Authentikator

Documentation utilisateur

A2.1 The void

Mattéo KERVADEC

Kylian Houedec

Gabriel FROC

Ewen JAIN

Antoine GUILLERM

Benjamin GIRRARD

IUT Lannion - SAÉ 4 2024-2025

Le projet TripEnArvor a pour ambition de mettre en place un système d'authentification à double facteur, permettant d'améliorer considérablement la sécurité des accès. En ajoutant une seconde couche de vérification, ce mécanisme vise à réduire les risques liés aux intrusions et aux usages frauduleux des comptes utilisateurs.

Ce document explique en détail l'utilisation de l'authentification à deux facteurs (A2F), un mécanisme de sécurité renforçant l'accès aux comptes en ligne en combinant un mot de passe et un code temporaire. Il décrit son fonctionnement.

Dernière modification : 2 avril 2025

Documentation : Authentification à Deux Facteurs (A2F) sur PACT

Gabriel Froc

2 avril 2025

1 Introduction

L'authentification à deux facteurs (A2F) est une méthode de sécurité qui requiert deux formes distinctes d'identification pour accéder à un compte ou un service. Sur PACT, nous avons mis en place une A2F via Google Authenticator afin de renforcer la sécurité des utilisateurs.

2 Pourquoi utiliser l'A2F sur PACT ?

PACT exige l'utilisation de l'A2F pour protéger les comptes contre les accès non autorisés. Cette mesure de sécurité repose sur :

— Un facteur de connaissance (mot de passe, code PIN)

— Un facteur de possession (smartphone avec Google Authenticator)

Cette double vérification empêche les intrusions, même en cas de vol ou de fuite du mot de passe.

3 Mise en place de l'A2F sur PACT

3.1 Activation lors de la création du compte

Lors de l'inscription sur PACT, l'utilisateur peut activer immédiatement l'A2F. Un QR code s'affiche à l'écran, que l'utilisateur doit scanner avec Google Authenticator, ou une clé secrète est fournie pour être saisie manuellement. Cette clé est nécessaire pour générer des codes d'accès temporaires.

3.2 Activation après la création du compte

Si l'A2F n'a pas été activée lors de l'inscription, l'utilisateur peut l'activer ultérieurement dans les paramètres de sécurité du compte sur PACT. Une fois activée, un code à 6 chiffres généré par Google Authenticator est demandé pour confirmer l'activation.

3.3 Connexion avec l'A2F activée

Lorsque l'A2F est activée sur PACT, la connexion au compte suit ces étapes :

1. L'utilisateur saisit son identifiant et son mot de passe.
2. Si l'A2F est activée, un champ supplémentaire s'affiche pour entrer un code de validation.
3. L'utilisateur ouvre Google Authenticator et saisit le code à 6 chiffres généré.
4. Une fois le code correct, l'accès est accordé.

En cas de tentative échouée pour entrer le mot de passe ou le code à 6 chiffres, l'utilisateur a droit à 3 essais. Après 3 tentatives échouées, l'accès est bloqué pendant 10 minutes. L'utilisateur devra attendre 10 minutes avant de pouvoir réessayer de se connecter.

3.4 Limitation des tentatives de connexion

Afin de protéger les comptes contre les attaques par force brute, PACT limite le nombre d'essais de connexion. L'utilisateur dispose de 3 tentatives pour saisir son mot de passe et le code d'authentification. Après 3 tentatives échouées, l'accès est temporairement bloqué et l'utilisateur doit attendre 10 minutes avant de pouvoir réessayer.

3.5 Récupération en cas de perte de l'accès à l'A2F

Aucune méthode de récupération n'est disponible en cas de perte d'accès à Google Authenticator. Il est donc essentiel de conserver la clé secrète ou les codes de secours fournis lors de l'activation de l'A2F.

4 Conclusion

L'authentification à deux facteurs sur PACT est essentielle pour sécuriser les comptes des utilisateurs. Il est fortement recommandé de l'activer et de conserver précieusement les codes de secours. En cas de problème, le support de PACT est disponible pour assister les utilisateurs dans la récupération de leur compte.