

Apex-Anwendungen im Internet

- aber sicher -

Jochen Kutscheruk

Oracle Certified Master

merlin.zwo InfoDesign GmbH & Co. KG

76228 Karlsruhe



Spitzenleistung heißt, sich auf seine Stärken zu konzentrieren.

merlin.zwo

Wir machen Oracle - nur Oracle.
Aus gutem Grund.

www.merlin-zwo.de



★★★★★
WANTED

~~DEAD~~ || **ALIVE**



CACHE REWARD



#F4240\$



Oracle DBA

(m/w/d/...)

und

Oracle Developer

(m/w/d/...)

SQL, PL/SQL, Apex

★★★★★
WANTED

~~DEAD~~ || **ALIVE**



CACHE REWARD



#F4240\$



Der Klassiker: SQL Injection

SSP: Session State Protection

Oracle APEX: Struktureller Aufbau

Aufgabentrennung

Konfiguration Apache, Tomcat, ORDS

Unerwünschte Zugriffe verhindern

Der Klassiker: SQL Injection

Haben Sie Ihren Sohn wirklich "Robert'); DROP TABLE SCHUELER;" genannt?

HI, THIS IS
YOUR SON'S SCHOOL.
WE'RE HAVING SOME
COMPUTER TROUBLE.



OH, DEAR – DID HE
BREAK SOMETHING?
IN A WAY—



DID YOU REALLY
NAME YOUR SON
Robert'); DROP
TABLE Students;-- ?



OH. YES. LITTLE
BOBBY TABLES,
WE CALL HIM.

WELL, WE'VE LOST THIS
YEAR'S STUDENT RECORDS.
I HOPE YOU'RE HAPPY.



AND I HOPE
YOU'VE LEARNED
TO SANITIZE YOUR
DATABASE INPUTS.

Nur ein Witz?

Es soll ja Witzbolde geben

<https://beta.companieshouse.gov.uk/>

Search the register

Enter company name, number or officer name

DROP TABLE



; DROP TABLE "COMPANIES";-- LTD

Company number **10542519**

Follow this company

File for this company

Overview

Filing history

People

Registered office address

**1 Moyes Cottages Bentley Hall Road, Capel St. Mary, Ipswich,
Suffolk, United Kingdom, IP9 2JL**

Company status

Active

Company type

Private limited Company

Incorporated on

29 December 2016

<https://www.domain.de/index.php?userid=7>

```
SELECT username  
FROM Tabelle  
WHERE ?
```



```
SELECT username  
FROM Tabelle  
WHERE userid=7
```

[https://www.domain.de/index.php?\(userid=7 or 1=1\)](https://www.domain.de/index.php?(userid=7 or 1=1))

```
SELECT username  
FROM Tabelle  
WHERE ?
```



```
SELECT username  
FROM Tabelle  
WHERE (userid=7 or 1=1)
```

SSP: Session State Protection

Leider schon viel zu häufig gesehen (nicht nur in APEX-Programmen):

https://www.domain.de/run_report?name=rechnung&format=pdf&Rechnung_Nr=22197863

Typische URL in Apex:

https://apex.oracle.com/pls/apex/f?p=12485:2:9641413517030::NO::P2_ID:1

https://apex.oracle.com/pls/apex/f?p=12485:2:9641413517030::NO::P2_ID:1

▼

Sicherheit

Autorisierungsschema	<div>- Auswählen -</div>	>
Authentifizierung	Seite benötigt Authentifizierung	▼
Sessions erneut beitreten	Anwendungsstandardwert	▼
Deeplinking	Anwendungsstandardwert	▼
Schutz für den Seitenzugriff	Argumente müssen Prüfsumme haben	▼

https://apex.oracle.com/pls/apex/f?p=12485:2:9641413517030::NO::P2_ID:1&cs=3JK1vvvssFLIicqDAkyzdSfBa6nVe3liugA3nm2mV6Z4foHT1v7O68rX05xPcAlZ4X3vPH89UiJJyNherMxuKw

https://apex.oracle.com/pls/apex/f?p=12485:2:9641413517030::NO::P2_ID:2&cs=3JK1vvvssFLiicqDAkyzdSfBa6nVe3liugA3nm2mV6Z4foHT1v7O68rX05xPcAlZ4X3vPH89UiJJyNherMxuKw



The checksum computed on the request,
clear cache, argument names, and
argument values (P2_ID2

[aPO_ouazlOLu5sz92WDIXLQ_3ysUIhGQN35rG8HByqjbsYdEJkXfesXZ7fCMhpII1R8uYTeIU3ZBT4qfF4gCEw])
did not match the checksum passed into the
show procedure

(JK1vvvssFLiicqDAkyzdSfBa6nVe3liugA3nm2mV6Z4foHT1v7O68rX05xPcAlZ4X3vPH89UiJJyNherMxuKw).

Note: End users get a different error
message.

Contact your application administrator.

SSP: Session State Protection auf Elementebene

▼ Sicherheit

Autorisierungssche

Schutz für den
Sessionzustand

Uneingeschränkt

Prüfsumme erforderlich: Anwendungsebene

Prüfsumme erforderlich: Benutzerebene

✓ Prüfsumme erforderlich: Sessionebene

Eingeschränkt: Darf nicht vom Browser festgelegt werden

Wert

verschlüsselt in
Sessionzustand
speichern

Ja

Nein

```
<input type="hidden" data-for="P3_SELECTED_NODE" value="lP_484j-  
ahXMtZmq3nXVhnsSraoQ_uLuTyMayLrM0FOSROFiImzRjE5fesqRUV0321iOk5Bdsqce8JwCOR47bQ">
```

Eingeschränkte
Zeichen

✓ Alle Zeichen können gespeichert werden.

Weiße Liste für a-Z, 0-9 und Leerzeichen

HTML-Befehlszeichen (<>) auf schwarze Liste setzen

&<>"/;,*|= % und -- auf schwarze Liste setzen

&<>"/;,*|= % oder -- und Zeilenendmarke auf schwarze Liste setzen

Steuerelemente für den Statusschutz der Anwendungssession

Durch den Schutz für den Sessionzustand kann verhindert werden, dass Hacker die URLs Ihrer Anwendung ändern, was Programmlogik, Inhalt des Sessionzustands und Datenschutz gefährdet.

Um den Schutz mithilfe eines Assistenten zu aktivieren, zu deaktivieren oder zu konfigurieren, klicken Sie auf **Schutz festlegen**.

Anwendung: **17852 - Sample Trees** ?

Schutz für den Sessionzustand: **Aktiviert** ?

