

E&S/S API Security (Authentication) Guide v1.1

Table of Contents

[Table of Contents 2](#_Toc43955486)

[Chapter 1.0 Certificate Registration 11](#_Toc43955494)

[Chapter 2.0 SAML2.0 Assertion Generation and Reference Implementation 13](#_Toc43955495)

[Overview 13](#_Toc43955496)

[Sample SAML Assertion and Reference Implementation 13](#_Toc43955497)

[Chapter 3.0 Consume Nationwide Auth APIs 15](#_Toc43955498)

[Prerequisites 15](#_Toc43955499)

[Overview 15](#_Toc43955500)

[Nationwide Authentication 15](#_Toc43955501)

[Nationwide Authentication Errors 18](#_Toc43955502)

[Re-Authentication (refreshing tokens) using “refresh\_token” 19](#_Toc43955503)

[Chapter 4.0 Consume Business APIs 20](#_Toc43955504)

[Prerequisites 20](#_Toc43955505)

[Overview 20](#_Toc43955506)

[Chapter 5.0 Troubleshooting & FAQ 21](#_Toc43955507)

[Chapter 6.0 Path to Production 22](#_Toc43955508)

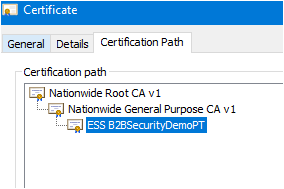
[Chapter 7.0 Document Info & Revision History 22](#_Toc43955509)

* 1. Certificate Registration

To access any API of Nationwide E&S/S, all the consumers (Agency or Nationwide internal applications) are required to register their public CA (Certification Authority) certificate with Nationwide for trusted authentication.

1. The Consumer should provide the following to the assigned contact person in E&S/S.
   * 1. **Certificate Chain** (ordered list of certificates containing an SSL certificate, CA certificates) **consisting of all or three different certificates (.cer) files.**
        + Root CA certificate
        + Intermediates certificate(s)
        + End-user certificate

*For reference purposes,* please see the below image where the entire certificate-chain (three certs) is shown.

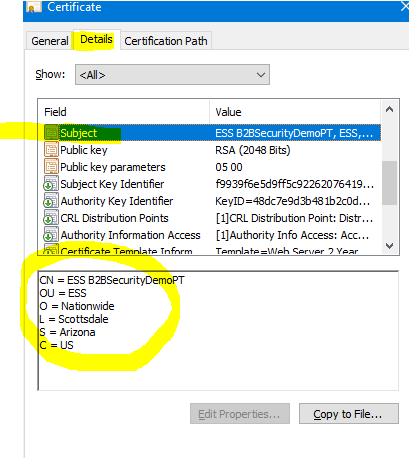


* + 1. **Certificate Subject DN** should be in the following pattern shown as in the example.

Please note to remove the any special characters such as *&, :, <, >, ;* but *c*ommas are allowed

**e.g.:** CN=<ESSDEMO>,OU=<ESS>,O=<Nationwide>,L=<Scottsdale>,ST=<Arizona>,C=<US>

The same details can be also be found from the end-user certificate as shown in the below image.



**Note**: *Please beware of Microsoft Outlook modifying/correcting the Issuer ID. Verify that the Issuer ID is not altered.*

Nationwide E&S/S IT team will raise a request in ServiceNow to the “IAM-Support-Access” team to install these certificates and issuer details in Nationwide certificate repo.

NOTE: If you choose to use a **self-signed certificate**, please follow the steps provided in the below document “A Guide to Self-Signed Certificate Creation .docx”.

* 1. SAML2.0 Assertion Generation and Reference Implementation

## Overview

Nationwide E&S/S has chosen the “SAML – Bearer Grant” pattern, an extension of OAuth framework, that provides a mechanism for exchanging SAML assertions for access tokens. This extension is described in the IETF specification ([RFC 7522](https://tools.ietf.org/html/rfc7522)).

In this pattern, the client application has already authenticated the user through some other means and has obtained a SAML assertion from the Identity Provider (IdP) representing this user context. This IdP may be a third-party IdP.

## Sample SAML Assertion and Reference Implementation

There are many ways to generate SAML2 Assertion as it completely depends on IT capabilities (OpenSaml2, OpenSaml3, or IdP) of a Consumer.

The following embedded ‘opensaml3-utils-0.0.1.jar.txt’ and ‘opensaml3-utils-usage.docx’ files have been developed as Proof of Concept for both internal and external (Agencies) consumers of Nationwide.

**Note**: To avoid the Jar files being blocked by Email filters, the jar is changed to .txt extention. Download ‘opensaml3-utils-0.0.1.jar.txt’ and change the extension to .jar.



The output, SAML Assertion, of ‘opensaml3-utils.jar’ is also embedded below.



