



Single Sign-On for everybody!

Niels de Bruijn
Business Unit Manager Low-Code
19-OCT-2022

About me

Niels de Bruijn

Twitter: @nielsdb

Personal Blog: nielsdebr.blogspot.com

Initiator of Flows for APEX, see flowsforapex.org

Business Unit Manager Low-Code @ MT AG

Leading a group of APEX experts

We share our passion for Oracle APEX through apex.mt-ag.com

Performing low-code evaluations, see www.mt-ag.com/lowcode

Director Development Community @ DOAG e.V.

Leading a group of volunteers

Initiator and conference chair for the conference **APEX connect**
by DOAG



About us



Founded
1994



Privately-Owned



> 44 Mio. Euro
Revenue in 2021



> 125 Active Clients



> 320 Employees
> 50 APEX Experts



Head Office
Ratingen

Branch Offices
Frankfurt am Main
Köln
München
Hamburg



certified partner for
leading
technologies

Your partner for digital change
Individual IT solutions from one source



Vendor neutral



Cross-Industry



Top Company for
Trainees & Students

Our Knowledgebase

knowledgebase.mt-ag.com

Search...

Type

- pdf (37)
- slideshare (24)
- youtube (17)
- edocr (5)
- blog (3)
- video (2)
- link (2)
- github (1)
- file

Year

- 2021 (6)
- 2020 (9)
- 2019 (17)
- 2018 (26)
- 2017 (22)
- 2016 (4)
- 2015 (2)

Tags

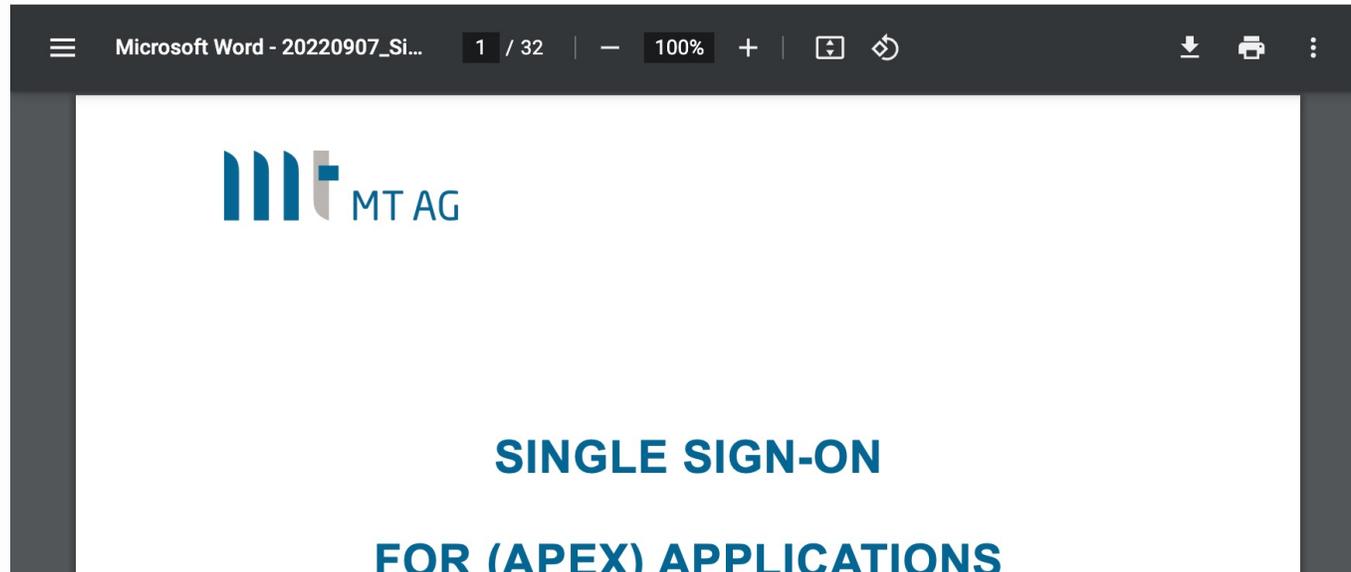


pdf

07.09.2022

Single Sign-On For (APEX) Application Using Kerberos

For APEX apps, you normally use a URL like <hostname>/apex/f?p=xxx after which by default you have to authenticate yourself using username/password credentials. However, most end users of APEX Applications already have authenticated themselves by logging on to the Windows domain, so why authenticate a second time to use the first APEX Application?



