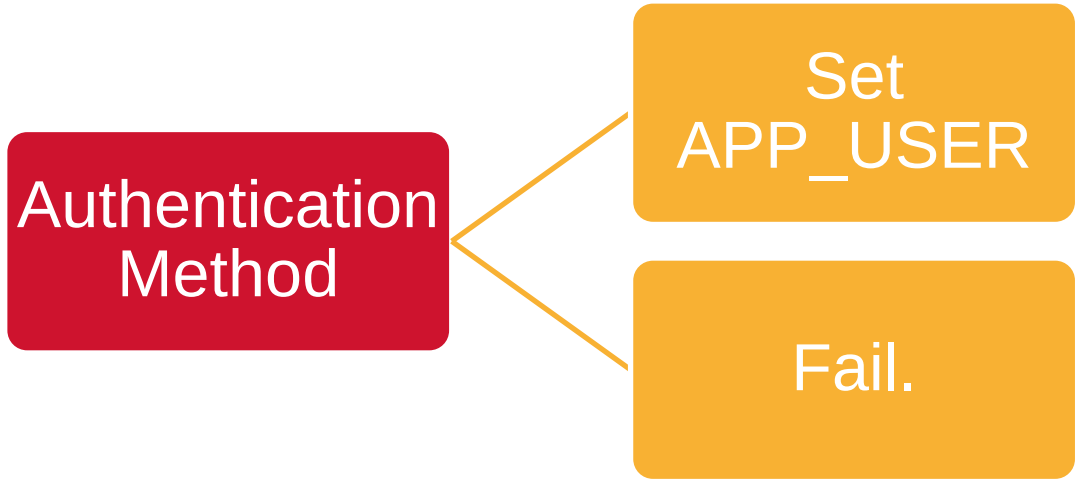
Identify yourself
e.g., with
username & password

