Standard: X-Axa-Context Token Policy

Status: VALIDATED

Overview

This page provides information on how to use the X-Axa-Context security policy.

The X-Axa-Context is an Identity Token based on the OAUTH2 JWT and proposed for internal usage by the AXA Identity and Access Management Group (IAM).

TOC

Principles

- This token must be used in the Internal API security
- Each system will be able to authenticate and authorize based on this *signed* X-Axa-Context token

Useful Links

RFC7515 JSON Web Signature

X-Axa-Context Header

Master Application List.xls

General

The X-Axa-Context security principal is a token based authorization scheme. It defines structured and signed token (based on JWS) that can provide authentication. This scheme relies on the signature of the token to trust its contents.

Usage

When a client wants to invoke an API that is protected by the X-Axa-Context security policy, it will create a JSON Web Token (JWT) with the necessary authorization information (subject field) and a specific expiration time. The application will then sign the token with its private key according to the JWS standard. This X-Axa-Context token is then placed in a specific HTTP Header named X-Axa-Context (This allows it to piggy-back with other authentication/authorization schemes). The receiving end will inspect the token: it will validate the signature with the public keys in its truststore. If the token is validated and trusted, the receiver can act on the subject in the token to validate if it has access to the requested resource.

Structure

The X-Axa-Context token follows the JWS specification. It comprises of 3 base64-encoded pieces devided by a dot-character:

JOSE Header

field	description	default	mandatory
alg:	Algorithmus used to sing the token.	"RS256"	yes
x5u:	URL of an endpoint providing the certificate used for the validation of the signature.		no
kid:	ID of the certificate which can be used for validating the signature. The ID is the SHA-1 Thumbprint (without blanks, capital letters) of the corresponding certificate		only if x5u is used

JWT Claims

field		description	default	mandatory
iss:		Issuer of the token in a descriptive manner (ESG, EIP, JAVA or NET)		yes
sub:	**value:**	subject id, the identifier of the user or application (MAL_ID)		yes
	domain:	subject domain, the domain of the user id (AXA-BE-MAL)		no
initialSub:	**value:**	initial subject is the account that created the initial request e.g. the first call to the AXA network.		yes
	domain:			no
iat:		Issued At, as Unix Timestamp (seconds since 01.01.1970)		yes
exp:		The expiration time on or after which the token must not be accepted, as Unix Timestamp (seconds since 01.01.1970)		yes
customData:		Custom JSON Object which can contain additional information about the authenticated user (e.g. roles).		no
contextVersion:		Version of the X-Axa-Context header	"1"	yes

initialClientId:	The initialClientId identifies the initial application at the very beginning of the service chain.		yes
amr:	The Authentication Method Reference describes the authentication method used for user authentication.	""	yes

Signature
The signature of the JWT Claims. Signed with the properties defined in the JOSE Header.

Unsigned X-Axa-Context token (not implemented)

Between ESG and EIP (Mediator) an unsigned token can be used. Trust must then be implied by the mutual SSL connection between these components. Setting up such an SSL-connection is quite costly from a performance perspective. However, we can reuse this connnections for subsequent calls. Given that the tokens don't need to be signed/validated on every call, this can have an overall positive performance impact.

The JWT will have the same Claims section, however the header and signature sections will be different:

JOSE Header			
field	**description**	**default**	**mandatory**
alg:	Algorithmus used to sing the token.	"none"	yes

JWT Claims
See Signed X-Axa-Context Structure

Signature
Blank

References