CONSEIL SUPÉRIEUR
DU NOTARIAT

ID.NOT
Présentation et guide d'intégration

SSO - Fédération d'identité - OpenIDConnect

31/01/2023

Qu'Est-ce qu'est ID.not ?

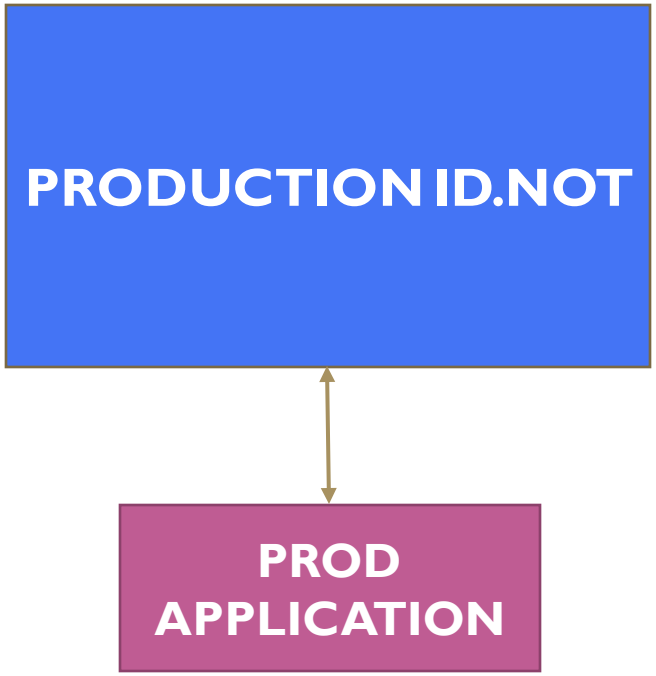
- ID.NOT offre un moyen d'authentification unique, simplifié et sécurisé aux applications de la profession.
- Chaque utilisateur accède aux applications métiers intégrantes ID.NOT grâce à un seul et unique identifiant / mot de passe.
- Les utilisateurs d'ID.NOT peuvent renforcer la sécurité de leur accès grâce à une application mobile disponible sur les 2 stores (Apple et Google).
- ID.NOT repose sur les protocoles d'authentification et d'autorisation OpenIDConnect et SAML.

Qui possède un compte ID.not?

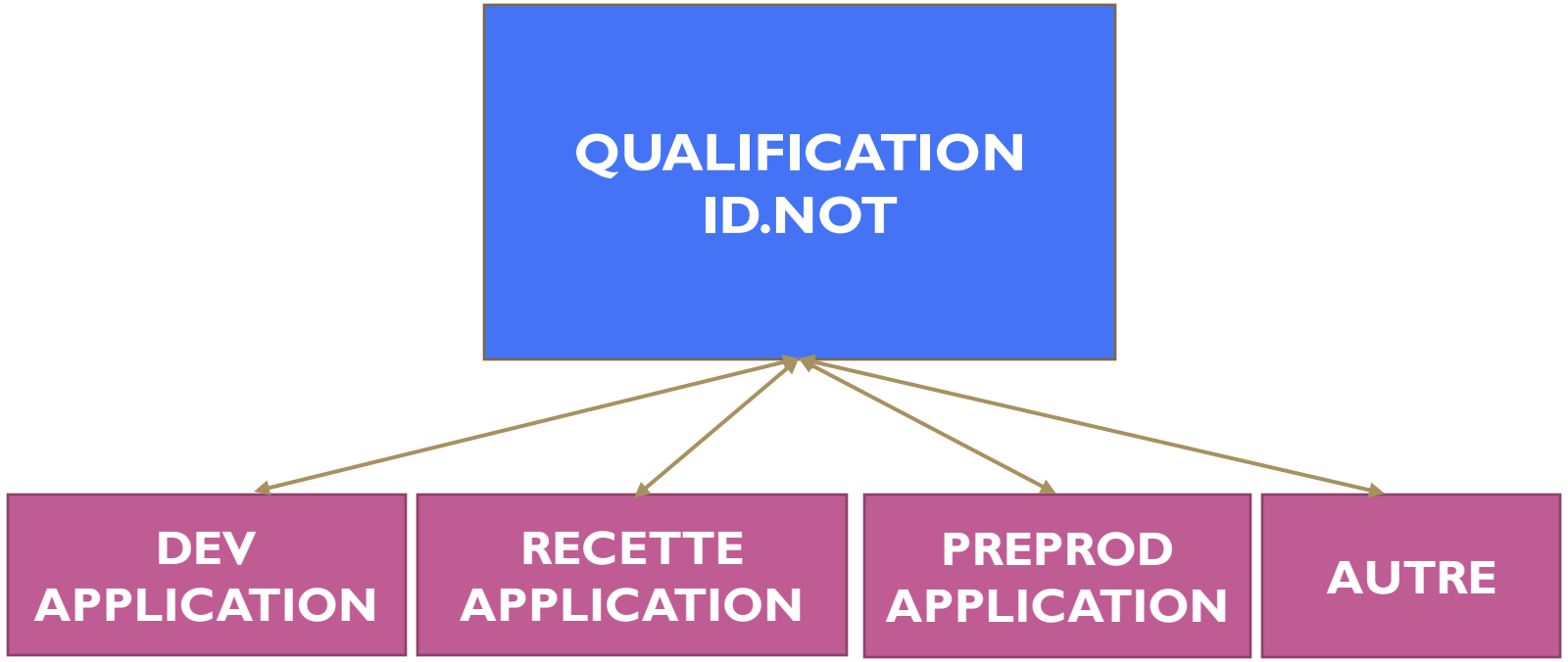
- L'ensemble des notaires possède un compte ID.NOT.
- Les collaborateurs des offices, des instances et des organisations de la profession peuvent se créer leur compte ID.NOT et demander aux gestionnaires de leurs entités de les rattacher à cette dernière.
- Les collaborateurs travaillant dans plusieurs entités de la profession ne possèdent qu'un seul compte ID.NOT : c'est au moment de l'authentification que le choix du profil entité est proposé.
- Il en est de même pour les notaires qui exercent en plus un mandat dans une instance.

