



ÆGIS AUTHENTICATION
TECHNOLOGIES

Roadmap Stratégie 2025

Étapes stratégiques vers un avenir numérique sécurisé

Contenu

Introduction	1	Stratégie de Produit	6
Notre mission et nos valeurs Nos solutions	2	Aperçu de la Roadmap	7
	3	Fonctionnalités de Nouvelle Génération	8
Qu'est-ce qui pourrait mal se passer?	4	Examen et Aajustements	9
Aperçu du Marché	5	Coordonnées	10

Pourquoi Aegis ?

Notre Mission

Offrir une sécurité de nouvelle génération sans mot de passe qui donne à votre entreprise un contrôle et une conformité complets.

Valeurs Fondamentales

- Une sécurité à la pointe du marché
- Conçue pour la Souveraineté et les Réglementations Européennes
- Une innovation qui s'adapte à vous
- Un accès transparent et convivial Approuvé par les plus grandes organisations mondiales



Présentation de Shield One

Shield One: Une sécurité inégalée
pour vos actifs numériques.

Ce que nous offrons :

Sécurité renforcée : protégez vos applications et vos données avec une protection puissante et transparente.

Compétence:

Plus de 10 ans d'expérience dans la fourniture et le support de solutions d'authentification de premier ordre.

Qu'est-ce qui pourrait Mal se passer?

Analyse des risques
d'authentification actuels



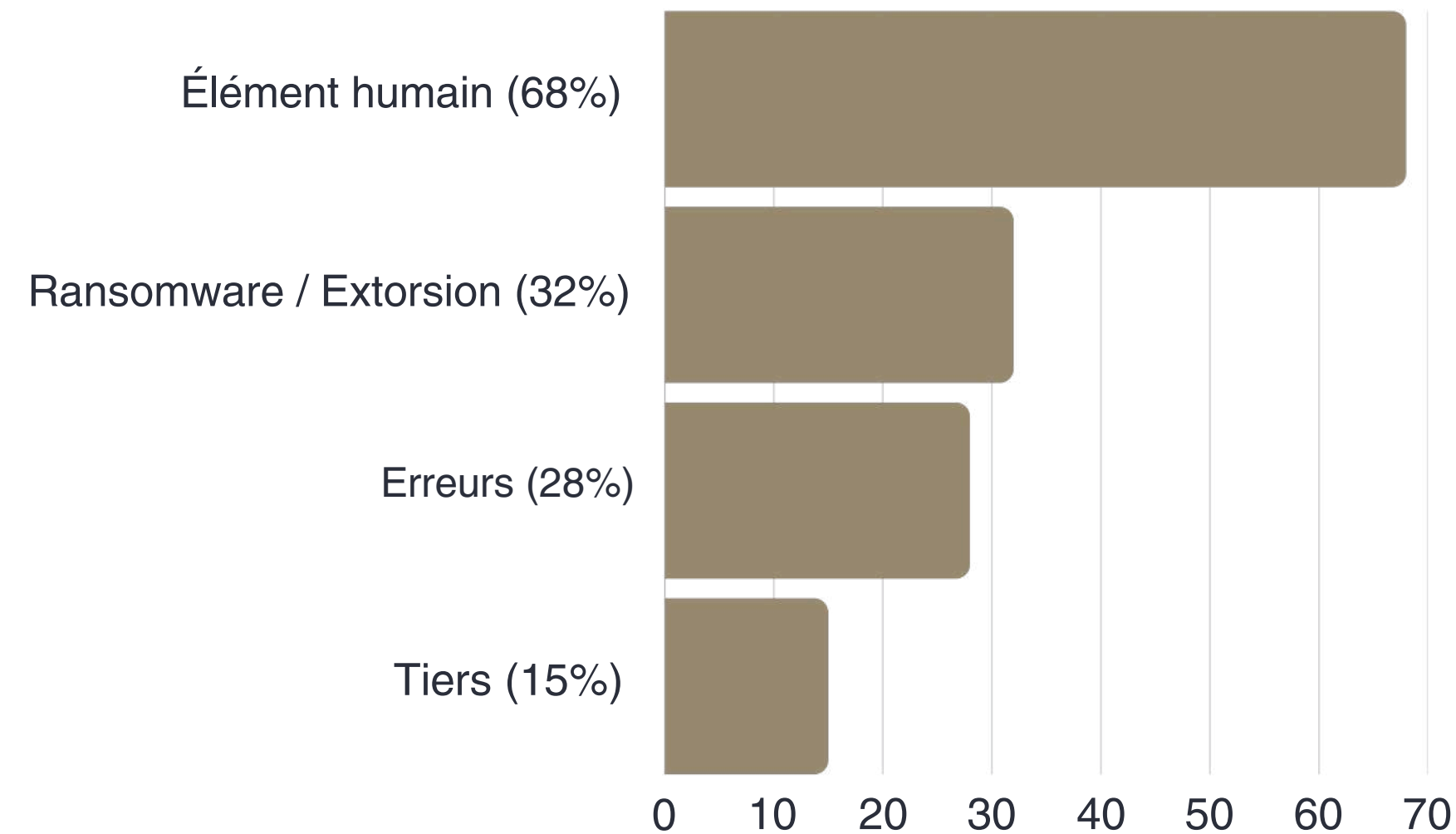
L'élément humain :
Un facteur clé



**Risques
d'authentification et
menaces liées aux
informations
d'identification**

L'élément humain : Un Facteur Clé

68 % des violations proviennent d'une erreur humaine, la menace silencieuse pour votre sécurité.



Réutilisation des informations d'identification:

amplifie les risques de bourrage d'informations d'identification.

Mots de passe faibles:

Laissez les systèmes exposés.

Erreurs internes:

Provoquent des violations accidentelles.