Our extensions for APEX developers

Low-Code Testing (LCT): Ict.software

LCT - Low Code Testing Log Out

Worksheets Queue Import/Export Test Suites Administration

Search: All Text Columns Go Actions

General			Execution				
Actions	Execution Name	Version	Execution Point	Status	Successful/Total Cases	(min)	Output Log
	test_suite_3 - Testing the Sample DB App - PLAYW-C...	#10	10.05.22 03:06	🔄	0/2	00:19	👁
	test_suite_3 - Oracle Sample DB App - PLAYW-CHRO...	#8	10.05.22 03:05	🔄	1/2	00:37	👁
	test_suite_6 - Place Order Test - PUPP	#10	09.05.22 15:45	🔄	1/1	00:32	👁
	test_suite_6 - Sample DB DEMO (Var Test) - PUPP	#6	09.05.22 15:43	🔄	3/4	01:10	👁
	Smample DB TS - Sample DB - Place Order - PUPP	#2	09.05.22 13:57	🔄	1/1	00:34	👁
	Smample DB TS - Sample DB DEMO (Var Test) - PUPP	#6	09.05.22 13:55	🔄	3/4	01:11	👁
	test_suite_3 - Testing the Sample DB App - PLAYW-C...	#10	09.05.22 03:06	🔄	0/2	00:20	👁
	test_suite_3 - Oracle Sample DB App - PLAYW-CHRO...	#8	09.05.22 03:05	⚠️	0/2	00:28	👁
	test_suite_6 - Place Order Test - PUPP	#10	08.05.22 15:44	🔄	1/1	00:32	👁
	test_suite_6 - Sample DB DEMO (Var Test) - PUPP	#6	08.05.22 15:43	🔄	3/4	01:07	👁
	Smample DB TS - Sample DB - Place Order - PUPP	#2	08.05.22 13:57	🔄	1/1	00:36	👁
	Smample DB TS - Sample DB DEMO (Var Test) - PUPP	#6	08.05.22 13:55	⚠️	3/4	01:12	👁
	test_suite_3 - Testing the Sample DB App - PLAYW-C...	#10	08.05.22 03:06	🔄	0/2	00:14	👁
	test_suite_3 - Oracle Sample DB App - PLAYW-CHRO...	#8	08.05.22 03:05	🔄	0/2	00:24	👁
	test_suite_6 - Place Order Test - PUPP	#10	07.05.22 15:45	🔄	1/1	00:31	👁
	test_suite_6 - Sample DB DEMO (Var Test) - PUPP	#6	07.05.22 15:43	🔄	3/4	01:08	👁
	Smample DB TS - Sample DB - Place Order - PUPP	#2	07.05.22 13:57	🔄	1/1	00:32	👁
	Smample DB TS - Sample DB DEMO (Var Test) - PUPP	#6	07.05.22 13:55	🔄	3/4	01:10	👁
	test_suite_3 - Testing the Sample DB App - PLAYW-C...	#10	07.05.22 03:06	🔄	0/2	00:14	👁
	test_suite_3 - Oracle Sample DB App - PLAYW-CHRO...	#8	07.05.22 03:05	🔄	0/2	00:24	👁
	test_suite_6 - Place Order Test - PUPP	#10	06.05.22 15:44	🔄	1/1	00:32	👁
	test_suite_6 - Sample DB DEMO (Var Test) - PUPP	#6	06.05.22 15:43	🔄	3/4	01:05	👁
	Smample DB TS - Sample DB - Place Order - PUPP	#2	06.05.22 13:56	🔄	1/1	00:31	👁
	Smample DB TS - Sample DB DEMO (Var Test) - PUPP	#6	06.05.22 13:55	🔄	3/4	01:06	👁
	test_suite_3 - Testing the Sample DB App - PLAYW-C...	#10	06.05.22 03:06	🔄	0/2	00:19	👁
	test_suite_3 - Oracle Sample DB App - PLAYW-CHRO...	#8	06.05.22 03:05	🔄	0/2	00:31	👁
	test_suite_6 - Place Order Test - PUPP	#10	05.05.22 15:45	🔄	1/1	00:36	👁

