

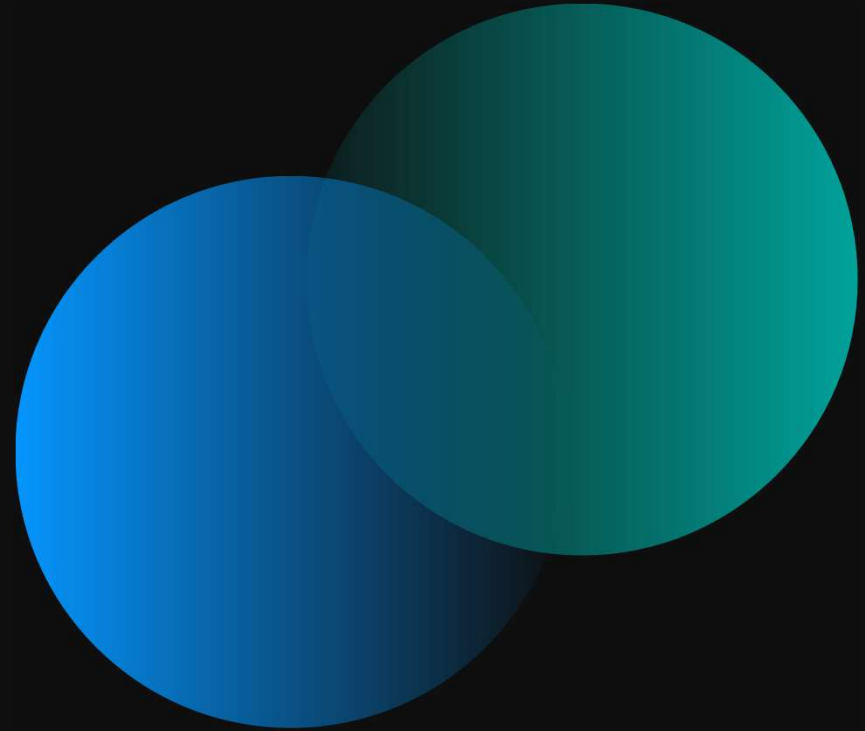
Evidian Web Access Manager

Franck Laloum
franck.laloum@atos.net

© Atos - For internal use

The Atos logo is displayed in a blue, stylized font. It features a large 'A' followed by 'tos', with the 'o' being a circle that has a small dot in the center, resembling an eye or a stylized '0'.

Introduction



AtoS

Atos en résumé



110,000 experts
dans 73 pays



12 Mds € de chiffre d'affaires &
1,2 Md € de marge opérationnelle



Partenaire informatique des
Jeux Olympiques



Leader Mondial du cloud et de
l'espace de travail digital



N ° 1 des services de sécurité gérés en
Europe et n ° 3 au niveau mondial



235 M € de R&D
4500 brevets par an



52,000 nouvelles certifications
numériques



20.97tCO₂/m€ de revenus de
l'industrie, meilleur de sa catégorie

Evidian



Editeur Logiciels de solutions de Gouvernance des Identités et des Accès

- Access Management
- Identity Governance
- On premise, As a Service, Managed Services

Gartner



Références mondiales

- Europe, Japon, Amérique du Nord, MEA
- +900 clients , +5 millions d'utilisateurs professionnels
- R&D en Europe

Partenariats Technologiques et interoperabilité



Références par marché, à l'échelle mondiale



5 M +
d'utilisateurs

Finance Service	Industrie, Vente de détail, Transport	Telco, Médias, Utilities	Publique Santé

Evidian IAM Offer at a glance



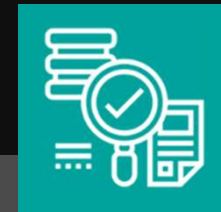
Identity Governance and Administration

Ensure easy management of digital user identities lifecycle and automates processes related to users and access entitlements



Single Sign-On and Access Controls

Enable users to login once and access multiple services and resources securely, with many MFA features increasing user experience and reducing risk



Advanced Analytics

Increase security compliance with advanced analytics and risk analysis such as access reviews, dashboards drill down

Training - Professional Services - Support - Global Delivery Center

Suite Identity and Access Management

La fondation pour une sécurité basée sur les métiers



Identity Governance & Administration

Gouverne, gère et contrôle les identités des utilisateurs

Approvisionnement - Réconciliation

Re certification



Web Access Manager

Fédération d'identité, Web SSO, authentification multifactorielle



Enterprise SSO

Accès sécurisé aux applications utilisant des mots de passe à partir du PC ou Mobiles



Authentication Manager

Authentification multifactorielle Windows pour les entreprises



Analytics and Intelligence

Analyses avancées pour l'Identité et l'Accès



Evidian IDaaS

Accès et Gouvernance



SafeKit

Répartition de charges, réplication synchrone des fichiers au niveau octet, reprise sur incident

Gestion des identités et des accès

Authentification multifactorielle

Fédération d'Identité
Authentication web

Libre-service sécurisé

Single Sign-On universel

Services gérés
On-Premise ou en mode SaaS

NTT Comware – Systems integration

Evidian WAM



- # users: 8 000+ (with potential of 270 000 in NTT group).
- Evidian Web Access Manager

Challenges

- ▶ Subsidiary of NTT group, formerly IT department
- ▶ 60+ in-house applications with proprietary authentication mechanism
- ▶ Replacement of legacy in-house developed Web-SSO system to comply with SAML enforcement policy of NTT group
- ▶ Authorizations stored in NTT Comware LDAP Directory
- ▶ Synchronization of corporate AD users to NTT Comware LDAP Directory
- ▶ Replacement of physical Load Balancer
- ▶ Architecture requirements: Specific requirements, HA, AD/LDAP infrastructure

Solution

- ▶ **Evidian WAM** for unique authentication across NTT Comware applications
- ▶ Turn legacy access to SAML Service Providers
- ▶ Specific development to support legacy authentication mechanism
- ▶ **IDSynchro** for synchronizing ID from corporate AD to OpenLDAP with attributes
- ▶ **Evidian Safekit** for Load Balancing and HA in replacement of physical legacy system



Benefits

- ▶ **Enhanced security** with enhanced authentication policies and NTT group rules compliance
- ▶ **Packaged solution** to support other affiliates with same challenges
- ▶ **Export of Packaged solution** to external NTT Comware customers
- ▶ **Reduced costs** of help desk, operation and maintenance of in-house products

FOYER Assurances

Evidian WAM, CIAM & IGA



- # users: 52 000+ (2000+ corporate users, 50 000+ customers and partners).
- Evidian Web Access Manager, Evidian IGA, Evidian ESSO

Challenges

- ▶ Several subsidiaries, each with its own customized access portal but single authentication for all
- ▶ Employees, partners and customers profiles with different access
- ▶ Access to services through native mobile application with integrated authentication
- ▶ Customer needed a web Single Sign-On across several applications, with adaptive authentication depending on security level required and based on the user rights policy
- ▶ Regulatory requirements: full audit, reports to comply and provide proofs to regulators
- ▶ Architecture requirements: Multi-sites, 24x7 access, LDAP infrastructure
- ▶ Manage corporate user life cycle: process automation and access governance