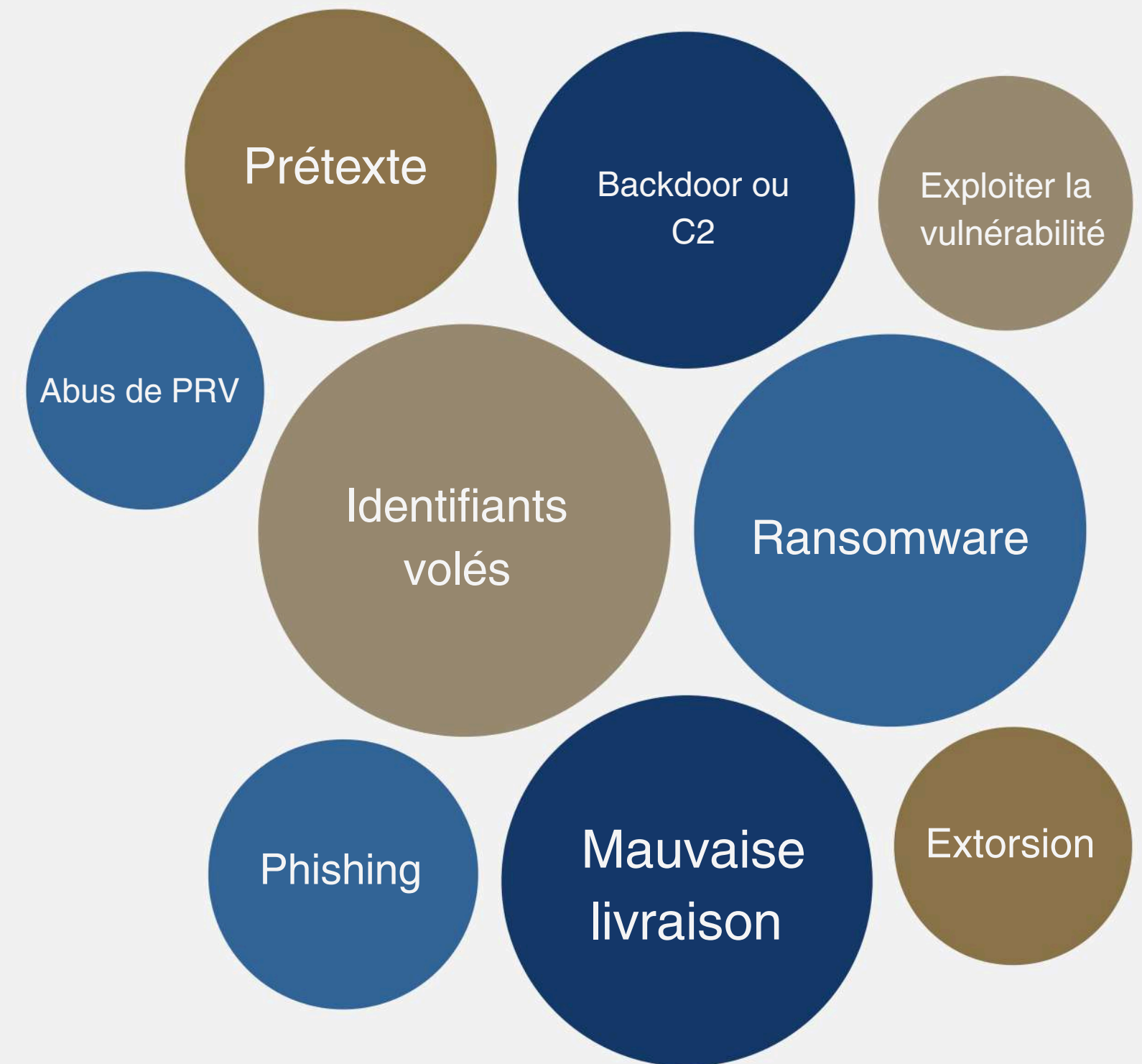


Risques d'authentification et **menaces** liées aux informations d'identification

Vol d'identifiants: 31% des violations de données en 2024 concernaient des identifiants volés (Verizon DBIR). Les pirates informatiques utilisent des données divulguées ou hameçonnées pour contourner l'authentification sans se faire repérer.

Risques liés aux mots de passe

Les mots de passe faibles et réutilisés alimentent les informations d'identification. Attaques par bourrage et par force brute, gardant votre organisation exposée.

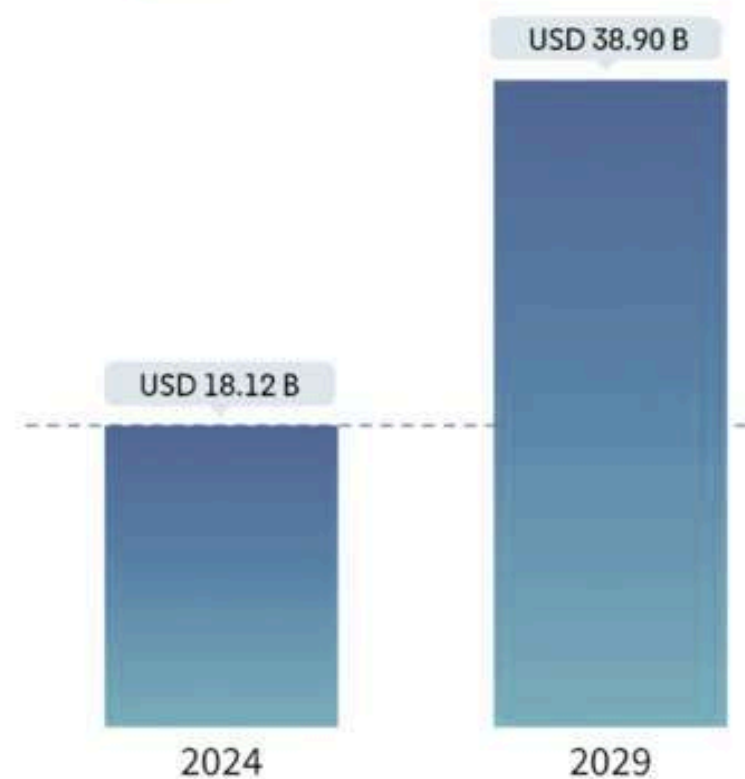


Aperçu du Marché

L'adoption de L'authentification s'accélère

93% des entreprises adopteront l'authentification multifacteur d'ici 2026. L'authentification sans mot de passe est en plein essor, avec un CAGR prévu de 22,6%, entraînant une évolution vers une sécurité plus intelligente et sans friction.

Multi-factor Authentication Market
Market Size in USD Billion
CAGR 16.5%



Marché de l'Authentification

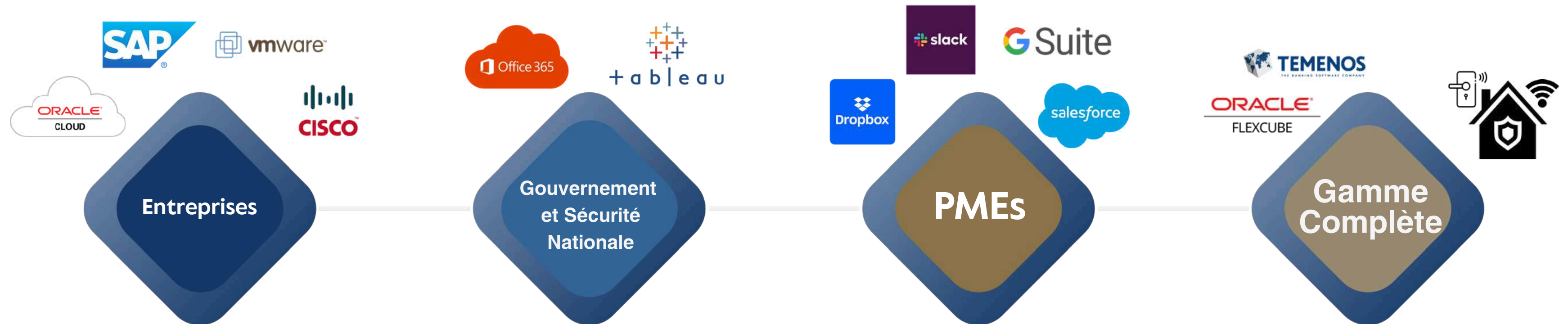
Évalué à 18,12 milliards de Dollars en 2024, le marché de l'authentification des utilisateurs devrait atteindre 38,90 milliards de Dollars d'ici 2029, grâce à un CAGR élevé de 16,5%. La demande d'accès sécurisé et transparent s'accélère.