Authorization

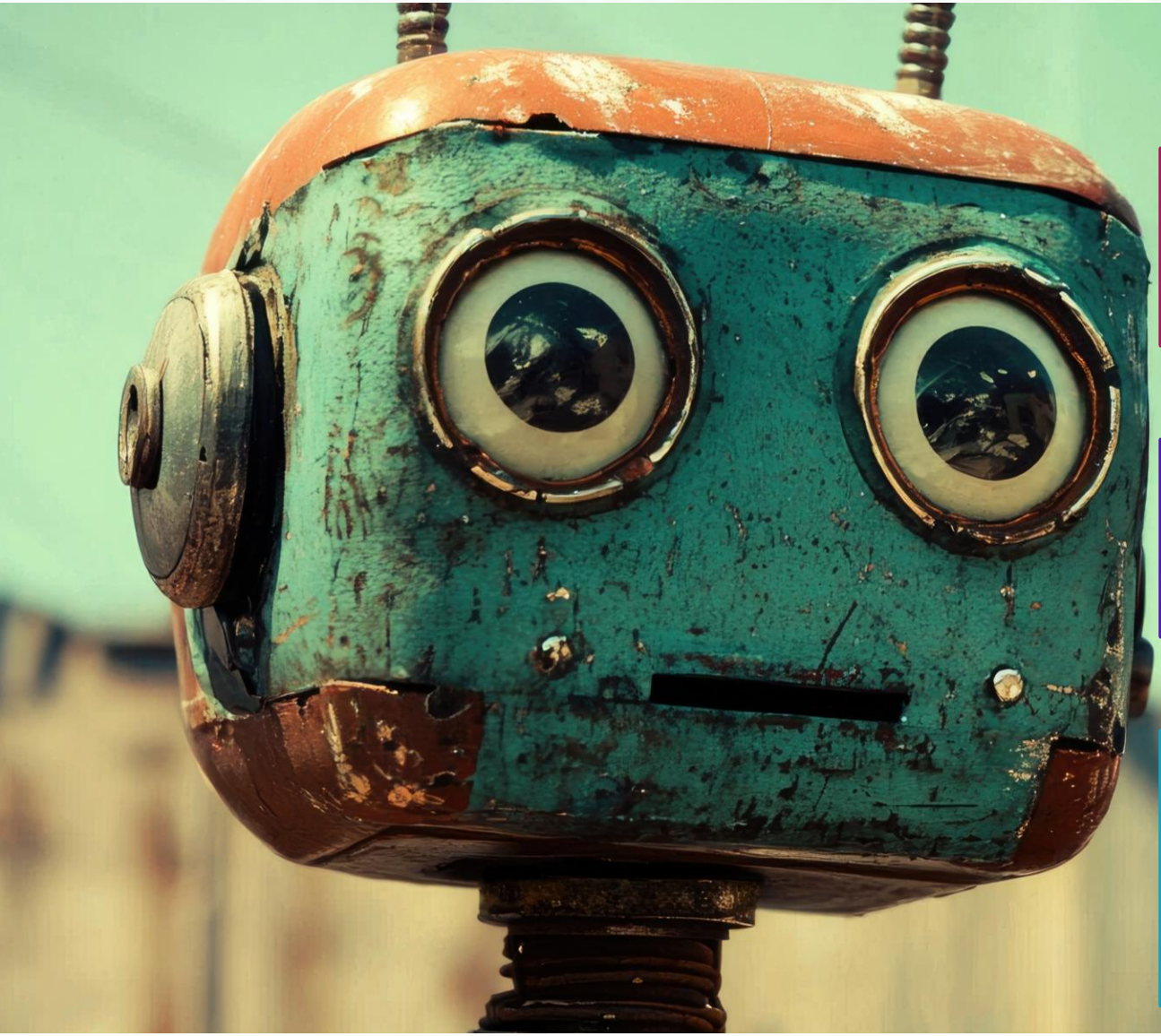
What permissions do you have

Stuff you allowed to do

Oracle APEX Authentication – Just one Job



Oracle APEX: Built-In Substitution String APP_USER



As a bind variable from either PL/SQL or SQL:

```
:APP_USER
```

From PL/SQL packages and triggers:

```
V('APP_USER')
```

As an attribute of the context APEX$SESSION:

```
sys_context(
'APEX$SESSION', 'APP_USER')
```

Oracle APEX Authentication Schemes

Builder Extension Sign-in

- The Extension Builder Sign-in enables users to log into an Extension App without having to sign-in again when already signed into a APEX session. The Extension Sign-in Authentication checks for a valid APEX session.

Custom Authentication

- Creating a Custom Authentication scheme from scratch to have complete control over your authentication interface.

Database Accounts

- Database Account Credentials authentication utilizes database schema accounts to authenticate users.

HTTP Header Variable

- Authenticate users externally by storing the username in a HTTP Header variable set by the web server.

Oracle APEX Authentication Schemes

Oracle Application Server Single Sign-On Server

- Delegates authentication to the Oracle AS Single Sign-On (SSO) Server. To use this authentication scheme, your site must have been registered as a partner application with the SSO server.