Key information in SAML Assertion:

|  |
| --- |
| <saml2:Issuer>ess-nationwide-test.***agencyname***.com</saml2:Issuer>  Please provide ess-nationwide-test.***agencyname***.com for the test environments and ess-nationwide.***agencyname***.com in the production environment for saml Issuer. The ***agencyname*** should be replaced with the actual agency name and the entire string should be in lower case.  Please note that *the consumer and Nationwide should agree upon the string*. |

|  |  |  |  |
| --- | --- | --- | --- |
| For General Agency level (System account in ESS Portal) account:     |  | | --- | | <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">[**nationwideess@youragencydomain.com**</saml2:NameID](mailto:nationwideess@youragencydomain.com%3c/saml2:NameID)>  <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:sender-vouches" />  **Note:** Contact Nationwide representative to know the correct NameID for agency to use. The Agency level accounts begin with “nationwideess@” prefix. |   For General Agent (User account in ESS Portal) account:   |  | | --- | | <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">**GeneralAgentIDInESSPortal@youragencydomain.com**</saml2:NameID>  <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:sender-vouches" />  **Note**: Contact Nationwide representative to know the correct NameID for General Agent to use. |   For Nationwide Internal (User or IIQServiceShared) account:   |  | | --- | | <saml2:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">**IIQREGISTEREDUSERNAME**</saml2:NameID>  <saml2:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:sender-vouches" />  **Note**: Reach out to Nationwide IT Asset Manager or Technical Owner to know the correct NameID for your IIQ Registered ID to use. | |

Nationwide will NOT accept SAML assertion with validity/expiration time more than 5 hours since it received the request.

|  |
| --- |
| <saml2:Subject>  <saml2:SubjectConfirmation  Method="urn:oasis:names:tc:SAML:2.0:cm:sender-vouches" />  <saml2:SubjectConfirmation  Method="urn:oasis:names:tc:SAML:2.0:cm:sender-vouches">  <saml2:SubjectConfirmationData  NotBefore="2019-09-11T20:25:41.250Z"  NotOnOrAfter="2019-09-11T21:25:41.250Z" />  </saml2:SubjectConfirmation>  </saml2:Subject>  <saml2:Conditions NotBefore="2019-09-11T20:25:41.253Z"  NotOnOrAfter="2019-09-11T20:35:41.253Z">  <saml2:AudienceRestriction>  <saml2:Audience>https://identity.nationwide.com</saml2:Audience>  </saml2:AudienceRestriction>  <saml2:OneTimeUse />  </saml2:Conditions>  <saml2:AuthnStatement  AuthnInstant="2019-09-11T20:25:41.258Z">  <saml2:AuthnContext>  <saml2:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</saml2:AuthnContextClassRef>  </saml2:AuthnContext>  </saml2:AuthnStatement>  **Note:** Reach out to Nationwide Technical Owner to know the correct **Audience** as it is dependent on runtime environment (e.g.: PT/Stage or Prod etc..). For Production: <https://identity.nationwide.com>, for Test(Stage): <https://identity-pt.nationwide.com> |

* 1. Consume Nationwide Auth APIs

## Prerequisites

The Consumer certificate chain (three or more .cer files) with Issuer ID have been installed in Nationwide’s certificate repository to establish the trusted relationship between Nationwide and Consumer.

## Overview

This section contains the instructions to consume the APIs.

In the Modern Web Architecture, there are new security risks within the client context (i.e., browser-based, mobile, etc.) and therefore can no longer be considered trusted. Application code is exposed to the browser, allowing the user to potentially manipulate the context of API calls.

OAuth 2.0 was created to address this problem. OAuth provides a new set of security patterns for APIs to provide authorization in a more secure way. Nationwide’s API Management team has developed the Enterprise User Auth API as a shared resource for implementing User Authorization.

The client application may exchange this SAML for an access token by making a request to EUA, passing along the SAML. EUA must validate the SAML prior to issuing an access token. If the SAML was generated by a third-party IdP, then EUA makes a back-end call for validation. Upon successful validation, EUA then issues an access token and returns it directly to the client without a redirect.