Schutzeinstellungen für vorhandenen Sessionzustand

Seiten >		Seitenelemente >		Anwendungselemente >	
Seitenzugriff	Seiten	Elementzugriffsebene	Elemente	Elementzugriffsebene	Elemente
Argumente müssen eine Prüfsumme haben	10	Eingeschränkt: Darf nicht vom Browser festgelegt werden	2	Uneingeschränkt	1
Keine Argumente zulässig	1	Prüfsumme erforderlich: Sessionebene	36		

Schutz festlegen >

SSP: Session State Protection auf Anwendungsebene - Seiten



Schutz für den Sessionzustand: Aktiviert ?				
<div><div>Q ▼</div><div></div><div>Los</div><div><div><div></div></div><div></div></div><div>Aktionen ▼</div></div>				
Seite ↑ ≡	Name	Schutz für den Seitenzugriff	Seitenelemente	Seitentyp
1	Home	Argumente müssen Prüfsumme haben	0	Home
2	Manage Sample Data	Argumente müssen Prüfsumme haben	0	Statische HTML
3	Project Tracking	Argumente müssen Prüfsumme haben	1	Navigationsformular
4	Help	Argumente müssen Prüfsumme haben	0	Bericht
5	Administration	Argumente müssen Prüfsumme haben	0	Navigationsseite
6	Project Dashboard	Argumente müssen Prüfsumme haben	0	Navigationsseite
7	Create/Edit Project	Argumente müssen Prüfsumme haben	7	DML-Form
8	Application Theme Style	Argumente müssen Prüfsumme haben	1	Dynamische Form
9	Create/Edit Tasks	Argumente müssen Prüfsumme haben	13	DML-Form
10	Modify Subtask Information	Argumente müssen Prüfsumme haben	14	DML-Form
101	Login	Keine Argumente zulässig	2	Dynamische Form

1 - 11

SSP: Session State Protection auf Anwendungsebene - Seitenelemente

Schutz für den Sessionzustand: **Aktiviert** ?

Q v

Los

Aktionen v

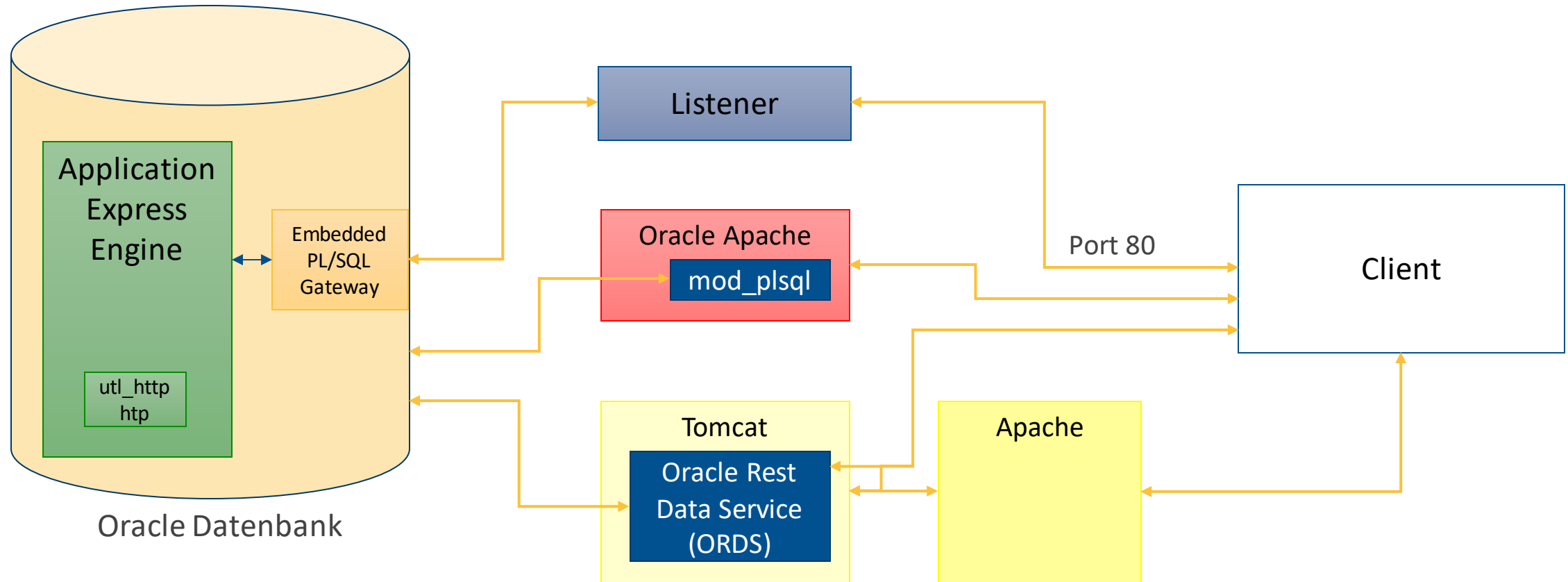
Seite ↑≡	Seitenname	Objektname	Sequenz	Region	Elementschutz für den Sessionzustand	Seitenschutz
3	Project Tracking	P3_SELECTED_NODE	10	Task Tree	Prüfsumme erforderlich: Sessionebene	C
7	Create/Edit Project	P7_STATUS	70	Create/Edit Project	Prüfsumme erforderlich: Sessionebene	C
7	Create/Edit Project	P7_COMPLETION_DATE	50	Create/Edit Project	Prüfsumme erforderlich: Sessionebene	C
7	Create/Edit Project	P7_UPDATED	80	Create/Edit Project	Prüfsumme erforderlich: Sessionebene	C
7	Create/Edit Project	P7_ESTIMATED_COMPLETION	40	Create/Edit Project	Prüfsumme erforderlich: Sessionebene	C
7	Create/Edit Project	P7_START_DATE	30	Create/Edit Project	Prüfsumme erforderlich: Sessionebene	C
7	Create/Edit Project	P7_PROJECT_NAME	20	Create/Edit Project	Prüfsumme erforderlich: Sessionebene	C
7	Create/Edit Project	P7_PROJ_ID	10	Create/Edit Project	Prüfsumme erforderlich: Sessionebene	C
8	Application Theme Style	P8_DESKTOP_THEME_STYLE_ID	10	items	Prüfsumme erforderlich: Sessionebene	C
9	Create/Edit Tasks	P9_TASK_ASSIGN	110	Create/Edit Tasks	Prüfsumme erforderlich: Sessionebene	C
9	Create/Edit Tasks	P9_TASK_STATUS	80	Create/Edit Tasks	Prüfsumme erforderlich: Sessionebene	C
9	Create/Edit Tasks	P9_TASK_PRIORITY	70	Create/Edit Tasks	Prüfsumme erforderlich: Sessionebene	C
9	Create/Edit Tasks	P9_TASK_COMP	60	Create/Edit Tasks	Prüfsumme erforderlich: Sessionebene	C
9	Create/Edit Tasks	P9_TASK_EST_COMP	50	Create/Edit Tasks	Prüfsumme erforderlich: Sessionebene	C
101	Login	P101_USERNAME	10	&APP_NAME.	Eingeschränkt: Darf nicht vom Browser festgelegt werden	U
101	Login	P101_PASSWORD	20	&APP_NAME.	Eingeschränkt: Darf nicht vom Browser festgelegt werden	U