Solution

- ▶ **Evidian WAM** for sharing authentication across several dedicated customers portal.
- ▶ SSO to public and private applications
- ▶ State of the art authentication for native mobile applications
- ▶ Adaptive and multifactor authentication.
- ▶ **Evidian IGA** to manage identities and authorizations based on extended RBAC (Role Based Access Control) model with approval workflow.
- ▶ **Evidian Enterprise SSO** for intranet access to thick client applications



Benefits

- ▶ **Enhanced security** with reinforced authentication policies and identity governance
- ▶ Improved **customers experience**
- ▶ **Reduced costs** of help desk & operation
- ▶ **Reporting capabilities** for administrators, internal audit and regulatory **compliance**
- ▶ **Automated user Life Cycle management** based on **reliable** identity sources

Assistance Publique – Hôpitaux de Paris

Complete IAM Suite



- # of users: 130,000+
- Evidian IGA – ESSO, Auth. Manager and WAM

Challenges

- ▶ Define and manage a unique identifier for each employee. of the 38 hospitals
- ▶ Allow hospital designed administrators to manage user's life-cycle.
- ▶ Make mobility easier for the employees.
- ▶ APHP needs to implement Strong Authentication to comply with French Health Regulations.
- ▶ Implement multiservice card system for logical and physical access.
- ▶ Allow doctors to connect and access patients' medical records from their office.

Solution

- ▶ **Evidian IGA** to define & maintain a central user repository.
- ▶ Defined a security policy and implement user life-cycle workflow process to manage and trace access grants.
- ▶ Delegated administration for their own employees and ensured employee mobility.
- ▶ **Evidian EAM** allows usage of the French Health smartcard to authenticate and provides SSO to access the applications.
- ▶ **Evidian WAM** allows doctors to access to patients' records from their own office in a secure way.



Benefits

- ▶ **Reduced costs** for helpdesk and IT and **Reduced delays** in the identity lifecycle and gain of time for patients: Evidian IAM Suite is managing 130 000+ employees live cycle, performing **automatic provisioning to 15 business applications** through an EAI Bus.
- ▶ **Simplification** of the identity management process: users authenticate using a multiservice smartcard and benefits of SSO.
- ▶ **Mobility and security**: External access to the patient information is granted to some doctors.

AGIRA -GPSA

Evidian IGA and WAM



GPSA

- # of users: 10,000
- 150 organizations
- Evidian IGA & WAM

Challenges

- ▶ Provide an authentication, access control and user management system for 10000+ users in more than 150 organizations.
- ▶ Let each organization manage the user and right's life cycle accessing to several applications.
- ▶ Be able to define different levels of User Administrators.
- ▶ Provide Federated Identity services.

Solution

- ▶ Evidian IGA and WAM to managed distributed User and Right's Life Cycle, Authentication and Authorization.
- ▶ Enabled local administrator and local access for every 150 organizations with identity management and federated identity-based authentication and authorization.
- ▶ Managed Services set-up hosted and managed by Atos.



Benefits

- ▶ AGIRA benefits from a **managed services solution**: simplification and reduced infrastructure and maintenance.
- ▶ Users administration **delegated** to each identity to reduce operational costs and **improve efficiency**.
- ▶ Reinforced access security with **federation of identities**.

Ordre National des Pharmaciens

Evidian IGA and WAM



Ordre national
des pharmaciens

- # users: 120,000+
- Evidian IGA & WAM

Challenges

- ▶ High complexity: 118 000 registered pharmacists, thousands of inscriptions and radiations a year, with 250 employees, 800 consultants and distributed to 21 French regional councils, delegations in the DOM and an office Brussels.
- ▶ Implement a Security data repository, in a security architecture to grant and control access based on individual rights.
- ▶ Implement a Directory Management system: white pages, yellow pages.
- ▶ Set up a Self-service process and emergency access.
- ▶ Allow the audit of the policy and access for compliance.
- ▶ Policy: Automate the management of access rights and delegate the rights approval procedure.

Solution

- ▶ Evidian IGA and associated security services (Web Authentication, Web SSO, provisioning, workflow, reconciliation...) to implement governance of access, role management with registration and deletion of users.
- ▶ Secured corporate website and availability of secured services through intranets or extranets.



Benefits

- ▶ Business driven governance of access and authorizations.
- ▶ Evidian IGA solution allowed the CNOP to implement procedures and automate identity and user management for each arrival of pharmacist and assistants by providing access to the applications and on-line services that are provisioned automatically.

Conformité

Exigences IAM et RGPD d'Evidian



Exigences GDPR



IGA



Analytics & Intelligence



E-SSO



Authentication Manager



Web Access Management

Suite Evidian IAM

Exigences GDPR	IGA	Analytics & Intelligence	E-SSO	Authentication Manager	Web Access Management
Accès aux données	Accès via interface libre service	Contrôle d'accès basé sur les rôles (RBAC)	Accès via interface libre service	Accès via pages libre service	
Modification & Suppression	Interface libre service pour modifications et suppression	Pseudonymisation automatique après une période de rétention	Interface libre service pour modification et suppression	Suppression sur demande et après inactivité	
Limitation de traitement	Demandes de limitation ou suspension avec le mode «Départ d'utilisateur»	Contrôle du traitement selon la politique IGA	Possibilité de désactiver/réactiver des comptes	Désactivation/Réactivation	
Notifications & consentement	Propagation automatique par provisionnement/déprovisi.	Rapports de consentement	Envoi d'email lorsque le mot de passe SSO primaire est changé.	Outil Pop-Up automatisé de gestion du consentement	
Portabilité des données	Données transférables via API	Données transférables	Possibilité de recevoir ses comptes SSO par email et de les révéler depuis le poste de travail ou depuis le portail Web	Export de données via pages libre service	
Sécurité du Traitement	Pseudonymisation des événements d'audit, compatible avec Atos HSM	Pseudonymisation des rapports, RBAC	Pseudonymisation des événements d'audit, compatible avec Atos HSM	Pseudonymisation des événements d'audit, compatible avec Atos	
Gouvernance basée sur le risque	Approche basée sur le risque avec outil de recertification.	Rapports ad hoc	Méthodes d'authentification fortes adaptées à chaque niveaux de risque	Authentification forte adaptative	
Audit & Contrôle	Accès aux événements d'audit via console	Rapports et tableaux de bords comme preuve de conformité	Accès aux événements d'audit (jour/semaine/mois). Rapports et tableaux de bords	Accès à l'historique des événements d'audit	

