Additional Authentication Options Configuration

The SAML 2.0 authentication plugin allows configuring the authentication process by specifying additional options (not related to metadata and certificates).

The following is an example of a SAML 2.0 plugin configuration:

```
{
"Name": "Aras.OAuth.Server.Plugins.Saml2Authentication",
"Enabled": true,
    "Options": [{
        "AuthenticationType": "<AuthenticationType>",
        "DisplayName": "<DisplayName>",
        "ServiceProviderOptions": {
            "EntityId": "<ServiceProviderEntityId>"
"OutboundSigningAlgorithm": "Sha256",
            "SigningBehavior": "IfIdpWantAuthnRequestsSigned",
            "NameIdPolicy": {
                "AllowCreate": true,
                "Format": "Persistent"
            },
            "RequestedAuthnContext": {
                "ClassRef": "urn:oasis:names:tc:SAML:2.0:ac:classes:Password",
                "Comparison": "Minimum"
            }
            },
        "IdentityProviderOptions": {
            "EntityId": "https://idp.example.com",
        }
    }]
}
```

This configuration example specifies the following parameters:

- **OutboundSigningAlgorithm:** The signing algorithm for metadata and outbound messages (the default is Sha256). The algorithm is used for both service and identity providers. Other possible values are Sha514, Sha384 and Sha1 (case-insensitive; full algorithms signatures are also supported).
- **SigningBehavior**: The signing behavior of generated authentication requests (the default is IfIdpWantAuthnRequestsSigned, sign authentication requests if the identity provider is configured for it using its WantAuthnRequestsSigned property). Other possible values are:

Always (always sign all authentication requests) and Never (never sign any authentication requests).

- **NameIdPolicy:** Controls the generation of the NameIDPolicy element in authentication requests to manage the name identifier returned in the subjects of assertions. The name identifier can be used to map an external user to an Aras Innovator user.
- **AllowCreate:** A nullable value (true or false) indicates whether the identity provider is allowed while fulfilling the request to create a new identifier to represent the principal (the default is null, meaning that the attribute is not included in generated authentication requests). When false, the requester constrains the identity provider to only issue an assertion to it if an acceptable identifier for the principal has already been established.
- **Format:** The requested format of NameIDPolicy for generated authentication requests (the default is Transient). Other possible values are: NotConfigured, Unspecified, EmailAddress, X509SubjectName, WindowsDomainQualifiedName, KerberosPrincipalName, EntityIdentifier, and Persistent.

Important

Setting this parameter does not guarantee returning the NameID in a specified format. Some identity providers may ignore the format of NameIdPolicy. If Transient format is specified, it is not permitted to specify AllowCreate according to the SAML 2.0 specification.

- **RequestedAuthnContext:** Specifies the authentication context requirements of authentication statements returned in response to a request or **Query**.
  ClassRef: The URL reference identifying authentication context classes or declarations. It can be a full URL or a single word if one of the predefined classes is used in the SAML 2.0 Authentication context specification.

Important

Refer to section 3.4 of the SAML 2.0 Authentication context specification for predefined classes: http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf.

- **Comparison:** The comparison method used to evaluate the requested context classes or statements (the default is Exact). Other possible values are Minimum, Maximum, and Better.