1 rows selected 1 2 3 4 5 ... > | 1-42 of 5013

LiveLog - Queue ID: 5600

```
30 I click "#B7496042880055189376"
31 I switch to "iframe"
32 I wait for element "#B7496042880055189376"
33 I click "#B7496042880055189376"
34 I wait for element "#B40969685215878798", 15
35 I wait for element "//div[@class='t-Region-body']//tr//td/a[text()='Belt']//following-sibling::td/td/select"
36 I select option "//div[@class='t-Region-body']//tr//td/a[text()='Belt']//following-sibling::td/td/select", ["2"]
37 I wait for element "#B403162600409924493"
38 I click "#B403162600409924493"
39 I wait for element "//div[@class='t-Region-body']//tr//td/a[text()='Belt']/following-sibling::td[@headers='QUANTITY'] [text()='2']"
40 I see element "//div[@class='t-Region-body']//tr//td/a[text()='Belt']/following-sibling::td[@headers='QUANTITY'] [text()='2']"
41 I wait for element "//div[@class='t-Region-body']//tr//td/a[text()='Belt']/following-sibling::td[@headers='TOTAL_COST'] [text()='$60.00']"
42 I see element "//div[@class='t-Region-body']//tr//td/a[text()='Belt']/following-sibling::td[@headers='TOTAL_COST'] [text()='$60.00']"
43 I wait for element "//div[@class='t-Region-body']//tr//td/b[text()='Report Total']//following-sibling::td[@headers='TOTAL_COST']/b[text()='$60.00']"
44 I see element "//div[@class='t-Region-body']//tr//td/b[text()='Report Total']//following-sibling::td[@headers='TOTAL_COST']/b[text()='$60.00']"
45 I wait for element "#B696563211816239755"
46 I click "#B696563211816239755"
47 I switch to
48 I wait for element "//div[@role='alertdialog']", 15
49 I see "Are you sure you want to place this order?", "//div[@role='alertdialog']//p"
50 I wait for element "//div[@role='alertdialog']//div[@class='ui-dialog-buttonset']/button[contains(@class, 'js-confirmBtn')]"
51 I click "//div[@role='alertdialog']//div[@class='ui-dialog-buttonset']/button[contains(@class, 'js-confirmBtn')]"
52 I switch to "iframe"
53 I wait for element "//h2[@class='t-Alert-title'] [text()='Order placed!]", 15
54 I wait for element "#B696525728662161651"
55 I click "#B696525728662161651"
56 I wait 6
57 ✓ OK in 35500ms
58
59
60 OK | 1 passed // 37s
61 Done in 38.85s.
62
```

Our extensions for APEX developers

Flows for APEX: flowsforapex.org

The screenshot displays the 'Flow Modeler' interface for 'Expense Claims - Version 0'. The interface includes a top navigation bar with 'Flows for APEX', 'Getting started', 'Configuration', 'Theme', and a user profile 'ndbruijn'. A left sidebar contains 'Dashboard', 'Flow Management', and 'Flow Monitor'. The main workspace shows a BPMN diagram with swimlanes for Employee, Company, Manager, Vice President, and Accountant. The process starts with 'Submit expense claim' (Employee), followed by 'Validate expense' (Company), 'Review expense' (Manager), and 'Correct expense claim' (Employee). A timer event 'Fires 2 times, each after 30 seconds' is associated with 'Correct expense claim'. The process then branches based on 'declined_mgr' (to 'Remind employee' and 'Inform employee2') and 'approved_mgr'. A decision diamond 'Expense exceeds 50 USD?' leads to 'Review expense' (Vice President) if 'yes', and 'Prepare payment' (Accountant) if 'no'. Another decision diamond 'Status?' leads to 'Inform employee2' (Manager) if 'declined_vp' and 'Prepare payment' (Accountant) if 'approved_vp'. The process ends with 'Execute transaction' (Accountant) and 'Expense repayed'. A right sidebar shows configuration for 'review_expense_mgr', including 'Call APEX Page', 'Input', 'Application', 'Page', and 'Page Items'. The 'Page Items' section contains a list of variables: 'P5_EXPE_ID:&F4A\$BUSINESS_RE', 'PROCESS_ID:&F4A\$PROCESS_ID', 'SUBFLOW_ID:&F4A\$SUBFLOW_ID', and 'STEP_KEY:&F4A\$STEP_KEY'. The bottom status bar indicates '0 Errors, 0 Warnings' and the BPMN.io logo is in the bottom right corner.

Single Sign-On for APEX environments

On today's menu:

- Why SSO?
- Authentication Schemes in APEX 22.1
- SSO for on-premises APEX environments
- SSO for APEX environments with Identity Provider in the Cloud
- SSO FAQ

This session is **not** (primarily) about...

- High availability
- Authorization
- Locking down your environment
- Machine-2-machine communication (ie. RESTfull web services based on ORDS)



Why Single Sign-On for my APEX apps?