|  |  |
| --- | --- |
| Nationwide Authentication |  |
| Get Authentication tokens before accessing functional (business application) API endpoints. Nationwide supports only one OAuth grant type (SAML2 Bearer Assertion) for **Distribution (Agency) Partners** for authentication  ***Example 1:***   |  |  | | --- | --- | | **Test** Endpoint: | *https://api-stage.nationwide.com/security-processing/enterprise-user-auth/v2/token.oauth2* | | **Prod** Endpoint | *https://api.nationwide.com/security-processing/enterprise-user-auth/v2/token.oauth2* | | Method | POST |   HTTP Request **Headers**:   |  |  | | --- | --- | | **Name** | **Value** | | Content-Type | application/x-www-form-urlencoded |   HTTP Request **Body**:   |  |  |  | | --- | --- | --- | | **Sr.No** | **Name** | **Value** | | 1 | grant\_type | *urn:ietf:paramsoap:oauth:grant-type:saml2-bearer* | | 2 | client\_id | <Enter value of **Consumer Key** obtained during App> | | 3 | scope | openid | | 4 | realm | distribution-partner | | 5 | auth\_method | ping-sts | | 6 | identity\_method | ness | | 7 | assertion | Some clients (e.g. Postman) require <Enter **Base64Encoded** of **SAML2 Assertion**>  Web applications require: <Enter **URLEncoded** and **Base64Encoded** of **SAML2Assertion**> |   For instructions on generating SAML Assertion, read the “SAML Assertion Generation” section.  **Note**: *For security purposes, Nationwide rejects any SAML assertion with a validity period (the value of NotOnOrAfter) more than 300 minutes from generated time. So please limit the validity period to less than 5 hours.*    HTTP Response **Body**:   |  |  | | --- | --- | | **Response** | {  "access\_token": "CRGX8kGDoSJh4HGbmYnggqYtr1C6",  "token\_type": "Bearer",  "expires\_in": 1199,  "scope": "openid",  "refresh\_token": "QAtJOvEqn6X0n1nJp49HUYopK7zqV3Gt",  "id\_token": "eyJqa3UiOiJodHRwczpcL1wvYXBpLXN0YWdlLm5hdGlvbnd…………………………”  } |   ***Example 2: The following image reflects the Authentication call from Postman***    **Explanation of Tokens in Response:**  **access\_token:**  The “access\_token” is generally needed in every subsequent request to any API to avoid re-authentication. It has a shorter (*20 minutes/*1199 seconds) validity period so that if an attacker obtains the access token, they have a limited time in which to use it.  **refresh\_token:**  The “refresh\_token” is valid for *8 hours* with the purpose of obtaining a new valid “access\_token” when prior issued “access\_token” is expired. The token can also be created for “revoking a token”. If the refresh\_token is compromised, the attacker also requires “client\_id” and “client\_secret”.  The goal of using two types of tokens is to enhance user security. | |

|  |  |
| --- | --- |
| Nationwide Authentication Errors |  |
| In the event of any of the following error conditions have been met the Nationwide Authentication API rejects the request.   * Invalid “client\_id” (Prod Key) * Invalid value in “assertion”   + Not *Base64 Encoded*   + Not *URLEncoded* over *Base64Encoded*   + Not matching the value of “<Saml2:Issuer>” to original **Issuer ID** of Certificate   + Not matching the value of “<ds:X509Certificate>” to the certificate(s) exchanged with Nationwide.   + Invalid value in “<saml2:Audience>” (<http://identity-pt.nationwide.com> or <https://identity.nationwide.com>   + Not matching the value of “<saml2:NameID> in Nationwide or ESS directories (repositories) | |

|  |  |
| --- | --- |
| Re-Authentication (refreshing tokens) using “refresh\_token” |  |
| If “access\_token” is expired in 20 min, the client is recommended to obtain new access\_token (re-authentication) using “refresh\_token”.  Please note that, if the “refresh\_token” is expired, then the client application is required to re-submit “SAML Assertion” to get both new “access\_token” and “refresh\_token”.  ***Example 1:***   |  |  | | --- | --- | | **Test** Endpoint: | *https://api-stage.nationwide.com/security-processing/enterprise-user-auth/v2/token* | | **Prod** Endpoint | *https://api.nationwide.com/security-processing/enterprise-user-auth/v2/token* | | Method | POST |   HTTP Request **Headers**:   |  |  | | --- | --- | | **Name** | **Value** | | Content-Type | application/x-www-form-urlencoded | | Authorization | Basic Base64Encode (${client\_id}**:**${client\_secret})  E.g.: Basic RGgysfsiewkjkfLIJIewljfjskafilkjegxZFc6emN5b2dOVGczMEx1WWk5cA== |   HTTP Request **Body**:   |  |  |  | | --- | --- | --- | | **Sr. No** | **Name** | **Value** | | 1 | grant\_type | *refresh\_token* | | 2 | refresh\_token | <Enter value of refresh\_token obtained during initial authentication> |   HTTP Response **Body**:   |  |  | | --- | --- | | **Response** | {  "access\_token": "2345GX8kxresdfesfJh4HGbmYnggqYtrsdDf",  "token\_type": "Bearer",  "expires\_in": 1199,  "scope": "openid",  "refresh\_token": "QAtJOvEqn6X0n1nJp49HUYopK7zqV3Gt",  "id\_token": "eyJqa3UiOiJodHRwczpcL1wvYXBpLXN0YWdlLm5hdGlvbnd…………………………”  } |   ***Example 2:***    **Explanation of Tokens in Response:**  **access\_token:**  The “access\_token” is new(refreshed) needed in every subsequent request to any API to avoid re-authentication. It has a shorter (*20 minutes/*1199 seconds) validity period so that if an attacker obtains the access token, they have a limited time in which to use it.  **refresh\_token:**  The “refresh\_token” is the same and valid for *8 hours* with the purpose of obtaining a new valid “access\_token” when prior issued “access\_token” is expired. The token can also be created for “revoking a token”. If the refresh\_token is compromised, the attacker also requires “client\_id” and “client\_secret”.  The goal of using two types of tokens is to enhance user security. | |