Environnements

https://connexion.idnot.fr



https://qual-connexion.idnot.fr

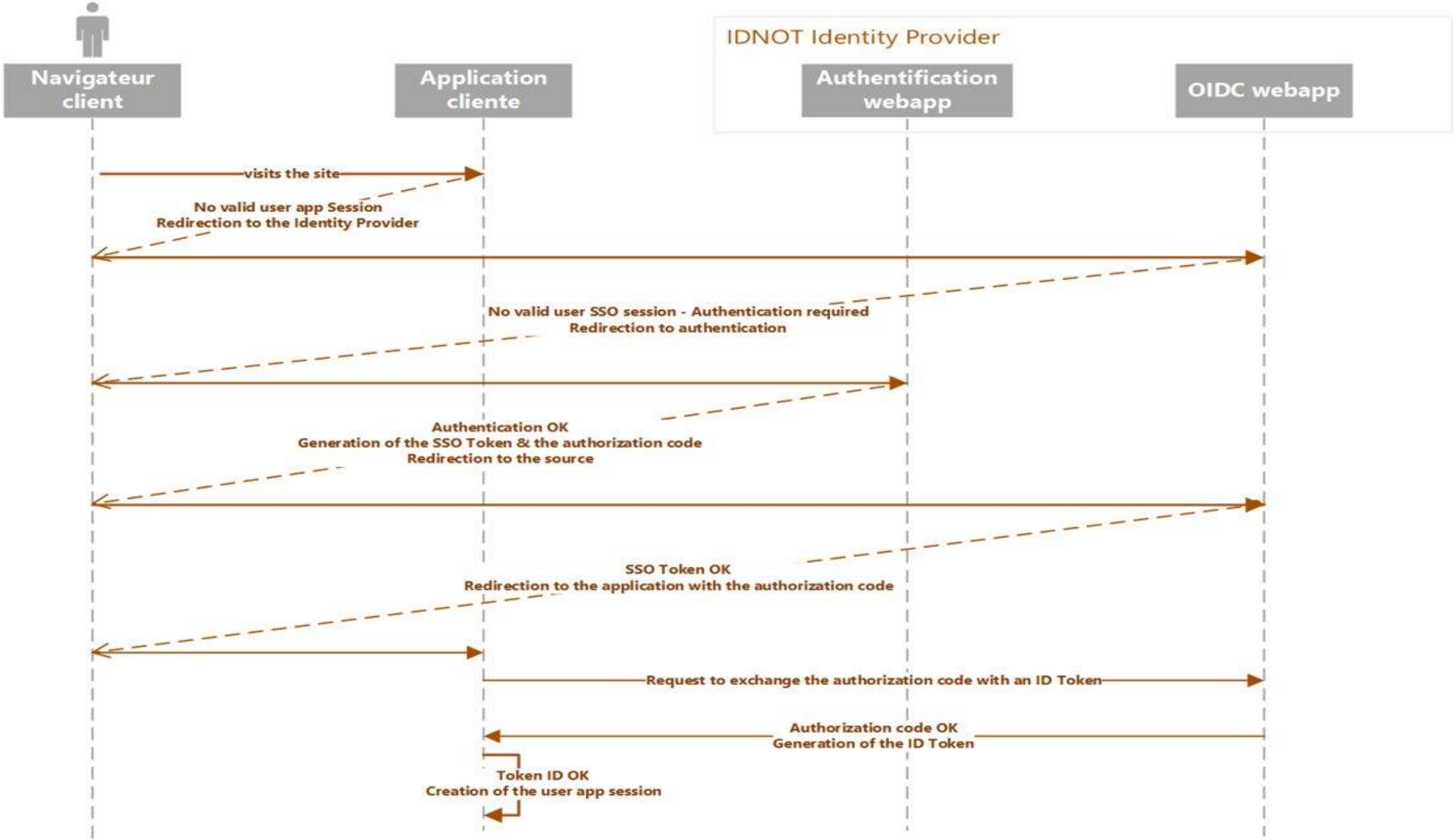


Gestion des raccordements OpenIDConnect

Après avoir créé l'application sur le portail des raccordements (https://portail-raccordement.api.notaires.fr)

1. Accéder à l'application qui doit être créée par la structure propriétaire.
2. Accéder à l'environnement concernée.
3. Le raccordement à ID.NOT se configure sur la partie « RACCORDEMENT ID.NOT».
    - Si aucun raccordement n'est en place, cliquer sur configurer.
    - Configurer les droits d'accès à l'application.
    - Configurer le raccordement OpenIDConnect.

Séquences. Cas OpenID Connect / Authorization code flow



Guide de mise en place rapide d'un raccordement OpenID Connect

Configuration

La configuration OpenIDConnect est disponible dans le lien ci-dessous

Production

https://connexion.idnot.fr/IdPOAuth2/idnot_idp_v1/.well-known/openid-configuration

Environnement d'intégration

https://qual-connexion.idnot.fr/IdPOAuth2/idnot_idp_v1/.well-known/openid-configuration

Guide de mise en place rapide de l'Authorization Code Flow pour un raccordement OpenID Connect

Etape 1 : Demander l'authentification de l'utilisateur et obtenir le code d'autorisation

```
Get https://connexion.idnot.fr/IdPOAuth2/authorize/idnot_idp_v1?
client_id=000087653287
