Contents

IAM Meets Developers Workshop – Overview

Bridging the Gap Between Identity & Application Development

A practical, demo-driven workshop designed for teams working with **Microsoft Entra ID**, focusing on the real-world issues that occur where **application code meets identity configuration**.

Using **AppConfig²**, participants learn *exactly* how authentication and authorization work, how to interpret tokens, and how to resolve complex misconfigurations efficiently.

Workshop Goal

Equip developers, support engineers, and IAM architects with the skills to **debug and fix authentication issues end-to-end**, understand OAuth2/OIDC flows, and collaborate effectively using shared terminology and methods.

Target Audience

- **Developers & Engineers** integrating or securing apps with Entra ID
- **L2/L3 Application Support** analyzing token/role issues
- **IAM Architects & Identity Engineers** guiding app teams
- **Security Engineers** reviewing permissions and API exposure
- **Solution & Cloud Architects** designing identity-aware systems

---

What Participants Will Learn

1. OAuth2/OIDC & MSAL: Practical Understanding

- `/authorize` vs `/token` endpoints
- Authorization Code Flow with PKCE
- ID tokens vs access tokens

- Consent, scopes, audiences, and resources
- Reading & validating JWTs

Authorization Code + PKCE Flow:

The authorization flow consists of three main stages:

1. **Front Channel (Browser Redirects via /authorize)**
   - User accesses the application
   - App redirects to `/authorize` endpoint with: `response_type=code`, `client_id`, `redirect_uri`, `scope`, `state`, `code_challenge`, `code_challenge_method=S256`
   - Authorization server presents login & consent prompt
   - User submits credentials and grants consent
   - Server redirects back with `authorization_code` in URL query parameters
2. **Back Channel (Secure Server-to-Server via /token)**
   - Client app POSTs to `/token` endpoint with: `grant_type=authorization_code`, `code`, `redirect_uri`, `code_verifier`
   - Authorization server responds with JSON containing: `access_token`, `id_token`, `refresh_token`
3. **Resource Access**
   - Client calls protected API with `Authorization: Bearer <access_token>` header
   - API validates token and returns protected data

---

2. Developer–IAM Interface: What Developers Need to Know

Question	Why It Matters	Provided By
Client ID, redirect URIs	Required for MSAL startup, must match	IAM / App Owner
Single vs multi-tenant	Determines authority endpoint	IAM Architect
Required API permissions	Drives requested scopes & consent	IAM / API Owner
Roles & optional claims	Determines token content	IAM / API Owner
Token types needed	Affects MSAL config & flow	Developer / IAM

Developer-IAM Collaboration Flow:

Developer requests configuration from IAM Team → IAM provides client IDs, roles, and redirect URIs → Developer builds MSAL configuration → Application requests tokens from Entra ID

---

3. App Registration vs Service Principal: Why It Matters

Participants learn how to diagnose issues where configuration looks correct but tokens don't match expectations.

Key Distinction:

- **App Registration (Definition)**: Template of the app living in the home tenant, defines redirect URIs, scopes, and roles
- **Service Principal (Instance)**: Tenant-specific instance with granted permissions and role assignments

Common Troubleshooting Scenarios:

- Role defined in registration but missing in token → Not assigned on Service Principal
- "User not authorized" error → Service Principal lacks consent
- Service Principal deleted but registration remains active
- Multi-tenant behavior: App Registration spawns Service Principals in consuming tenants

---

4. Common Issues & How to Fix Them

- **X** Wrong or mismatched redirect URIs
- **X** PKCE not working (MSAL misconfiguration)
- **X** Missing role assignment in Service Principal → "role missing in token"
- **X** Incorrect audience (`aud`) for protected API
- **X** Permissions granted but not consented
- **X** Conditional Access silently blocking authentication
- **X** Using legacy implicit flow

---

5. Hands-On Troubleshooting with AppConfig^2

Participants use **AppConfig^2** to accelerate problem resolution:

