Case Study

THALES

CYBERSECURITY

Transition to Passwordless Authentication: The Experience of Grand Reims Urban Community

Grand Reims Urban Community strengthens its protection against digital identity theft using Thales security keys.

cpl.thalesgroup.com

THALES

CYBERSECURITY

Executive Summary

In response to the growing prevalence of phishing attacks and the increasing use of cloud and SaaS services, the Grand Reims Urban Community initiated a fundamental transformation of its authentication model. By deploying Thales hardware security keys to their most exposed agents, enabling both FIDO2 authentication for Cloud and SaaS environments and certificate authentication for on-premises environments, the organization opted for a passwordless authentication mechanism that is resistant to phishing and based on trusted hardware.

The first phase of the project significantly reduced the risk of compromise for the most sensitive accounts. The use of hybrid Fast IDentity Online (FIDO) and Personal Identity Verification (PIV) keys enabled comprehensive identity protection across all environments, both cloud and on-premises, without undermining the overall consistency of the information system.

In this context, Thales played a decisive role by providing FIDO and PIV keys compatible with Grand Reims's identity providers, as well as management tools that allowed the Grand Reims teams to control the entire lifecycle of the keys. This deployment demonstrates that a pragmatic and well-structured passwordless approach is well accepted by the users.

GRAND REIMS
COMMUNAUTÉ URBAINE

Industry
Local Authority / French Public Sector

Population
300,0000

Employees
4,000

Project Context

The City of Reims and the Grand Reims Urban Community are two local authorities bringing together nearly 4,000 employees. Like many public sector organizations, their information system has evolved toward a hybrid model combining on-premises infrastructure, cloud services, SaaS applications, and collaborative office suites.

This transformation has profoundly changed the threat model. Applications and services are no longer protected by a single network perimeter, and identity has become the primary attack vector. In this context, the passwordless authentication project is part of a broader initiative to strengthen the security of all components of the information system, with a clear objective: securing access to internet-exposed platforms while simplifying the user experience.

Challenges Faced by Grand Reims

Before launching the project, the authority's administrators relied on traditional multi-factor authentication (MFA) mechanisms, such as one-time password (OTP) codes sent by SMS or generated by mobile applications. These methods are now insufficient against modern attacks.

Grand Reims is regularly exposed to phishing attacks using AITM (Adversary-in-the-Middle) kits designed to bypass multi-factor authentication. Other attacks involve the installation of password-stealing malware (infostealers). In both cases, attackers are often able to take control of compromised accounts almost immediately.

Additionally, the increasing complexity of passwords and their frequent renewal following suspected compromises place a heavy burden on users, without providing a satisfactory level of security.

In addition, the increasing complexity of passwords and their frequent renewal following suspected compromises place a heavy burden on users, without providing a satisfactory level of security.

Overall Strategy and Passwordless Solution Adopted

The strategy adopted by Grand Reims was to prioritize the most at-risk populations, namely administrators, for whom the use of hardware security keys is progressively being made mandatory across all environments.

The passwordless solution is based on an OpenID Connect identity provider acting as a central authentication platform, capable of managing FIDO keys and passwordless authentication policies. Grand Reims chose to deploy Thales SafeNet eToken Fusion NFC PIV keys, certified FIDO 2.1, to benefit both from FIDO functionality for cloud environments and from PIV certificates for more traditional environments.

This hybrid approach protects administrative access to collaborative office suites and SaaS applications via FIDO2 authentication, while also enabling certificate-based authentication for on-premises environments using the same device. Administrators therefore use a single key for all their use cases, simplifying operations while strengthening security.

Benefits Achieved

From a security perspective, the project placed the targeted accounts at a very high level of protection, resistant to advanced phishing attacks.

From a user experience standpoint, adoption was smooth, including among non-technical users. Users particularly appreciate the use of a PIN code, perceived as simpler and more reliable than complex passwords that must be memorized and frequently changed.

Recommendations

Feedback shows that successful passwordless adoption relies above all on appropriate user education. Grand Reims implemented simple, practical materials distributed when the keys were issued, reminding users of primary use cases and best practices in case of incidents. This pragmatic approach proved highly effective and complemented awareness and training sessions on the use of the new keys.

In on-premises Windows environments, the use of the PIV standard made it possible to rapidly generalize certificate-based authentication without requiring the installation of specific drivers. The deployment relied on proven standards and well-recognized hardening guides, securing Active Directory without unnecessary complexity.

What Thales Brought to the Project

Thales provided Grand Reims with hybrid hardware keys supporting both FIDO and certificate-based authentication, capable of covering all use cases, as well as mature, easy-to-deploy and easy-to-use key management tools. The richness of certificate-related features, along with compatibility with the identity provider's key attestation policies, were key differentiators in the solution selection.

Beyond the products themselves, the support provided by Thales and its partner helped secure architectural decisions and establish solid foundations for scaling passwordless authentication across the entire organization.

> " The need for hybrid information systems have multiplied: SaaS applications, collaborative office suites, exposure of business applications to partners or mobile devices, etc. In this context, the firewall is no longer the entry point to the information system — the boundary is identity. Our objective is to strengthen authentication protection for the most at-risk populations, such as IT administrators, and then gradually extend passwordless authentication to all our employees."
>
> **Matthieu S., CISO, Grand Reims**

> " We chose Thales for their long-standing experience in strong authentication as well as for the richness of their authentication key management tools."
>
> **Matthieu S., CISO, Grand Reims**

Conclusion

Grand Reims has demonstrated that a FIDO-based passwordless authentication strategy can be successfully deployed in a public sector organization, provided it is well planned and properly supported. Prioritizing high-risk accounts, selecting FIDO and PIV keys suited to different environments, and delivering clear user education enabled rapid and secure adoption.

The use of a hardware security key proved to be simple and reliable for users, reinforcing acceptance. Finally, controlling the chain of trust, particularly during enrollment, is essential to guaranteeing security. Thanks to Thales' expertise and the use of recognized standards, Grand Reims has laid the groundwork for a scalable passwordless approach accessible to all types of organizations.

About

As a global leader in cybersecurity, Thales safeguards sensitive data, identities, applications, and software for the most trusted brands in the world. Through advanced encryption, identity access management, application security, and software entitlement, Thales secures cloud environments, defends against cyber threats, ensures compliance, and enables trusted digital experiences.

Contact us – For contact information, please visit cpl.thalesgroup.com/contact-us