ÆGIS AUTHENTICATION
TECHNOLOGIES

Public Cible

Segments de Clientèle



- Protection évolutive
- Solutions personnalisées
- Sécurité informatique complexe
- Défense de bout en bout

- Sécurité du Secteur Public
- Authentification axée sur la Conformité
- Protection des Infrastructures Critiques
- Solutions de Sécurité Nationale

- Solutions de Sécurité pour PME
- Protection flexible et évolutive
- Cybersécurité rentable
- Défense alignée sur la croissance

- Sécurité Gouvernementale et Financière
- Protection des PME
- Cybersécurité à domicile
- Conformité haute sécurité

Tendances Techniques

Technologies Biométriques émergentes



Sécurisé, Compatible et Convivial



Scanners Certifiés FBI pour la Sécurité



Identification précise et Infalsifiable des veines



Rapide, Durable et Fiable dans tous les Secteurs



Solutions Biométriques Veineuses de Précision



Identification Faciale et par Empreintes Digitales Sécurisée

Tendances Techniques

Intégration et Interopérabilité axées sur les normes



Accès Multiplateforme Transparent et Sécurisé

Autorisez les utilisateurs en toute sécurité sur tous les systèmes sans exposer leurs informations d'identification.



Authentification sans mot de Passe Sécurisée

Norme ouverte utilisant la cryptographie à clé publique pour une vérification rapide, sécurisée et sans friction des utilisateurs.



SSO Transparent avec Échange de Données Sécurisé

Permet l'authentification unique par échange de données sécurisé entre des parties de confiance.



Identité Unifiée avec OAuth2

Ajoute une couche d'identité sécurisée à OAuth2 pour une authentification utilisateur transparente sur les systèmes et les applications.



ÆGIS AUTHENTICATION
TECHNOLOGIES

Accès et Conformité

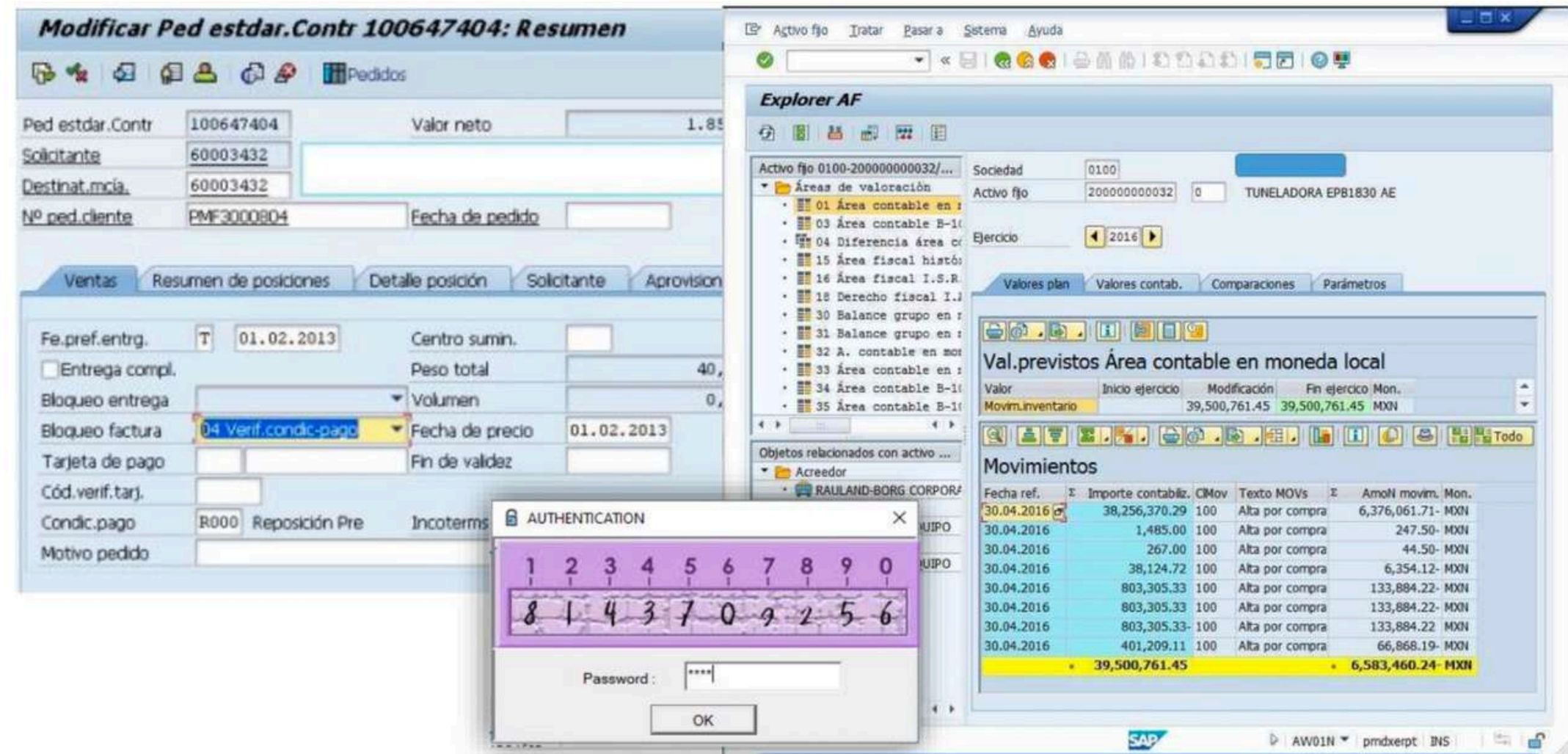
SAP Sécurisés

- 2FA pour les transactions et SAP Logon pour empêcher les accès non autorisés.
- Chiffrement, signatures numériques et interopérabilité pour garantir la sécurité et la conformité réglementaire.
- Respectez les exigences réglementaires grâce à une authentification forte et des pistes d'audit.
- Prise en charge de la migration Cloud vers SAP S/4HANA pour une Gestion Optimisée des accès.
- Garantisiez des transitions fluides grâce à une activation guidée et à une assurance qualité.



Shield One et les Paradigmes SAP

Cette démonstration met en évidence une transaction SAP sécurisée alimentée par notre méthode d'authentification brevetée sans jeton, garantissant un accès fort et transparent basé sur un code PIN sans mot de passe, entièrement intégré aux processus SAP.