WAM Value proposition

Evidian WAM pour faciliter et sécuriser l'accès aux ressources de l'entreprise



Evidian
WAM

Evidian WAM
IdP & web SSO



Identity Federation

Pour tous les usages: B2E, B2B and B2C



Digital transformation

Un point d'accès unique aux applis traditionnelles et modernes



Authentication

Large choix de méthodes d'authentification



Intégration facilitée dans l'infrastructure

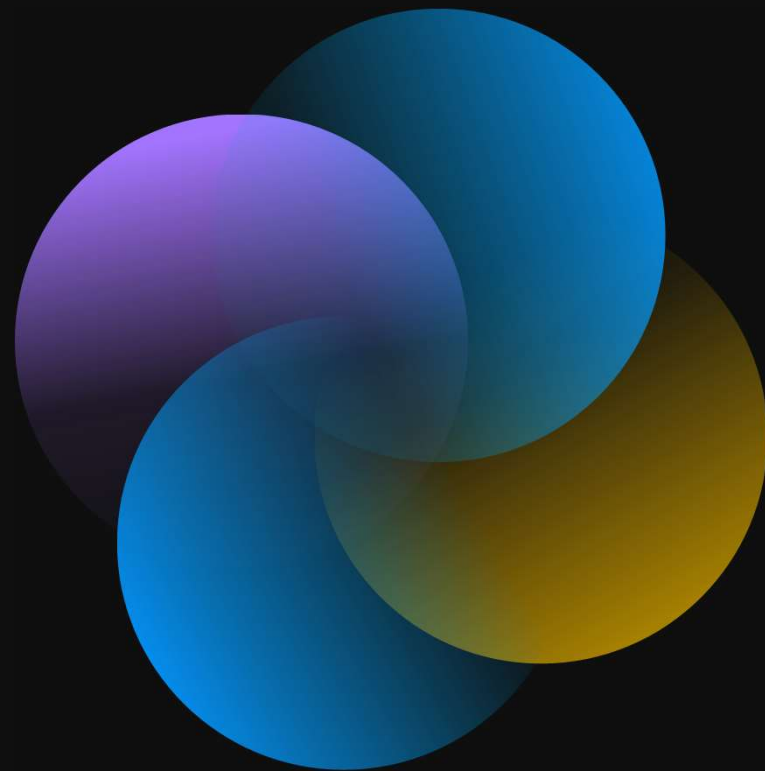
WAM Connect SDK, portail d'accès



Evidian IAM: une suite intégrée

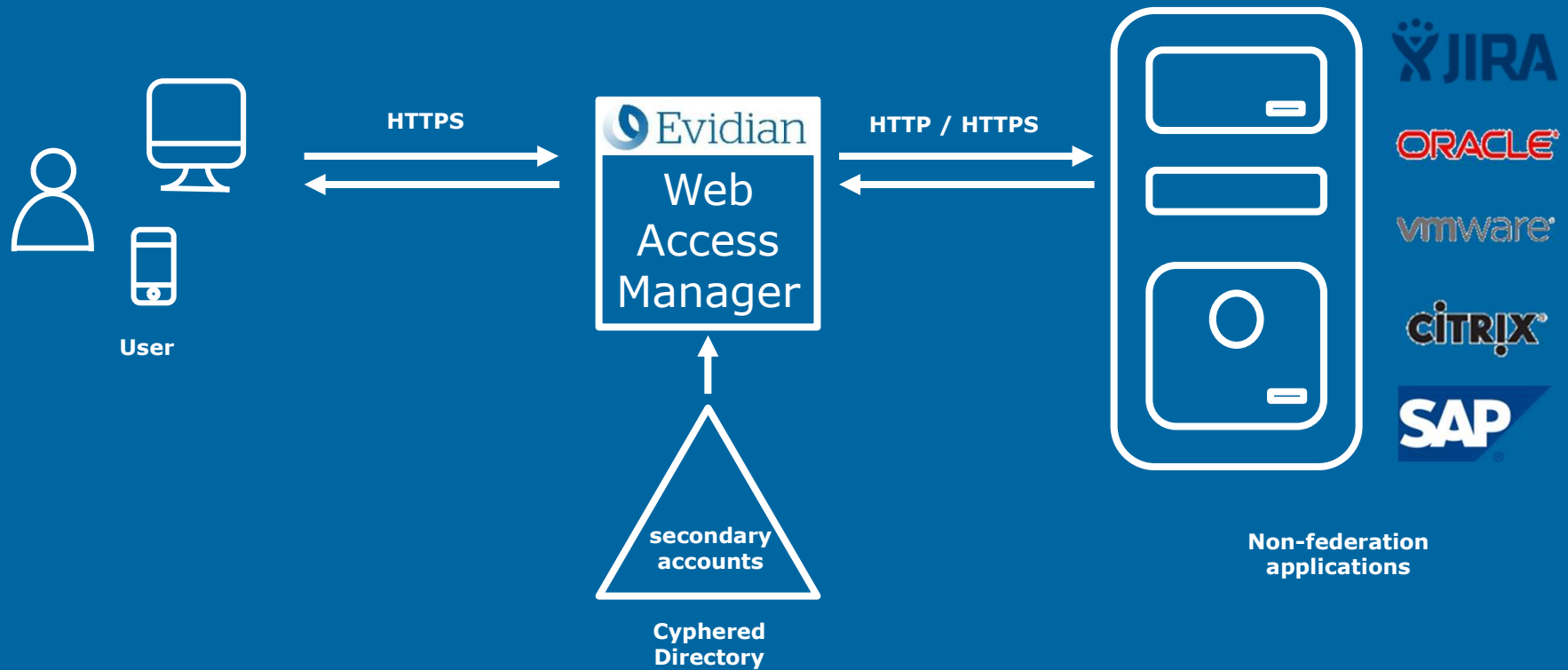
Pour la gestion des identités et tous les scénarios d'accès

Applications traditionnelles



AtoS

Reverse Proxy / Web-SSO



Reverse Proxy / Web-SSO



Web-SSO non-intrusif

- Pas de **modification** des applications
- agent-less / **pas de plugin**
- **Modification** des pages à la volée

Méthodes supportées :

- Formulaire d'authentification
- HTTP Basic Authentication
- NTLM v2 / Kerberos (IIS)
- HTTP headers attributes injection

Reverse Proxy / Web-SSO



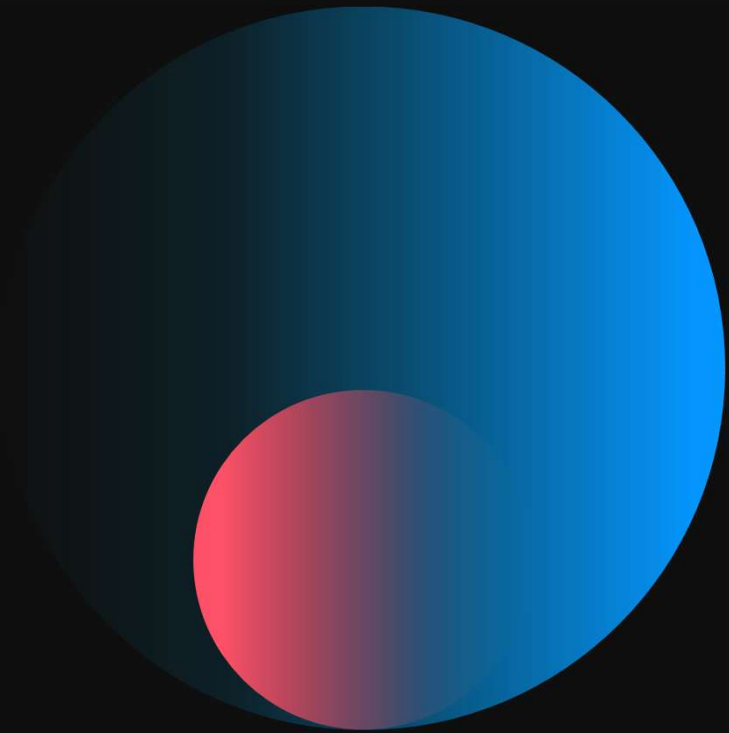
Amélioration de la **sécurité**

- accès permis uniquement par **HTTPS**
- **filtrage** des URLs
- gestion du cycle de vie des mots de passe

