



Specsavers

CASE STUDY

Multinational optical chain Specsavers needed to act quickly to secure its remote access network, while taking into account the needs of its rapidly growing business. SafeNet Authentication Service proved to be the right solution.

The Organization

Established in 1984 with two offices in the UK, Specsavers now has more than 1,300 branches and 26,000 staff across Europe and Australasia. The company has firmly established a reputation for trust and value, and thrives on a joint-venture approach where the company and store directors work together in partnership, while managing a smaller number of wholly owned and franchised branches.

The Benefits

Having deployed the SafeNet Authentication Service to an initial group of 700 users, Specsavers has seen all its initial security solution requirements met and exceeded.



Authentication SERVICE

The Business Need: Optimizing Security

With a reputation for responding quickly to market opportunities, Specsavers is also quick to act when faced with risk and is conscious of the potential security issues that can affect a rapidly growing, multi-national business. Specsavers currently has hundreds of remote users accessing a range of central resources such as email, web applications and financial applications daily, and are aware that in order to ensure the security of its data, a data protection strategy was required.

Scalability, Flexibility & Simplicity

With its dramatic growth over the last 10 years, staff numbers continue to grow, as does the need for secure remote access. So Specsavers required a secure remote access solution that would be:

- Scalable and able to cope with the growth in staff levels across existing and new markets
- Flexible enough to suit different user working practices and technical capabilities
- Simple to administer
- Reducing the cost of implementation, deployment and ongoing resource requirements.

Solution

Specsavers chose SafeNet Authentication Service to secure remote access to their internal applications and databases.

With SafeNet Authentication Service, Specsavers is now able to deploy authentication tokens to users globally and on demand through the unique tiered user-group structure. By creating groups within the SafeNet Authentication Service management portal to represent each location, Specsavers' Head Office is able to pass management of each group to a local administrator.

Specsavers chose a mix of token formats: hard, soft and SMS, to meet various end user needs. The tokens, combined with a unique PIN code, deliver a one-time password (OTP) which can include letters, numbers and characters, offering the most secure OTPs on the market. When the user enters the correct PIN and OTP to the Specsavers remote gateway, they are securely authenticated and granted access to the server. With SafeNet Authentication Service in place, Specsavers has enabled its mobile and remote users to easily connect to the company's resources and applications securely.

Scalability and Empowerment

Specsavers' short term goal is to expand the use of two factor authentication to their office-based staff in the UK & Ireland, and ultimately internationally.

A critical element to achieving this goal is the tiered user group function, which eases the burden on Specsavers' central IT department, and empowers local offices to instantly allocate and retract tokens as required. SafeNet Authentication Service is the only vendor with this level of functionality. For Specsavers, this means they can benefit from the economy of scale of having one global service, instead of having to purchase and manage a different server in each location.

“We have been using CRYPTO-MAS for over two years now, and have yet to replace a single token or battery. There are obvious cost and resource savings for us when using reliable long-life tokens and we are already seeing those benefits.”

Angus Dorey, IT Security Manager Specsavers

Token Longevity

Specsavers have a mix of hard, soft and SMS tokens. The software tokens which are most suitable for users with access to a single desktop or laptop, the BlackBerry tokens are deployed for users who require portability, and users preferring a hardware token have been issued with keyfob tokens.

Soft and SMS tokens significantly reduce token costs, additionally the keyfob token has a 5-year warranty and no expiry date, and should a battery run out they are easy for the user to replace. Previously, Specsavers had found hardware tokens to be problematic, because they were unreliable and the token expired within three years.

Lower TCO

Specsavers have confidence in SafeNet Authentication Service simple annual subscription fee which includes the service's software components and applications. With this opex model, they have been able to eliminate the hassle and cost of up-front investment in software and hardware, and by taking the complexity and cost out of implementation and ongoing support, SafeNet Authentication Service has enabled Specsavers' IT staff to focus on more profitable activities. As Angus Dorey, IT Security Manager of Specsavers confirms, “We have been using SafeNet Authentication Service for over two years now, and have yet to replace a single token or battery. There are obvious cost and resource savings for us when using reliable long-life tokens and we are already seeing those benefits.”

The Future

Eventually, sensitive patient data will be accessible remotely by Specsavers staff in line with changing healthcare requirements and regulations, and Specsavers is confident in the knowledge that SafeNet Authentication Service two-factor authentication will meet the PCI compliance requirements for providing remote access to such data.

“SafeNet Authentication Service has brought several benefits to Specsavers, the tiered user-groups have allowed us to implement and manage two-factor authentication globally, and delegate administration. The tokens work out cheaper and the technology offers us the highest level of security on the market. Feedback from our offices and end users has been really positive.”

Angus Dorey, IT Security Manager Specsavers

About SafeNet Authentication Service

SafeNet Authentication Service delivers fully-automated, highly secure authentication-as-a service with flexible token options that are tailored to the unique needs of your organization and substantially reduces the total cost of operation.

Strong authentication is made easy through the flexibility and scalability of SafeNet Authentication Service's automated workflows, and vendor-agnostic token integrations and broad APIs. In addition, management capabilities and processes are fully automated and customizable—providing a seamless, and enhanced, user experience.

With no infrastructure required, SafeNet Authentication Service enables a quick migration to a multi-tier and multi-tenant cloud environment, and protects everything, from cloud-based and on-premise applications, to networks, to users and devices.



THE
DATA
PROTECTION
COMPANY

Contact Us: For all office locations and contact information, please visit www.safenet-inc.com

Follow Us: www.safenet-inc.com/connected

©2012 SafeNet, Inc. All rights reserved. SafeNet and SafeNet logo are registered trademarks of SafeNet. All other product names are trademarks of their respective owners. CS (EN) A4-10.12.12