Étude de Cas

THALES
CYBERSECURITY

Transition vers le Passwordless : L'Expérience de la Communauté Urbaine Grand Reims

La Communauté urbaine du Grand Reims renforce la sa protection contre l'usurpation d'identité grâce waux clés de sécurité Thales.

cpl.thalesgroup.com

THALES

CYBERSECURITY

En résumé

Face à la montée en puissance des attaques par phishing et à l'utilisation de plus en plus importante de services cloud et SaaS, la Communauté Urbaine du Grand Reims a engagé une transformation structurante de son modèle d'authentification. En déployant des clés de sécurité matérielles Thales permettant à la fois l'authentification FIDO2 sur les environnements Cloud/SaaS ainsi que l'authentification par certificat sur les environnements on-premises, l'organisation a fait le choix d'un mécanisme d'authentification sans mot de passe, résistant au phishing et reposant sur du matériel de confiance.

Le premier lot du projet a permis de réduire significativement le risque de compromissions des comptes les plus sensibles. Le recours à des clés hybrides FIDO/PIV (Fast IDentity Online / Personal Identity Verification) a permis une sécurisation à 360° de l'identité sur l'ensemble des environnements, cloud comme on premise, sans remettre en cause la cohérence du système d'information.

Dans ce contexte, Thales a joué un rôle déterminant en fournissant des clés FIDO/PIV compatibles avec les fournisseurs d'identité du Grand Reims, ainsi que des outils de gestion permettant aux équipes du Grand Reims de maîtriser le cycle de vie des clés. Ce déploiement illustre qu'une approche passwordless pragmatique et cadrée est bien acceptée par les utilisateurs.

GRAND REIMS
COMMUNAUTÉ URBAINE

Industrie
Collectivité locale / service public

Habitants
300,000

Agents
4,000

Contexte du projet

La ville de Reims et la Communauté Urbaine du Grand Reims sont deux collectivités territoriales qui regroupent près de 4 000 agents. Comme de nombreuses organisations publiques, elle a vu son système d'information évoluer vers un modèle hybride combinant infrastructures on premise, services cloud, applications SaaS, et suite bureautique collaborative.

Cette transformation a profondément modifié le modèle de menace. Les applications et services ne sont plus protégés par un périmètre réseau unique, et l'identité est devenue le principal vecteur d'attaque. Dans ce contexte, le projet d'authentification sans mot de passe s'inscrit dans une démarche globale de renforcement de la sécurité de l'ensemble des composantes du SI, avec un objectif clair: sécuriser les accès aux plateformes exposées sur Internet tout en simplifiant l'expérience des utilisateurs.

Problèmes rencontrés par Grand Reims

Avant le lancement du projet, les administrateurs de la collectivité utilisaient des mécanismes de double authentification classiques, tels que les codes OTP par SMS ou application mobile. Ces méthodes se révèlent aujourd'hui insuffisantes face aux attaques modernes. Grand Reims est en effet régulièrement exposé à des attaques par des kits de phishing AITM (Adversary In The Middle), mettant en œuvre des techniques de contournement de l'authentification multifacteurs. D'autres attaques peuvent conduire au téléchargement de logiciel voleur de mots de passe (infostealer). Dans les deux cas, une prise de contrôle quasi immédiate par l'attaquant du compte compromis est très souvent constatée.

Par ailleurs, l'augmentation continue de la complexité des mots de passe et leur renouvellement à chaque suspicion de compromission de compte impose une contrainte forte aux utilisateurs, sans pour autant offrir un niveau de sécurité satisfaisant.

Stratégie globale et solution sans mot de passe adoptée

La stratégie retenue par Grand Reims a consisté à cibler en priorité les populations les plus à risque, à savoir les administrateurs, pour lesquels l'usage de clés matérielles est progressivement rendu obligatoire sur l'ensemble des environnements.

La solution passwordless repose sur un fournisseur d'identité OpenID Connect comme plateforme d'authentification centrale, capable de gérer les clés FIDO et les politiques d'authentification sans mot de passe. Grand Reims a choisi de déployer auprès des populations les plus à risque les clés SafeNet eToken Fusion NFC PIV de Thales, certifiées FIDO 2.1, afin de bénéficier à la fois des fonctionnalités FIDO pour les environnements cloud, et des certificats PIV pour les environnements plus traditionnels.