- Test authentication flows
- Inspect raw request/response pairs
- Decode and analyze JWTs
- Validate roles and claims
- Compare app registration vs Service Principal configuration
- Explore configuration using integrated Graph Explorer
- See the difference between classic troubleshooting and AppConfig^2 diagnostics

Systematic Troubleshooting Workflow:

1. Test Authentication Flow
2. Analyze Tokens
3. Validate Roles & Claims
4. Review App Registration
5. Inspect Service Principal
6. Resolve Issue or Export Findings

Workshop Format

Aspect	Details
Duration	8 hours (delivered over 2 half-days)
Format	Online or on-site (Prague, Czechia only)
Group Size	6-10 participants (optimal for interaction)
Delivery Options	Live virtual sessions or in-person training
Materials Included	Slides, diagrams, token cheat sheets, troubleshooting guides
Hands-On Practice	Live demos with AppConfig² Suite
Post-Workshop	30-day access to AppConfig² demo environment + email Q&A support

---

Key Takeaways

Participants will be able to:

- Understand how Microsoft Entra ID authentication works end-to-end
- Configure MSAL reliably for any application type (SPA, Web App, Web API)
- Diagnose token, scope, and role issues quickly using systematic methods
- Use a repeatable troubleshooting framework for auth problems
- Improve collaboration across development, support, IAM, and security teams
- Map error codes (AADSTS) to root causes efficiently
- Reduce authentication issue resolution time by an estimated 60%+

Workshop Modules

Module 1: Where IAM Meets App Development

Identify gray zones where IAM and developer responsibilities overlap, leading to common misconfiguration issues.

Module 2: App Registration vs Service Principal

Understand the two-object architecture and why configuration can look correct but tokens don't match expectations.

Module 3: OAuth2.0 Endpoints & Flows

Compare `/authorize` vs `/token` endpoints across different OAuth grant flows (Implicit, Authorization Code, Client Credentials).

Module 4: MSAL Under the Hood

Debug MSAL effectively, understand caching, and trace authentication flows using network tools.

Module 5: Developer-IAM Interface

Learn what developers need from IAM to configure MSAL correctly and create valid token requests.

Module 6: SPA vs Web App vs Web API

Understand application architecture patterns and their specific authentication requirements.

Module 7: Permissions & Consent

Master static vs dynamic consent, delegated vs application permissions, and user vs admin consent endpoints.

Module 8: Token & Claims Validation

Learn JWT structure, v1/v2 token differences, optional claims configuration, and token validation techniques.

Who Should Attend

This workshop is ideal for:

- **Developers** integrating applications with Microsoft Entra ID
- **Support Engineers (L2/L3)** troubleshooting authentication issues
- **IAM Administrators** managing app registrations and permissions
- **Security Engineers** reviewing permission models and API exposure
- **DevOps Engineers** deploying identity-aware applications
- **Solution Architects** designing authentication architectures
- **Technical Consultants** working with Microsoft identity platform

Prerequisites:

- Understanding of web applications and HTTP requests/responses
- Basic knowledge of JSON structure and JWT concepts
- Familiarity with authentication vs. authorization concepts
- Experience with web application development or troubleshooting

Not suitable for:

- Complete beginners to web authentication
- Business stakeholders seeking high-level overview only

Perfect for Teams Experiencing:

- Migration to Microsoft Entra ID authentication
- Frequent auth-related support tickets bouncing between teams
- Communication gaps between IAM and development teams
- Need to reduce Mean Time To Resolution (MTTR) for authentication issues
- Need to upskill junior/mid-level engineers on IAM concepts
- Building or maintaining Entra ID integrated applications

Contact & Booking

Interested in booking this workshop for your team?

Email: support@appconfig.app

Subject: Workshop Booking Request - IAM Meets Developers

Include in your message: - Preferred format (Online / On-site) - Number of participants - Preferred dates - Organization name - Any specific scenarios or challenges your team faces

We typically respond within 1 business day with availability and pricing information.

Last Updated: February 2026

Workshop by: AppConfig^2 Suite | www.appconfig.eu