* 1. Consume Business APIs

## Prerequisites

The Consumer has been set up in Nationwide and successfully completed all the following.

1. Registered Account in Nationwide Developer API portal.
2. Registered App and obtained OAuth Keys from the Nationwide Developer API portal.
3. Acquired OAuth tokens (*access\_token* and *refresh\_token*) from Nationwide’s Authentication (EUA) API.
4. Nationwide Business Unit (e.g.: ESS) has completed activities of consumer account profile set up in corresponding directories/repositories.

## Overview

Please refer to the documentation (OAS and Help Guide) of Business API that you are interested in.

* 1. Troubleshooting & FAQ

1. Consumer has an **account registered** in <https://developer.nationwide.com>
2. Consumer has created **Two different (**Test and Prod) **Apps** and **obtained different OAuth Keys (Prod Key** and **Prod Secret)**
3. Consumer has added or subscribed all the required **API Products**
4. Consumer (Agency application or Nationwide application) has **Public CA (third-party) approved certificate** (a cert chain with three files) and **Issuer Id**. Nationwide **does not recognize Private CA** Cert due to the Business-to-Business interaction.
5. How many certificates are needed?

*Though* ***one certificate is enough for both*** *Test and Production environments, two-separate certificates will offer more security.*

1. What are the requirements on Certificate key length and Expiration Dates?

*A* ***2048-bit*** *is required with* ***longer validity period*** *to avoid frequent certificate lifecycle issues.*

1. Consumer is using correct **Issuer ID** in <saml2:Issuer> element in SAML Assertion matching to Issuer ID used in during the installation of certificates in Nationwide repository (PingFed).
2. Consumer is using the **appropriate user account** in <saml2:NameID> element in SAML Assertion.

* For Agency Level user account (e.g. [nationwideess@testagency.com](mailto:nationwideess@testagency.com))
* For General Agent account (e.g. [fname.lname@testagency.com](mailto:fname.lname@testagency.com))
* For Internal Nationwide User account (e.g.: LASTNF1)
* For Internal Nationwide System/IIQ account (e.g.: parentOrgAssetName or sgESS\*\*\*)

1. Consumer is using correct value in <**saml2:Audience**>.
2. For Test (Stage): <https://identity-pt.nationwide.com>
3. For Production: <https://identity.nationwide.com>
4. Consumer generated SAML Assertion should only be **active at least 10 min and less than 5 hours** from it is submitted to Nationwide for successful authentication.
5. Consumer should use the ZULU time format in the assertion.
6. Consumer should use RSA-256 for signature and digest algorithms.
7. Consumer **first applied Encoded with Base64 on SAML Assertion before URLEncoded** to avoid the loss of data during HTTP transfer.

Nationwide IAM Support Access group has installed the certificates (three .cer) with correct Issuer ID. No additional whitespace characters unless the consumer provided it.

* 1. Path to Production

1. Initially during registration, if you had created 2 separate apps for test and production, use the API Key of the Prod App, if you have just one app, then use the same API Key which you have been using until now.

2. Verify with Nationwide representative if your Agency ID ([nationwideess@xxxxx.com](mailto:nationwideess@xxxxx.com)) has been created in production.

2.1 Nationwide representative should verify if the ID is available in the production LDAP, B2B Container and EC2 and has the correct roles and group membership.

3. Procure production certificates and provide to Nationwide.

4. Use ess-nationwide.agencyname.com for the SAML Issuer id instead of ess-nationwide-test.agencyname.com.

5. Use the production URL for the Security, Reference and the Quote APIs.

6. Schedule a validation session to ensure that there are no issues in connectivity with the production environment.

* 1. Document Info & Revision History

**References:**

**Document Revisions**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Author(s)** | **Revision Notes** |
| 1.0 | 10/31/2019 | Yaman Rangineni | Initial Draft |
| 1.1 | 12/10/2019 | Yaman Rangineni | Added FAQ |
| 1.2 | 05/15/2020 | Nitin Jha | Updated SAML Issuer ID |
| 1.3 | 06/01/2020 | Nitin Jha | Updated troubleshooting section |
| 1.4 | 06/17/2020 | Nitin Jha | Added path to production |