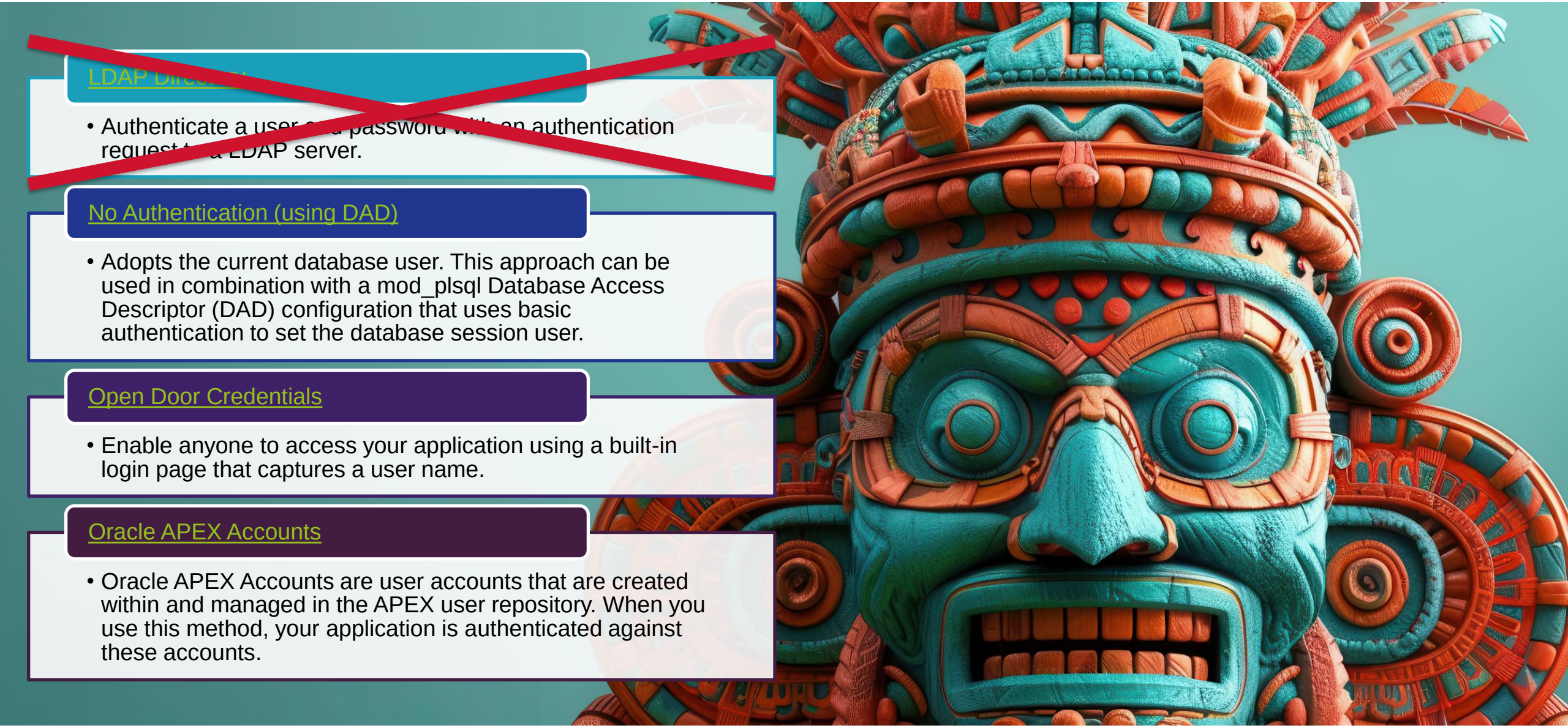
SAML Sign-In

- Delegates authentication to the Security Assertion Markup Language (SAML) Sign In authentication scheme.

Social Sign-In

- Social Sign-In supports authentication with Google, Facebook, and other social networks and enterprise identity providers that support OpenID Connect or OAuth2 standards.

Oracle APEX Authentication Schemes



LDAP Directory

- Authenticate a user and password with an authentication request to a LDAP server.

No Authentication (using DAD)

- Adopts the current database user. This approach can be used in combination with a mod_plsql Database Access Descriptor (DAD) configuration that uses basic authentication to set the database session user.

Open Door Credentials

- Enable anyone to access your application using a built-in login page that captures a user name.

Oracle APEX Accounts

- Oracle APEX Accounts are user accounts that are created within and managed in the APEX user repository. When you use this method, your application is authenticated against these accounts.

