Create JWT Functions Plugin - V2.0.0

Features

Create JWT Token with RS256 and PS256 signing algorithms using private key with Appian Secure Credentials.

1. **createjwttokenrs256withscs()** - Create and return a signed JWT using the RS256 algorithm.
2. **createjwttokenps256withscs()** - Create and return a signed JWT using the PS256 algorithm.

Create JWT Token With RS256 - createjwttokenwithrs256()

This function has been deprecated. Use **createjwttokenrs256withscs()** instead.

Create JWT Token RS256 With SCS - createjwttokenrs256withscs()

This function returns a signed JWT with the RS256 signature algorithm.

Parameters

Sl No	Name	Type	Description
1	kid	Text	The value to identify which key was used in signing the JWT.
2	issuer	Text	The value to identify the principal that issued the JWT.
3	subject	Text	The value to identify the principal that is the subject of the JWT.
4	audience	Text	The value to identify the recipients the JWT is intended for.

5	jti	Text	The value to uniquely identify the generated JWT. Provide null to disable jti.
6	expiry	Number(Integer)	Provide a non-negative value in seconds to modify the expiry time of the generated JWT. Default 3600 seconds (1 hour)
7	scope	Text	Provide the scope for the token.
8	scsKey	Text	Provide the Third-party Credential Store key. The Credential Store must contain the field 'privatekey' which must hold the private key content without the BEGIN and END markers. And not in DER format.
9	usePerUserCredentials	Text	Provide whether to use user specific credentials.

Output - The RS256 signed JSON Web Token (JWT)

Create JWT Token PS256 With SCS - createjwttokenps256withscs()

This function returns a signed JWT with the PS256 signature algorithm.

Parameters

Sl No	Name	Type	Description
1	kid	Text	The value to identify which key was used in signing the JWT.
2	issuer	Text	The value to identify the principal that issued the JWT.
3	subject	Text	The value to identify the principal that is the subject of the JWT.
4	audience	Text	The value to identify the recipients the JWT is intended for.
5	jti	Text	The value to uniquely identify the generated

			JWT. Provide null to disable jti.
6	expiry	Number(Integer)	Provide a non-negative value in seconds to modify the expiry time of the generated JWT. Default 3600 seconds (1 hour)
7	scsKey	Text	Provide the Third-party Credential Store key. The Credential Store must contain the field 'privatekey' which must hold the private key content without the BEGIN and END markers. And not in DER format.
8	usePerUserCredentials	Text	Provide whether to use user specific credentials.

Output - The PS256 signed JSON Web Token (JWT).