- Security
- Productivity

APEX Authentication Schemes: from worst to best

Authentication Schemes in APEX 22.2:

-  • No authentication
 - only for a public app ok, but be aware of DDoS if on internet
-  • Open Door
 - only allowed in a dev/test environment (with non-prod data)
-  • Custom
 - why reinvent the wheel and store passwords yourself?
-  • LDAP Directory
 - insecure
-  • Database Accounts
 - use only for legacy reasons

-  • Oracle APEX accounts
 - use if no external Identity Provider (IdP) is available
-  • Social Sign-In (OAuth2)
 - delegates authentication to external IdP
-  • SAML Sign-In
 - delegates authentication to external IdP
-  • HTTP Header Variable
 - delegates authentication to external IdP*

*) APEX by default only reachable *after* authentication

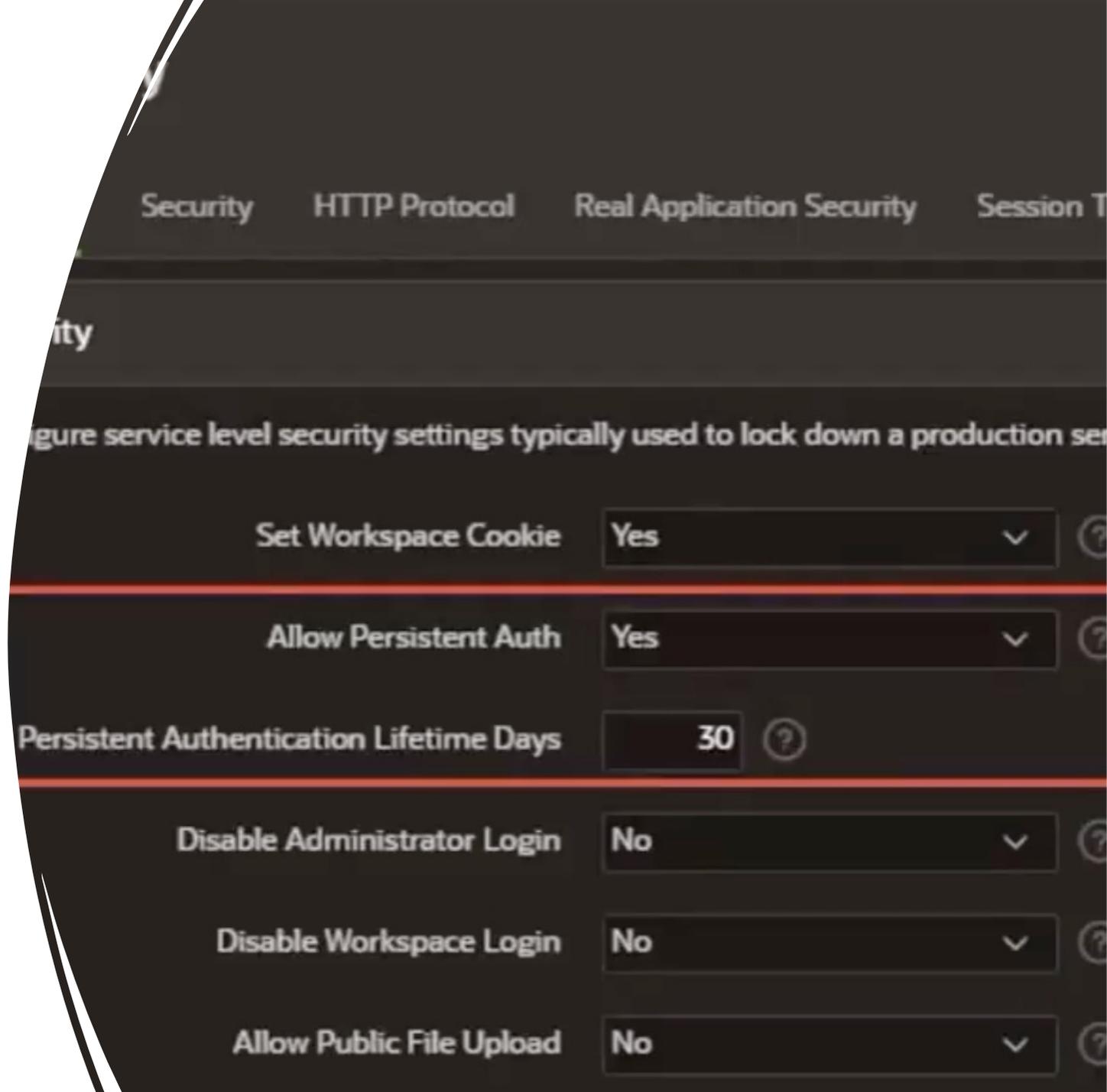
Important side note: be aware of DDoS attacks!



