versasec

Solution Brief: Easy and Secure Access to Shared Workstations

Thanks to a revolutionary solution combining phishing-resistant PKI authentication and physical access

Across industries, organizations are adopting phishing-resistant multi-factor authentication since the sharp rise of hacking, phishing, and account takeovers. Organizations are leaving behind passwords and legacy authenticators, for more robust, secure methods. Versasec and Thales are leading the way in modern authentication. Let's take a closer look at the health and manufacturing industries where shared workstations add a layer of complexity.

Challenges

Several industries, such as healthcare and manufacturing, use **shared workstations**, where individual employee accounts are accessed with passwords. Some of these organizations enable single sign-on solutions (SSO) to allow login with employees' physical access cards. Such solutions provide good user experience thanks to SSO but still use passwords that present security concerns.

Financial Investment

The usage of a physical smart card or a USB PKI token is definitely an appropriate method to implement strong multi-factor authentication (MFA) with user convenience in shared environments. However, it could be a significant investment and an added layer of complexity for stock and operational management.

On the other hand, virtual smart cards (VSC) are excellent for protecting organizations from external threats and mitigating unauthorized access, everything PKI is known for. Additionally, they are great alternatives to standard smart cards, eliminating the need to invest and deploy hardware, and reducing reliance on USB ports and smart card readers. Organizations don't have to invest in another card for their employees with "PKI/PIV smart card" technology, but can alternatively gain the same benefits from cost-effective virtual smart cards.

Poor User Experience

In a shared workstation environment, virtual smart cards present a poor user experience. All users VSCs need to be accessible on all workstations bringing a large amount of virtual smart cards to the screen. The user is forced to scroll, experiencing a time consuming task. The process risks being circumvented by its own users. The best security solutions provide alignment to the organization's goals and a user-centered design.

Fail to Meet Requirements

RFID and NFC cards do not meet the multi-factor authentication (MFA) requirements as they are not logical authenticators, but physical access authenticators. Enabled by Single Sign On products, these cards can sometimes be used to login to Windows, but more to identify the user than authenticate him. Password authentication is triggered behind scenes and is not phishing-resistant.

Unlike RFID and NFC cards, virtual smart cards are considered authenticators and therefore meet MFA requirements. Virtual Smart Cards allow Certificate-Based Authentication with MFA, which is fully phishing-resistant.

A Versasec - Thales Solution

Versasec and Thales are joining forces to provide an innovative solution combining RFID technology with PKI Virtual smart cards. With this new solution, frontline workers can access buildings and shared workstations quickly and securely, using their existing RFID badge.

The solution allows companies to implement a user-friendly experience, add SSO but with phishing-resistant MFA based on PKI. It replaces weak password authentication, and it does not require the deployment of additional hardware.

Virtual Smart Cards

Hardware-based PKI enables phishing-resistant MFA authentication for employees. It can be delivered in the form of a physical smart card, a USB PKI token, and a virtual smart card. Virtual Smart Cards provide the same level of functionality as a standard physical card by emulating the smart card. The keys can be stored either on the client workstation using the Trusted Platform Module (TPM) or on a server using a Hardware Security Module (HSM).

Fast and Convenient User Experience with Phishing-Resistant Authentication

The user, who is issued a physical access device to move between floors or access controlled locations, can now authenticate into a workstation with the same device, enjoying phishing-resistant MFA. No password to remember, no scrolling required to select the right certificate, and no risk to be phished.

The Versasec - Thales solution gives companies the option to implement secure modern SSO as well. This SSO solution is based on phishing-resistant MFA with PKI. The workstation will prompt users for their PIN the first time each day, but automatically sign them on to all other applications.

Traditional SSO usually refers to the Password Single Sign On feature, where the password only has to be remembered once and the user is automatically signed on to all other applications. Behind the scenes, target applications and systems still store passwords which can be stolen.