Analyse Concurrentielle

Leader du marché avec des Solutions Supérieures

Nos avantages

Fonctionnalités Exclusives: Dépassez les solutions standard.

Convivialité: SSO et libre-service pour un accès fluide.

Intégration Facile: Prise en charge étendue des API pour un système connectivité fluide.

Authentification Avancée: au-delà d'OATH, simple, sécurisée, sans mot de passe.

Déploiement Flexible: Cloud, On-Premise ou Hybride.

MSP Ready: Prise en charge complète des fournisseurs de services gérés.

Évolutif par Conception: architecture moderne pour des performances élevées.

Features Evaluation	DUO	ForgeRock	Starlink 2FA	Onelogin	MS Azure (enterprise)	Aegis Shield One
Mobile Application	✓	✓	✓	✓	✓	✓
SAML Integration	✓	✓	✓	✓	✓	✓
Oauth2 Integration	✓	✓	✓	✓	✓	✓
MFA	✓	✓	✓	✓	✓	✓
Single Sign-On Portal	✓	✓	✓	✓	✓	✓
User self service portal	✓	✓	✓	✓	✓	✓
Integration API	✓	✓	✓	✓	✓	✓
Risk Management	✓	✓	✓	✓	✓	✓
Keychain Risk Authentication	✓	✓	✓	✓	✓	✓
Microsoft Authentication with offline support	✓	✗	✗	✗	✗	✓
Web based SAP Logon authentication	✗	✗	✗	✗	✗	✓
SAP MPA	✗	✗	✗	✗	✗	✓
Patented MFA	✗	✗	✗	✗	✗	✓
AI for local application authentication	✗	✗	✗	✗	✗	✓

Stratégie Produit

Positionnement sur le marché et
Proposition de Valeur Unique

**Plus de 15 Méthodes d'authentification,
dont la méthode brevetée ePinsafe®.**

**SSO transparent et convivial pour
tout environnement, accès sécurisé
avec une expérience simplifiée.**

**Intégration avec Office 365, Salesforce, SAP,
Azure et plus encore.**

**Évolutivité et efficacité optimisées avec un
support multi-locataire robuste.**

Prend en charge les protocoles standard et personnalisés pour une flexibilité et une compatibilité maximales.

Accès sans effort via SSO et portails en libre-service intuitifs.

Prise en charge multi-locataire pour une évolutivité et une efficacité améliorées.

Diverses Méthodes d'authentification alimentées par des technologies brevetées pour une sécurité supérieure.

Stratégie Produit

Positionnement sur le marché et
Avantage Concurrentiel

Avantages Concurrentiels

Innovation de Niveau Entreprise

- ◆ Sécurité adaptative avec authentification globale basée sur les risques.
- ◆ Intégration transparente via OAuth2 personnalisable et APIs robustes.
- ◆ Compatible biométrique pour une authentification nouvelle génération.
- ◆ Architecture évolutive avec multi-tenant efficace pour répondre aux exigences croissantes.



Priorités de Développement de Produits



Nouvel Appareil

Architecture de serveur et de système d'exploitation moderne pour une stabilité, des performances et un support complet à long terme.



Fonctionnalités Multi-location

Améliorez l'expérience utilisateur et protection avec une sécurité transparente accéder.



Authentification Biométrique

Élargissez l'authentification avec des solutions biométriques avancées de nouvelle génération.



Authentification sans Mot de Passe

Activez un accès sécurisé et sans mot de passe avec l'authentification FIDO2 intégrée.



Intégration d'OpenID Connect

Authentification transparente et sécurisée dans tous les environnements.



Serveur Oauth2

Autorisation personnalisable adaptée à divers systèmes et applications

Aperçu de la Feuille de Route

Façonner l'avenir de l'authentification

Prise en charge de Fido 2 et Multi-tenant

Fido2 et Multi-tenant o365, sur SSO
Connexion Windows au pont SSO

Biométrie Avancée

Nos propres brevets biométriques
Intégration BlockChain

l'environnement AR

Technologie d'authentification
par détection de l'environnement



2024

2025 T2

2025 T3

2026 T2

2026 T4

2028 T3

Aegis Shield One

Migration directe à partir de SwivelACS
Contrôle du flux Radius
Meilleure prise en charge de la base de données

Pivotant ACS 4.X

Aegis Shield One 1.1

Migration directe depuis SwivelACS
Moteur Radius
Corrélateur IA

Pivotant ACS 4.2.4
Par Aegis

Aegis Shield 1.5

Migration à partir d'Aegis Shield One
Compatible MSP
Compatible FIDO2

Pivot ACS EOL

Aegis Shield 1.6

Intégration BC
ePinsafe
Aegis Biometrics

Aegis Shield Deux

Nouvelles Méthodes OEM
PLEngine

Support pivotant ACS LTS EOL

Soutenir EOL

Shield One Multi Location

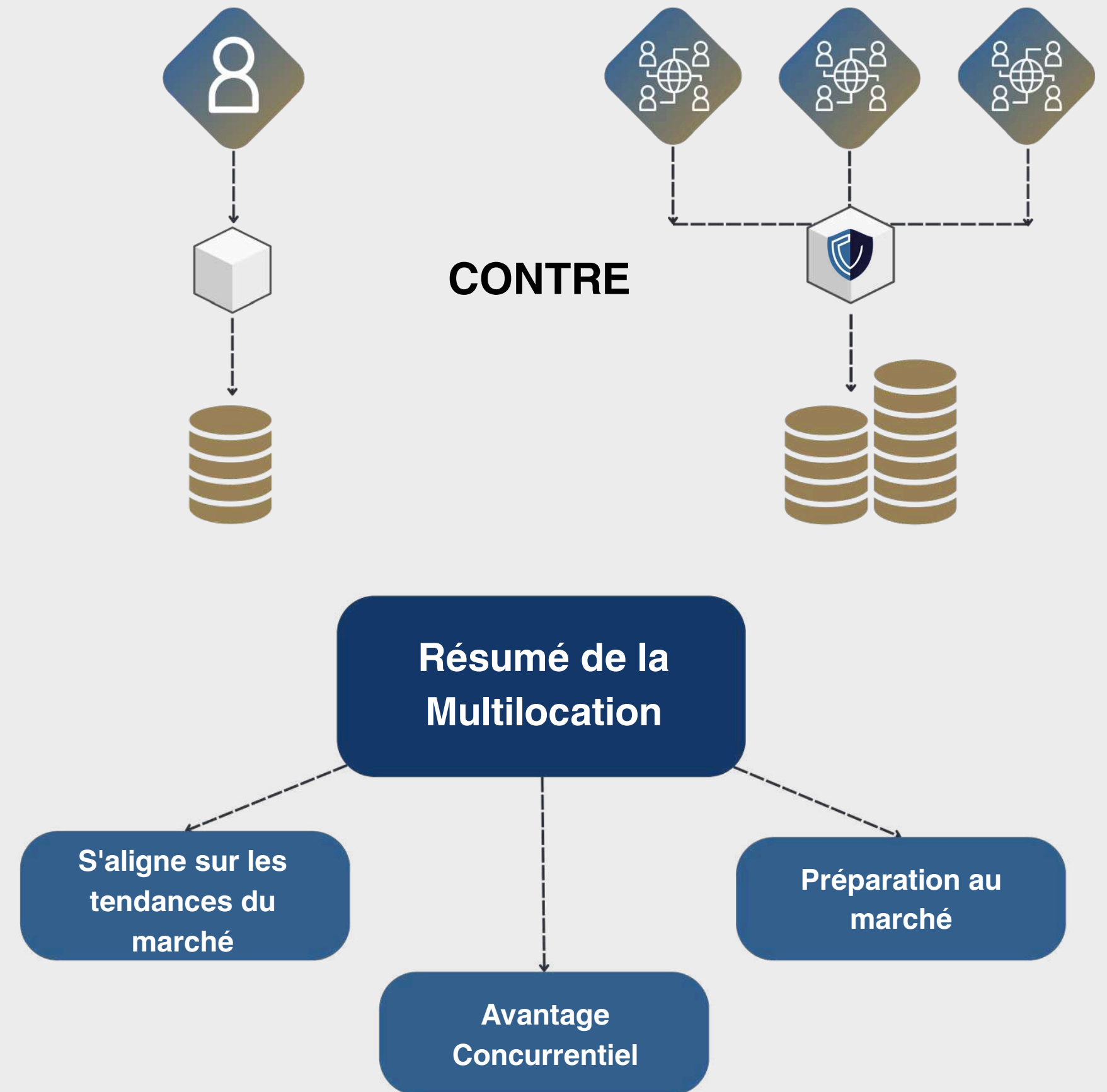
Gestion isolée: chaque unité organisationnelle (UO) fonctionne avec ses propres configurations et politiques.