LDAP Directory Authentication Scheme – The Problem

Credentials

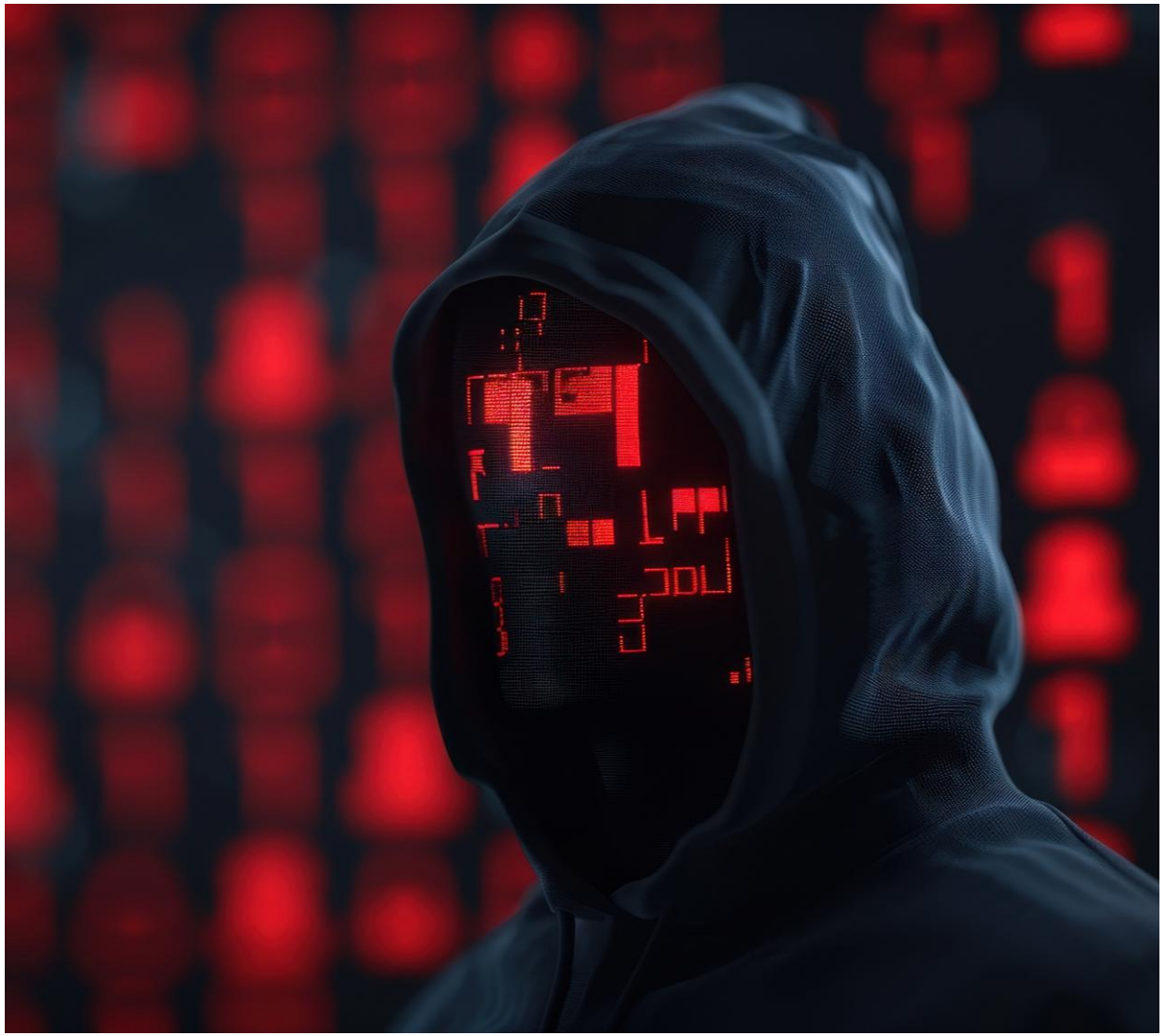
- collected by APEX app

LDAP

- Authenticates and Authorizes for multiple Apps across the Enterprise

Security Concerns

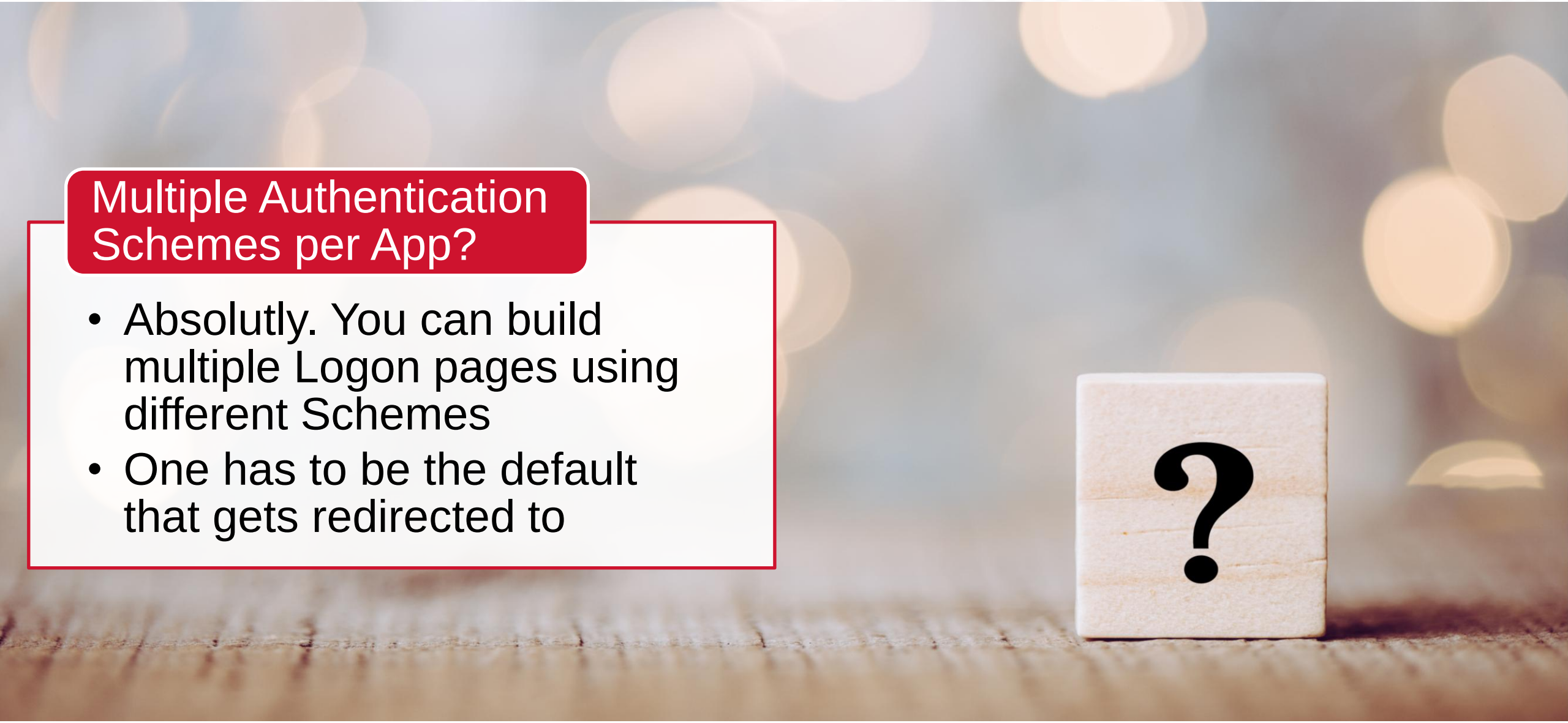
- User trust your app without knowing
- Potentially log & debug enterprise account credentials



Oracle APEX Authentication Schemes FAQ

Multiple Authentication Schemes per App?

