**ARM – Authentication and token handling**

The current implementation of the ARM APIs supports two types of JWT token-based authentication mechanisms:

1. **ARM Internal Tokens** – Tokens issued by ARM (Axpert Rapid Response Manager).
2. **External SSO Token** (using JWKS file)– Issued by an Client’s internal Identity Provider (IdP).

**🔧 Configuration**

**ARM Internal Tokens**:

The ARM generates the JWT tokens for authentication. Configured using the following configuration in appsettings.json file:

"Jwt": {

"Key": "ARM-JWTKEY-12evbayut23y4ejhsd621362qgad",

"KId": "ARM-INTERNAL-170B360CEC1906992A328RS256",

"Issuer": "Axpert - ARM",

"Audience": "Axpert - ARM",

"ExpiryMinutes": 300

},

| **Setting** | **Description** |
| --- | --- |
| Key | Symmetric key used for signing and validating JWT tokens with HMACSHA256. |
| Kid | The Kid should start with ‘ARM-INTERNAL-’ prefix for internal tokens. |
| Issuer / Audience | Used to validate that the token is from and for your system. |
| ExpiryMinutes | Token lifespan in minutes (300 = 5 hours). |

Note: The Kid should start with ‘ARM-INTERNAL-’ prefix for internal tokens.

**External SSO Tokens (using JWKS File) (Optional)**:

ARM can be configured to supports the external tokens of Client’s internal Identity Provider (IdP) additionally. This is configured via the following settings:

"SSO-JWT-AUTH": {

"Issuer": "https://sso.google.com",

"Audience": "ERP",

"JWKSFilePath": "SecureData\\JWKS\\E2E\_JWKS.json"

}

"AppConfig": {…

"SSO-JWT-AUTH": true

}

| **Setting** | **Description** |
| --- | --- |
| SSO-JWT-AUTH | This key in Appconfig node should be set to **true** to use the customer’s tokens for authentication. |
| JWKSFilePath | The File path for JWKS file inside the ARM folder. |
| Issuer / Audience | Used to validate that the token is from and for your system. |