Efficacité des ressources: plusieurs clients partagent un serveur unique, avec des performances optimisées.

Croissance évolutive: ajoutez de nouveaux locataires sans investir dans du matériel supplémentaire.

Réduction des coûts: infrastructure consolidée pour des coûts d'exploitation réduits.

Avantage concurrentiel: répondez au marché avec une architecture moderne et évolutive.



Shield One 1.5

Multi-location



Multi-location :

Serveur multi-locataire avec unités d'organisation isolées pour une gestion sécurisée et flexible.



Gestion de Configuration Moderne

Gestion de configuration modernisée avec un schéma de base de données dynamique, remplaçant les fichiers XML pour plus de flexibilité, d'agilité et de contrôle.



Service d'Authentification Robuste :

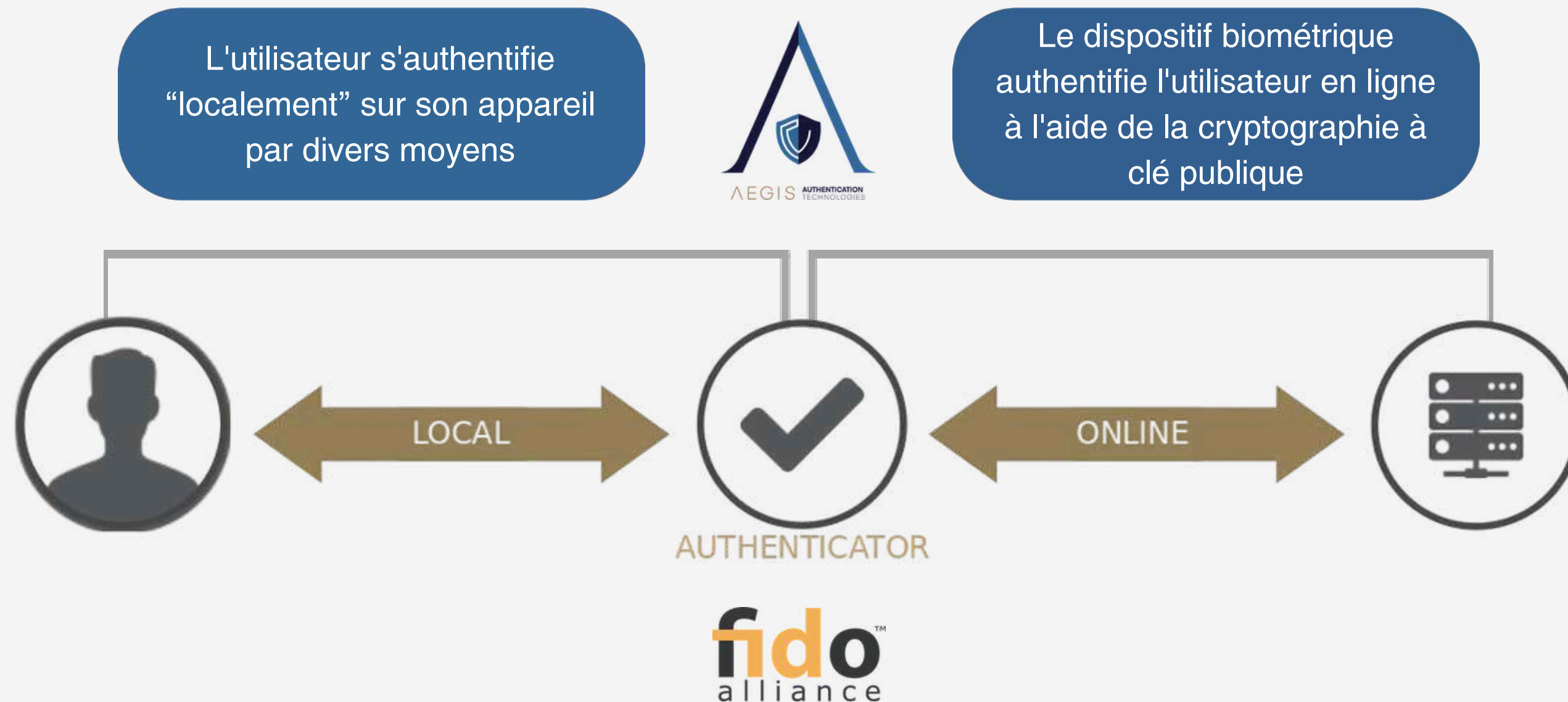
Authentification robuste avec MFA, SSO et Multi-location, conçue pour un accès évolutif et sécurisé dans tous les environnements.



Principaux points saillants de la mise en œuvre :

Isolation de l'UO et de la base de données pour une gestion sécurisée et autonome des locataires.

Introduction à la Technologie Sans Mot de Passe



Avantages de la Technologie Sans Mot de Passe



Sécurité renforcée

MFA résistant au phishing qui empêche le vol d'informations d'identification et garantit une authentification forte et sécurisée.



Parcours Utilisateur Amélioré

Connexion transparente et sans mot de passe avec authentification rapide et sans friction.