- Absolutly. You can build multiple Logon pages using different Schemes
- One has to be the default that gets redirected to



Architectural Approach

Developers

- want to get the job done
- close their tickets
- try stuff out
- learn something interesting

- Energy & Expenses
- Knowledge
- Interest

IT Architects

- focus on user requirements
- fit solutions into enterprise landscape
- tries to reuse as much as possible
- considers security rules

- Requirements
- deployed base
- Re-use and integrate

Authentication Usecases

- Open Web App
- Internal App with restricted Access
- Internet App with Registration
- Intranet App with SSO
- Many more

Usecase Open Web-App

Every one is allowed to access

e.g. Newspage or Info-Screen

No authentication needed

Assuming a default Username

Open Door Credentials

Usecase Internet App with Registration

App is exposed to the Internet

Everyone can register

Custom Authentication Scheme

you are responsible for storing username and passwords secure (only salted hashes!!)

attractive target for hackers

Social Sign-In

Let others do the dangerous part

Usecase Internal App with restricted Access

Intranet App

Read mostly, very limited editing

- shared group passwords

Speciality App with Power Users

- Very small Number of well known users

Authentication Schemes

- Database Accounts (not really)
- Apex Accounts
- Custom Scheme
- SSO (SAML or Social Sign-In)

Usecase Intranet App many Users

Intranet App

- many users
- different roles and rights

Authentication Schema

- SSO
  - SAML
  - Social-Sign-In (MS Entra ID and co)

