SPYRUS®

103 Bonaventura Drive | San Jose, CA 95134
USA +1-408-392-9131 | FAX +1-392-0782
https://www.SPYRUS.com

SPYRUS Solutions for Insurers

Ensuring Data Protection for Privacy Compliance

Nearly 6000 insurance companies in the United States provide and manage insurance services for consumers and businesses. Increasingly, insurers have become targets of cyber criminals and identity thieves due to the wealth of data they have on clients, such as personal, financial, property and health. Insurers must know exactly where personal identifiable information (PII) and other highly confidential data about specific clients is stored, its accuracy, and how it is used and protected. Should this data be compromised, potential violations of the Health Insurance Portability and Accountability Act (HIPAA), the Gramm-Leach-Bliley Act (GLBA) and/or General Data Protection Regulation (GDPR) could lead to fines and reputational damage with long-term financial implications.

However, insurers are depending increasingly on data repositories, application hosting companies, and external agents to conduct business. Rather than dealing solely with their own employees—who can be directly trained, monitored and managed—insurers often rely on agents and systems beyond their direct supervision to access and protect data. While insurance agents help firms reach a wide breadth of markets with tailored services, they also are one of the most difficult workforces to protect from cyberattacks or cyber accidents. Insurance agents support multiple clients at once, and often handle confidential data while visiting client sites or other premises with internet access. These third-party networks may not provide adequate security, leaving data vulnerable to cyberattack. And the insurance company-specific information could be shared inadvertently or otherwise with competitors.

Insurers are looking for solutions to manage and protect data and ensure privacy compliance. Accordingly, many insurers' IT departments provide agents with a company issued device or Virtual Desktop Infrastructure (VDI) access. Providing company issued devices is extremely costly, requiring substantial financial investments in computer hardware which can be stolen and is expensive to maintain and replace. As agents frequently change, IT personal are constantly collecting, wiping and reformatting used devices and resetting security settings and access credentials—resulting in many lost labor hours. VDI terminals require an internet connection and uses the hardware on the host computer, thus limiting both flexibility and security.

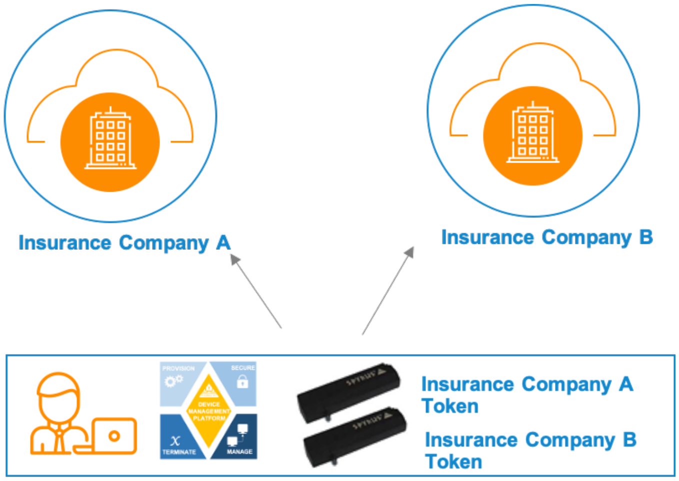
Customer Challenge

SPYRUS Solutions currently works with several U.S.-based insurance companies serving more than 3.7 million customers. Insurers are looking for solutions that meet the following requirements:

- Verified Security: Solution must protect data-at-rest, in-motion, and in-process while also being “tamper-proof” and the ability for IT departments to “destroy” the data on devices remotely.
- Cost-effective: Solution must reduce both CAPex and OPex, particularly with regards to set-up, turn-down time, and security enforcement.
- Flexibility: Works with any existing computing device online and offline.

The SPYRUS Device Management Platform

SPYRUS recommends insurers follow the NIST Cyber Framework, which consists of standards, guidelines and best practices to manage cybersecurity risk. Our security experts help insurers understand the framework and deploy a comprehensive solution called the SPYRUS Device Management Platform that meets the above requirements. This solution includes the SPYRUS Device Management Server and SPYRUS hardened and encrypted tokens.


Insurance Company A
Insurance Company B
PROVISION
SECURE
DEVICE MANAGEMENT PLATFORM
TERMINATE
MANAGE
Insurance Company A Token
Insurance Company B Token

The SPYRUS Device Management Server provides enterprise management capabilities that enable an insurer’s IT administrators to centrally register, block/unblock, revoke, set polices, and integrate third-party applications for secured access and audit. IT administrators can also “kill” the data on SPYRUS tokens remotely if they are compromised, lost or stolen–or when an agent departs. While the token contents—and access to them—are deleted, the tokens can be reformatted for continued use.

Additionally, each time the user is connected to the Server, the audit functionality is synchronized, allowing the enterprise to monitor user actions as well as control access to the use of the devices in the ecosystem. By capturing log-on and log-off activity, device disabling, and enabling and activation code recovery actions, the insurance company’s IT department can monitor users and devices from structured data that allows the determination of patterns of use and detection of suspect operational behavior, informing corrective action; with the highest level of confidence.

SPYRUS hardened tokens are the only Microsoft-certified Windows-to-Go endpoints—and offer military-grade cybersecurity to the private sector. They are able to boot (Windows or Linux O/S) on any standard computing device (Apple or PC), fully segregated from the host computer’s operating system, data and applications from other insurance companies. Proprietary data and applications are isolated. Tokens come in a variety of storage sizes, ensuring data and operating environment security in a FIPS 140-2 level 3 certified “tamper-proof” case.

Secured by an embedded SPYRUS Rosetta security module built on an EAL 5+ microprocessor with software that provides precise protection and management of all key material and algorithms necessary to achieve the highest levels of encryption and strong multi-factor authentication (MFA) managed by an easy to use, central, web-based interface for controlling and monitoring all secured endpoints. The tokens meet all Federal and Military standards necessary to ensuring the highest level of encryption security and support for in-house or third-party PKI implementations.

This approach is more cost effective than giving agents laptops. And it supports offline use, which is crucial when there is limited access to or either overloaded Internet infrastructure or VPN gateways.

The Results

By combining the SPYRUS Device Management Server and the SPYRUS encrypted and hardened tokens as a complete platform, insurers now have a secure, cost-effective solution that ensures their agents comply with data protection and privacy requirements. And insurers can delete access to data and applications if an agent departs.

The SPYRUS Device Management Platform meets the following requirements for insurers:

- Secure: FIPS 140-2 level 3 validated, SPYRUS tokens provide the highest-grade data protection and key protection for MFA in the commercial market. No data is stored on the host computer and the device can be "zeroed" remotely.
- Cost-effective: SPYRUS deployments dramatically reduce CAPex and OPex. Paired with SPYRUS' Device Management Software, IT departments can manage the devices remotely, reducing call center costs and downtime associated with changing permissions and wiping data.
- Flexibility: Preloaded with the corporate operating system and user MFA/SSO, the SPYRUS tokens can be plugged into any device. Unlike VDI solutions, SPYRUS tokens provide secure offline work that synchronizes when connectivity is available eliminating agent downtime protecting against data compromise.

About SPYRUS

SPYRUS develops and deploys cryptographic solutions in innovative ways, providing the strongest protection for data in motion, data at rest and data in process. For more than 20 years, SPYRUS has delivered encryption, authentication, and digital content security products to government, financial, and healthcare enterprises. SPYRUS solutions enable customers to meet stringent regulatory requirements for data protections across industries.