versasec

Case Study: North American Automotive Dealership

An automotive dealer approached Versasec due to their need to deploy credentials in an easy and effective manner for their employees. The IT Director who oversees strategic planning concerning technology infrastructure and compliance led the project. Part of a small IT department, the IT Director reached out to Versasec to request a complimentary product demonstration.

Introduction

Federal Trade Commission Safeguard Rule
The Federal Trade Commission (FTC) Safeguard Rule established in 2003, enforced security safeguards around customers' personal information. In 2021, it was amended by the Federal Trade Commission to keep pace with current technology.

FTC Safeguards Rule ensures that financial institutions develop and maintain information security programs to protect customer information from unauthorized access and potential harm.

Automotive Dealer as a Financial Institution
Automative dealerships fall under the FTC Safeguards Rule umbrella: when the entity is engaged in financial activities or activities incidental to financial operations, such as offering financing or leasing options to customers, and if it handles or maintains customer information, making it subject to data security and privacy regulations.

Automotive dealers that engage in leasing or selling options, for example, to facilitate their customer's purchasing process, must follow FTC Safeguards Rules.

The Challenge

As part of the day to day activities of a dealership, it is normal that employees from multiple departments, numerously the sales team, often rotate between different computers or workstations on the showroom floor. As their trained workforce assisted prospective clients, finalized deals, and access crucial information, they rely on the ability to utilize any available computer. They perform workstation login with passwords, accessing the necessary tools and resources for their sales activities.

After their awareness of the strict regulations of FTC Safeguards, they launched themselves into a journey of higher security:

"We explored various options, including software-based applications. However, we found that while they met the MFA (multi-factor authentication) requirement [of FTC], they were not ideal for the user experience. Logging in with a second device, dealing with unlock codes or push notifications every time they accessed their computers, proved to be cumbersome for our team."

Personal Identifiable Information (PII)
"The FTC Safeguard Rule [also] broadened the definition of Personal Identifiable Information (PII) we previously used, which solely covered Social Security numbers and account numbers. Now, the primary objective is to protect everyone and any information that can individually identify a person. This includes seemingly basic details like phone numbers, names, and addresses."

While the United States hasn't adopted tighter regulations around PII, Europe has the General Data Protection Regulation (GDPR). U.S. government agencies continue to stress the importance of protecting PII. However, looking at recent headlines and cybersecurity reports can bring awareness and incentive for companies wondering if higher security is worth pursuing.

The Stats

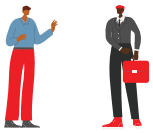
Statistics at the time of the project when the IT Director reached out to Versasec.

- **Identity theft:** The Federal Trade Commission (FTC) received over 6.2
- million reports of identity theft and fraud in 2023, representing a 14% increase from 2020.
- Financial losses: In 2023, the total reported losses due to identity theft exceeded $4.2 billion, according to the FTC's Consumer Sentinel

Network Data Book.

- **Business impact:** The average cost of a data breach was $4.45 million in 2023, according to IBM's Cost of a Data Breach Report.
- **Privacy concerns:** A Pew Research Center survey in 2023 found that 81% of Americans are concerned about how companies use their personal data.

In conclusion, safeguarding PII can be crucial for maintaining consumer trust, complying with regulations, and mitigating financial and reputational damages associated with data breaches and privacy violations.



The Multi-Factor Authentication Journey

"Under the new law, it's required to ensure that no PIN information would be stored locally on the workstation; it was obvious at this point that access to the workstation had to have MFA as well. As we examined this aspect, we needed to consider our specific use cases. For example, our workers frequently rotate and move between different computers. They simply walk up to a workstation and start working."

The company, led by the IT Director, started its search journey for multi-factor implementation for workstation logon to replace passwords and adhere to regulations.

FTC Safeguards Rule does require Multi-Factor Authentication (MFA) as part of the information security program for covered financial institutions. The goal is to enhance the protection of customer information and reduce the risk of unauthorized access.

"Ultimately, we chose Yubikeys to satisfy the MFA requirement. Despite requiring more on the infrastructure side, Yubikeys offered a superior end-user experience. The ease of rolling out features and the simplicity of using Yubikeys, along with a PIN, made it the better choice for our team."