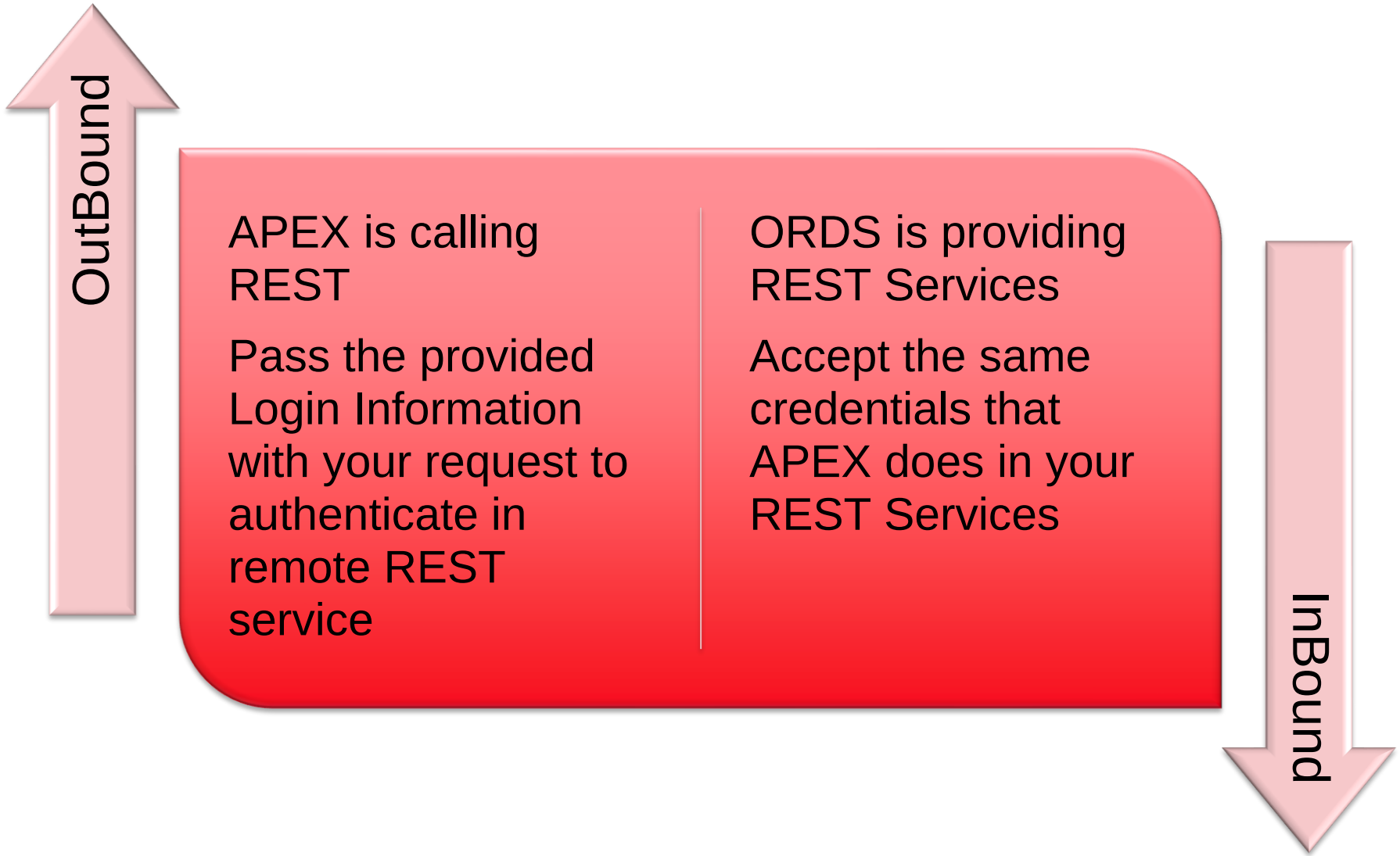
The Architects choice

Architect (me) suggests (mostly)

- Open Door Credentials
- SSO

Sharing Auth between APEX and REST

REST & APEX Scenarios



Two Scenarios, One Solution: JWTs

JWT (JSON Web Token)

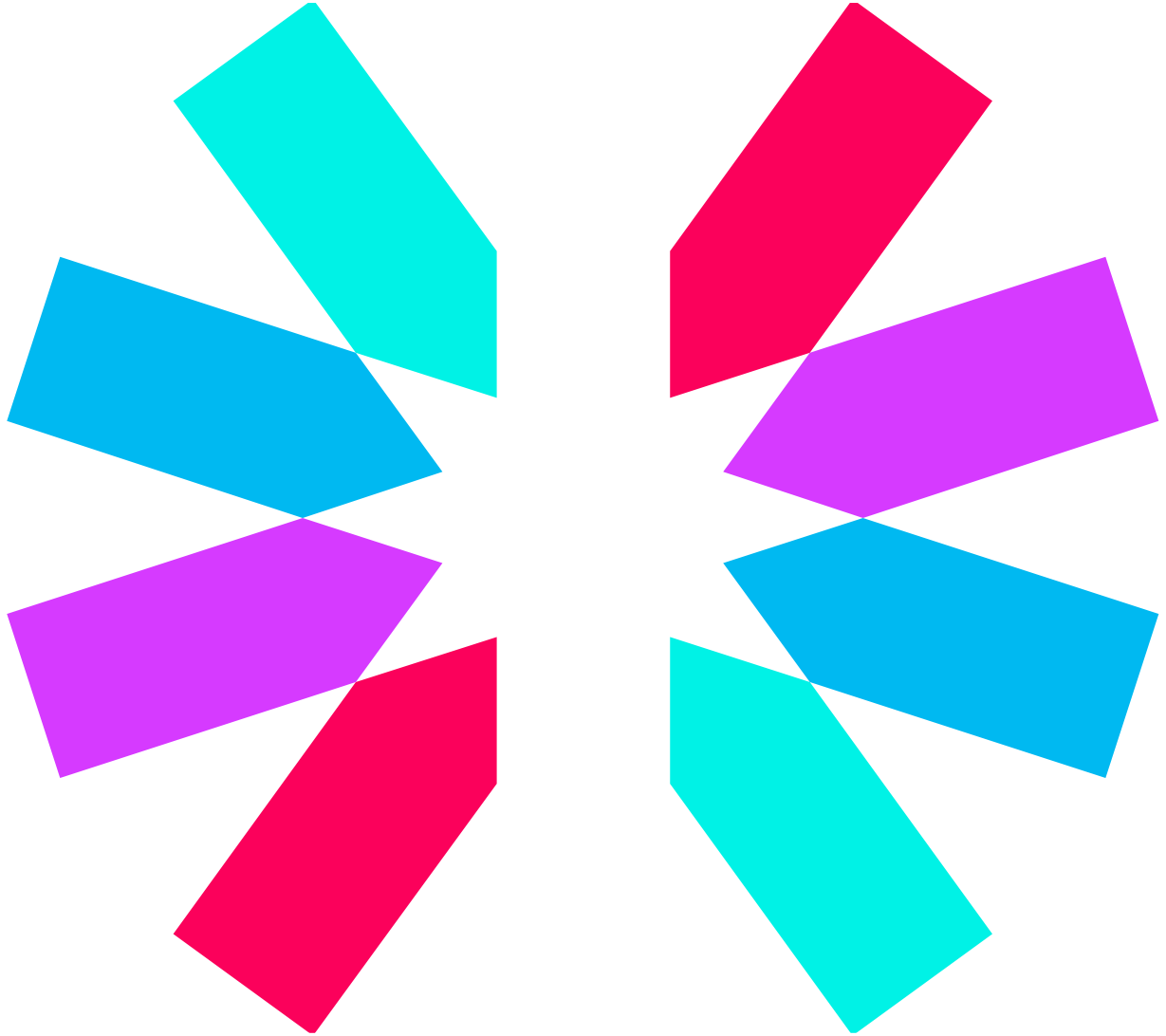
- industry standard RFC 7519
- represent claims securely between two parties

