AGENCE DU NUMÉRIQUE EN SANTÉ

PRO SANTÉ CONNECT

Démonstration OpenID CIBA

22/03/2021

AGENCE DU NUMÉRIQUE EN SANTÉ

Sommaire

AGENCE
DU NUMÉRIQUE
EN SANTÉ

Norme OpenID CIBA

Norme OpenID CIBA

CIBA signifie ‘Client Initiated BackChannel Authentication’

Cette norme, Open Source, sortie en mai 2020, est en cours de spécification actuellement chez Open ID (Draft #3) :

- La norme Open ID CIBA permet d’authentifier des utilisateurs n’ayant pas de navigateur ou de web agent. Les applications lourdes ou mobiles natives pourront utiliser le mode Open ID CIBA
- La norme Open ID CIBA se base sur un mécanisme de flux découplé, sans redirection, rendant ainsi meilleure l’expérience utilisateur

CIBA est un nouveau mécanisme Open ID qui permet aux parties de confiance (poste client), à partir d’un identifiant d’utilisateur, de démarrer un processus d’identification pour l’utilisateur sans que l’utilisateur ait besoin d’interagir davantage

Ce mécanisme implique une communication directe entre l’utilisateur et le fournisseur d’identité sans redirection dans le navigateur de l’utilisateur

L’utilisateur ne doit pas fournir son moyen d’identification à l’appareil consommateur

