KEOPASS

Security
@ Your Fingertips

Dispositif d'Authentification Biométrique Autonome

Accroître la sécurité des accès et faciliter la vie des utilisateurs

CONSTATS

- 80% des cyber-attaques = **défaillances humaines**
- **Compromission de mots de passe** = 29% des brèches
- **Impacts des failles de sécurité** > 300K€
  - Renouvellement de tous les mots de passe
  - Image d'entreprise affectée
- **Coût hotline** lié aux mots de passe : 240€ / An / Utilisateur
- **La perte ou vol de badges** peut compromettre la sécurité

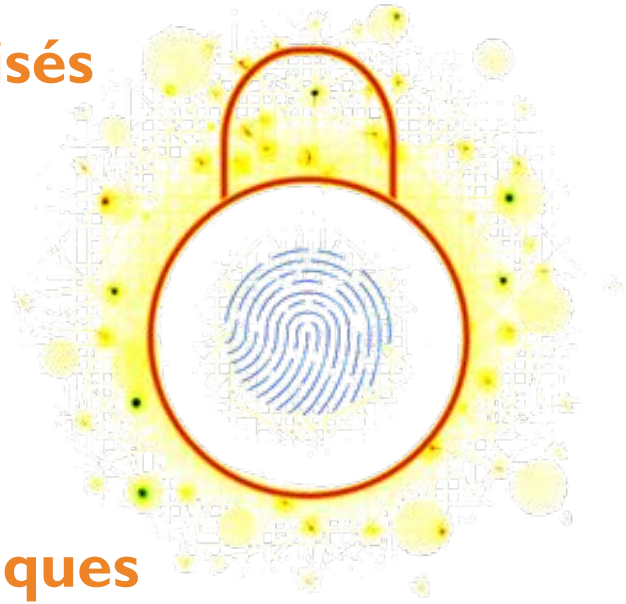
KeoPass

PROBLEMATIQUES DSI / RSSI / HOTLINE IT / SECURITE

KeoPass

NOTRE VISION

- Concevoir des dispositifs de sécurité **autonomes et décentralisés**
- Libérer l'utilisateur de la **gestion des mots de passe**
- **Garantir l'identité** de l'utilisateur grâce à la biométrie
- Réduire les cyber-attaques liées au **facteur humain**
- Faciliter l'application du **MFA – RGPD – NIS2 – Zero Trust**
- Ajouter la **sécurité biométrique** aux **accès logiques et physiques** sans installation logicielle, ni modification de l'infrastructure



KeoPass

LA CLE BIOMETRIQUE KEOPASS POUR TOUS LES ACCES

Accès Logiques

Mots de Passe

Certificats

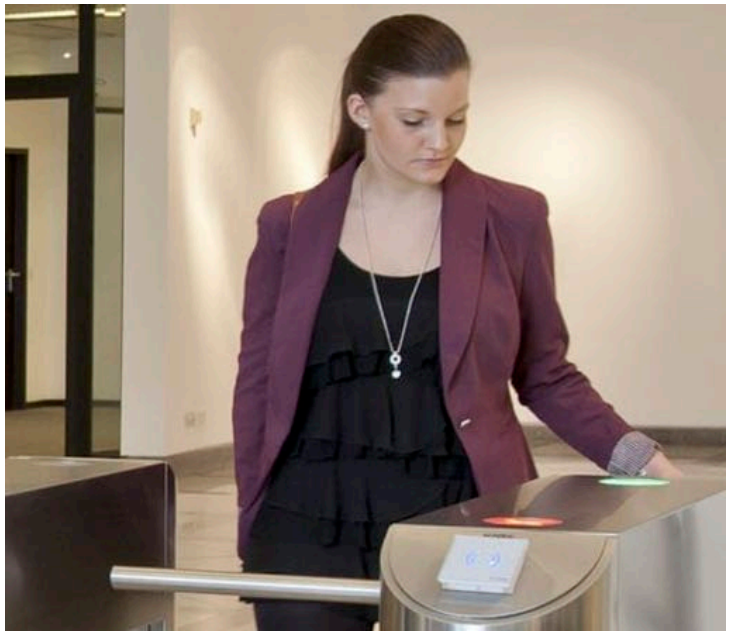
OTP

FIDO2.1

Sécurité Biométrique

MADE IN FRANCE

Accès Physiques



MIFARE DESFire

DESFire EV3C

CARACTERISTIQUES (1/2)

« Universelle » : Fonctionne avec tous terminaux fixes ou mobiles, et tous les lecteurs NFC / RFID

« Agent-less » : Aucune installation ou modification logicielle nécessaire (NO app ou pilote)

« Agnostique » : Compatible avec tout service, application locale ou SaaS, sans intégration d'API

« Easy-Setup » : Personnalisation et paramétrage via pages web statiques (html+javascript)

KEOPASS

CARACTERISTIQUES (2/2)

« Frictionless »