JSON

- Base64 encoded
- Sections:
  - Header
  - Payload
  - Signature

Transport

- http header field
- Authentication: Bearer {{token}}

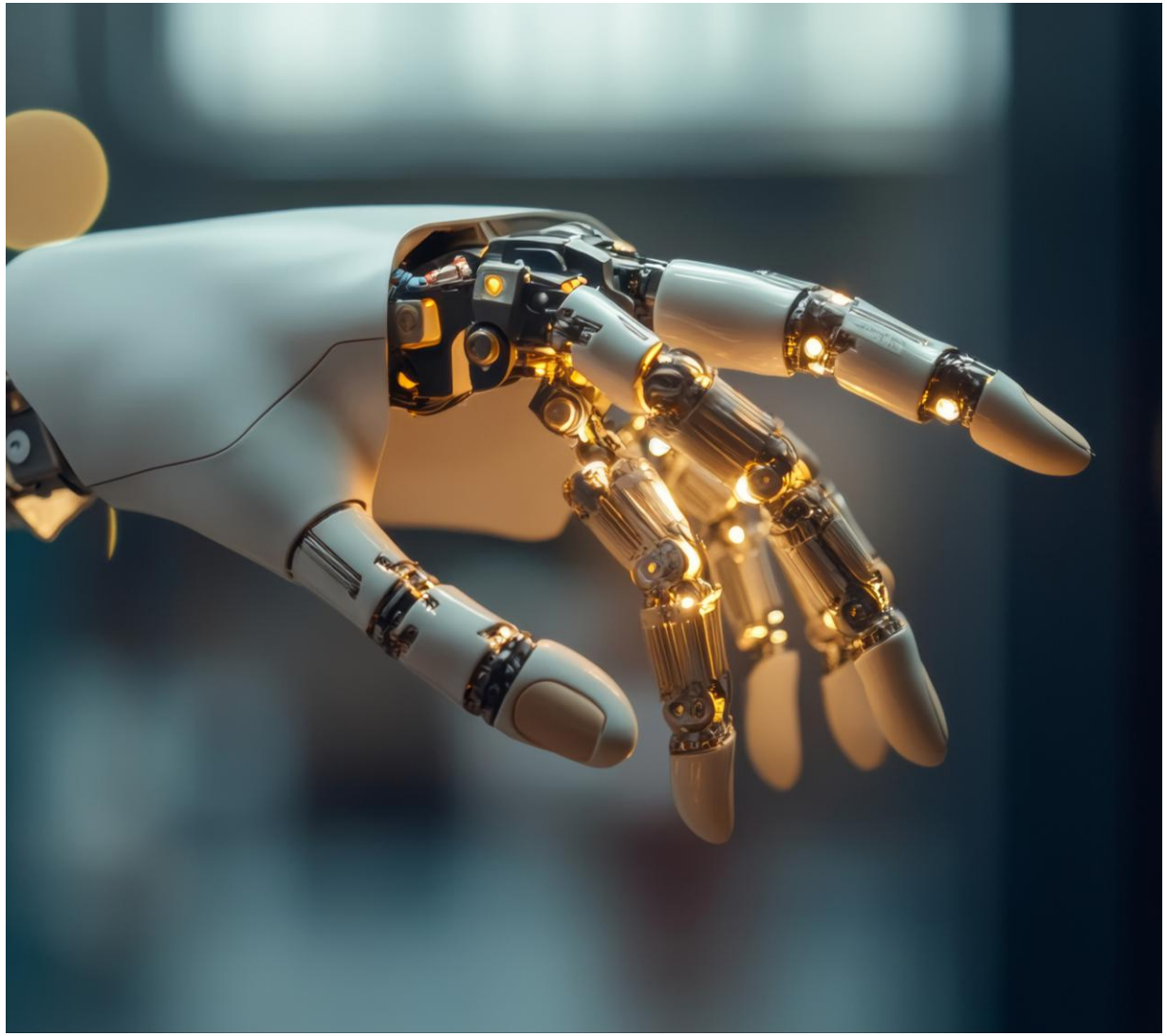


Java Web Token – How it works


```
{
  "exp": 1732104719,
  "iat": 1732102919,
  "jti": "874be9ae-b186-4684-af50-f1cfa726e581",
  "iss": "https://host.examle.com/realms/tenant1",
  "sub": "5db8e25d-21c7-4cd4-ac1e-a26832b46850",
  "typ": "Bearer",
  "azp": "Dispo",
  "session_state": "8af6a246-7277-4216-b660-4c44b95a5c20",
  "acr": "1",
  "allowed-origins": [
    "https://host.examle.com/Acceptance/dispoManager/",
    "http://localhost:5000",
    "https://host.examle.com/dispoManager/"
  ],
  "scope": "openid email profile",
  "sid": "8af6a246-7277-4216-b660-4c44b95a5c20",
  "name": "Robert Marz",
  "groups": ["/Dispatcher","/Technican"],
  "preferred_username": "postman-test-user-03",
  "given_name": "Robert",
  "family_name": "Marz",
  "email": "robert.marz@databee.org"
}
```