Compliant with Highest-Security Regulations

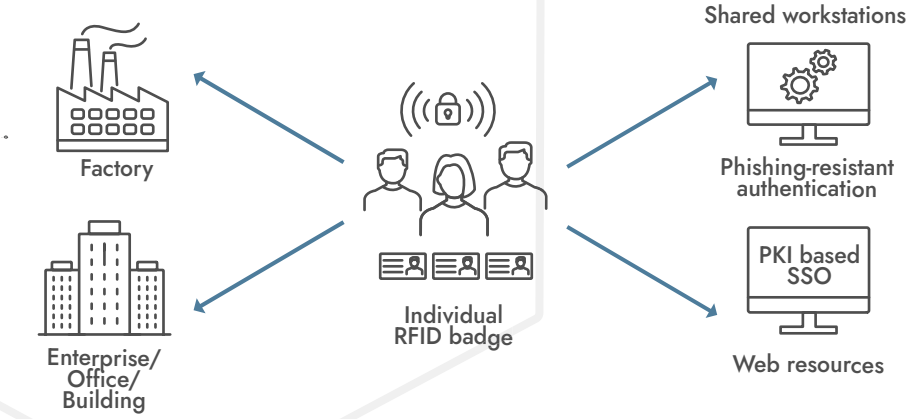
This innovative solution complies with the highest security regulations thanks to phishing-resistant authentication based on cryptography (PKI) and HSM-based protected keys.

Cryptographic Operations

Frontline workers can benefit from cryptographic operations, such as encryption and digital signatures, without any additional investment by using virtual smart cards with the same badge. The operations ensure:

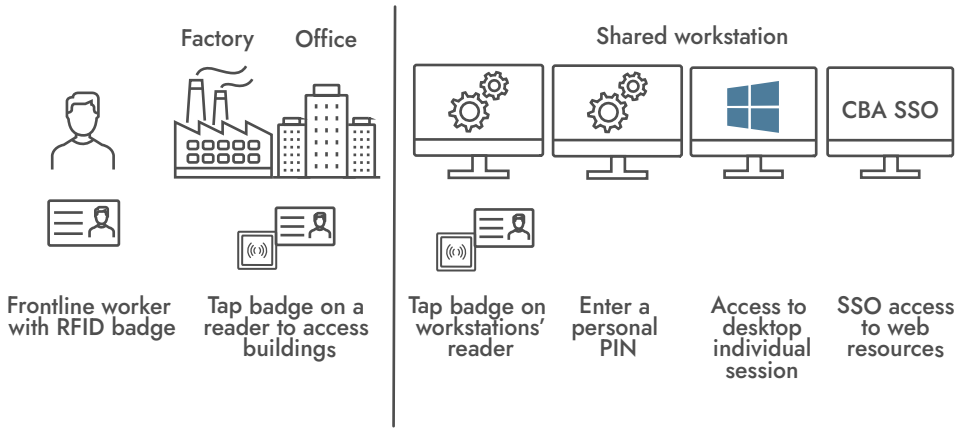
- Confidentiality, where the communication between parties includes the protection of sensitive information from being intercepted and read by unauthorized individuals.
- Integrity, where the data transmitted can be ensured not to be altered during transmission, and
- Non-repudiation, the sender of a message cannot later deny having sent it.

One single badge to access quickly and securely to buildings and shared workstations