Cette approche hybride permet de protéger les accès en administration à la suite bureautique co laborative et aux applications SaaS au travers de l'authentification FIDO2. Elle permet également d'authentifier par certificat les accès aux environnements on-premises en s'appuyant sur le même périphérique. Les administrateurs utilisent ainsi une clé unique pour l'ensemble de leurs usages, ce qui simplifie l'exploitation tout en renforçant la sécurité.

Bénéfices obtenus

D'un point de vue sécurité, le projet a permis de placer les comptes concernés à un niveau de protection élevé, résistant aux attaques de phishing avancées.

Sur le plan de l'expérience utilisateur, l'adoption s'est faite de manière f luide, y compris auprès de populations non techniques. Les utilisateurs apprécient particulièrement l'usage d'un code PIN, jugé plus simple et plus fiable qu'un mot de passe complexe à mémoriser et à renouveler.

Recommandations

Le retour d'expérience montre que l'adoption du passwordless passe avant tout par une pédagogie adaptée. L'équipe a mis en place des supports simples et concrets remis lors de la distribution des clés, rappelant les usages principaux et les bonnes pratiques en cas d'incident. Cette approche pragmatique s'est révélée très efficace et complémentaire des sessions de information/sensibilisation à l'utilisation des nouvelles clefs.

Sur les environnements Windows on premise, le recours au standard PIV a permis de généraliser rapidement l'authentification par certificat sur les environnements Windows, sans nécessiter l'installation de driver spécifique. Le déploiement s'est appuyé sur des standards éprouvés et des guides de durcissement reconnus, permettant de sécuriser Active Directory sans complexifier inutilement l'infrastructure.

Ce que Thales a apporté au projet

Thales a apporté au Grand Reims des clés matérielles hybrides supportant FIDO et les certificats capables de couvrir l'ensemble des cas d'usage, ainsi et des outils de gestion de ces clés matures, faciles à installer et utiliser. La richesse des fonctionnalités liées aux certificats, ainsi que la compatibilité avec les politiques d'attestation de clé du fournisseur d'identité du Grand Reims, ont constitué des éléments différenciants dans le choix de la solution.

Au delà du produit, l'accompagnement de Thales et de son partenaire a permis de sécuriser les choix d'architecture et de poser des bases solides pour une généralisation du passwordless à l'échelle de la collectivité.

« Les besoins d'hybridation du système d'information se sont multipliés : applications SaaS, suite bureautiques collaboratives, exposition d'applications métier vers des partenaires ou des terminaux mobiles, … Dans ce contexte, le pare-feu n'est plus la porte d'entrée du Système d'Information, la frontière c'est l'identité. Notre objectif est de renforcer la protection de l'authentification des populations les plus à risque comme les administrateurs du S.I. puis d'élargir progressivement l'utilisation de l'authentification sans mot de passe à l'ensemble de nos agents. »

Matthieu S., RSSI, Grand Reims

« Nous avons choisi Thales pour leur expérience de longue date dans le domaine de l'authentification forte ainsi que pour la richesse de leurs outils de gestion des clés d'authentification »

Matthieu S., RSSI, Grand Reims

Conclusion

La communauté urbaine du Grand Reims a prouvé qu'une stratégie d'authentification sans mot de passe fondée sur FIDO peut être déployée efficacement dans une organisation publique, à condition d'être bien planifiée et accompagnée. La priorisation des comptes à risques, le choix de clés FIDO/PIV adaptées aux différents environnements et une pédagogie claire ont permis une adoption rapide et sécurisée. L'utilisation d'une clé matérielle s'est révélée simple et fiable pour les utilisateurs, renforçant l'acceptation. Enfin, le contrôle de la chaîne de confiance, notamment lors de l'enrôlement, est essentiel pour garantir la sécurité. Grâce à l'expertise de Thales et à des standards reconnus, Grand Reims a posé les bases d'une généralisation du passwordless, accessible à tous types d'organisations.

A propos de Thales

Thales est un leader mondial de la cybersécurité, aidant les organisations les plus fiables à protéger leurs applications, données, identités et logiciels critiques, partout et à grande échelle. Grâce aux plateformes intégrées de Thales, nos clients bénéficient d'une meilleure visibilité des risques, se protègent contre les cybermenaces, comblent les failles de conformité et offrent chaque jour des expériences numériques fiables à des milliards de consommateurs.