Délégation d' **authentification**

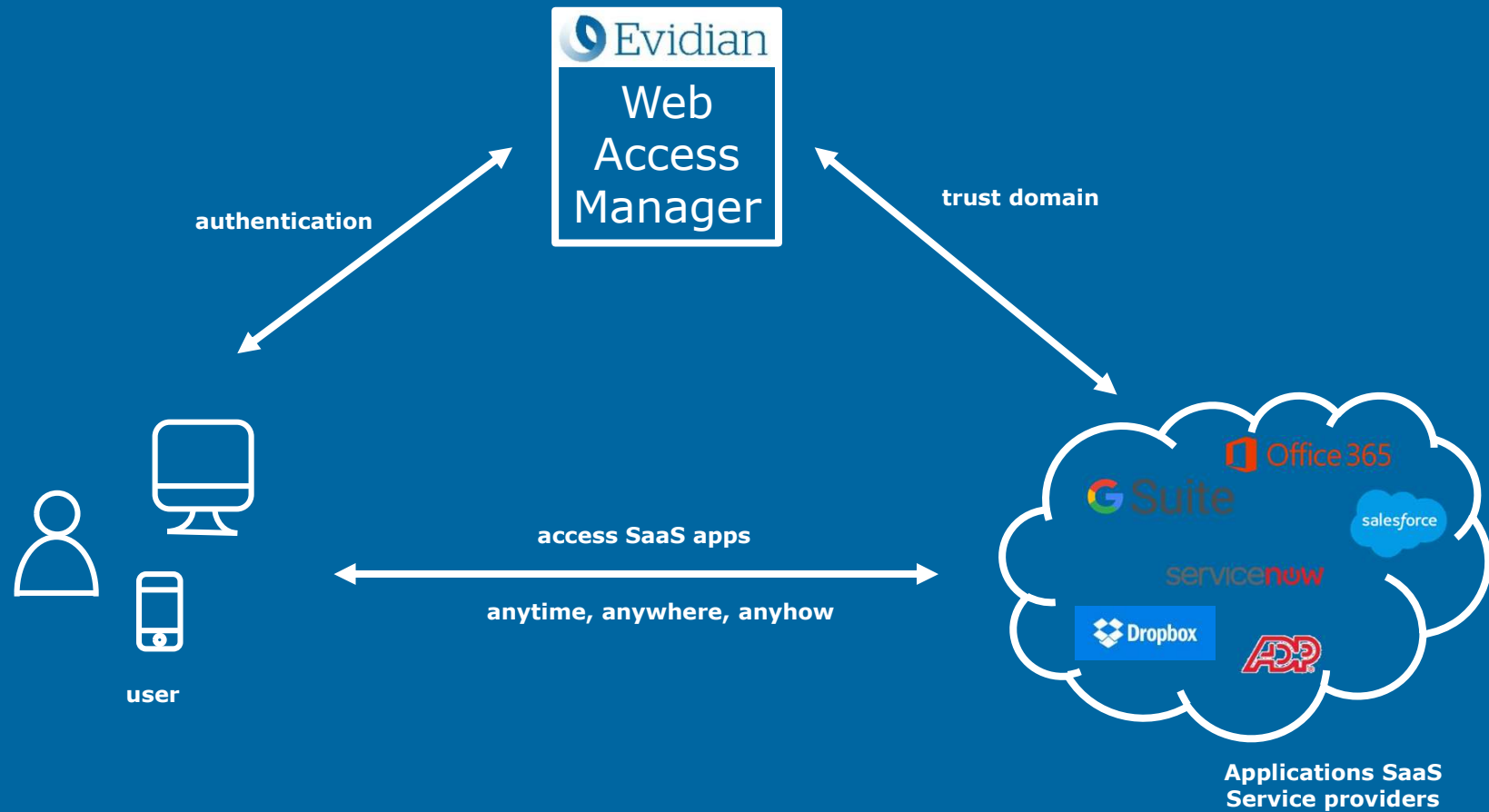
- gestion du paysage applicatif **legacy**
- pour les applications **maisons**
- injections des attributs nécessaires
- activation de **SAML/OIDC** pour les applications traditionnelles

Fédération d'identité



AtoS

Identity Provider





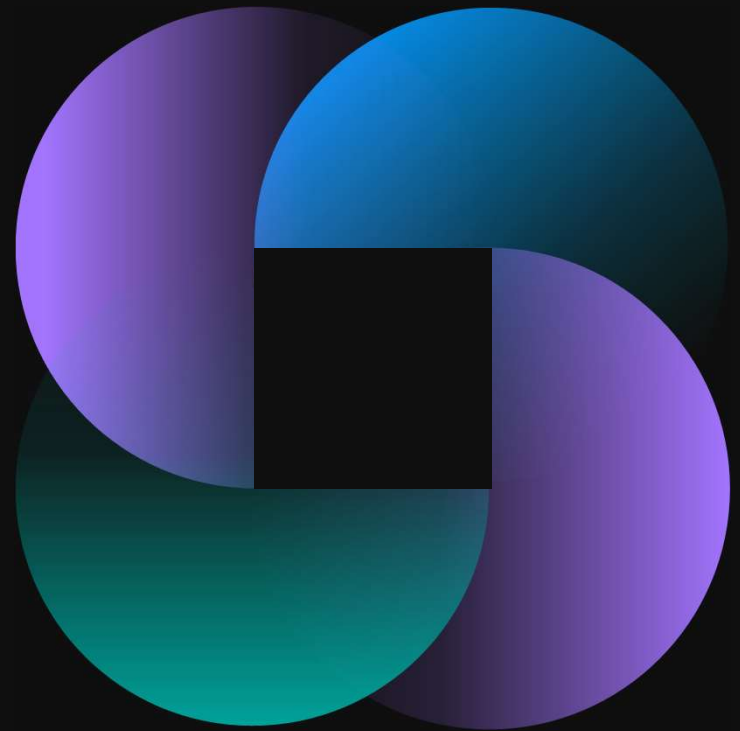
Support étendu des protocoles de **Fédération**

