CASE STUDY

Industry

- Local government

Protocols

- FIDO
- OTP

At a glance

- Headquartered in Créteil (Val-de-Marne)
- Public administrative entity, owned and operated by the French state
- Created in 1968

Key results

- 5,000+ YubiKey users
- 5 external audits with 0 breaches
- Secure VPN access

Yubico solutions deployed

- YubiKey 5 NFC
- YubiKey 5C NFC

Val-de-Marne secures 5,000 remote workers with phishing-resistant YubiKeys

Departmental council improves cyber resilience without compromising usability

> “What’s great about the YubiKey is that you don’t have to think about codes. You just plug it in, tap it, and you’re done. With OTP tokens, I constantly have to pull out my phone, enter a 6-digit code and race against the 30-second timer. Compared to that, the YubiKey just works. It does the job better than any of those other solutions.”

Mikaël Auzanneau | Networks and Security Engineer | Val-de-Marne Departmental Council

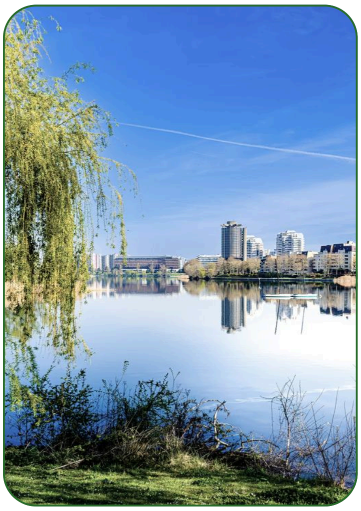
Val-de-Marne is a department in the Île-de-France region, located to the east of Paris, with a population of more than 1.4 million. The departmental council (CD94) plays a key role in local governance, managing public services such as education, social welfare and cultural development. The departmental council focuses on urban planning, sustainability and supporting local businesses. It also fosters community engagement through various initiatives and resources for residents.

Securing the shift to hybrid and remote work

Public sector organizations like CD94 are prime targets for cyberattacks. A successful breach has the potential to compromise sensitive citizen data or disrupt the critical infrastructure that underpins essential public services. This underscores the critical need for a cyber resilient posture to protect against espionage, disruption and politically motivated attacks.

Mikaël Auzanneau, Networks and Security Engineer at CD94, oversees the implementation of strong authentication via the company’s VPN, enabling secure remote work for all employees. He introduced the system currently in use and has been leading authentication and endpoint security projects since 2007.

Phishing is a significant threat, largely due to low user awareness. To address this, the IT team developed an internal open-source tool that simulates phishing attacks to assess how employees respond. If a user clicks a phishing link and enters their login credentials, they are redirected to an informational page and required to complete a brief 10-minute training. This session covers how to identify suspicious emails, avoid unsafe links and recognize common red flags. “While these educational efforts are in place, weak passwords, such as ‘valdemarne’, are still frequently used, underscoring the need for continued user education and stronger security habits”, says Auzanneau.



Prior to the pandemic, CD94 had already had a VPN for some time, but it was dedicated to a few employees and elected representatives. This solution was very practical, because it enabled easy access to the information system for up to 50 people across the whole department—at a time when there was no remote work at all. Anyone else who might have required access, whether during an on-call shift or in another context, had to authenticate using certificates. For VPN access, a very specific list of people were able to access with a combination of login and password, which led to worries about its vulnerability to cyber threats.

A growing remote workforce requiring elevated security

The challenge became more urgent for CD94 when, during the pandemic, the entire department had to shift to remote work. The department's employees didn't have professional laptops, and had to be equipped with these so that no personal laptops were used for professional purposes. Moreover, this rapid expansion of remote work exposed security vulnerabilities, especially regarding weak passwords. The department faced the difficulty of balancing security with ease of access as it transitioned from a restricted setup to a more open and critical network access model for the entire workforce.

CD94 explored the possibility of utilizing smartphones as part of the authentication process; however, several challenges quickly emerged. First, not everyone was equipped with smartphones, necessitating the provision of at least a basic device to every individual. While low-cost, entry-level smartphones were available, the acquisition of such devices at scale would have represented a substantial investment.