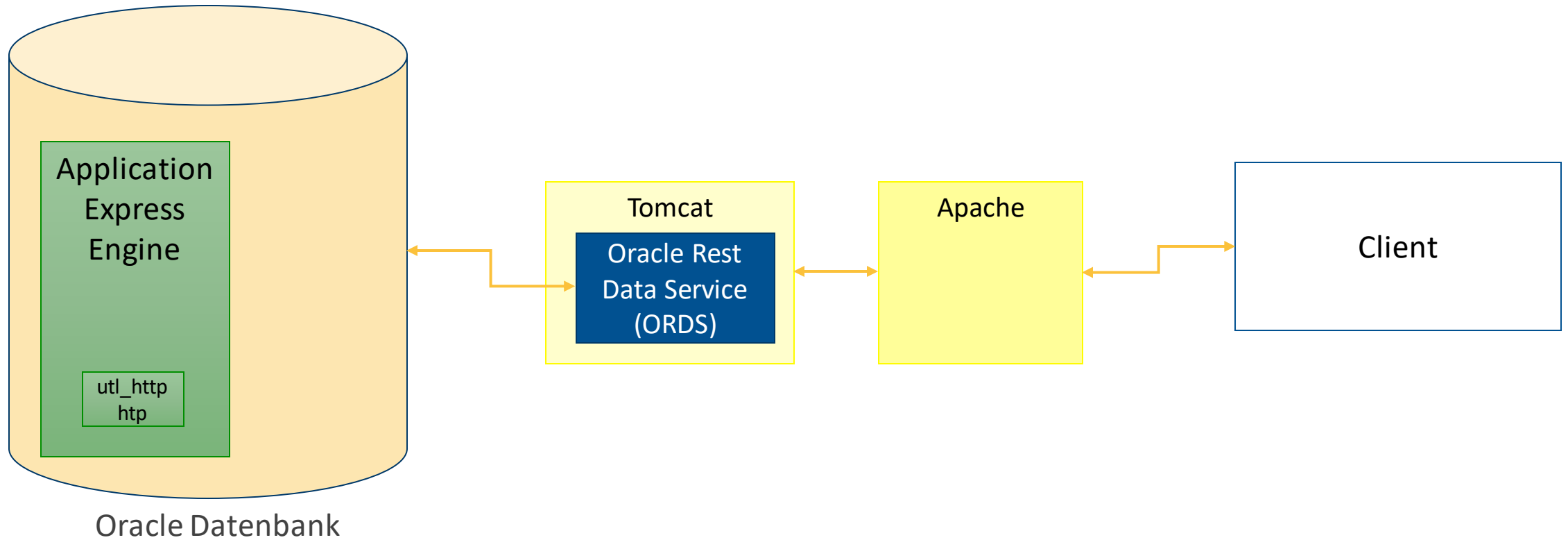
Weitergehende, ausführlichere Beschreibung

Vortrag von Denes Kubicek DOAG Konferenz 2014:

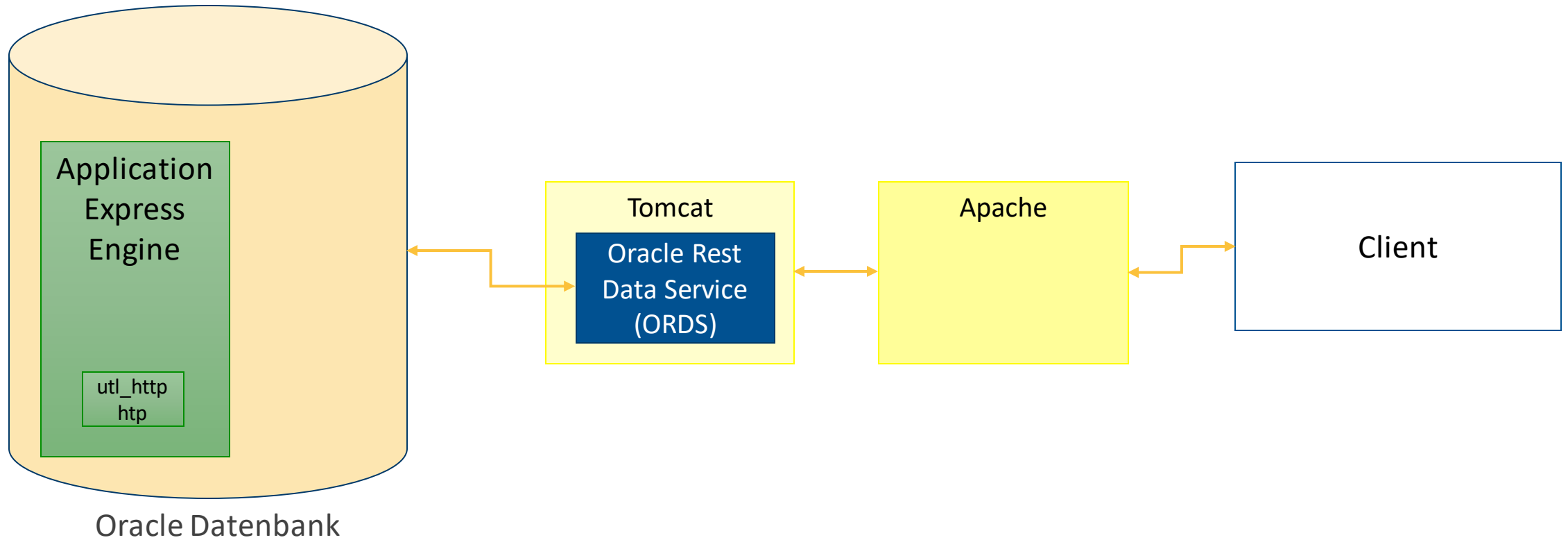
[https://www.doag.org/formes/pubfiles/6459628/2014-DEV-Denes_Kubicek-APEX_Security -
_Wie sicher sind Ihre Anwendungen -Praesentation.pdf](https://www.doag.org/formes/pubfiles/6459628/2014-DEV-Denes_Kubicek-APEX_Security_-_Wie_sicher_sind_Ihre_Anwendungen_-_Praesentation.pdf)