&redirect_uri=RP_redirect_uri
&scope=openid,profile,offline_access
&response_type=code
```

- *Si l'authentification ID.NOT n'est pas déjà effectuée, l'utilisateur est redirigé vers la page d'authentification ID.NOT.*
- *L'utilisateur se connecte et choisit son entité de rattachement.*
- *Si l'accès est accordé, ID.NOT génère un code d'autorisation.*
- *ID.NOT redirige l'utilisateur vers l'application appelante en utilisant l'URL de callback avec le code d'autorisation en paramètre.*

Guide de mise en place rapide de l'Authorization Code Flow pour un raccordement OpenID Connect

Etape 2 : Demander l'identification de l'utilisateur et obtenir l'ID Token JWT

```
POST https://connexion.idnot.fr/IdPOAuth2/token/idnot_idp_v1?
client_id=000087693287
&client_secret=48BA750DC1B31064FFA91D8B7DF...
&redirect_uri=RP_redirect_uri
&code=code d'autorisation
&grantType=authorization_code
```

- *ID.NOT génère un ID Token.Vous pouvez appeler l'"Annuaire API" en utilisant les informations de l'ID Token pour une identification plus poussée.*

Exemple

Header : algorithme et type de jeton


```
{
  "x5t#S256": "yKOx98Mi59XsrWKQcU1P5gCJiULT0wmm2LShlkFvEeM",
  "x5t": "49W-offRFWPPrAyDBuw0g0sDwBM",
  "kid":
"bd343d26a5608c5e3241b457c6b805306a2ee44a4b46c1481d664a4bbdd02cf616c7d2d69ed607422f818d51
6743427a081657bc72e176ed2dcd946b786259d3sig",
  "alg": "RS512"
}
```

