Secure Remote Access with MobilePASS

CASE STUDY

Background

A leading sports and entertainment organization has over 50 business entities and features the broadest portfolio of multimedia sports assets.

Customer Need

A leading sports and entertainment organization has a nimble and skilled professional IT team, whose primary focus is managing the information systems and networking infrastructure of the company's core business—sports broadcasting and media. Due to the extremely high value of the group's intellectual property, and the damage that could result from a data breach or unauthorized access to proprietary content, the company had implemented two-factor authentication for employees who access its systems remotely. Over time, this system proved to be inadequate from both a security and usability perspective, leading the organization to search for an alternative solution that would meet its needs.

These needs included:

- **Reduce the IT Resources Dedicated to Managing Its Authentication Systems** - The IT team wanted to focus on its core responsibilities of maintaining the company's media-related infrastructure and did not want to have to dedicate IT resources to the authentication system. Therefore, one of the key factors for selecting an authentication platform was the ease with which such a platform could be implemented and maintained.
- **Reduce Helpdesk Calls and Support Costs** - Since the IT team did not want to assign dedicated IT resources to maintain the new authentication platform, an important requirement was the ability to offer Web-based self-service portals that allow employees to manage most token-related administration by themselves, with as little IT intervention as possible.
- **Straightforward Migration from the Existing Authentication System** - The company's existing authentication platform was not providing an adequate level of security. It was imperative, therefore, to get the new system up and running in as little time as possible and reduce security vulnerabilities in the interim. In addition, the new system had to be able to support the mass migration of all employees and business partners smoothly.
- **Convenience for Employees** - Employees were using hardware tokens with their existing system. In order to offer users the most convenient solution, the company wanted to implement the use of software tokens that could be installed on users' mobile phones. At the same time, the company wanted to enable those employees who preferred a hardware token to continue using it alongside their software token.

Solution: SafeNet Authentication Manager with MobilePASS

The sports and entertainment organization chose SafeNet Authentication Manager (SAM), SafeNet's versatile authentication server, with two types of authenticators—: MobilePASS software authenticators and eToken PASS hardware tokens. SAM, together with MobilePASS and eToken PASS, proved to be a winning solution, allowing them to set up a proof-of-concept (POC) and go ahead to proceed with full deployment within two weeks. Moreover, SAM's unique brokering tool allowed the company to smoothly transition all its employees to SafeNet tokens, resulting in a rapid yet problem-free phase-out of their existing RSA authentication solution.

By replacing its existing authentication system with a SafeNet authentication solution, the comapny gained significant IT and security benefits. Thanks to SAM's easy implementation, maintenance, and Web-based self-service portals, it was able to sharply reduce the IT resources dedicated to managing its authentication environment. Employees also benefitted by being able to choose the authentication form factor that best suits their work routine. From a security standpoint, a speedy POC and rapid implementation on the part of SafeNet, allowed the company to quickly overcome the vulnerabilities it had experienced with their previous system.

Solution Benefits:

Streamlined Management and Lower TCO

- Central mangement and administration of numerous form factors and authentication methods allowed the company to deploy different types of tokens and optimize convenience for its employees without increasing IT overhead.
- Web-based self-service portals enabled the company to significantly streamline its authentication operations and lower TCO by reducing the IT staff needed to maintain the system, and also resulting in a lower number of helpdesk calls.
- One-click automatic activation of MobilePASS software authenticators significantly facilitated deployment and implementation for IT staff and employees.

Convenience for End Users

- Employees are issued hardware and software tokens allowing them to choose the token that they prefer.
- Employees can manage most token administrative tasks by themselves and do not have to wait for IT staff.

Requirements vs. Deliverables

The main focus of the requirements centered on improving IT's ability to easily manage and maintain the company's authentication platform, and facilitating authentication procedures for employees. The requirements were met in full, allowing the company to completely retool its authentication processes, improve security, and allow its employees to become more self-sufficient.

Requirement	Solution
Reduce the IT Resources Dedicated to Managing Authentication Systems Reduce Helpdesk Calls and Support Costs	The IT team was able to move from POC to full implementation within two weeks, attesting to SAM's streamlined interfaces and wizard-based processes.
Effortless Migration from the Existing Authentication System	SAM's extensive Web-based self-service portals allowed the company to completely re-tool their authentication solution and provide their users independence in managing their tokens. These self-service features mean that the IT team doesn't have to devote dedicated resources to ongoing administration and can focus on its core competencies. Another direct impact is a sharp drop in helpdesk calls and support costs associated with using the self-service portals.
Convenience for Employees	The company is offering its employees two types of tokens, which are both mangaged by SAM and which can be used side by side. eToken PASS is a compact hardware token that generates an OTP at the click of a button. MobilePASS is a software OTP token that is installed on employees' mobile phones. Employees can choose the token they want to use depending on their work habits.