Efficacité

Opérationnelle

Coûts de support réduits, évolutivité sans effort et conformité réglementaire totale.



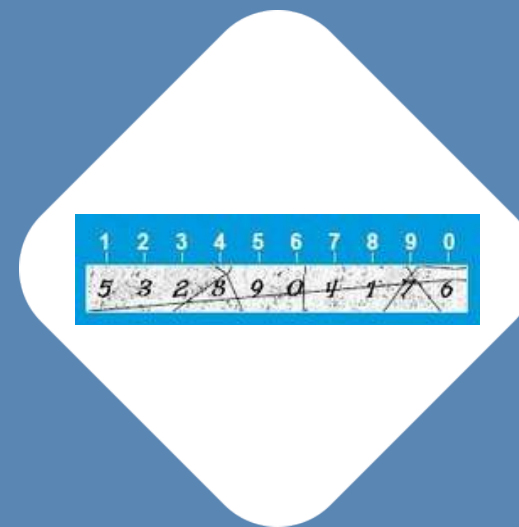
AEGIS AUTHENTICATION
TECHNOLOGIES

FIDO2 Sans Mot de Passe et ePinsafe® :

Un changement de Jeu



+



=



Conformité et normes alignées

Assure une conformité réglementaire totale (ag, RGPD) et suit les meilleures pratiques du secteur, auxquelles font confiance les principaux acteurs.

Accès Sécurisé TURING

Authentification brevetée sans jeton utilisant des codes PIN dynamiques basés sur des images, uniques à chaque connexion, jamais saisis et impossibles à reproduire.

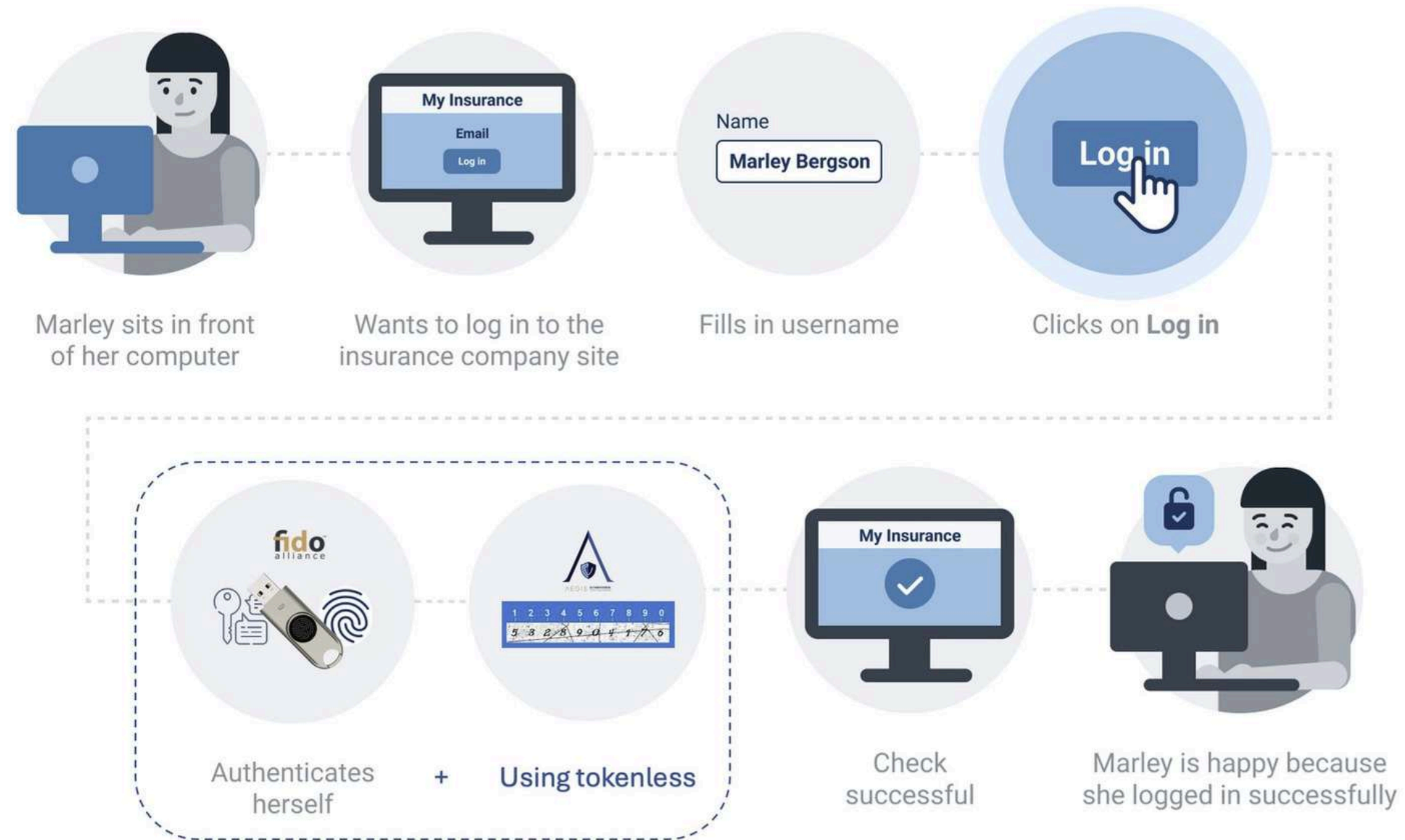
Sécurité de Connexion de Niveau Supérieur

Connexion avancée sans jeton avec codes PIN dynamiques extraits d'images, jamais saisis, jamais répétés. Sécurité maximale à chaque session.

