PRD 2 - 2FA utilisant Google Authenticator

Nom du projet : Ajout de l'authentification à deux facteurs (2FA) utilisant Google Authenticator

Statut du document : En cours

Date de sortie cible : Fin du T3 2018

1. Introduction

L'objectif de ce document est de définir les exigences pour l'ajout de l'authentification à deux facteurs (2FA à notre plateforme en utilisant Google Authenticator. Cette fonctionnalité vise à améliorer la sécurité des comptes en fournissant une couche d'authentification supplémentaire pour les utilisateurs accédant à leurs comptes via nos portails mobiles, web et de bureau.

2. Objectifs

- Renforcer la sécurité : Offrir aux clients et utilisateurs la possibilité d'ajouter une couche de sécurité suppl
- Assurer l'intégrité : Maintenir l'intégrité de la connexion client-serveur.
- Expérience utilisateur : Interface fluide et conviviale pour activer la 2FA.
- Communication : Développer une campagne marketing pour informer les clients.
- Processus de récupération : Proposer un processus clair en cas de perte d'accès.

3. Contexte

L'authentification à deux facteurs est devenue une norme de sécurité sur les principales plateformes techn Notre entreprise manipulant des informations sensibles, il est essentiel de proposer cette sécurité supplém Google Authenticator fournit un mot de passe à usage unique basé sur le temps (TOTP) qui change toutes secondes, obligeant les utilisateurs à posséder leur appareil pour l'authentification.

4. Portée

4.1 Inclus

- Implémentation de la 2FA via Google Authenticator sur mobile, web et desktop.

- Développement d'interfaces utilisateur pour activer et gérer la 2FA.

- Intégration avec les systèmes d'authentification existants.

- Mécanisme de récupération en cas de perte du dispositif.

- Campagne marketing pour promouvoir la fonctionnalité.

4.2 Exclusions

- Support pour d'autres méthodes de 2FA (SMS, email).

- Refonte complète du système d'authentification.

- Changements dans l'onboarding utilisateur non liés à la 2FA.

5. Types d'utilisateurs

- Tous les utilisateurs enregistrés.

6. Hypothèses

- Les utilisateurs accèderont à la 2FA via applications mobiles, navigateurs web et applications de bureau.

- Un compte Google n'est pas requis pour utiliser Google Authenticator.

- Tous les appareils utiliseront le protocole NTP pour la synchronisation de l'heure.

- Les utilisateurs possèdent un appareil compatible avec Google Authenticator.

7. Cas d'utilisation

1. Activation de la 2FA

2. Connexion avec la 2FA activée

3. Récupération en cas de perte d'accès

4. Désactivation de la 2FA

5. Obligation de la 2FA pour transactions à risque

8. Exigences Fonctionnelles

8.1 Activation de la 2FA

- FR1 : Activation de la 2FA depuis les paramètres de compte.
- FR2 : Affichage d'un QR code et d'une clé manuelle pour configuration.
- FR3 : Vérification de la configuration avec un code généré.

8.2 Connexion avec la 2FA

- FR4 : Demande de code après saisie des identifiants.
- FR5 : Validation du code avant accès au compte.
- FR6 : Limitation des tentatives en cas d'échec.

8.3 Mécanisme de récupération

- FR7 : Fourniture de codes de secours.
- FR8 : Utilisation des codes en cas de perte de l'appareil.
- FR9 : Assistance client en cas de besoin.

8.4 Désactivation de la 2FA

- FR10 : Désactivation après ré-authentification.
- FR11 : Confirmation avant désactivation.

8.5 Consistance multi-plateforme

- FR12 : Fonctionnalité uniforme sur mobile, web et desktop.
- FR13 : Expérience utilisateur homogène.

8.6 Notifications et communication

- FR14 : Notifications d'activation et désactivation.
- FR15 : Communication marketing.

9. Exigences non fonctionnelles

- Sécurité : Conformité aux normes.

- Ergonomie : Interface intuitive.

- Performance : Aucune latence excessive.

- Fiabilité : Haute disponibilité.

- Scalabilité : Gestion d'une adoption massive.

10. Risques et mesures

- Risque 1 : Faible adoption -> Sensibilisation.

- Risque 2 : Perte d'accès -> Processus de récupération efficace.

- Risque 3 : Problèmes de synchronisation -> Utilisation de NTP.

11. Dépendances

- Intégration avec l'API Google Authenticator.

- Collaboration UX/UI.

- Support client mis à jour.

12. Questions ouvertes

- La 2FA doit-elle être obligatoire pour certains utilisateurs ?

- Comment gérer les échecs répétés ?

- Comment mesurer le succès de la 2FA ?