



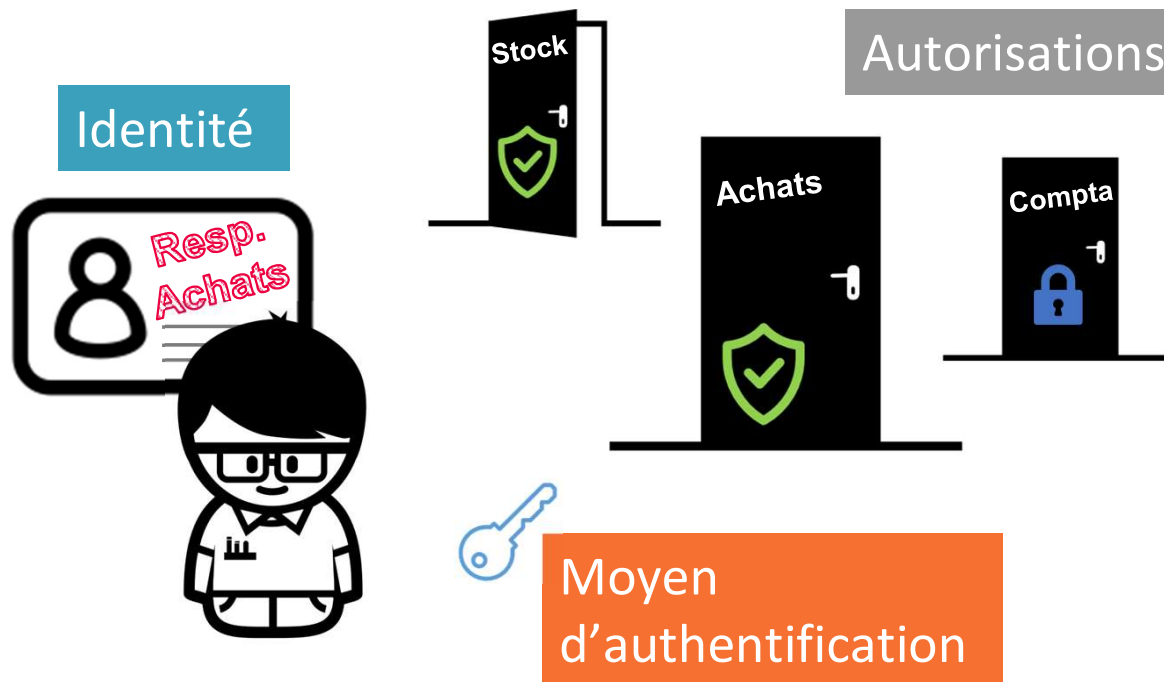
LES CONTRÔLES D'ACCÈS

M. Thomas VIERLING

**La gestion des accès :
comment et pourquoi ?**

1. La gestion des accès

Maîtrise des accès



2. Absence de gestion : quels sont les risques?

Perte de maîtrise du SI

Perte de traçabilité

Perte de confidentialité

Manque de segmentation

Propagation de ransomware, data miner

Fuite de données

Par erreur humaine ou par malveillance

3. Comment maîtriser les accès ?

**Comprendre
l'organisation
de l'entreprise**

Pour se projeter dans la
segmentation des accès

**Impliquer les
responsables
métiers**

Pour concevoir
l'organisation des droits
de leurs profils métiers

**Connaître
son SI**

Pour faire le lien
entre les
applications et
métiers

**Définir des
processus**

Afin d'automatiser
l'attribution et
révocation de
droits

4. Le mot de passe

**Responsabiliser
les utilisateurs**

Le mot de
passe est
confidentiel

et personnel

Aussi précieux que le code de votre
carte bancaire !



Fournir un
moyen de
sécurisation
du mot de
passe

Définir des
règles
d'utilisation

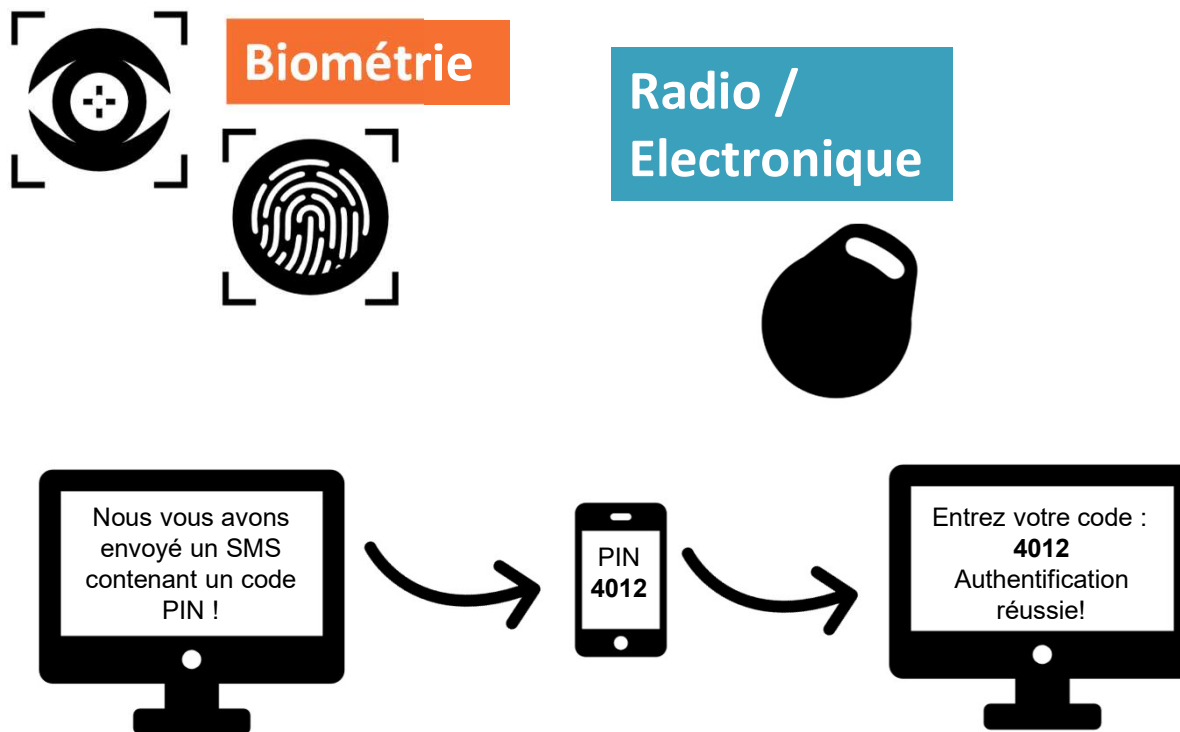
Ne jamais
le **divulguer**
ni le réutiliser

Utiliser un **coffre fort
sécurisé** ou **fédérer
l'identité : OpenID**

Chaque utilisateur pourra stocker des mots
de passe de façon sécurisée et en partager
en interne et externe, ou se connecter à
l'aide d'un compte unique !

5. Les nouveaux moyens d'accès

Authentification multi-facteurs



Conclusion

Niveau de confidentialité

Qu'est ce qui est réellement confidentiel ?

Contrôle et sécurisation des accès machines

Réseau d'entreprise 802.1X

IoT

Analyser le risque et connaître ses obligations

Classifier les données

Données sensibles

RGPD