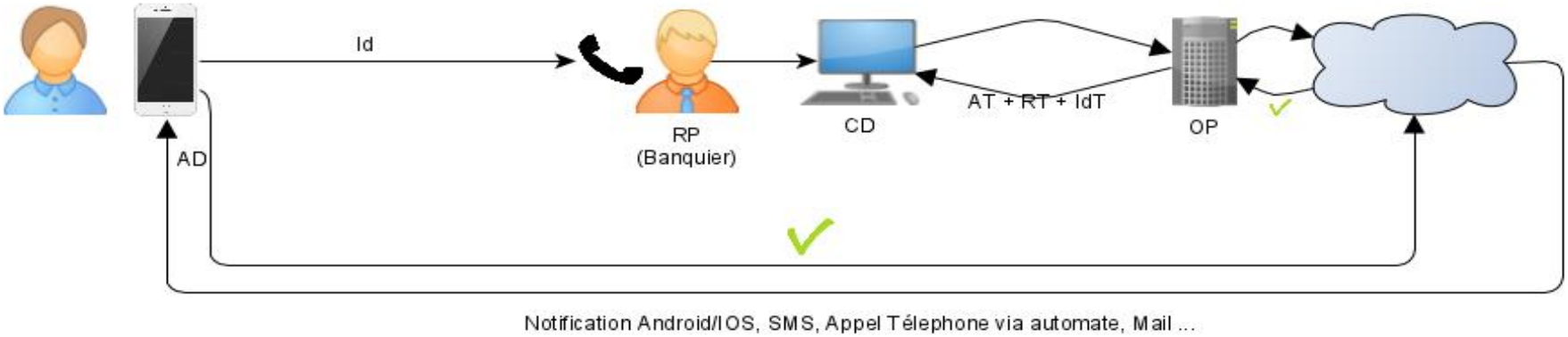
AGENCE
DU NUMÉRIQUE
EN SANTÉ

Cas d’usage

Le banquier

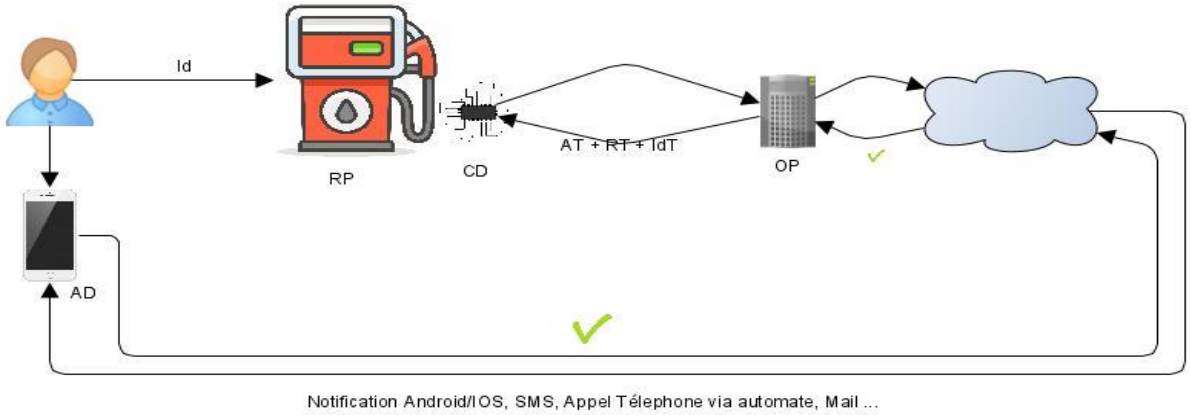
La pompe à essence

Cas d'usage – le banquier



1. Un utilisateur appelle son banquier pour opérer un virement
2. Le banquier effectue une opération sur son système d'information qui envoie une notification à l'utilisateur
3. L'utilisateur reçoit une notification et l'accepte
4. L'opération sur le système d'information du banquier est confirmée

Cas d'usage – la pompe à essence



1. Un utilisateur veut utiliser une pompe à essence connectée à un système d'information
2. La pompe à essence effectue une opération sur son système d'information qui envoie une notification à l'utilisateur
3. L'utilisateur reçoit une notification et l'accepte
4. L'opération sur le système d'information de la pompe à essence est confirmée
5. L'utilisateur peut se servir

AGENCE
DU NUMÉRIQUE
EN SANTÉ

Besoin

Pourquoi CIBA

Besoin – Pourquoi CIBA

Certains fournisseurs et grands acteurs du monde de la Santé sont demandeurs de ce mécanisme.

L'ensemble des services dédiés aux personnels de Santé pourront bénéficier de Pro Santé Connect grâce à ce mécanisme.

Les usages de la e-CPS seront renforcés pour devenir le mode d'authentification principal pour l'ensemble des acteurs de la Santé.

L'ANS souhaite que soit implémentée ce mécanisme CIBA au plus tôt dans la e-CPS en 3 étapes :

- POC de l'intégration du mécanisme CIBA à la e-CPS (déjà réalisé)
- Intégration du mécanisme CIBA dans l'environnement Bac à Sable dédié aux fournisseurs de service (Courant S2)
- Intégration du mécanisme CIBA dans l'environnement de production (Courant S2)

AGENCE
DU NUMÉRIQUE
EN SANTÉ

Travaux réalisés

Travaux réalisés

L'ANS participe activement à la communauté Open Source en charge de définir la norme OpenID CIBA.