Paradigme

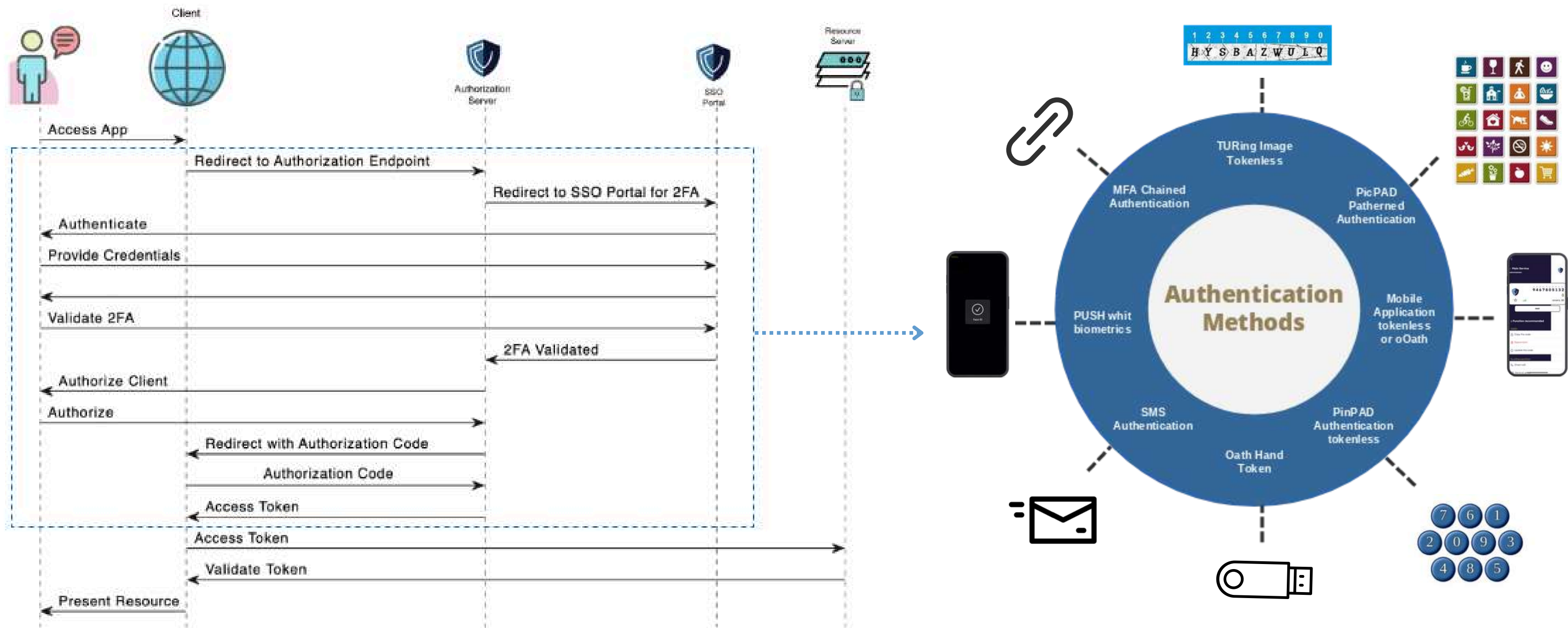
FIDO2 et ePinsafe®

Aegis Shield One propose une solution d'authentification de pointe et conviviale, alliant innovation et sécurité avancée pour un accès numérique fiable.



Paradigme d'Autorisation Shield One + SSO

Le nouveau module serveur OAuth2 inclut la prise en charge PKCE, ajoutant une couche de sécurité supplémentaire pour les clients publics et améliorant la protection globale.



Serveur de Protocole Shield One

Serveur de Protocole: MFA transparente pour les systèmes hérités et modernes

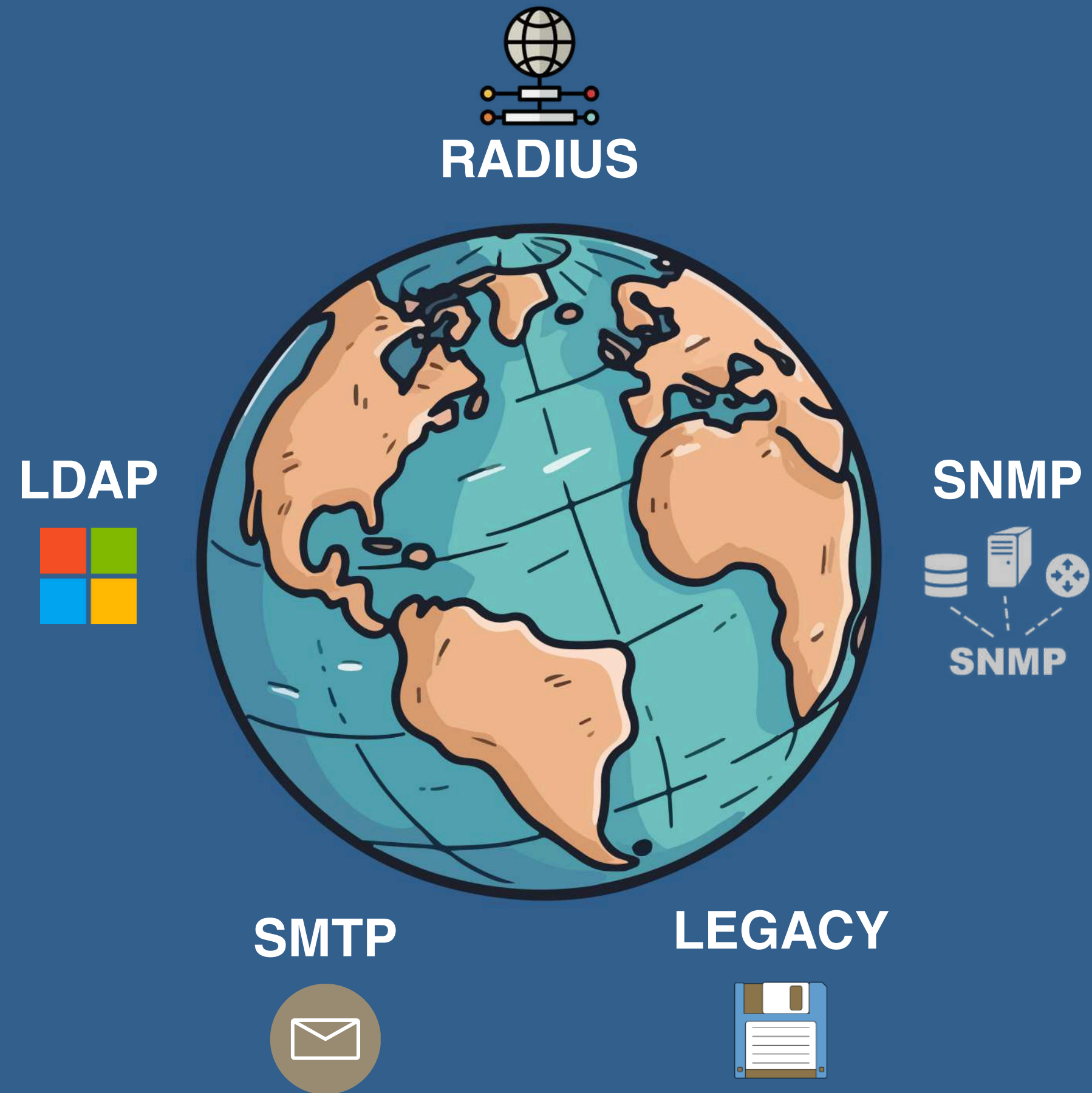
Renforcez votre infrastructure grâce à un serveur d'authentification intégré qui permet l'authentification multifactorielle pour des protocoles tels que RADIUS et LDAP, Garantir un accès sécurisé, même dans les environnements ne prenant pas en charge nativement l'authentification multifactorielle (MFA).

Principaux avantages:

- **Chaînage de Protocoles:** Permet des flux de travail RADIUS à RADIUS
- **Prêt pour l'avenir:** conçu pour les intégrations de protocoles à venir
- **Intégration polyvalente:** compatible avec les systèmes existants et modernes

Exemple en Action :

Shield One gère l'authentification multifacteur (MFA), transmet les informations d'identification pour la validation LDAP et renvoie en toute sécurité l'approbation d'accès, simplifiant ainsi l'authentification sécurisée sur toutes les plateformes.