- Appairage Bluetooth standard ou Plug&Play USB via dongle ou câble – aucun pilote requis
- Plus de saisie de mots de passe = facilité d'usage, moins d'erreurs et de demandes de réinitialisation
- Renouvellement des mots de passe par simple appui sur un bouton

« Secure »

- Mots de passe et empreintes enregistrés dans la mémoire sécurisée de la clé (OTP en option)
- Effacement de la mémoire en cas d'ouverture de la clé
- Communications: Bluetooth5 chiffrées en AES avec pré-appairage, USB2, NFC / RFID

« Pérenne »

- Jusqu'à 3 000 authentifications par charge, rechargeable via port micro-USB
- Mise à jour via navigateur web
- Conçue et fabriquée en France - Garantie 5 ans

KeoPass

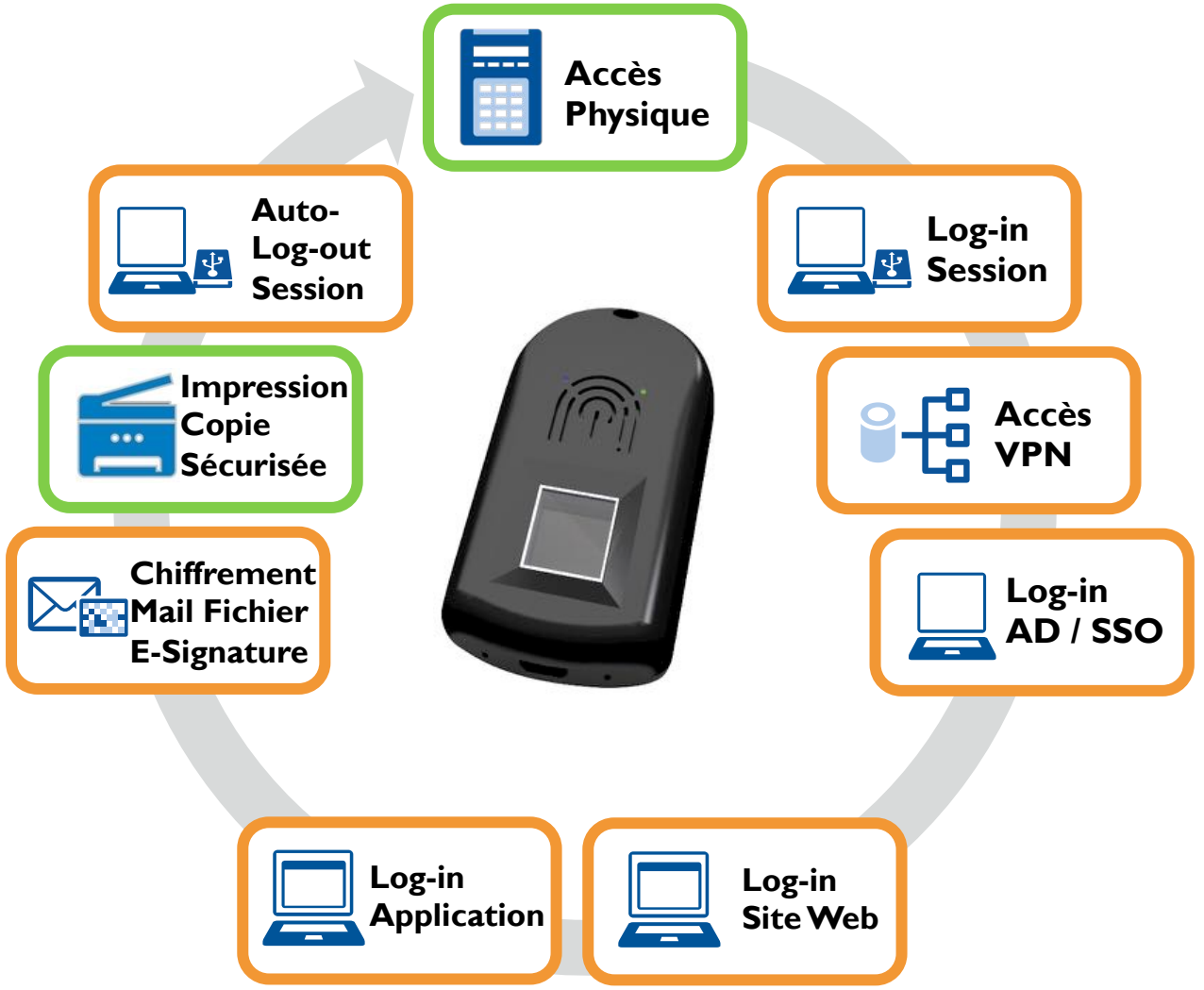
DISPOSITIF AUTONOME "SECURE-BY-DESIGN"

- **Analyse d'empreintes digitales intégrée** (13 points) = usurpation impossible
- **Sans OS** = insensible aux virus, malwares ou autres vecteurs d'attaques
- **Inviolable** : mémoire et communications chiffrés en AES & auto-effacement
- **Plug&Play** : pas de pilote, ni d'agent, ni d'App – pas d'intégration d'API
- **Déploiement immédiat** avec auto-enrôlement des utilisateurs via navigateur