Client	establishes Session with ID Provider
	Receives Bearer Token with Claims
	Sends Token as http-header to Server
Server	Decodes Token
	Validate Token (online or offline)
	Extracts Information: Username; Full-Name; Groups

JWTs and Apex



Apex

- Built-In Support

Social-Sign-In Auth Scheme

- social networks and enterprise identity providers that support OpenID Connect or OAuth2 standards
  - - MS Entra ID (ex Azure Active Directroy)
  - - KeyCloak
  - …

JWTs and REST outbound

```
/* We want to mimic this curl command in PL/SQL.
curl --request POST 'https://host.example.com/cool/service' \
--header 'Authorization: Bearer eyJhbGciOiJI ... '
*/

DECLARE
  l_response      CLOB;
  jwt_token       VARCHAR2(32000) := 'eyJhbGciOiJI ... ';
BEGIN
  -- Set the Request HTTP Headers.
  apex_web_service.set_request_headers
   (p_name_01  => 'Authorization',
    p_value_01 => 'Bearer ' || jwt_token,
    p_reset    => TRUE);

  -- Call API using Username and Password.
  l_response := apex_web_service.make_rest_request
    (p_url                  => 'https://dummyjson.com/auth/login',
     p_http_method          => 'POST');
END;
```

JWTs and REST inbound

Parse incoming JWT

Package APEX_JWT

- encode
- decode
- validate – no session verification!

Check if Session is valid

online: REST call to ID Provider

offline: check signature against public key

Make user details available

Set package Variables

set session context

ORDS Pre Hook

ORDS Pre Hook

PL/SQL function called before every ORDS Request

returns boolean

- true: all good
- false: HTTP status 403 forbidden
- unavailable: HTTP status 500 internal error

Configure

per connecton pool

ords setting procedure.rest.preHook

→ Perfect place for JWT validation

ORDS PreHook best Practices

small pre_hook function

- place in schema on its own
- standalone function (no package)
- call pre_hooks function in REST-enabled-Schema
- return true if not needed

pre_hooks

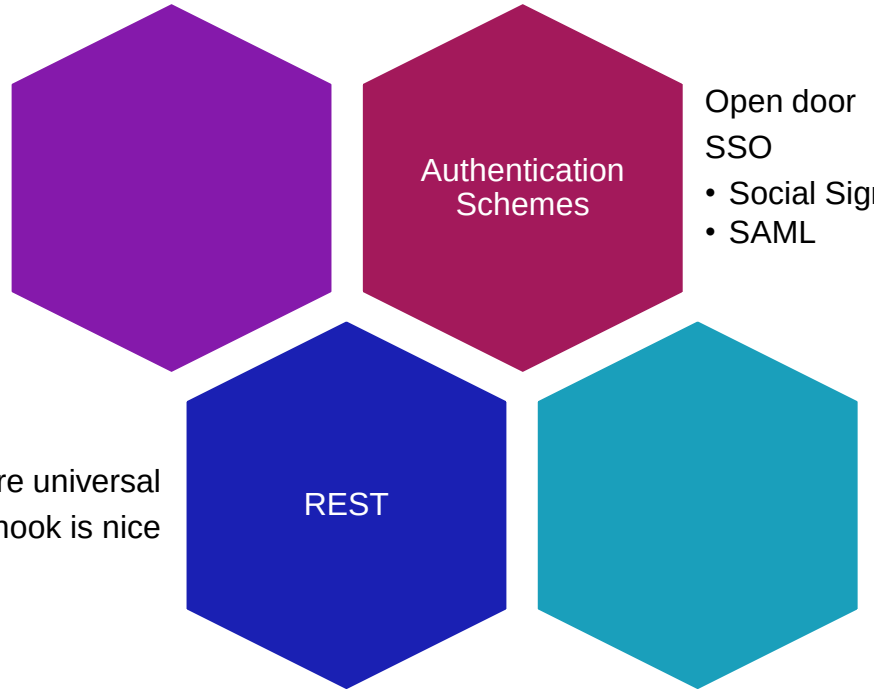
- for every REST enabled schemas
- or even for every module
- put in package

Be careful

- defect pre_hook stops REST Services and Apex for your ords-pool

Apex & REST JWT Auth: Demo

Apex Authentication the architectural approach



Open door

SSO

- Social Sign-in
- SAML

JWTs are universal

ORDS pre_hook is nice

ora2know

The German Oracle Database Community