- **SAML** v2
- OpenID Connect
- WS-Federation
- **OAuth 2.0**

Mais plus qu'un **simple** Fournisseur d'identités

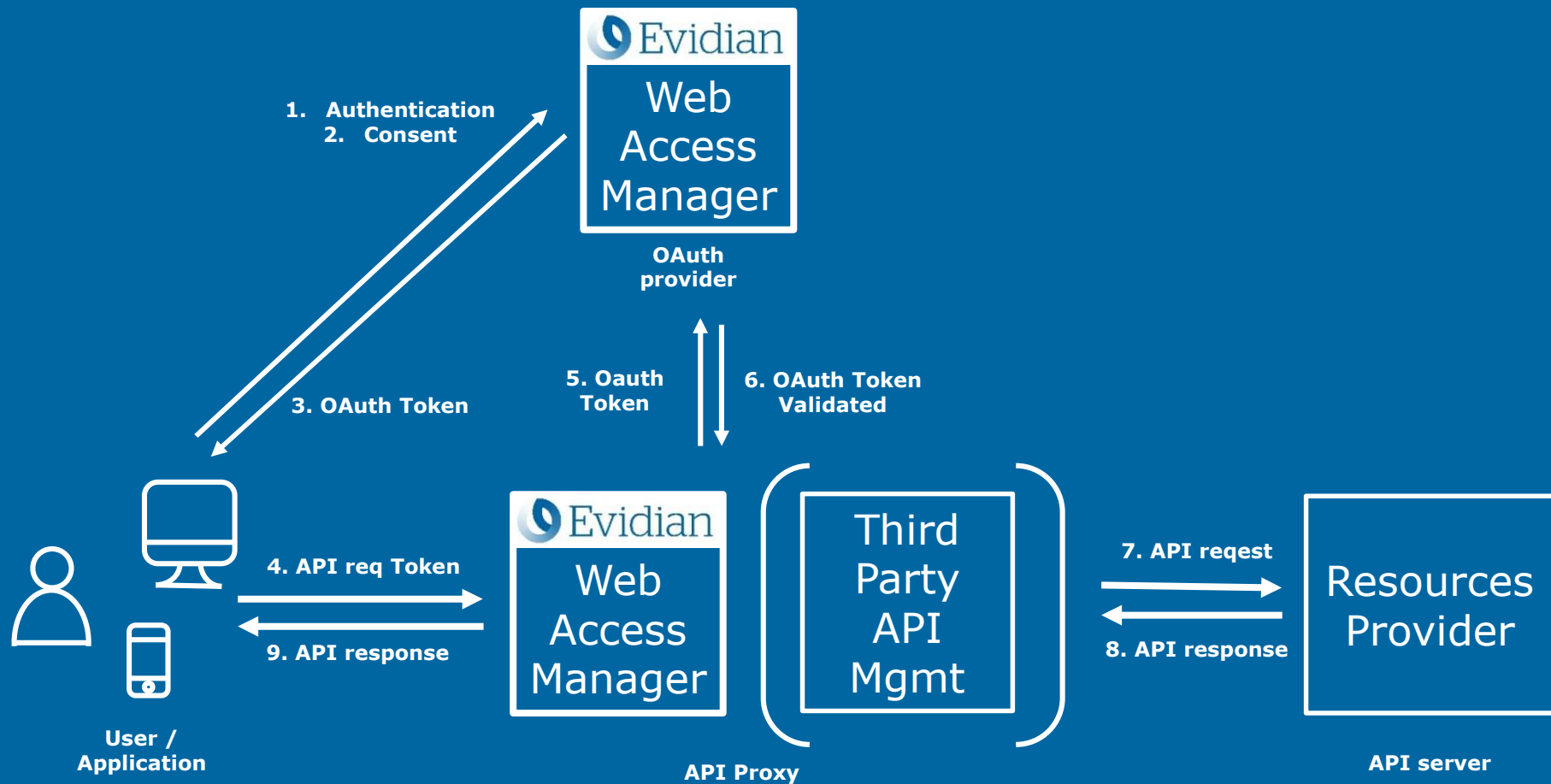
- Fournisseur de **services**
- **IdP Proxy** – Les scénarios partenaires
- “Just in Time provisioning” avec Evidian IGA
- OAuth 2.0 pour le monde **mobile**
- **Office365** clients lourds

Protection des APIs



Atos

API Protection



Protection des APIs avec OAuth 2.0



Fournisseur de jeton OAuth

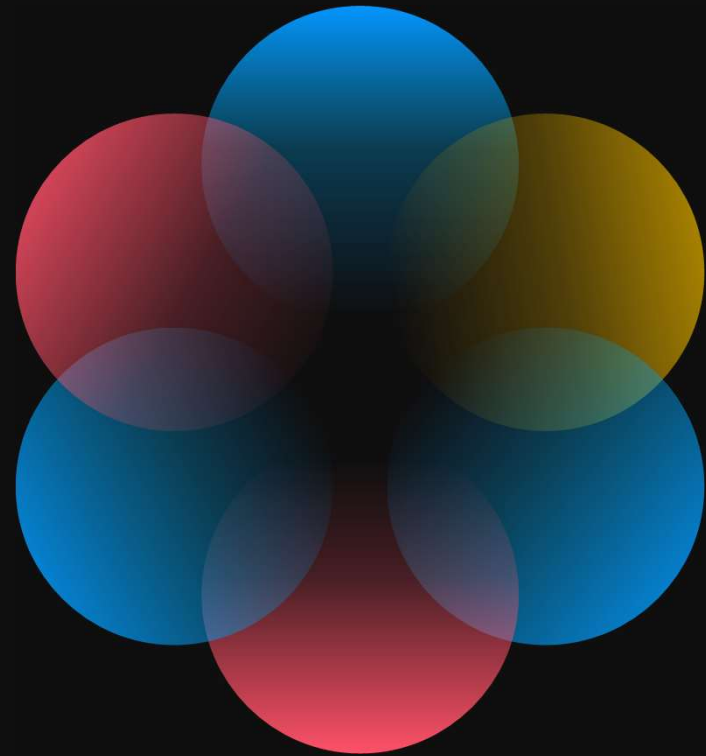
- Client credentials grant => two legged
- Authorization code grant => three legged
- Implicit grant => three legged
- ~~Resource Owner Password Credentials~~
- Fournisseur de jeton OAuth
- Device code grant => IoT