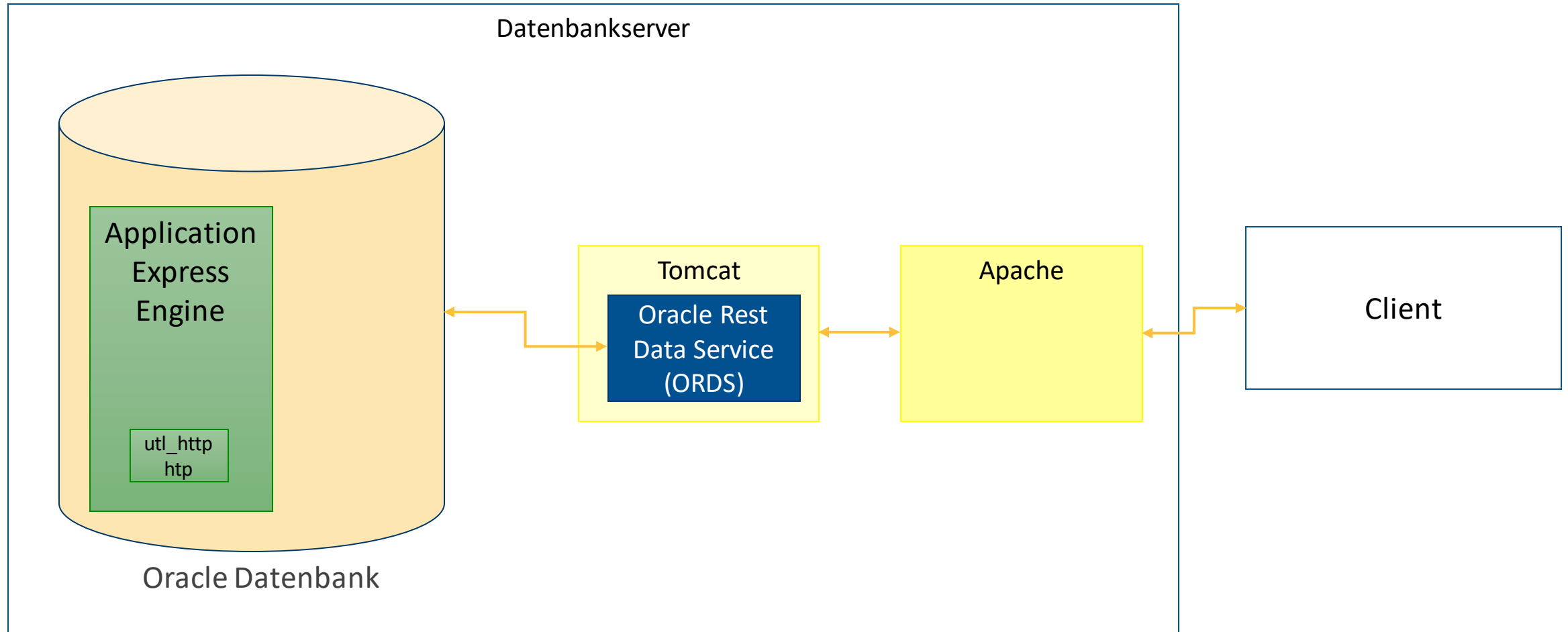
Oracle APEX: Struktureller Aufbau

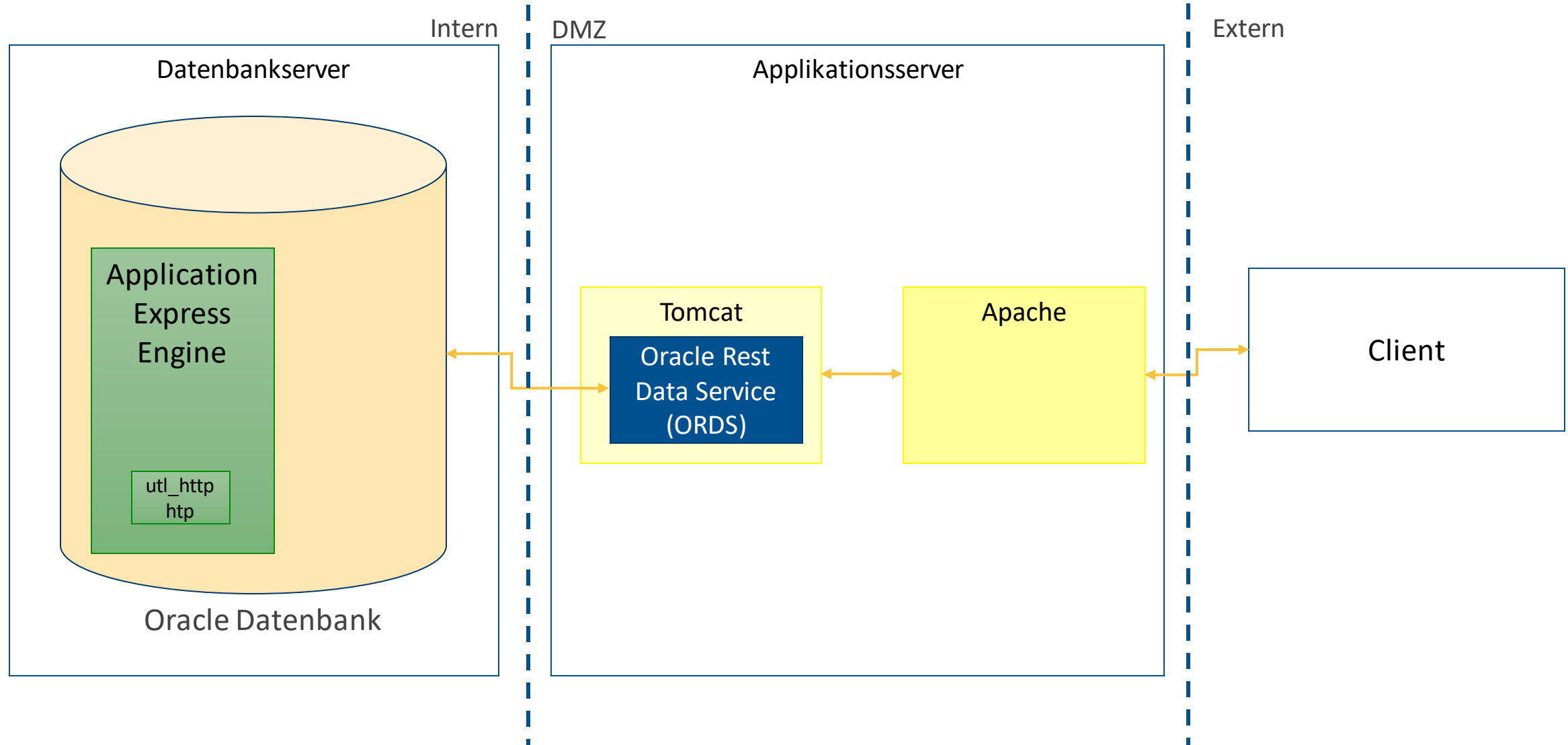


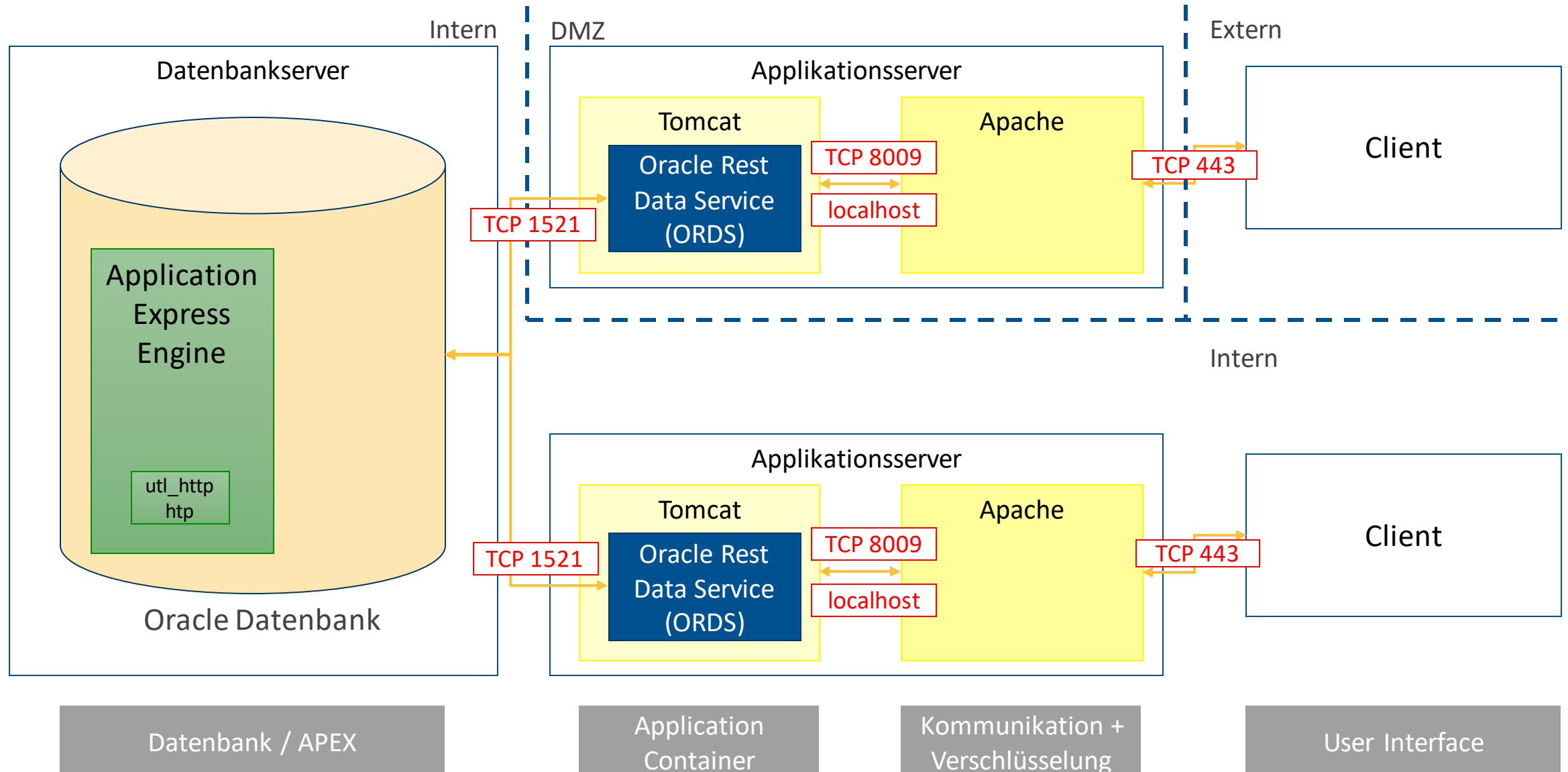


Aufgabentrennung

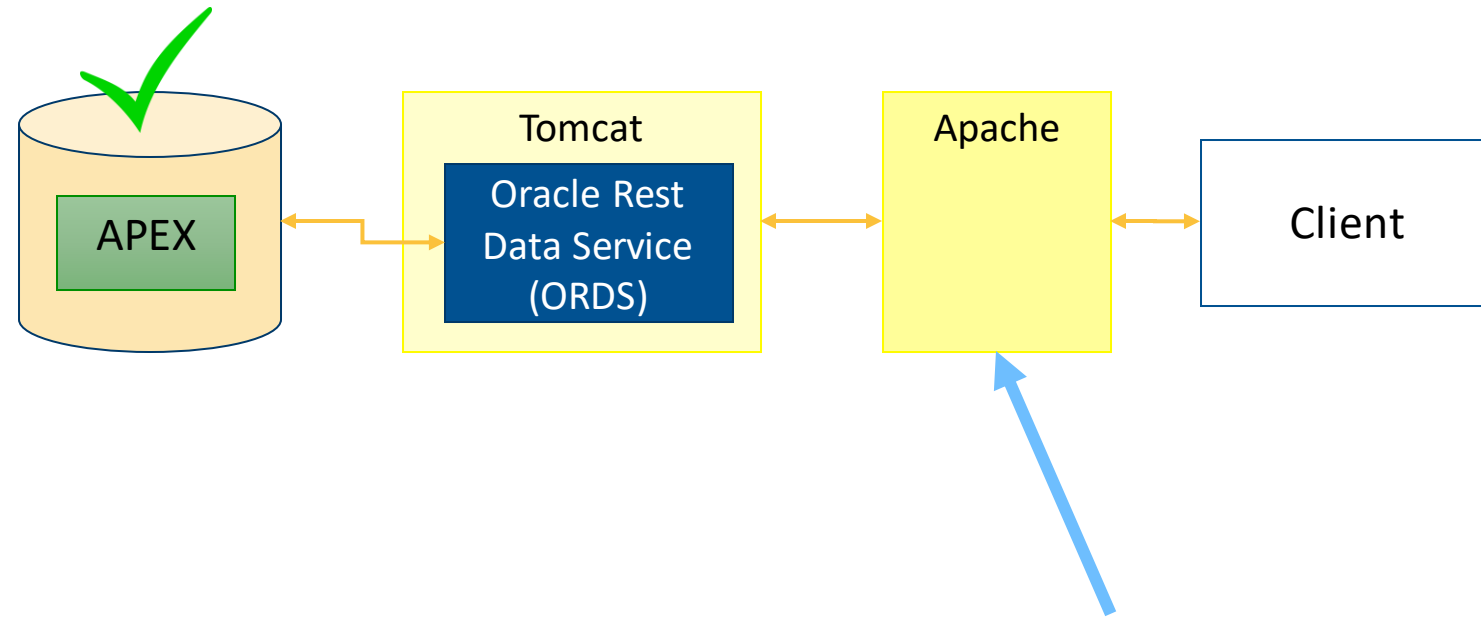








Konfiguration Apache, Tomcat und ORDS



Kommunikation verschlüsseln (https)

/etc/httpd/conf.d/ssl.conf:

```
<VirtualHost *:443>
    SSLEngine on

# SSL Zertifikate
    SSLCertificateFile ?
    SSLCertificateKeyFile ?
    SSLCertificateChainFile ?

# SSL Einstellungen
    SSLProtocol ?
    SSLCipherSuite ?
</VirtualHost>
```

Woher kommt das Zertifikat?

SSLCertificateFile ?

SSLCertificateKeyFile ?

SSLCertificateChainFile ?



Let's Encrypt

[Dokumentation](#)

[Hilfe bekommen](#)

[Spenden ▾](#)

[Über uns ▾](#)

[Sprachen ▾](#)

Let's Encrypt ist eine **freie, automatisierte** und **offene** Zertifizierungsstelle.

