

Présentation sur  
l'Authentification  
Sans Mot de Passe

# PASSWORDLESS

PAR LE ROI DU CSS



# Introduction

L'authentification sans mot de passe, ou "passwordless", est une méthode moderne qui remplace les mots de passe traditionnels par des technologies plus sécurisées et pratiques. Cette approche vise à améliorer la sécurité tout en simplifiant l'expérience utilisateur.



# Pourquoi Passer au Sans Mot de Passe ?

- Sécurité Renforcée
  - Élimine les risques de phishing et de bourrage d'identifiants.
  - Réduit les vulnérabilités liées aux mots de passe faibles ou réutilisés.
- Expérience Utilisateur Améliorée
  - Simplifie le processus de connexion en éliminant la nécessité de mémoriser des mots de passe complexes.
  - Réduit la fatigue liée aux mots de passe et les coûts associés aux réinitialisations.
- Efficacité et Réduction des Coûts
  - Diminue les coûts opérationnels liés à la gestion des mots de passe et au support technique.
  - Améliore la productivité en réduisant le temps passé à gérer les mots de passe.



# Méthodes d'Authentification

## Sans Mot de Passe



### ***Biometrics***

- Utilisation des empreintes digitales, reconnaissance faciale, ou scanner d'iris pour une authentification unique et sécurisée.



### ***Security Tokens***

- Dispositifs physiques (clés USB) ou logiciels (applications mobiles) générant des codes d'authentification uniques.



### ***One-Time Passwords (OTP)***

- Codes temporaires envoyés par SMS ou générés par une application, valables pour une seule session.



### ***Magic Links***

- Liens envoyés par email qui authentifient l'utilisateur lorsqu'ils sont cliqués, sans nécessiter de mot de passe.



### ***Public-Key Cryptography***

- Utilisation de paires de clés cryptographiques pour une authentification sécurisée sans partage de secrets.



### ***FIDO2 et WebAuthn***

- Normes ouvertes permettant l'utilisation de dispositifs comme les smartphones ou les clés de sécurité pour une authentification sans mot de passe.



# Évolution et Adoption



## ***Technologies Émergentes***

- Les avancées technologiques, comme la prolifération des dispositifs biométriques et des smartphones, favorisent l'adoption du sans mot de passe.

## ***Normes et Standards***

- Des standards ouverts comme FIDO2 et WebAuthn facilitent l'intégration et l'adoption des technologies sans mot de passe.

## ***Changements Culturels***

- L'acceptation croissante de la biométrie et la décentralisation des forces de travail encouragent les entreprises à adopter des solutions sans mot de passe.

# Défis et Considérations

## Compatibilité et Intégration

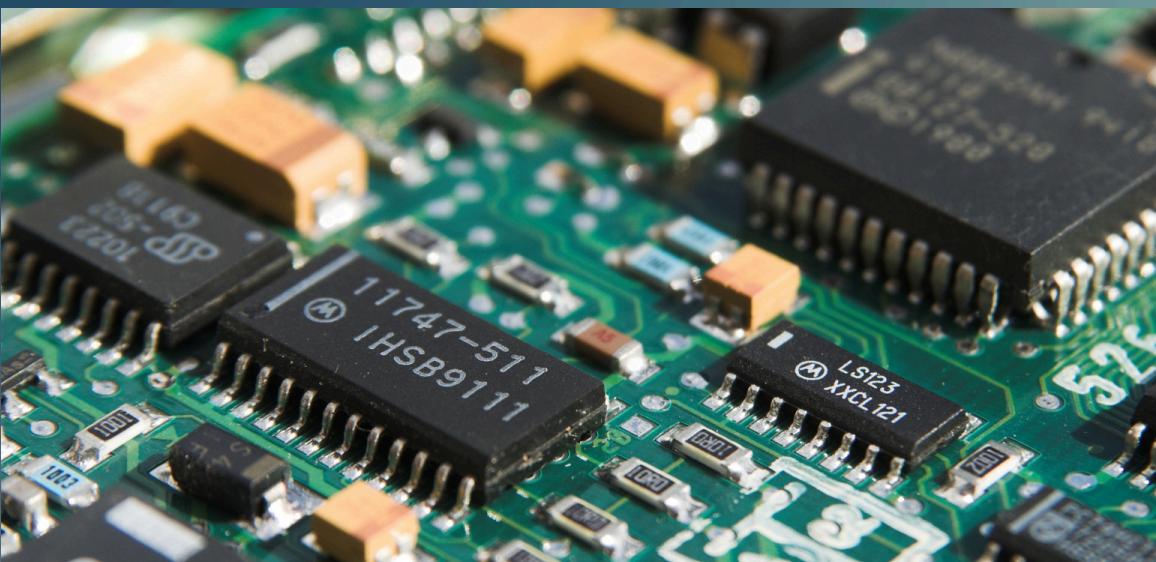
- Toutes les plateformes ne supportent pas encore les méthodes d'authentification sans mot de passe.

## Coût Initial

- La mise en place peut nécessiter des investissements initiaux en termes de technologie et de formation.

## Éducation des Utilisateurs

- Former les utilisateurs à adopter de nouvelles méthodes d'authentification est crucial pour une transition réussie.



```
18   int iN;
19   double dblTemp;
20   bool again = true;
21
22   iN = -1;
23   again = false;
24   getline(cin, sInput);
25   system("cls");
26   stringstream(sInput) >> dblTemp;
27   iLength = sInput.length();
28
29   if (iLength < 4) {
30     again = true;
31     continue;
32   } else if (sInput[iLength - 3] != '.') {
33     again = true;
34     continue;
35   } while (++iN < iLength) {
36     if (isdigit(sInput[iN])) {
37       again = true;
38     } else if (sInput[iN] == '.') {
39       again = false;
40     }
41   }
42 }
```

# Conclusion



L'authentification sans mot de passe représente une évolution significative vers une sécurité accrue et une meilleure expérience utilisateur. Bien que des défis subsistent, les avantages en termes de sécurité et de commodité en font une tendance prometteuse pour l'avenir.



# THANK YOU



Le Roi Du CSS