PROJET IAM

Neobanque

Mission

Mise en place d'un nouveau référentiel plus flexible, qui sécurise les échanges, avec l'intégration du MFA, la gestion du consentement pour l'app mobile et l'intégration d'un self service pour l'app mobile

Problématique

Besoin initial : Le client souhaite une mise en conformité à PSD2

-Mise en place d'un annuaire client maîtrisé indépendamment du cœur de l'application bancaire.
-Sécuriser les transactions en particulier dans l'application mobile client en reposant sur le protocole Open ID Connect.
-Mettre en place une plateforme de gestion des accès pour les clients.

Notre réponse

- **Mise en place d'un nouveau référentiel client synchronisé avec le CBS**
- **Evolution applicatives :**

-Utilisation de protocoles normés dans l'application mobile (OIDC et token oauth2) pour la sécurisation des échanges
-Intégration du MFA dans l'application mobile
-Ajout de la gestion du consentement dans l'application mobile
-Intégration d'un self-service dans l'application mobile

Mission

Contexte :
En outre, le référentiel client de la banque en ligne dit « CBS » (Core Banking Service) ne donne pas beaucoup de souplesse d'évolution, elle souhaite donc la mise en place d'un nouveau référentiel client maîtrisé qui sera synchronisé avec le CBS.

Notre réponse

Mise en place d'un nouveau référentiel client synchronisé avec le CBS

Le référentiel client actuel, le CBS, est vu comme une « boite noire » et ne peut permettre simplement des évolutions. Pour cette raison, le client souhaite disposer d'un référentiel plus flexible.
Le CBS restant maître sur la gestion des comptes, il convient donc de mettre en place un système de synchronisation monodirectionnel, pour répliquer les changements réalisés sur le CBS dans le nouveau référentiel.
Le nouveau référentiel a, pour l'heure, l'ambition de devenir le référentiel d'authentification et d'autorisation des clients de la neobanque. L'annuaire pourra donc permettre d'enrichir les données issues du CBS avec des informations pertinentes dans le cadre pour lequel il est défini (ajout d'attributs, création de groupes, gestion de nouvelles populations...).

PROJET IAM
Neobanque

Evolution applicatives :

-Utilisation de protocoles normés dans l'application mobile (OIDC et token oauth2) pour la sécurisation des échanges

Le client ne disposant à ce jour que d'une seule application mobile, on partira sur le flux OIDC authorization code de type client public (le flux implicit qui était jusqu'à présent préconisé pour ce genre d'utilisation est aujourd'hui considéré comme « depreciated » du fait de la baisse de sécurité que cela implique).

On choisira une implémentation du flux avec PKCE pour des raisons de sécurité.

L'application mobile utilise aujourd'hui le jeton FMS pour réaliser les opérations techniques. Pour des raisons multiples, on souhaite passer à l'utilisation d'un jeton normé au format Oauth2. Or si l'application repose sur ce type de jeton, les API existantes vont probablement continuer à utiliser l'ancien format de jeton. Il convient donc de s'assurer que le changement de jeton utilisé par l'application permet toujours un fonctionnement sans régression.

-Intégration du MFA dans l'application mobile

On souhaite ajouter un deuxième facteur d'authentification lors de l'ouverture de l'application ou de l'absence de session. On souhaite également que chaque action sensible dans l'application déclenche le deuxième facteur.

-Ajout la gestion du consentement dans l'application mobile

On souhaite utiliser les fonctionnalités Forgerock en ce qui concerne la gestion du consentement de l'utilisateur et les intégrer dans l'application mobile.

-Intégration d'un self-service dans l'application mobile

Le client souhaite mettre à profit les fonctionnalités de selfservice offertes par la stack ForgeRock dans son application mobile.