<https://letsencrypt.org/de/>

 <https://www.merlin-zwo.de>

 DST Root CA X3
↳  Let's Encrypt Authority X3
↳  **www.merlin-zwo.de**



www.merlin-zwo.de

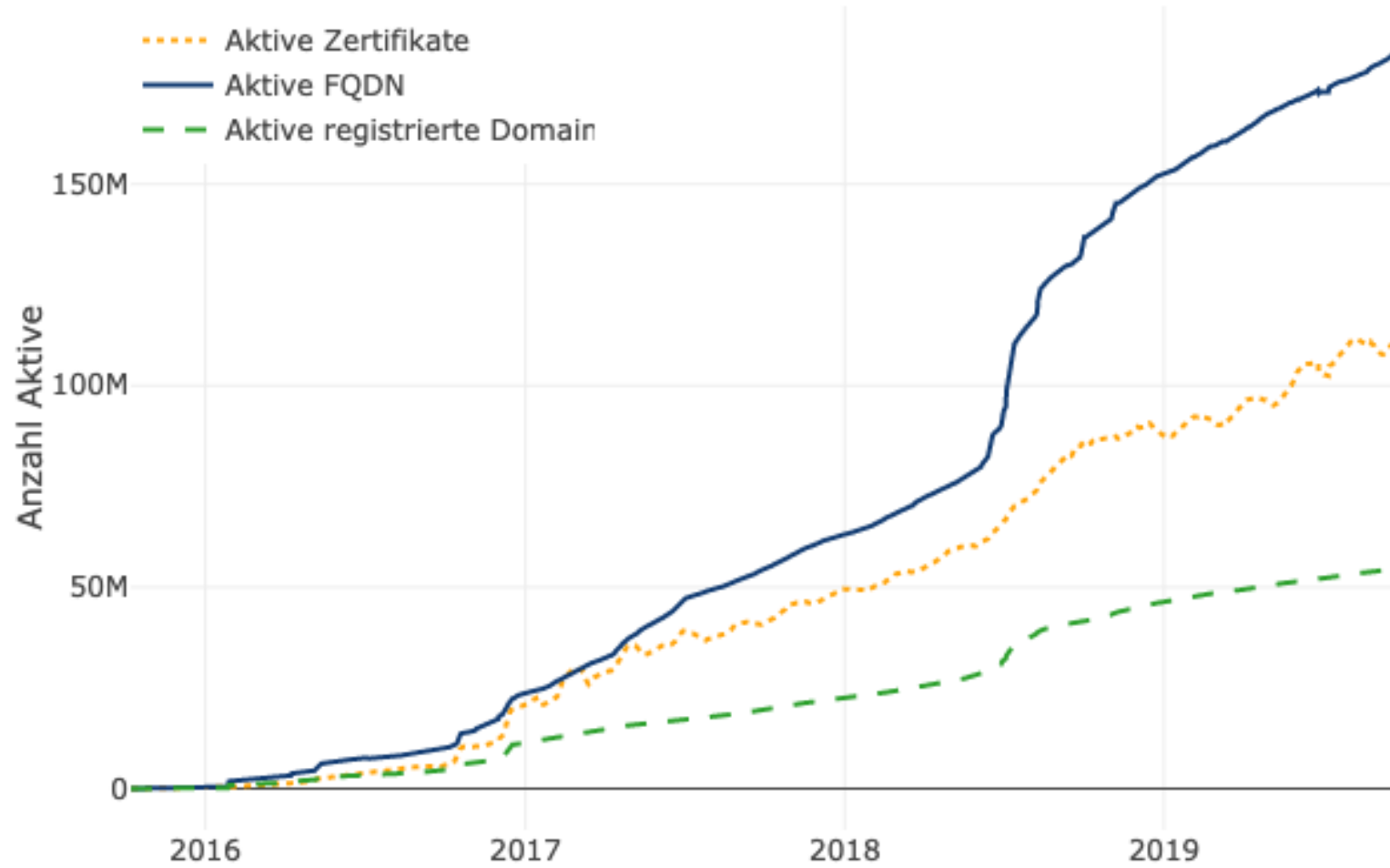
Ausgestellt von: Let's Encrypt Authority X3

Ablaufdatum: Donnerstag, 21. November 2019 um 10:03:25

Mitteeuropäische Normalzeit

✓ Dieses Zertifikat ist gültig.