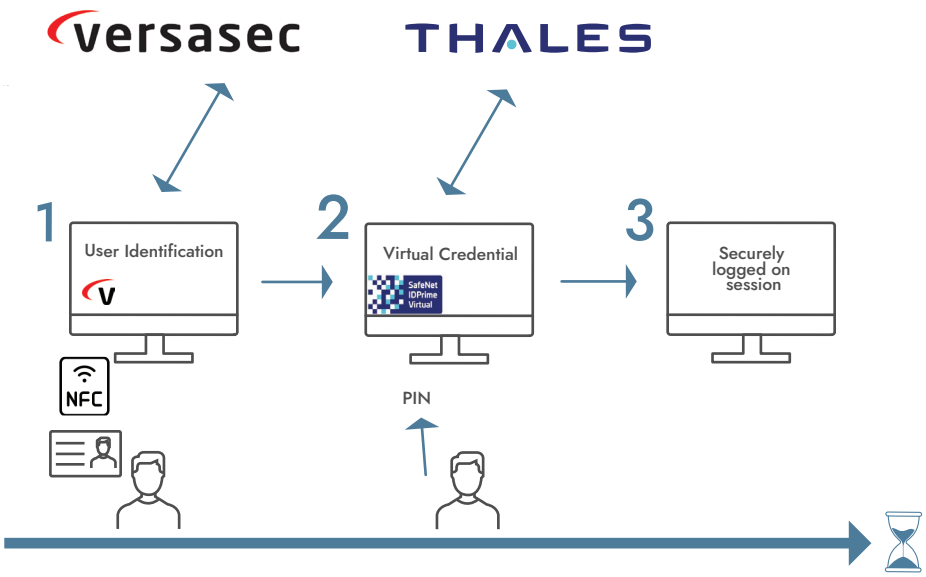


Comprehensive User Experience

The frontline workers present the RFID badge at the workstation on an NFC reader, Versasec vSEC:CMS credential provider makes the link between the RFID badge and the active directory account of the badge owner. vSEC:CMS contacts Thales IDPrime Virtual (IDPV) Server to request the activation of a server-based virtual smart card; then the user can simply authenticate using his virtual smart card PIN.



Architecture Diagram of Solution



Walk through of architecture diagram:

1. The employee's RFID badge is read by the NFC reader on the client-workstation. The Versasec service uses information from the RFID badge to identify the user and instructs Thales SafeNet IDPrime Virtual to load the user's virtual smart card.
2. The Thales SafeNet IDPrime Virtual credential will be made available as a virtual smartcard on the logon screen.
3. The virtual smart card certificate(s) are presented and the user is able to authenticate by entering their virtual smartcard PIN.

Definitions of acronyms

PKI — Public Key Infrastructure

Foundational infrastructure component used to securely exchange information using digital certificates. PKI is the collection of policies, processes, and technologies that allow signing and encrypting data.

SSO — Single Sign On

Provides the capability to authenticate once and be subsequently and automatically authenticated when accessing various resources.

IDPV — IDPrime Virtual

SafeNet IDPrime Vitual enables organizations to secure their cloud transformation by building on their current PKI authentication framework for cloud access, allowing users to carry PKI operations from any device and reducing Hardware-based PKI operational costs.
To know more about IDPV visit https://cpl.thalesgroup.com/access-management/authenticators/pki-smart-cards/safenet-idprime-virtual

vSEC:CMS — Versasec Credential Management System

vSEC:CMS streamlines all aspects of managing credentials by connecting to enterprise directories, certificate authorities, physical access control systems, email servers, log servers, biometric fingerprint readers, PIN mailers, and more. With vSEC:CMS, enterprises can issue Credentials to employees, personalize the Credentials for authentication and manage the credential lifecycle – all features available directly from the shelf. Available for on-prem and in the cloud.

HSM — Hardware Security Module

A dedicated crypto processor that is specifically designed for the protection of the crypto key lifecycle. Hardware security modules act as trust anchors that protect the cryptographic infrastructure of some of the most security-conscious organizations in the world by securely managing, processing, and storing cryptographic keys inside a hardened, tamper-resistant device. Thales Hardware Security Modules provide the highest level of security by always storing cryptographic keys in hardware.

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.

Thales Identity & Access Management solutions for B2E

Thales's industry-leading Access Management and Authentication solutions let enterprises centrally manage and secure access to enterprise IT, web and cloud-based applications. Utilizing policy based SSO and modern authentication methods, enterprises can effectively prevent breaches, migrate to the cloud securely and simplify regulatory compliance.
To learn more, visit: cpl.thalesgroup.com/access-management

About Thales

The people you rely on to protect your privacy rely on Thales to protect their data. When it comes to data security, organizations are faced with an increasing number of decisive moments. Whether the moment is building an encryption strategy, moving to the cloud, or meeting compliance mandates, you can rely on Thales to secure your digital transformation. Decisive technology for decisive moments.