<https://nielsdebr.blogspot.com/2022/01/protect-your-public-server.html>

Single Sign-On in your APEX workspace

- Use shared cookie: logon once across all APEX apps
- Enable "Remember me" in APEX 22.1+ at instance level
 - A persistent cookie is created and will require you to logon each x days after starting a new browser session (default are 30 days, max = 99 days)



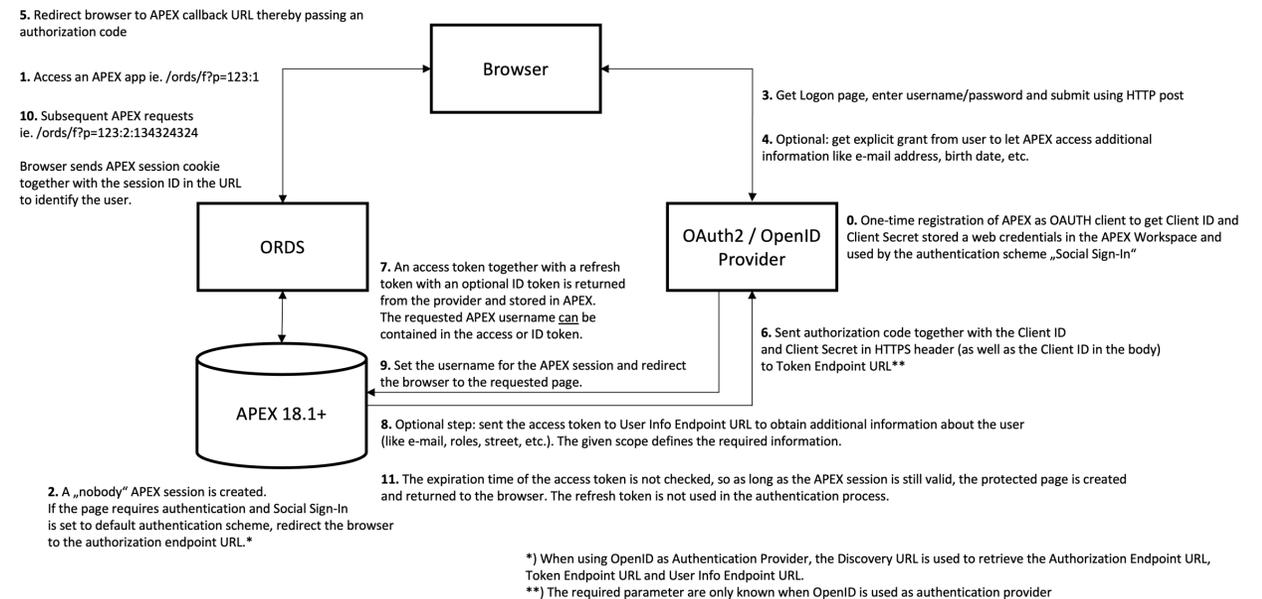
OAuth2/OpenID APEX authentication (aka Social Sign-In)

- Step-by-step guide:
https://knowledgebase.mt-ag.com/q/apex_sso_oauth2

- Nice video from Maximilian:
<https://www.youtube.com/watch?v=fAdhxFmvLI4>

- Blog post by Jon Dixon:
<https://blog.cloudnueva.com/oracle-apex-builder-social-sign-on>

Communication Flow when using Social Sign-In Feature of APEX 18.1+ and „Generic OAuth2 Provider“ or „OpenID“ as Authentication Provider