KeoPass

UNE CLE POUR TOUS LES ACCES

Accès Physiques



Accès Logiques

KEOPASS

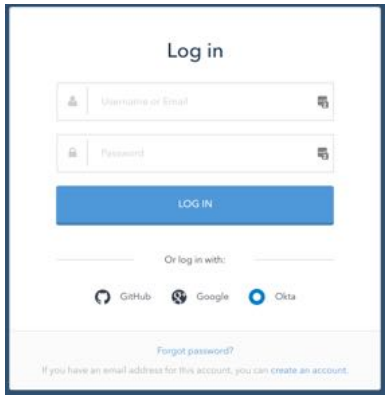
CAS D'USAGES – ACCÈS LOGIQUE

Déverrouillage par mot de passe :

- Ordinateurs, tablettes, smartphones, IoT
- Applications logicielles (locales ou SaaS)
- VPN, AD, SSO, Cloud… (sans agent, ni API)

Gestionnaire de mots de passe web :

- Mot de passe unique pour chaque site (anti-phishing)



Sécurisation des postes de travail :

- Fermeture de session lors de l'éloignement du PC (option)
- Postes partagés entre plusieurs collaborateurs

Evolutivité, MFA & Passwordless :

- Mise à jour des clés à distance via navigateur web
- PKI / FIDO2.1 : Certificats stockés dans un Secure-Element

KEOPASS

MODES D'AUTHENTIFICATION

- **« Standard »** 1 empreinte = 1 mot de passe
- **« Web »** mot de passe unique pour chaque URL
- **« TOTP »** code éphémère OATH (remplace Authenticator)
- **« HOTP »** mot de passe unique à chaque activation
- **« PKI / FIDO2 »** certificats intégrés dans un Secure-Element

KeoPass

AUTHENTIFICATION PAR CERTIFICAT INTÉGRÉ / PKI / FIDO

- **Certificats** d'authentification client (X.509) stockés dans un Secure Element (certifié ANSSI CC EAL6+ & FIPS140-3)
- Insertion du code PIN après **validation d'empreinte**
- Emulation d'un lecteur de carte à puce – **Plug&Play sans installation**
- Compatibilité avec **smartcard logon / FIDO2.1** sous Windows / AD

KeoPass

CAS D'USAGES – ACCÈS PHYSIQUE

Accès Physiques par identification biométrique :

- Portes, portillons, tourniquets, barrières, …
- Equipements: copieurs, distributeurs, boite à clés, …

➔ Remplacement des badges RFID / NFC :

- Multi-technologies: HID Prox, iClass, MiFare, DESFire EV3
- Options mono-badge ou multi-badges / sous contrainte
- Utilisation via lecteurs NFC/RFID standards
- Aucune modification de l'infrastructure

➔ Passerelles Bluetooth KeoPass :

- Contrôle de gâches et verrous électriques
- Géolocalisation des clés (option)

KeoPass

COMPATIBILITÉ - RÉGLEMENTATIONS

CNIL.
COMMISSION NATIONALE
INFORMATIQUE & LIBERTÉS

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

RGPD

- Dispositif biométrique personnel recommandé par la CNIL (Type 1)
  https://www.cnil.fr/fr/le-controle-dacces-biometrique-sur-les-lieux-de-travail
- Aucune base de données biométriques à créer, déclarer ou à protéger,
  pas d'autorisation des utilisateurs requise :
  - Dispositif autonome: les données biométriques sont résidentes et chiffrées
  - Pas d'impact sur le RGPD et facilite son application dans l'entreprise ➔ Déploiement sans contraintes
- Conforme aux recommandations de l'ANSSI : Secure Element intégré certifié CC EAL6+

KEOPASS

BÉNÉFICES

- **Clef Unique** garantissant l'identité de la personne pour les :
  - **Accès Logiques** (login, AD, SSO, applications…) sur ordinateurs, tablettes, smartphones, terminaux mobiles
  - **Accès Physiques** (portes, portillons, équipements…) via protocoles NFC/RFID standards ou Bluetooth
- Solution **Ultra-Sécurisée & Customisable**
  - Conception « Secure-by-Design » : circuits durcis, mémoire et communications chiffrées, effacement en cas d'ouverture
- **Déploiement facile & Adoption immédiate** :
  - Solution agnostique & cross éco-systèmes : aucun impact sur les autres solutions de l'entreprise
- Conçue pour l'**Humain** :
  - **Accélère** l'authentification : plus besoin de créer, mémoriser, ni de saisir de mots de passe complexes
  - **Economise** le support technique : limitation des appels liés aux mots de passe oubliés
  - **Protège** contre le hameçonnage : génération automatique et contextuelle de mots de passe complexes

KeoPass

SNCF

EDF

NAVAL GROUP

THALES

The 2024 French CYBER-SECURITY INNOVATION radar

By WAVESTONE & bpifrance Le Hub

CONTACT

Hervé-François Le Dévéhat

herve@keopass.com

+33.623.65.61.28

www.keopass.com

KeoPass