Proxy d'APIs

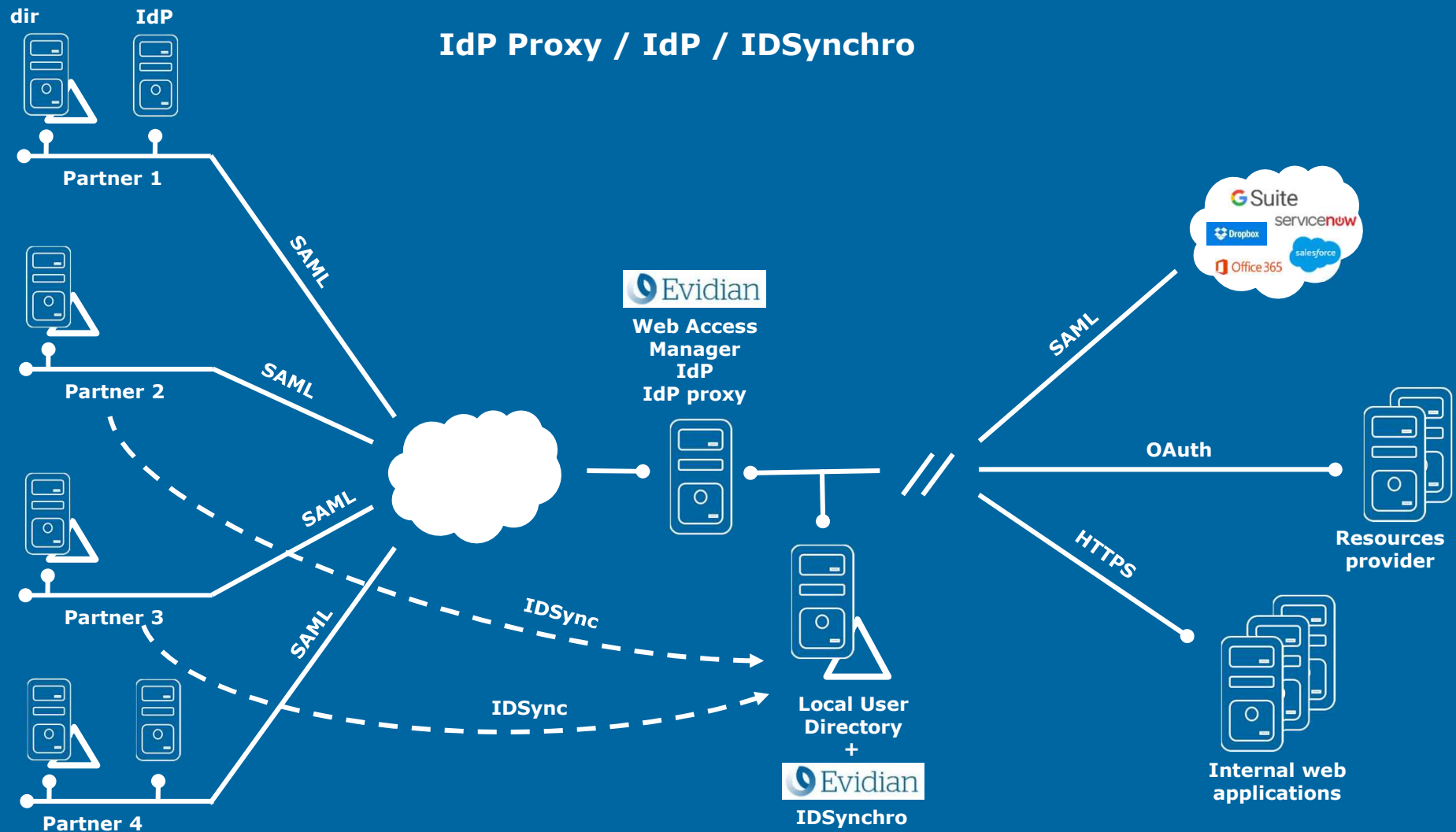
- Evidian ou tierce partie
- Filtrage sur les verbes
- géré en tant que collection d'URL
- métriques de monitoring



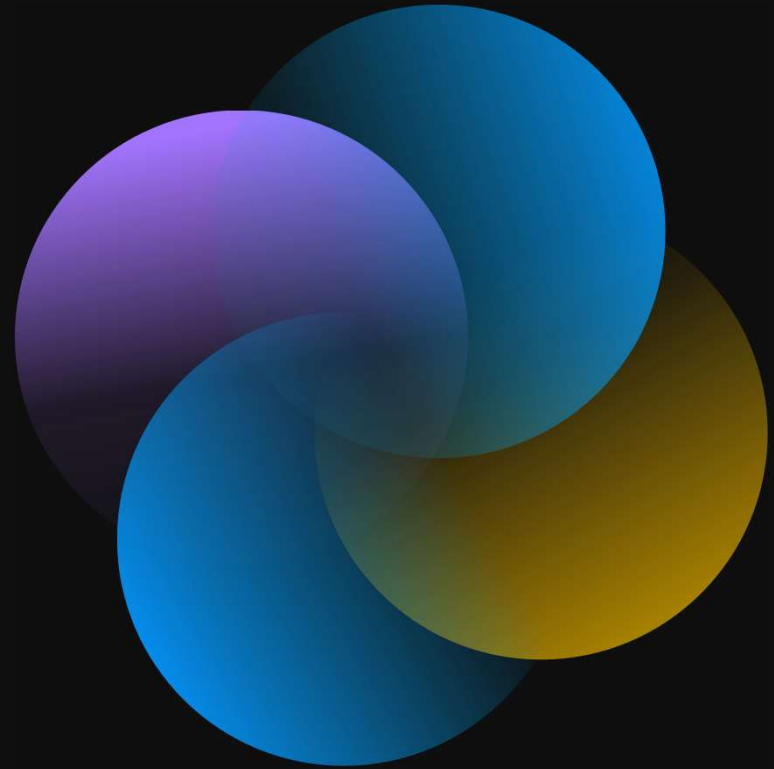
05. Partenaires / Proxy d'IdP



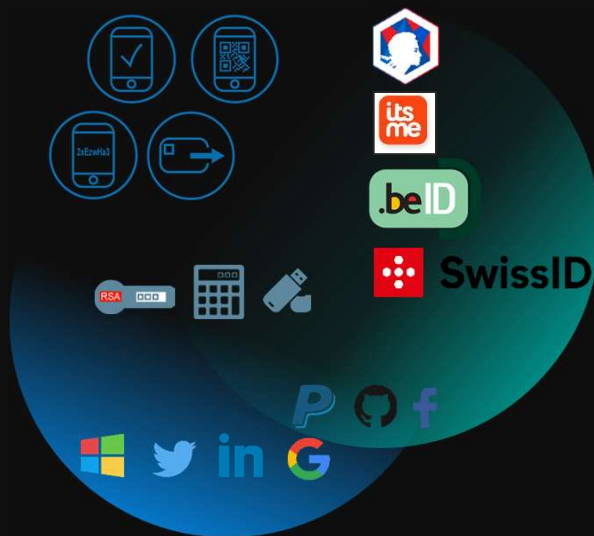
IdP Proxy / IdP / IDSyncro



o6. Authentication



Authentication



Méthodes d'authentification incluses

- Evidian Push Authentication / Evidian QREntry*
- email, SMS, TOTP (OATH)
- Délégation d'authentification tierce (RADIUS/SAML)
- Certificats X509
- FIDO 2
- Authentications nationales ou sociales
- Simplement mot de passe!