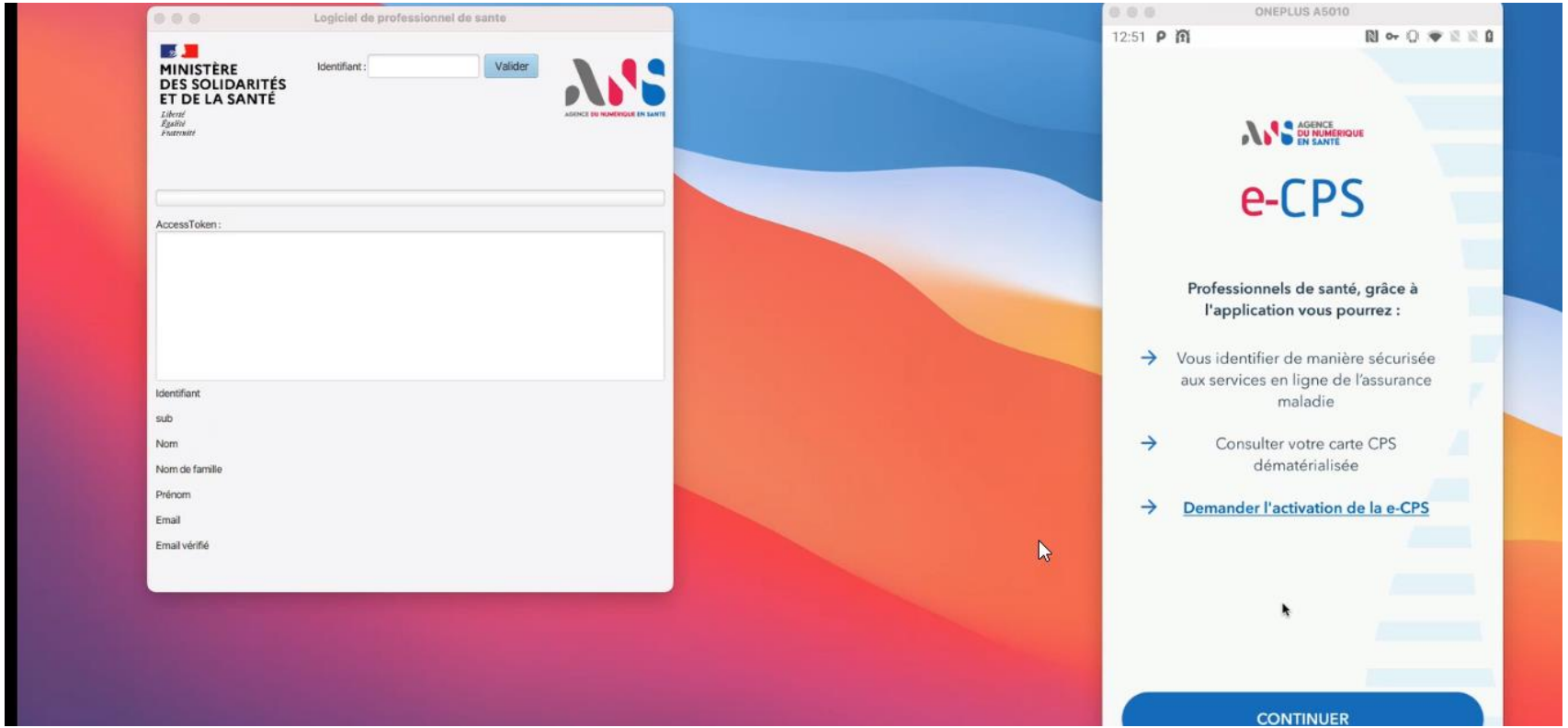
La norme OpenID CIBA est intégrée en POC à Pro Santé Connect et la e-CPS :

- Développement d'un contexte client lourd

Le POC a été présenté à nos partenaires :

- Démonstration technique interne à l'ANS en décembre
- Démonstration technique à la CNAM et au GIE SESAM-Vitale en janvier
- Démonstration en vue utilisateur à la DNS en février

Démonstration



Le POC

Le périmètre de ce POC est réalisé :