► **Details**



Konfiguration Apache, Tomcat und ORDS

HAUPTSPONSOREN UND SPENDER

moz://a



EFF

OVHcloud



facebook

IdeaTrust
part of HID Global



AUTOMATTIC

ALA
American Library Association



CYON

infomaniak

HOSTPOINT



SUCURI

VULTR



fastly



3CX

SQUARESPACE



DuoCircle

ServerPilot

GitHub



UptimeRobot



ise

domainname.shop

umbraco

thebestvpn

DigitalOcean

PANTHEON
Website Management Platform



privateinternetaccess
always use protection

easyname

UNRAID

JIMDO

zendesk

dnsimple

SAKURA internet

brave

WORLD4YOU
INTERNET SERVICES GMBH

KEENETIC

Rainway

THE BEST RUN SAP

ProPrivacy

ipinfo.io

WiX.com

HOSTING REVIEW

HAPROXY

verizon
digital media services

nazwa.pl

GreenGeeks
WEB HOSTING

Engine Forex

HEROKU

smallstep

datto

mongoDB

clever cloud

Red Hat

ZEIT

SNIP-IT
OPEN SOURCE ASSET MANAGEMENT

AXIOM

Livesport

render

NABU CASA

codeinwp

TOP10VPN

Kommunikation verschlüsseln (https)

```
<VirtualHost *:443>
    SSLEngine on
# SSL Zertifikate
    SSLCertificateFile /etc/letsencrypt/live/meinedomain.de/cert.pem
    SSLCertificateKeyFile /etc/letsencrypt/live/meinedomain.de/privkey.pem
    SSLCertificateChainFile /etc/letsencrypt/live/meinedomain.de/chain.pem

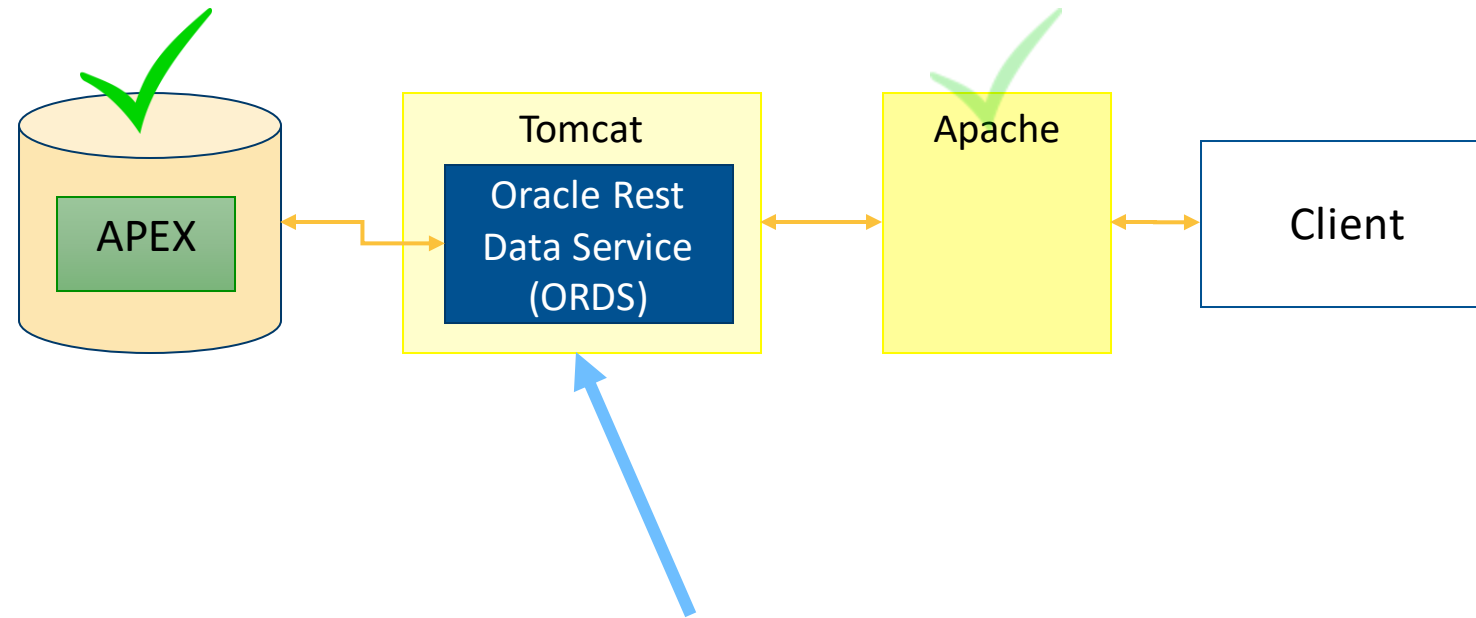
# SSL Einstellungen
    SSLProtocol               all -SSLv2 -SSLv3 (-TLSv1 -TLSv1.1)

    SSLCipherSuite             ECDHE-ECDSA-CHACHA20-POLY1305:ECDHE-RSA-CHACHA20-POLY1305:ECDHE-ECDSA-AES128-GCM-
    SHA256:ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:DHE-RSA-
    AES128-GCM-SHA256:DHE-RSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-
    AES128-SHA:ECDHE-RSA-AES256-SHA384:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES256-SHA384:ECDHE-ECDSA-AES256-
    SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-RSA-AES256-SHA256:DHE-RSA-AES256-
    SHA:!DSS

    SSLHonorCipherOrder       on
</VirtualHost>
```

Alle unverschlüsselten Zugriffe auf https umleiten

```
<VirtualHost *:80>  
    ServerName meinedomain.de  
  
    RewriteEngine On  
    RewriteRule ^/.* https://meinedomain.de/ [L,R=302]  
</VirtualHost>
```



Tomcat und ORDS konfigurieren

Tomcat herunterladen: tomcat.apache.org

OpenJDK herunterladen: openjdk.java.net oder **yum install java-latest-openjdk.x86_64**

ORDS herunterladen: www.oracle.com/database/technologies/appdev/rest-data-services-v192-downloads.html

Tomcat als User „tomcat“ entpacken und konfigurieren

Umgebungsvariable CATALINA_HOME (Tomcat-Verzeichnis) setzen: Datei <tomcat-dir>/bin/catalina.sh

<CATALINA_HOME>/conf/server.xml:

```
<Connector port="8009" protocol="AJP/1.3" URIEncoding="UTF-8" redirectPort="8443" />
```

Apex-Image Verzeichnis nach \$CATALINA_HOME/webapps/i kopieren (oder Link)

Tomcat starten: \$CATALINA_HOME/bin/startup.sh

Tomcat und ORDS konfigurieren

ORDS ebenfalls als User „tomcat“ konfigurieren

ORDS entpacken

ORDS konfigurieren:

```
java -jar ords.war
```

ords.war nach \$CATALINA_HOME/webapps kopieren, 1 Minute warten

Funktion testen: <http://<meintomcatserver>:8080/ords>

http://<server-ip>:8080

[Home](#) [Documentation](#) [Configuration](#) [Examples](#) [Wiki](#) [Mailing Lists](#)

[Find Help](#)

Apache Tomcat/8.0.30



If you're seeing this, you've successfully installed Tomcat. Congratulations!



Recommended Reading:

[Security Considerations HOW-TO](#)

[Manager Application HOW-TO](#)

[Clustering/Session Replication HOW-TO](#)

[Server Status](#)

[Manager App](#)

[Host Manager](#)

Developer Quick Start

[Tomcat Setup](#)

[First Web Application](#)

[Realms & AAA](#)

[JDBC DataSources](#)

[Examples](#)

[Servlet Specifications](#)

[Tomcat Versions](#)

Managing Tomcat

For security, access to the [manager webapp](#) is restricted. Users are defined in:

`$CATALINA_HOME/conf/tomcat-users.xml`

In Tomcat 8.0 access to the manager

Documentation

[Tomcat 8.0 Documentation](#)

[Tomcat 8.0 Configuration](#)

[Tomcat Wiki](#)

Find additional important configuration

Getting Help

[FAQ](#) and [Mailing Lists](#)

The following mailing lists are available:


[tomcat-announce](#)

Important announcements, releases, security


Konfiguration Apache, Tomcat und ORDS


http://<server-ip>:8080/ords


ORACLE®



Oracle Application Express

 workspace

 username

 password

Sign In

[Reset Password](#)

[Deutsch](#) · [English](#)

Weitergabe Apache -> Tomcat

```
<VirtualHost *:443>
# SSLKonfiguration
....
ProxyRequests off
ProxyPreserveHost On
RewriteEngine On
  RewriteRule ^/i/.* - [L]
  RewriteRule ^/ords/.* - [L]
  RewriteRule ^/$ /ords/f?p=2000:1 [R=301]

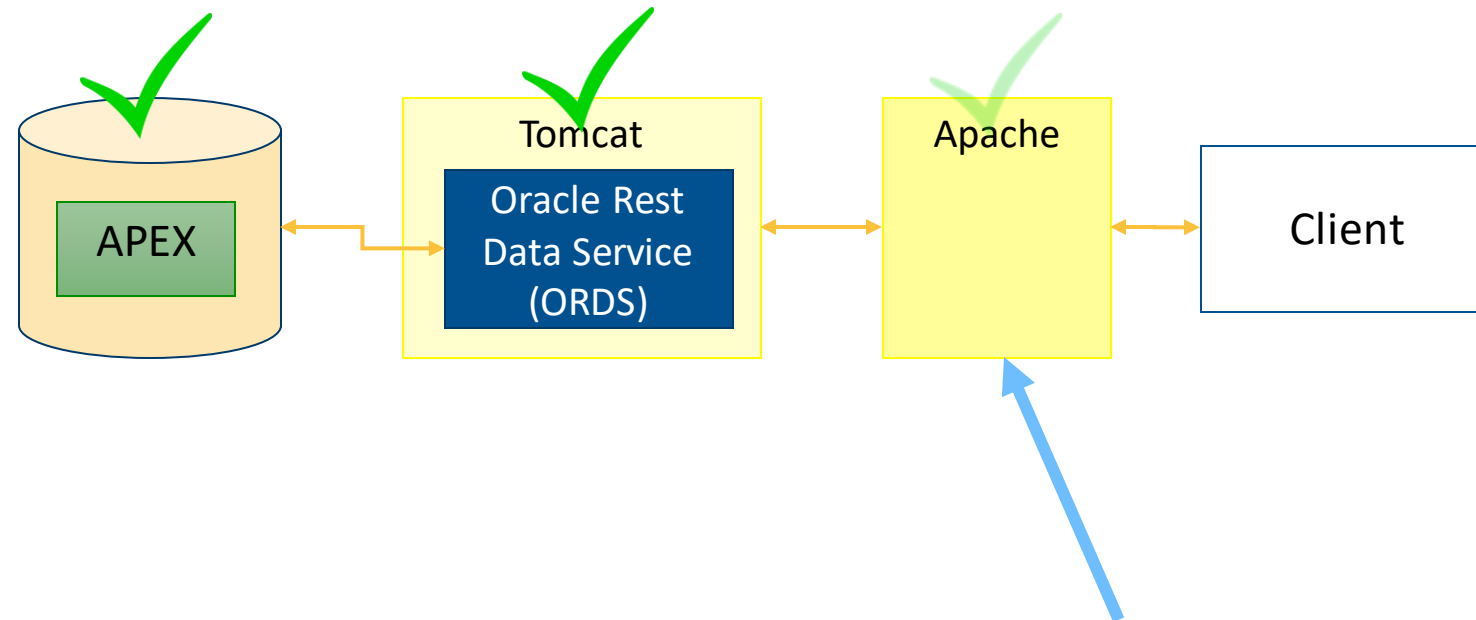
<Location /ords/>
  ProxyPass ajp://127.0.0.1:8009/ords/
</Location>
<Location /i/>
  ProxyPass ajp://127.0.0.1:8009/i/
</Location>
</VirtualHost>
```