Authentications Second ou Multi-factors

- Combinaison de méthodes
- Chaque méthode se voit attribuer une force
- step-up authentication – pour une durée donnée

Evidian Authenticator

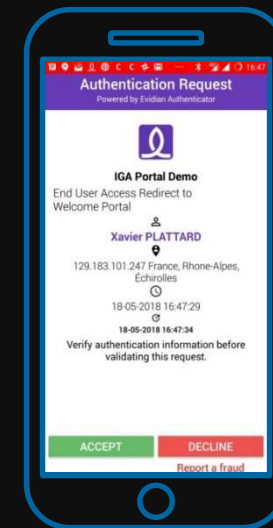


L'authentification par notification Push

- Authentification sans friction : one touch authentication
- une notification est envoyée à chaque demande d'authentification
- protection par empreinte digitale ou PIN code
- facteur supplémentaire possible : badge RFID
- enrôlement du smartphone par l'utilisateur

Pour plus de sécurité

- construit sur des principes cryptographiques éprouvés
- contexte anti-usurpation
- notification lors de la modification du profil de l'utilisateur
- Également client TOTP



Evidian Authenticator

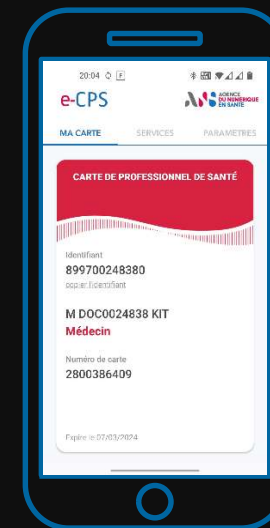


E-CPS : La carte CPS dématérialisée

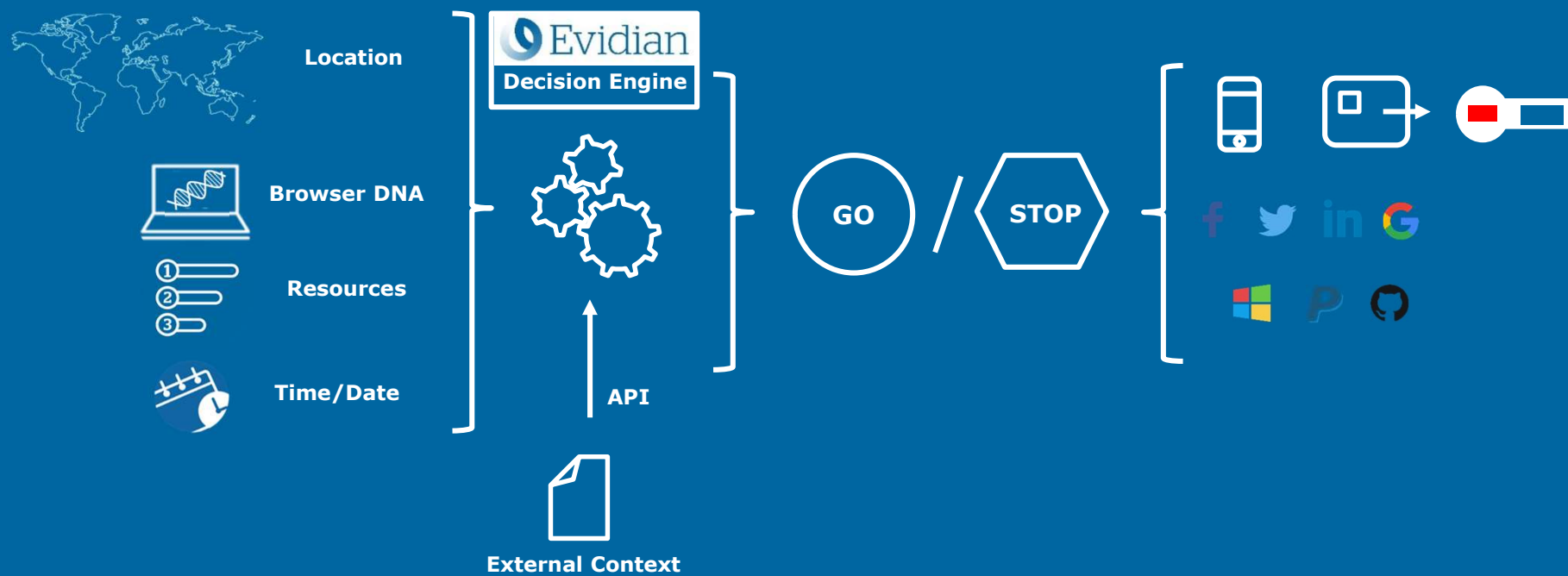
- D'un niveau de sécurité équivalent à la CPS
- Pour les usages en mobilité...
- ... et pour étendre l'usage de la CPS
- Utilisable auprès de nombreux services en ligne, depuis tablette, smartphone et poste sans lecteur de carte
- La carte physique n'est plus indispensable une fois son enrôlement effectué

Pro Santé Connect :

- Fournisseur national d'identité sectoriel pour les professions de santé
- Permet l'authentification par e-CPS (et CPS classique)
- Complètement supporté par Evidian, pour simplifier son intégration dans un paysage IT existant



Adaptive Authentication



Authentification contextuelle



Contexte d'Authentification

- browser DNA
- ressources
- localisation
- planning

Contexte externe

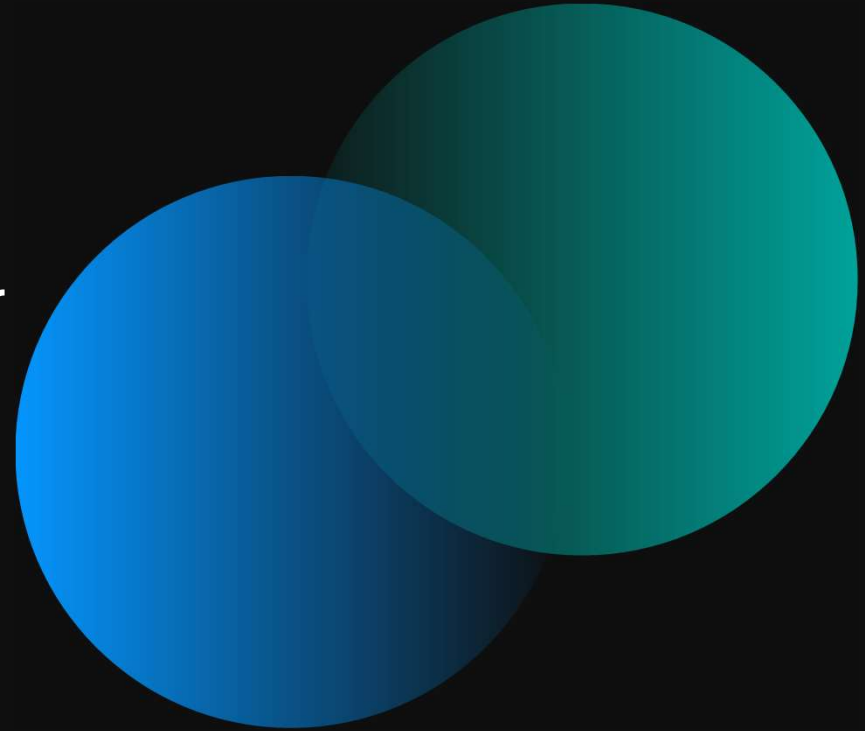
- API REST de gestion du niveau de risque externe
- Serveur de risque inclus (fast security level switch)