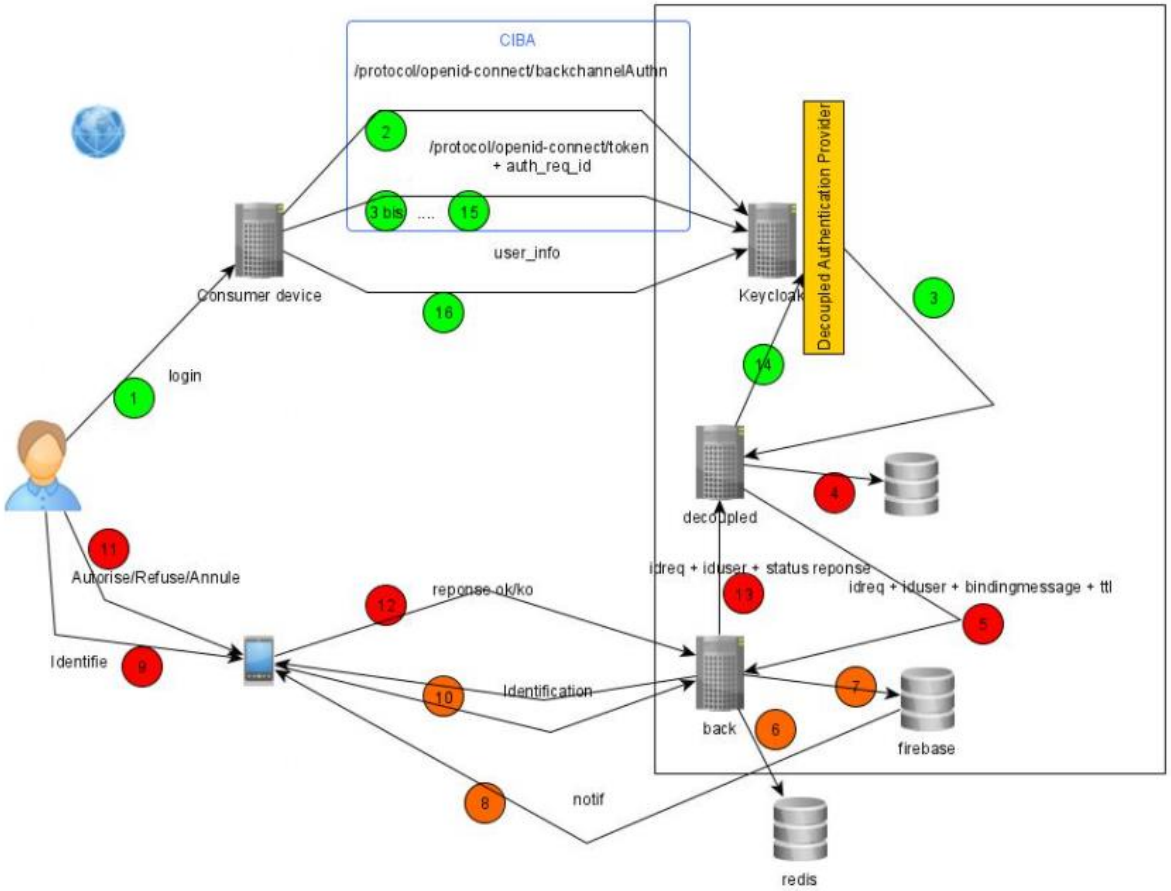
- Sur la base d'une version de Keycloak 12 qui a servit de POC d'implémentation de CIBA par Hitachi
- En Mode POLL uniquement
- Dans un espace de développement dédié à CIBA

AGENCE
DU NUMÉRIQUE
EN SANTÉ

Détails techniques

Dans le détail des flux

A droite, une vue détaillée de l'ensemble des flux d'échange entre les différents systèmes de PRO Santé Connect afin de réaliser le mécanisme « Client Initiated Backchannel Authentication »



Requête d'authentification et réponse

```
POST /auth/realms/test_ciba/protocol/openid-
connect/backchannelAuthn HTTP/1.1

Host: localhost:8080

Authorization: Basic
Y2RfdGVzdDo3MGJjNzI0MC1iZTgwLTQ4NGEtOGJjYS1lZDAwNGUyO
TgwN2Q=

Content-Type: application/x-www-form-urlencoded



login_hint=FCQfvLxxyCSOJ1jLw9i0cBBwNlrduys=&scope=ope
nid profile&binding_message=L'application
ConsumerDeviceApplication demande l'accès a votre
compte, demande : 929107
```

TLS

Client Authentication

Login → AES128

```
HTTP/1.1 200 OK

{
   "auth_req_id": "eyJ__n0..Hh__uVg.iP__JWM.7U__Yw",
   "expires_in": 120,
   "interval": 2
}
```