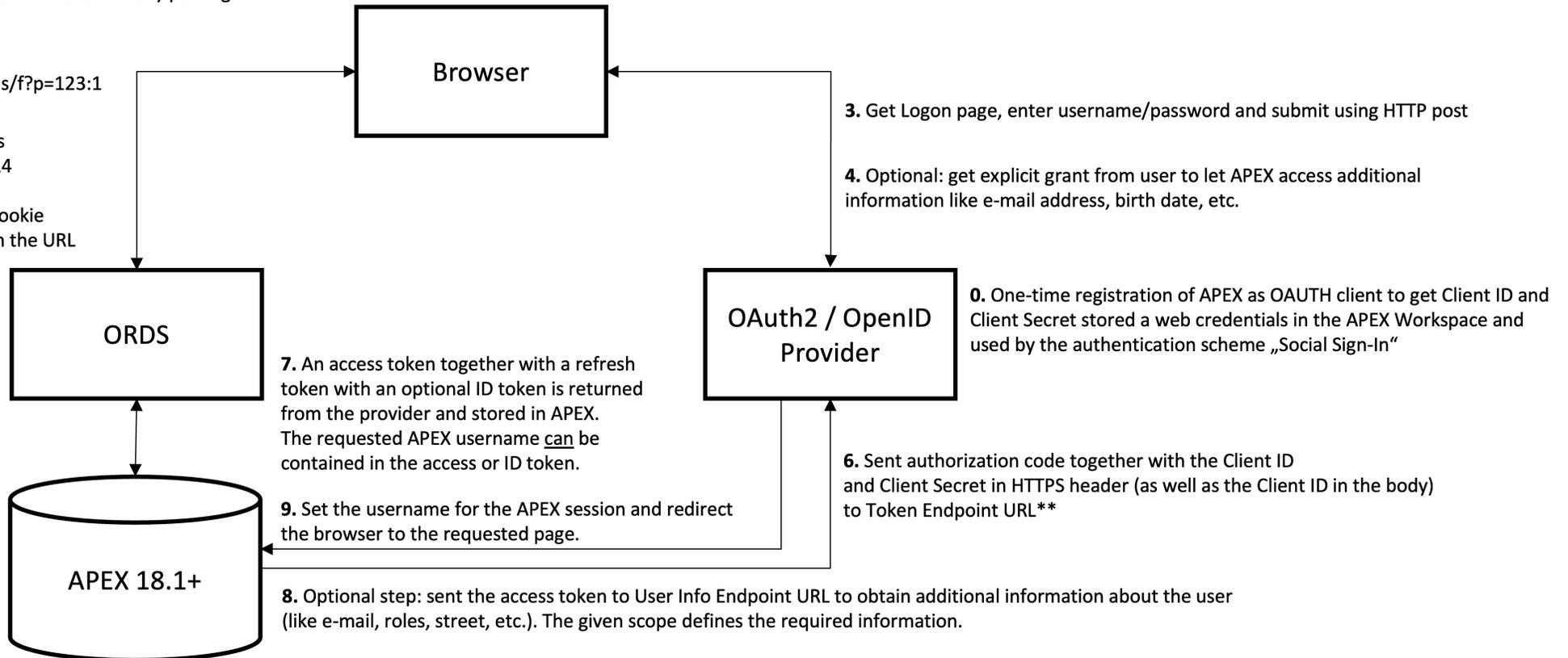
Communication Flow when using Social Sign-In Feature of APEX 18.1+ and „Generic OAuth2 Provider“ or „OpenID“ as Authentication Provider

5. Redirect browser to APEX callback URL thereby passing an authorization code

1. Access an APEX app ie. /ords/f?p=123:1

10. Subsequent APEX requests ie. /ords/f?p=123:2:134324324

Browser sends APEX session cookie together with the session ID in the URL to identify the user.



2. A „nobody“ APEX session is created. If the page requires authentication and Social Sign-In is set to default authentication scheme, redirect the browser to the authorization endpoint URL.*

11. The expiration time of the access token is not checked, so as long as the APEX session is still valid, the protected page is created and returned to the browser. The refresh token is not used in the authentication process.

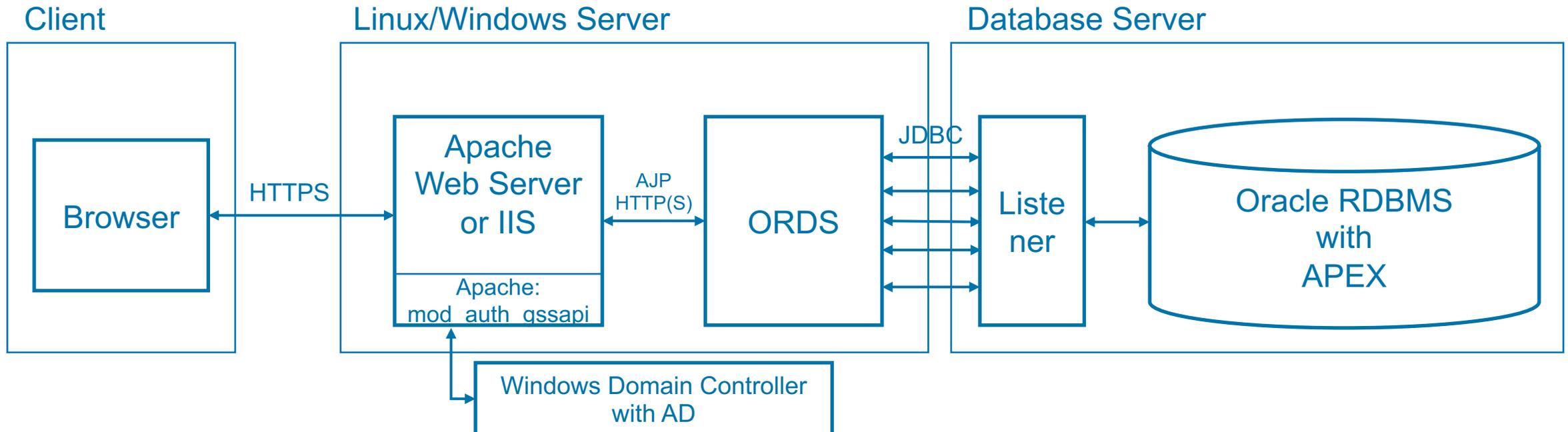
*) When using OpenID as Authentication Provider, the Discovery URL is used to retrieve the Authorization Endpoint URL, Token Endpoint URL and User Info Endpoint URL.