Guide de mise en place rapide de l'Authorization Code Flow pour un raccordement OpenID Connect

Etape 2 : Demander l'identification de l'utilisateur et obtenir l'ID Token JWT

Payload : données


```
{
  "at_hash": "DQLI1_wBg085t3f0fq8BYxghzIXaMBaQu4UWz07iG7o",
  "sub": "IDN26889949I",
  "profile_idn": "IDN26889949I_IDN009850",
  "amr": [
    "11"
  ],
  "iss": "https://connexion.idnot.fr/IdPOAuth2/idnot_idp_v1",
  "given_name": "Marie",
  "aud": "8B157912AFEEC6D1",
  "nbf": 1669713196,
  "auth_time": 1669713195,
  "entity_idn": "IDN009850",
  "name": "DUPONT",
  "exp": 1669720396,
  "iat": 1669713196,
  "email": "marie.dupont@notaires.fr"
}
```

Intégration OpenID Connect

Recommandations de l'ANSSI

https://www.ssi.gouv.fr/uploads/2020/09/anssi-guide-recommandations_pour_la_securisation_de_la_mise_en_oeuvre_du_protocole_openid_connect-v1.0.pdf

Contenu du Jeton d'identification

- Le jeton d'identification contient les informations suivantes
  - Sub: identifiant unique de l'utilisateur.
  - Name : Nom usuel de l'utilisateur.
  - Given_name: prénom de l'utilisateur.
  - Entity_idn: identifiant de la structure liée au profil de connexion.
  - Profile_idn: identifiant du rattachement lié au profil de connexion.
    - Le rattachement est le lien entre la personne et son entité, il porte la fonction et les données professionnelles.
  - Email: email professionnel (donnée du rattachement)
    - ➢ Information non présente par défaut. Le besoin doit être justifié.

- Toute information complémentaire peut être récupérée via l'API Annuaire (https://api.notaires.fr/annuaire) en utilisant l'identifiant unique de l'utilisateur, l'identifiant du profil de connexion (profile_idn) ou l'identifiant de la structure (entity_idn)

Gestion des raccordements SAML

Etapes

Après avoir créé l'application sur le portail des raccordements, l'échange des informations techniques se fait par email (raccordement.application.csn@notaires.fr)

1. L'équipe de raccordement vous transmet les métadonnées Idp (fournisseur d'identité)
    - Urls de connexion et de déconnexion.
    - Clé publique du certificat de signature de l'Idp
2. Vous transmettez à l'équipe de raccordement les métadonnées SP (fournisseur de service)
    - Url de réception de l'assertion ou de la réponse SAML
    - Clé publique du certificat de signature du SP
3. L'équipe de raccordement intègre les métadonnées SP et vous intégrez les métadonnées Idp.

Gestion des raccordements SAML

Réponse SAML

La réponse SAML contient

- Le prénom de l'utilisateur.
- Le nom de l'utilisateur.
- L 'identifiant unique de l'utilisateur dans l'annuaire de la profession.
- L'identifiant de l'entité liée au profil de connexion.

Gestion des raccordements SAML

Exemple de réponse SAML - Signature

```
<?xml version="1.0" encoding="UTF-8"?>
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" xmlns:ds="" xmlns:saml="" xmlns:xenc=""
Destination="https://callback/SAMLAssertionConsumer" ID="" InResponseTo="" IssueInstant="2023-02-03T16:11:35Z" Version="2.0">
 <saml:Issuer>IDNOT</saml:Issuer>
 <ds:Signature>
  <ds:SignedInfo>
</ds:SignedInfo>
  <ds:SignatureValue>xM4h4aHmF06+cgW8mgwLhqGWyibuU7+Da1CvUtusgOZKHqSRAz3ZF7BAwLxZupQNi1KKjbfhw...</ds:SignatureValue>
  <ds:KeyInfo>
   <ds:X509Data>
<ds:X509Certificate>MIIEgzCCA2ugAwIBAgIBATANBgkqhkiG9w0BAQsFADCB0DELMAkGA1UEBhMCRlIxFjAUBgNVBA...</ds:X509Certificate>
   </ds:X509Data>
   <ds:KeyValue>
    <ds:RSAKeyValue>
     <ds:Modulus>yAo4WugtdFVEp57lC2nvxrxBXFRvwH+NtmCqA7xDLfCeNGaep36YQa77sSK3+5PRPfYzwWCU1qbfNyvIq1yeBtw...</ds:Modulus>
     <ds:Exponent>AQAB</ds:Exponent>
    </ds:RSAKeyValue>
   </ds:KeyValue>
  </ds:KeyInfo>
 </ds:Signature>
 <samlp:Status>
  <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"></samlp:StatusCode>
 </samlp:Status>
```