Polling timeout

Interval entre chaque Poll

Mode Poll : requête de jeton et réponse 1/2

```
POST /auth/realms/test_ciba/protocol/openid-
connect/token HTTP/1.1

Host: localhost:8080

Authorization: Basic
Y2RfdGVzdDo3MGJjNzI0MC1iZTgwLTQ4NGEtOGJjYS1lZDAwNGUyO
TgwN2Q=

Content-Type: application/x-www-form-urlencoded


grant_type=urn:openid:params:grant-
type:ciba&auth_req_id=eyJ__n0..Hh__uVg.iP__JWM.7U__Yw
```

TLS

Client Authentication

```
HTTP/1.1 400 BAD REQUEST

{

    "error": "authorization_pending",

    "error_description": "The authorization request
is still pending as the end-user hasn't yet been
authenticated."

}
```

```
HTTP/1.1 400 BAD REQUEST

{

    "error": "slow_down",

    "error_description": "Too early access."

}
```

```
Mais aussi : expired_token, access_denied,
invalid_grant
```

Mode Poll : requête de jeton et réponse 2/2

```
POST /auth/realms/test_ciba/protocol/openid-
connect/token HTTP/1.1

Host: localhost:8080

Authorization: Basic
Y2RfdGVzdDo3MGJjNzI0MC1iZTgwLTQ4NGEtOGJjYS1lZDAwNGUyO
TgwN2Q=

Content-Type: application/x-www-form-urlencoded


grant_type=urn:openid:params:grant-
type:ciba&auth_req_id=eyJ__n0..Hh__uVg.iP__JWM.7U__Yw
```

```
HTTP/1.1 200 OK

{
            "access_token": "...",
            "expires_in": 300,
            "refresh_expires_in": 1800,
            "refresh_token": "...",
            "token_type": "bearer",
            "id_token": "...",
            "not-before-policy": 0,
            "session_state": "...",
            "scope": "openid profile email"
}
```

Gestion de l'intervalle de Poll

L'intervalle de Poll est généré suivant les règles :

- Si la valeur de l'intervalle n'est pas présente dans la réponse de la requête « Authentication », elle est de 5 sec par défaut.
- Ne pas faire de Poll plus fréquemment que l'intervalle fourni.
- L'intervalle correspond au délai entre 2 débuts de requête (si on obtient la réponse au Poll en 2 sec., le Poll suivant sera dans 3 sec.).
- Attendre la réponse du Poll précédent avant d'effectuer un nouveau Poll.
- Si l'intervalle est dépassé lors de la réponse, le Poll suivant peut être immédiat.
- L'OpenID Provider peut mettre plus de 30 sec. à répondre (Long Polling), Il est recommandé au client un Timeout de 30 sec. (le Poll suivant peut être immédiat).
- Si l'OpenID Provider répond « slow_down » → intervalle += 5 sec.
- Une réponse de l'OpenID Provider avec un statut HTTP 503 et son header : Retry-After doivent être respectés.
- Si le client Poll de façon continue plus vite que le délai de l'intervalle, l'OpenID Provider peut répondre invalid_request dans ce cas auth_req_id → n'est plus valide.

AGENCE
DU NUMÉRIQUE
EN SANTÉ

Prochaines étapes

Prochaines étapes

La phase 1 du projet a abouti avec succès.

La phase 2 a démarré par l'intégration du mécanisme CIBA dans l'environnement Bac à sable pour une mise à disposition aux fournisseurs de services.

La feuille de route :

- Définir l'architecture technique.
- Valider l'interopérabilité des composants.
- Commencer la rédaction de la documentation (spécifications, etc.) qui sera immédiatement mise à disposition des FS.

AGENCE
DU NUMÉRIQUE
EN SANTÉ

esante.gouv.fr

Le portail pour accéder à l'ensemble des services et produits de l'agence du numérique en santé et s'informer sur l'actualité de la e-santé.

@esante_gouv.fr

linkedin.com/company/asip-sante