**) The required parameter are only known when OpenID is used as authentication provider

Kerberos Authentication for on-prem APEX environments

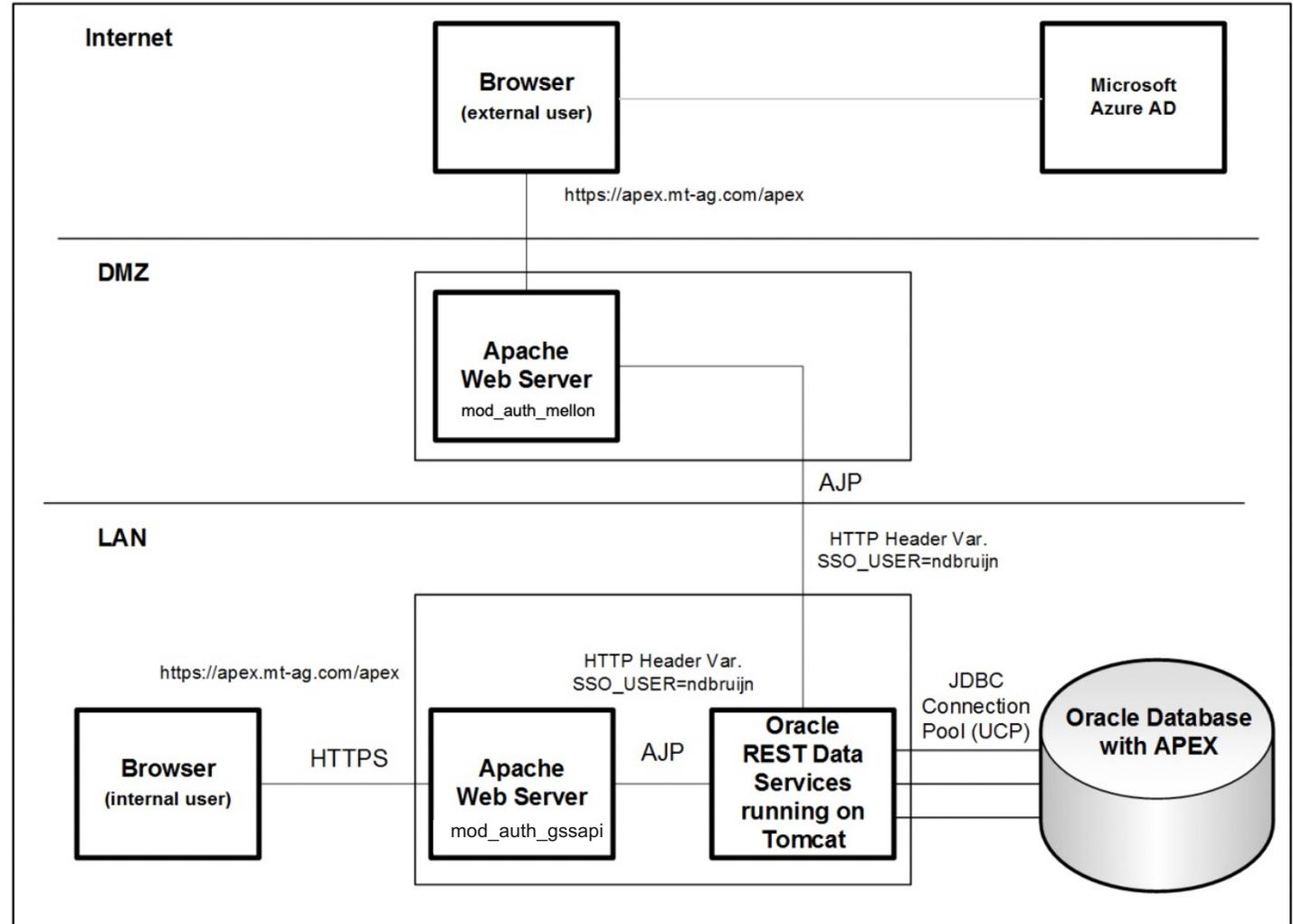
Based on kerberos

- Great for internal APEX environments with Active Directory as IdP (true SSO here!)
- Works for MacOS as well (run the app Ticket Viewer)
- Takes about 4-8 hours to setup
- Step-by-step guide available on <https://knowledgebase.mt-ag.com/q/kerberos>