Konfiguration Apache, Tomcat und ORDS

<http://meinedomain.de/ords>



Unerwünschte Zugriffe verhindern



Zumindest peinlich....

https://www.██.de/phpMyAdmin/



Willkommen bei phpMyAdmin

Sprache - *Language*

Deutsch - German

Anmeldung

Benutzername:

Passwort:

OK

Zugriff auf Anwendung 4550 von Extern blockieren

← → ↻ apex.oracle.com/pls/apex/f?p=4550:1:20650245258440:....

ORACLE APEX



Oracle Application Express



INTERNAL



ADMIN|



.....



☒ Workspace und Benutzernamen speichern ?

Anmelden

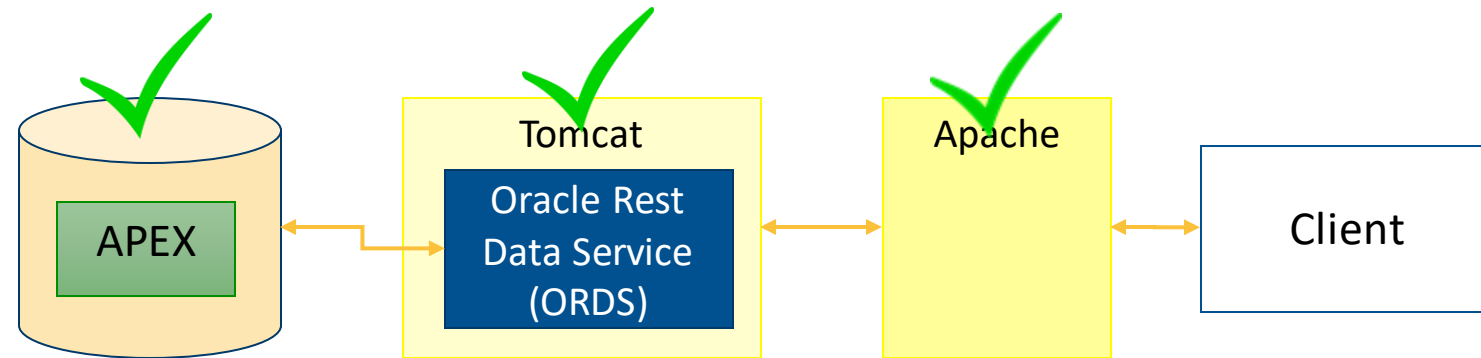
[Kennwort zurücksetzen](#) [Workspace anfordern](#)

Weitergabe Apache -> Tomcat

```
<VirtualHost *:443>
# SSLKonfiguration
....
ProxyRequests off
ProxyPreserveHost On
RewriteEngine On
  RewriteRule ^/i/.* - [L]
  RewriteRule ^/ords/.* - [L]
  RewriteRule ^/$ /ords/f?p=1000:1 [R=301]

# Nur in der Apache-Konfiguration für den externen Zugriff:
  RewriteCond %{THE_REQUEST} ^.*(f\?p=4550).* [NC]
#   RewriteCond %{THE_REQUEST} ^.*(f\?p=4\d\d\d).* [NC]
  RewriteRule ^(.*) /ords/f?p=1000:1 [R=301]

<Location /ords/>
.....
```



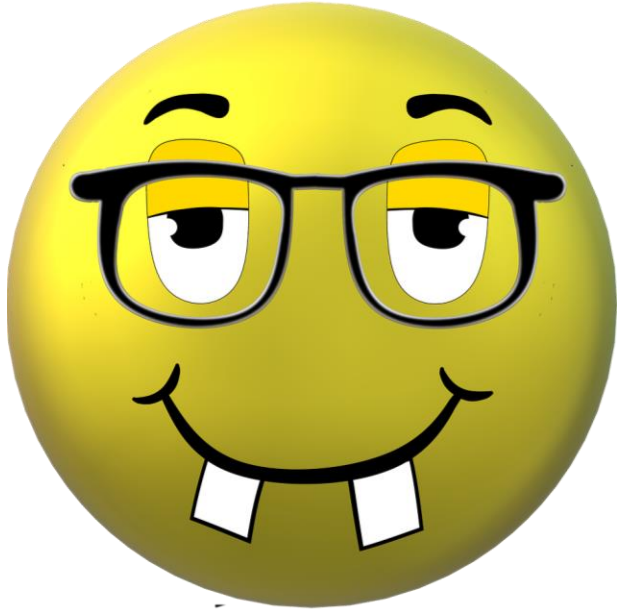
Noch nicht erwähnt:

SELINUX einschalten / eingeschaltet lassen

Apache-Konfiguration: maximal restriktiv halten

.....

Bliebe nur noch ein Problem



Anwender/in
(Abbildung ähnlich)

Anwender*innen recyceln gerne ihr Passwort (für alle Anmeldungen)

Anwender*innen lieben gelbe Zettel

Anwender*innen geben Ihr UN/PW gerne auf Fake-Seiten ein

Da hilft die Zwei-Faktor Authentifizierung:

<https://github.com/fuzziebrain/orclapex-tfa-demo>

<https://apexutil.blogspot.com/2018/07/two-factor-authentication-with-apex.html>

Fragen?



merlin.zwo

Wir kümmern uns!



merlin.zwo InfoDesign GmbH & Co. KG

Jochen Kutscheruk

Elsa-Brändström-Straße 14

76228 Karlsruhe

Tel. 0721 – 132 096 0

jochen.kutscheruk@merlin-zwo.de

<https://www.merlin-zwo.de>