Gestion des raccordements SAML

Exemple de réponse SAML - Contenu de l'assertion

```
<saml:Assertion ID="_19689848748452c64c9a34d6b26c3e80" IssueInstant="2023-02-03T16:11:35Z" Version="2.0">
  <saml:Issuer>IDNOT</saml:Issuer>
  <saml:Subject>
   <saml:NameID  Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">IDN26279949I</saml:NameID>
   <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <saml:SubjectConfirmationData InResponseTo="_cd16720b" NotOnOrAfter="2023-02-03T16:13:35Z"
Recipient="https://callback/SAMLAssertionConsumer"></saml:SubjectConfirmationData>
   </saml:SubjectConfirmation>
  </saml:Subject>
<saml:AuthnStatement AuthnInstant="2023-02-03T16:11:35Z" SessionIndex="_19689848748452c64c9a34d6b26c3e80">
   <saml:AuthnContext>
    <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified</saml:AuthnContextClassRef>
   </saml:AuthnContext>
  </saml:AuthnStatement>
  <saml:AttributeStatement>
   <saml:Attribute Name="givenName">
    <saml:AttributeValue xmlns:xs="" xmlns:xsi="" xsi:type="xs:string">Marie</saml:AttributeValue>
   </saml:Attribute>
   <saml:Attribute Name="name">
    <saml:AttributeValue xmlns:xs="" xmlns:xsi="" xsi:type="xs:string">DUPONT</saml:AttributeValue>
   </saml:Attribute>
   <saml:Attribute Name="uid">
    <saml:AttributeValue xmlns:xs="" xmlns:xsi="" xsi:type="xs:string">IDN26279749I</saml:AttributeValue>
   </saml:Attribute>
   <saml:Attribute Name="entities">
    <saml:AttributeValue xmlns:xs="" xmlns:xsi="" xsi:type="xs:string">IDN008961</saml:AttributeValue>
   </saml:Attribute>
  </saml:AttributeStatement>
 </saml:Assertion>
</samlp:Response>
```

Gestion des personas – Comptes de test

Il est possible de créer des comptes de test sur l'environnement d'intégration (https://qual-connexion.idnot.fr) via le portail des raccordements https://portail-raccordement.api.notaires.fr/

Composant cartouche

Homogénéité de l'identité visuelle

Le cartouche est composé de 4 éléments :

- Photo de l'utilisateur connecté: la photo peut être récupérée via l'API Annuaire
  - Si la photo est absente , il convient d'utiliser les avatars suivants


- Prénom / Nom de l'utilisateur connecté.
- Menu contextuel.
- Bouton Applications : lien vers le portail des applications de la profession (optionnel : à considérer en fonction du contexte du projet).
  - Tooltip: Portail REAL – Services
  - Lien: https://intra.notaires.fr/jcms/lpo_3000242/fr/services

Composant cartouche

Menu contextuel

En cliquant sur le groupe « photo/nom complet/flèche », un menu contextuel s'affiche avec les liens suivants :

- « Mon Compte ID.NOT » : ce lien mène l'utilisateur vers le site de gestion de son compte ID.NOT. Ouverture dans un nouvel onglet.
  - Compte ID.NOT Qualif : https://qual-moncompte.idnot.fr
  - Compte ID.NOT Prod : https://compte.idnot.fr
- « Se déconnecter ou Déconnexion » : Ce lien déconnecte l'utilisateur de l'application et de ID.NOT.
  - SAML: L'url de « Single logout » est présente dans le fichier de métadonnées de l'IDP.
  - OpenID Connect : se fait en deux étapes :
    - Fermer la session de l'application.
    - Fermer la session SSO ID.NOT en appelant l'url :
      - Qualif : https://qual-connexion.idnot.fr/auth/logout
      - Prod : https://connexion.idnot.fr/auth/logout

Support

@mail: raccordement.application.csn@notaires.fr

Conseil Supérieur
du Notariat