SAMLv2 APEX authentication

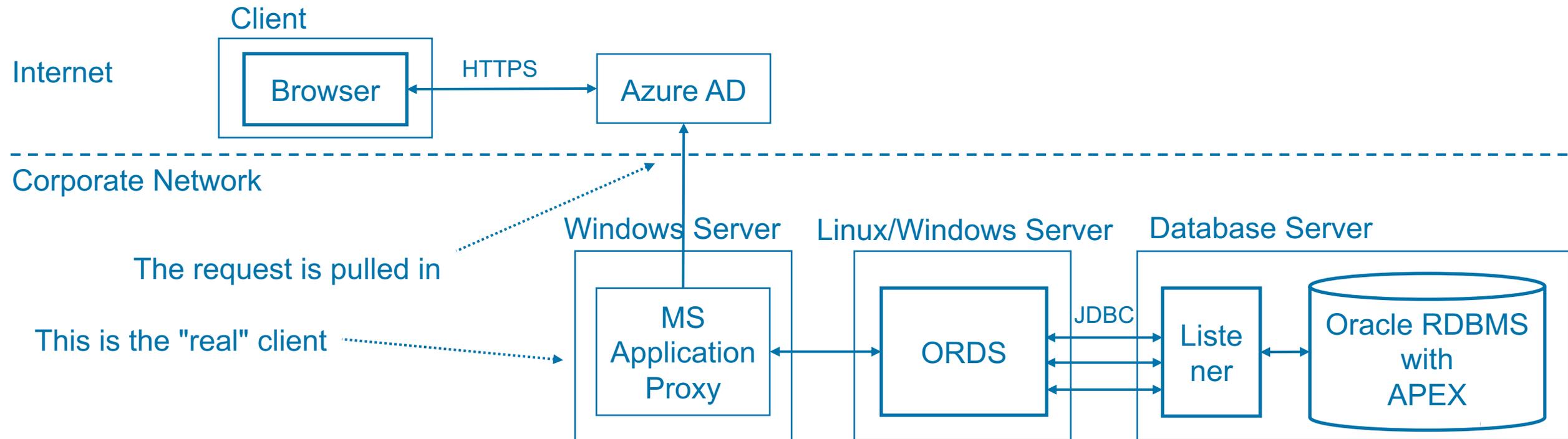
- No experience yet made with the built-in authentication scheme in APEX 21.2+
 - Requires DB 19+ and latest patchset for APEX 21.2
- Alternative: use Apache Web Server with mod_auth_mellon
 - Step-by-step guide available on https://knowledgebase.mt-ag.com/q/apex_sso_samlv2
- SAMLv2 is more cumbersome to setup compared to OAuth2, but therefore less redirects. OAuth2 has my preference.



Delegated SSO with APEX on-prem and Azure AD as IdP

Based on MS Application Proxy (that acts as client and handles **kerberos** or **SAMLv2**)

- Great for home-office, no need for a VPN connection anymore!
- Enables secure access to external users, that are registered in Azure AD
- Takes about 2-4 hours to setup
- Step-by-step guide available for Kerberos on https://knowledgebase.mt-ag.com/q/apex_proxy



SSO FAQ

Specific questions related to authentication

- Q: I need two-factor authentication
- A: Azure AD already has it (and most likely your users are already used to it), otherwise use Ecosia to search for a custom solution based on APEX
- Q: How to handle session expiration in APEX?
- A: Set it to 0, if you have delegated authentication to an external IdP (max is 12 hours)
- Q: I need more in-depth background information about Windows SSO, kerberos, etc.
- A: Have a look here: <https://syfuhs.net/understanding-windows-auth>

Q&A



Niels de Bruijn
Business Unit Manager Low-Code

Twitter: @nielsdb
Mail: niels.debruijn@mt-ag.com

MT AG
Balcke-Dürr-Allee 9
40882 Ratingen

www.mt-ag.com