Browser DNA

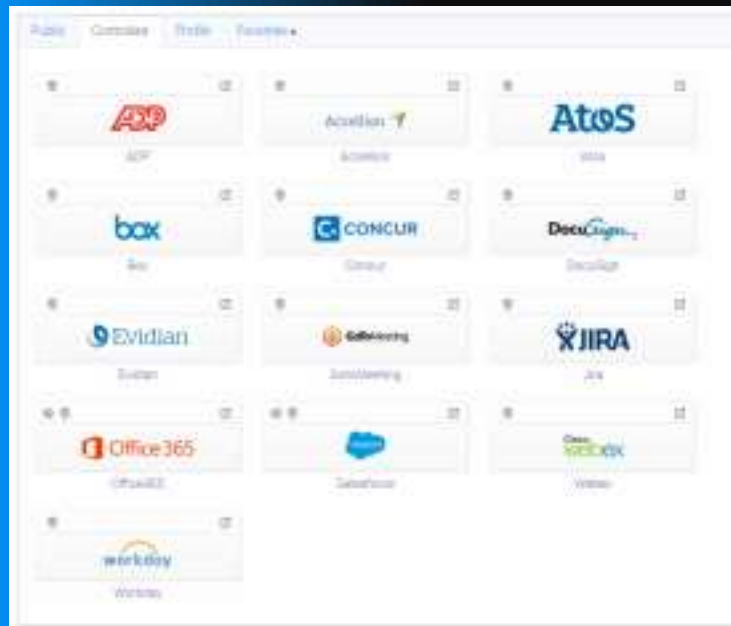
- 8 profils
- Notifications email/SMS à chaque nouvel environnement



07. Expérience utilisateur



Portail d'accès



Portail intégré

- Prêt à l'emploi
- Plusieurs portails personnalisés possibles

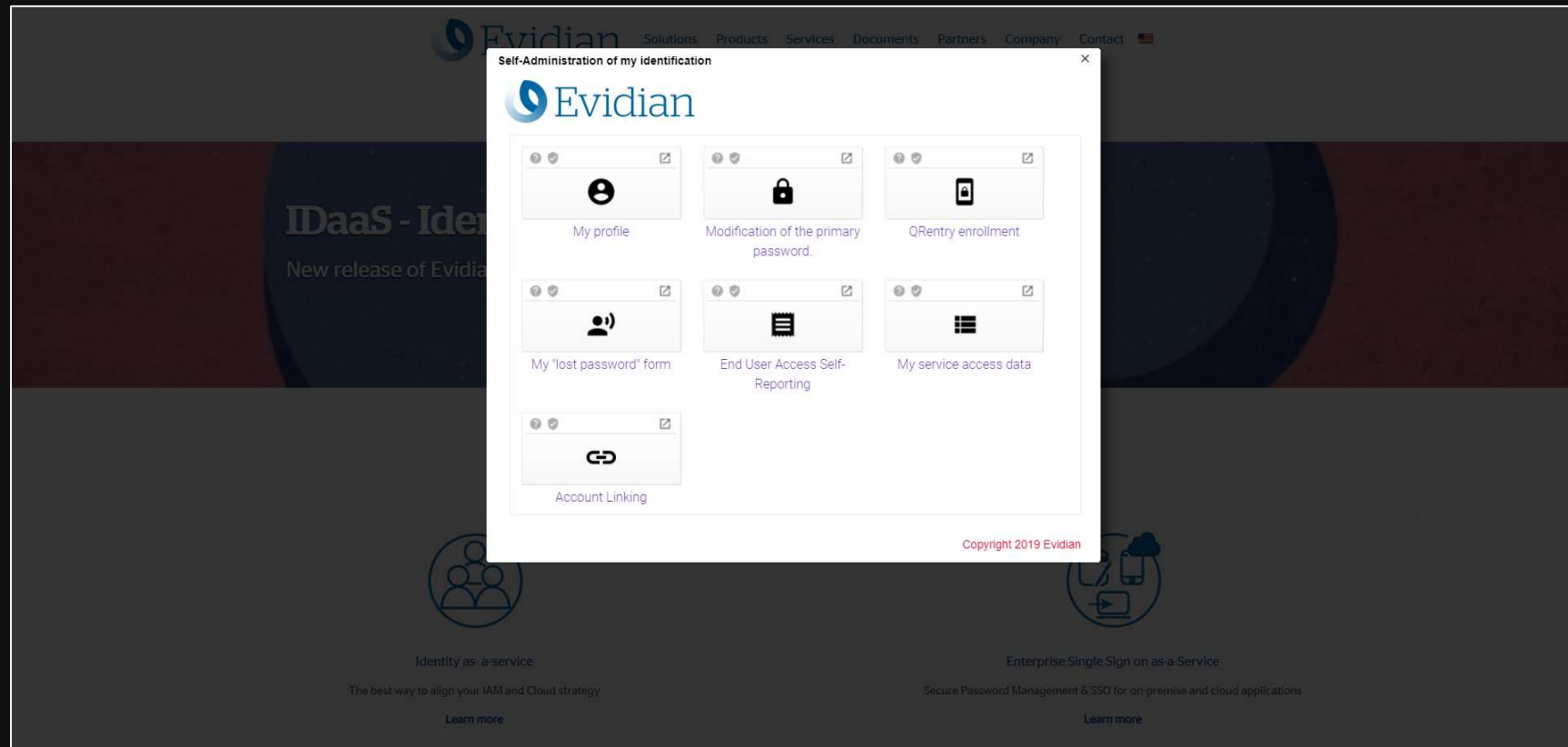
Reverse Proxy

- Modification de la page à la volée
- Personnalisable
- Attention à la maintenabilité

Intégration par le "connect" SDK

- Le style de la page est conservé
- Facile à déployer
- Maintenabilité accrue

Self-service utilisateur



Auto-enregistrement

L'enregistrement des clients doit être simple et rapide

- dicté par les standards actuels
- renseigner un formulaire exhaustif peut être un frein

Enregistrement implicite

- quand un consommateur utilise son identité sociale lors de sa première visite
- avec tous les fournisseurs



Pour les utilisateurs existant : l'account linking

- sans perte d'information

Il est toujours possible d'utiliser des formulaires complets



Confiance des utilisateurs



Deux exigences

- Respect réglementaire
- Respect de la vie privée

L'utilisateur est en contrôle

- Avec son propre tableau de bord
- Et la possibilité d'accéder et de modifier ses données

Gestion du consentement intégrée

- Au moment de l'enregistrement
- Ou à posteriori depuis le portail

Signalement d'activités malicieuses « one-click »

Q & A



Atos

For more information please contact:

M+ 33 6 33191029

xavier.plattard@atos.net

Sales Manager

Franck.laloum@atos.net

M+336 87 73 53 70

Atos, the Atos logo, Atos | Syntel are registered trademarks of the Atos group.
August 2021. © 2021 Atos. Confidential information owned by Atos, to be used by
the recipient only. This document, or any part of it, may not be reproduced,
copied, circulated and/ or distributed nor quoted without prior written approval
from Atos.



© Atos - For internal use

Atos