Secure Authentication for Upgraded Security

GDPR demands better data security and privacy. Enter two-factor authentication. Using virtual smart cards, Versasec makes it easy to roll out two-factor authentication throughout your organization.

Virtual Smartcards (VSC) are excellent for protecting companies' IT systems from external threats such as hacking and other unauthorized access from external devices. A Virtual Smart Card enables two-factor authentication (2FA) on a user's device without making use of extra hardware, such as smart cards, smart card readers and USB tokens.

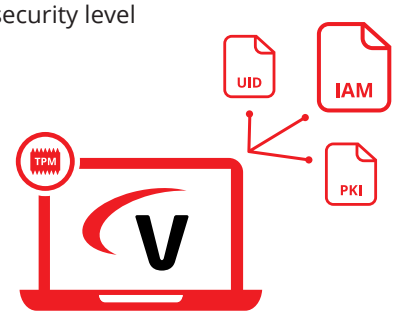
Two-Factor Authentication

Two-factor authentication (2FA) augments "something you know," (typically a user's password), with "something you have," which often is a physical device in the user's possession, such as a smart card. With Windows 8, Microsoft introduced the concept of Virtual Smart Cards (VSCs) that emulate smart cards in a virtual sense by making use of the Trusted Platform Module (TPM) on the computer's motherboard. The same cryptographic operations that take place in a physical smart card also take place in the TPM. As with a smart card, cryptographic keys can be securely stored in the TPM. Using vSEC:CMS from Versasec, it is possible to create and manage the lifecycle of a virtual smart card leveraging the Microsoft implementation.

Versasec makes strong authentication easy. We help organizations securely authenticate, issue and manage their multi-factor digital identity tools more easily and cost effectively no matter the size of the organization.

vSEC:CMS Lifecycle Management

- Quick and simple installation and configuration
- User self-service to simplify deployment
- Management of TPM-enabled devices
- Low total cost of ownership
- High security level



REIST TELECOM®
CREATING NETWORKS

Case Study: *Mobiliar*

Mobiliar, founded in Bern in 1826, is the oldest private insurance company in Switzerland. The company, which operates as a cooperative, employs more than 4,900 staff in the Switzerland and Liechtenstein and offers 327 training places. One in every three Swiss households is insured through Mobiliar.

When Mobiliar made the decision to upgrade its end-user hardware, new Lenovo X1 Yoga laptops were provided to employees throughout the company. While the new computers offered better processing power, they lacked the integrated physical smart cards readers which Mobiliar had relied upon for two-factor user identity authentication. They needed a solution that would allow them the flexibility afforded by laptops without confidential client data.

Understanding the challenges of deploying laptops without smart card readers, Versasec and its partner Reist-Telecom, a specialized IT-authentication, credential management and user monitoring solutions company, recommended Mobiliar to deploy virtual smart card (VSC) solutions for all of its company sites and agencies across Switzerland and Liechtenstein. Virtual smart card technology offers comparable security benefits to physical smart cards by using two-factor authentication.

The virtual solutions emulate the functionality of physical smart cards, working with the Trusted Platform Module (TPM) chip within the laptops instead of a separate physical smart card and reader.

> "Reist-Telecom and Versasec provided the best, most cost-effective solution for our identity and access management needs. Employees spread throughout our 200+ office sites are now able to securely sign on and access critical data without physical smart cards – even if they are working in their home office or as 'mobile workers.'" **- Hans Probst, Mobiliar**

In addition, Reist-Telecom and Versasec worked together to provide a custom Remote Service Device Manager (RSDM), which is now a standard feature in vSEC:CMS 4.9 S-Series deployments. The RSDM tool enables Mobiliar to remotely and centrally manage company-deployed virtual smart cards on any employee's device, regardless of the device's location. The following graphic depicts the ease of management and usefulness of the RSDM feature. The RSDM service can be used to communicate with any device, including VSCs using the TPM.

REIST TELECOM® CREATING NETWORKS

Versasec: https://versasec.com
Reist-Telecom: https://www.reist-tele.com