Cas d'utilisation du serveur de Protocole Shield One

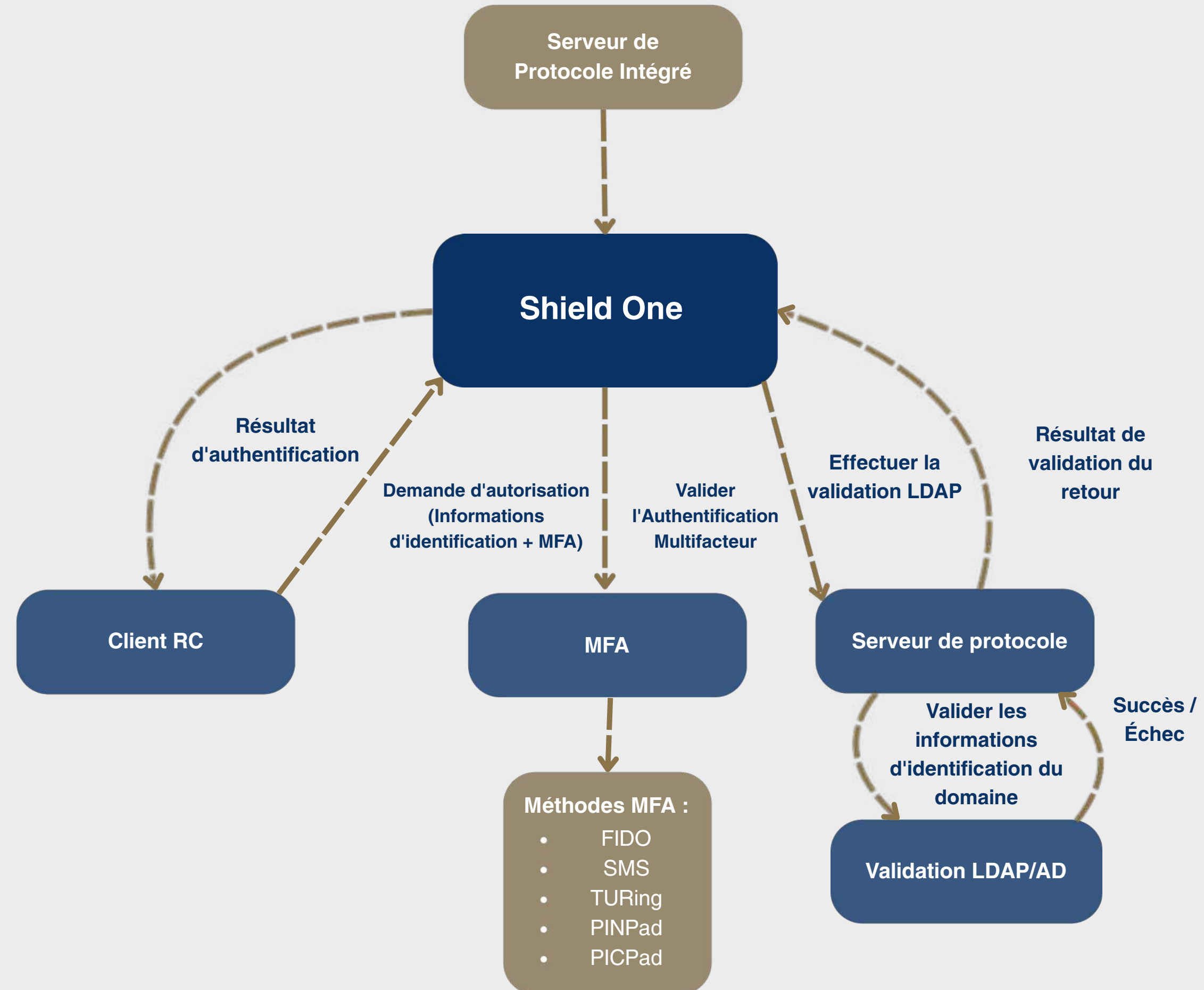
Flux de Travail d'Authentification Sécurisée:

1 - L'utilisateur final soumet ses informations d'identification + MFA à Shield One.

2 - Shield One valide l'authentification multifacteur et la transmet Informations d'identification LDAP/AD via RADIUS.

3 - Le serveur VPN vérifie les informations d'identification avec le domaine.

4 - Shield One livre la finale réponse d'authentification au client.



Appareil de marque Aegis

Fondation de Confiance:

Transition vers une base Debian robuste et fiable pour notre appareil de marque.

Sécurité Intégrée

Protection renforcée grâce à l'architecture axée sur la sécurité de Debian et aux mises à jour régulières.

Stabilité à Long Terme

Support étendu et fiabilité du système pour les opérations commerciales critiques.

Compatibilité Évolutive

Debian assure un meilleur alignement avec les technologies émergentes et les intégrations tierces.

Approuvé dans le Monde Entier

Adopté par les leaders de tous les secteurs:



Révision et Ajustements

Nous menons...

...des points réguliers avec les membres clés de l'équipe pour examiner les progrès et relever les défis.

...des observations des tendances du marché pour garder un œil sur les changements du marché et les concurrents.

...un développement réactif utilisant des méthodes de type agile adaptées à notre équipe.

...une analyse concurrentielle pour comprendre les vulnérabilités potentielles des autres.

...des tests de sécurité internes de nos solutions.





Conclusion

Récapitulatif des Points Clés:

- 1** **Intégrations complètes:** intégration prise en charge avec les principales plateformes telles qu'Office 365, Salesforce, SAP, Azure, etc.
- 2** **Solutions conviviales:** des portails SSO et libre-service transparents sont fournis pour améliorer l'expérience utilisateur.
- 3** **Différenciation du marché:** fonctionnalités uniques proposées, notamment des technologies brevetées et une prise en charge flexible des protocoles.
- 4** **Sécurité avancée:** authentification multifactorielle robuste et intégration biométrique pour une protection renforcée.

Vision Stratégique:

- 1** La solution la plus avancée et la plus complète du marché, alliant innovation de pointe, sécurité robuste et expérience utilisateur inégalée.
- 2** **Partenariats stratégiques:** établir des alliances solides pour améliorer les capacités des produits et la portée du marché.
- 3** **Évolutivité:** prise en charge efficace de plusieurs locataires, garantissant évolutivité et rentabilité.
- 4** **Prêt pour l'avenir:** Positionné pour s'adapter aux tendances et technologies émergentes en matière de cybersécurité.



AEGIS AUTHENTICATION
TECHNOLOGIES

Merci!

**Des questions? Des commentaires?
Des compliments? Je les prends dans
l'ordre que vous voulez.**



sales@aegisauth.com



www.aegisauth.com