Another consideration was mobile device management (MDM). While an MDM solution was in place, it was solely used to manage tablets, not smartphones—this decision had been made at a strategic level to ensure that work-issued phones remained free of additional configurations. As a result, preinstalling or even manually installing authentication applications would have proven to be a complex and challenging task. Managing user accounts for these applications would have introduced further administrative burdens, as Android devices require Google accounts, while iPhones necessitate Apple accounts.

YubiKeys provide a cost-effective solution to secure remote access

Ultimately, the most cost-effective and user-friendly solution proved to be the YubiKey, a hardware security key that counters phishing attacks by requiring physical touch for authentication. The YubiKey provided a way to bolster security without the need to equip every remote worker with new hardware or contend with the logistical complexities associated with mobile authentication applications.

A broader initiative to deploy laptops among employees of CD94 offered the opportunity to smoothly implement YubiKey authentication. Employees picking up their new laptops were provided with a YubiKey at the same time, and the enrollment process was simplified via integration with their RADIUS server. Users would log into a web portal, insert their YubiKey and the system would automatically associate the key's serial number with their Active Directory profile. This shift ensured that security was embedded into the authentication process while maintaining accessibility. Office-based employees were equipped accordingly, while field workers without remote responsibilities continued to operate under a shared-access model. By integrating the YubiKey as a standard authentication tool, the department strengthened security without compromising usability, allowing for a more scalable and resilient remote work strategy. "Currently, we don't limit remote work to any specific group; s long as someone has a laptop and a YubiKey, they're considered able to work remotely", says Mikaël Auzanneau.

> “The YubiKey is the safest and easiest to use of all security keys available in the market. You just have to plug, press and the authentication is successfully done. It doesn’t require a battery, which is a great advantage. It's the safest and easiest to implement, because it requires little investment, and it's the most secure.”
>
> **Mikaël Auzanneau** | Networks and Security Engineer | Val-de-Marne Departmental Council

“We're extremely satisfied with the way this key is currently working, because we've had very few losses overall, and everything's working as planned, with no glitches. Yubico has been able to meet our needs and expectations with a perfect solution to secure our IT systems and users whether they work on-site or remotely.”

Mikaël Auzanneau | Networks and Security Engineer | Val-de-Marne Departmental Councilil

A cyber resilient posture validated by audits and user feedback

The deployment process took a few months and was carried out in stages. It started with an initial wave of around 150, to quickly equip the IT Department—those with potentially great powers from an information system point of view—and thus restrict access to these privileged accounts. Shortly after this initial purchase, CD94 acquired 3,000 additional keys for the majority of its staff. Within six to eight months, a fully secured VPN was established, with access exclusively dependent on YubiKey authentication. CD94's VPN solution has been audited by five different external organizations and none have been able to breach the YubiKey-secured system, confirming the reliability and robustness of their cybersecurity posture.

Feedback from users has been overwhelmingly positive. While broad internal communication regarding the YubiKey was not deemed necessary, employees have been encouraged to use it for other strong authentication needs beyond VPN access. CD94 is also an AWS customer, and the use of the YubiKey has been extended to enable authentication for all employees accessing AWS consoles on the company's premises. “Personally, I also use it to authenticate my Dashlane password manager”, says Auzanneau.

“With the YubiKey, we have found the right balance between security and simplicity. It has enabled us to protect more than 5,000 employees without complicating their daily lives. It is a robust and effective solution, perfectly suited to our cybersecurity challenges. We are continuing to roll it out and will soon be providing YubiKeys to our closest partners so that the department benefits from the same level of protection when they access our information system”

Gilles Tartivel | Head of the Systems Architecture | Val-de-Marne Departmental Council

This expansion into new use cases is possible because the YubiKey is a multi-protocol security key, giving CD94 a flexible tool that can secure more services, including web applications, in the future. By deploying phishing-resistant authentication, CD94 are protecting not only their employees but also the critical public services and citizen data under their care—and building a future-ready foundation of trust and cyber resilience.

Learn more about CD94 at https://www.valdemarne.fr.

Learn more | yubi.co/customers | yubi.co/contact

yubico