Yubikeys were the preferred choice due to their compatibility with mobile devices and their integration with Apple. Apple's launch of support for

security keys as a part of their iOS 16.3 update allows users to register their YubiKeys to their iCloud account.

However, they faced the challenge of managing the physical credentials. Initially, they considered using other software and their existing Public Key Infrastructure (PKI) to manage the keys. After testing, they found it too difficult to keep track of the physical keys, and manage the revocation and renewal of the certificates. This challenge prompted them to search for third-party card management solutions to ensure the project was done correctly and effectively.

The Solution

"I initially considered deploying tokens with simple credential issuance software for a quick solution. However, after testing with some users, I realized it became challenging to manage the physical keys, with people losing and breaking them and the complex process of revoking and renewing certificates. That's when I began searching for a card management solution."

After researching card management solutions and trying out a few providers, the automotive dealership focused on Versasec's credential management. *"I preferred the Versasec product the most as it perfectly aligned with my requirements, geared towards what I was looking for, perfect for card management."*

During a 30-minute product demo, Versasec showcased its product capabilities, bringing the IT Director's top priority use cases to life:

- Ease of deployment of end user credentials,
- Credential tracking,
- Lifecycle management, and
- Certificate renewal.

The demo provided a clear and comprehensive understanding of how Versasec's solution could streamline its operations, leading to the decision to purchase and initiate the deployment of Yubikeys using Versasec's credential management software.

A few weeks later, he was ready to purchase and start deploying the Yubikeys with Versasec credential management software. *"We chose Versasec for our credential management because the product was simply the best, tailored exactly to our needs, and solely focused on efficient card management without unnecessary complexities."*

Deploying YubiKeys with Versasec Credential Management

For the beginning phase of the deployment, the organization deployed to department heads and relied on their feedback before extending it to all users. After a few months, the organization explored allowing power users to self-issue temporary access cards. In case of forgotten credentials, this would reduce the burden on IT.

Now, after deploying to their entire Sales Team and workforce, the automotive dealership is more secure than ever. They are not only following compliance but also reaping many benefits. Improved efficiency, being one of them, by eliminating multiple MFA solutions, some of which did not provide a high level of assurance. And finally, an improved user-employee experience. The employees no longer have to rely on their personal phones to authenticate or remember long, vulnerable, and forgotten passwords. The employees, the critical actors, understood the change, saw the importance of switching, and embraced it.

In just 45 days, the dealership not only identified a suitable solution but also had it up and running for power users. They chose to gradually implement the solution across the entire organization, a process that spanned a few months. This deliberate approach allowed them to ensure maximum security, provide thorough employee training, and minimize any potential vulnerabilities.

Versasec Credential Management

Versasec is known for innovating and developing the leading credential management for on-premise, cloud, and hybrid deployments. Versasec software is built with businesses and IT professionals in mind, helping companies of all sizes quickly deploy and manage virtual and physical smart cards, tokens, RFID, FIDO, and other PKI credentials throughout their lifecycle.

versasec

Why choose Versasec?

INTUITIVE	EASY MIGRATION
FAST	CUSTOMIZABLE
FLEXIBLE	COST EFFECTIVE
SECURE	SCALABLE

البترول الوطنية KNPC

EDAG

ebay

TEXTRON

die Mobiliar

serco

Versasec Products

Versasec Products out-of-the-box offers a no-code credential orchestration platform, integrating all systems involved in the credential lifecycle. With Versasec credential orchestration, the organization can free up resources and time, previously allocated to manual tasks or through various software. The process of orchestration guarantees results and workflows are consistent, efficient, secure, and compliant with company policies and preferences.

About Versasec

Versasec, an established global leader in Identity and Access Management, provides highly secure, powerful systems for end-to-end credential orchestration. In an increasingly connected world with growing numbers of remote workers, cyber threats, and legacy authenticators, Versasec serves as a cornerstone in every enterprise security implementation to build a zero-trust architecture. Trusted by organizations and corporations worldwide, Versasec serves the public and private sectors in government, defense, manufacturing, healthcare, financial services, and more. Versasec is headquartered in Stockholm, Sweden.