Echidna

Case Study

Law Enforcement

Highlights

Our client is an Australian Law Enforcement agency that was seeking a contemporary, flexible, and secure Two Factor Authentication (2FA) solution to protect the organisation's critical data and systems.

- ☑ The Client was looking for a more cost-effective solution than the incumbent RSA SecurID hardware tokens.
- ☑ The Client needed to be able to upgrade seamlessly to the new solution.
- ☑ The Client used Salt Group’s Echidna and Salt Mobile products as the security platform to enable a fast and efficient "out-of-the-box" rollout from their existing authentication system to Salt Mobile and new tokens.
- ☑ The use of Salt Mobile tokens with their support for biometric authentication (fingerprint and facial recognition) improved security and user experience.
- ☑ Following the success with Echidna and Salt Mobile tokens, the Client extended 2FA to desktop.

The Client

Our Client is one of the largest Law Enforcement agencies in Australia covering a jurisdiction that is 2.5M SQ Km’s with 10,000 staff and officers in over 150 locations.

The Law Enforcement agency had a key requirement for Two Factor Authentication (2FA) for staff and officer access to protect critical data and systems access; where staff and officers required both on-site and remote access into systems.

With a growing workforce accessing the organisation's environment remotely and changes in the cyber threat landscape, the client had responded with the use of traditional hardware based Two Factor Authentication (2FA) security tokens.

The Challenge – A seamless migration to a flexible 2FA security AND a superb customer experience

The Client had been using RSA SecurID tokens to authenticate remote users accessing systems containing sensitive information. This required staff and officers to carry the RSA SecurID tokens with them in order to login and access systems.

Typical of all hardware based security tokens, the use of a discrete personal token greatly increased the risk of staff losing or forgetting their security token. Over time, these lost/forgotten hardware tokens led to an increase in token replacements and exemptions on security policies, resulting in an ever-increasing cost for the organisation due to logistical, deployment and operational management overheads in addition to the costs of token replacements.

RSA SecurID tokens require replacement and re-licensing every three years which also resulted in a significant cost to our Client.

Moreover, RSA SecurID tokens have limited functionality in that they only generate One-Time Passwords (OTP) and were not PIN or biometrically protected.

Our Client was seeking an alternative to RSA SecurID hardware tokens that would not limit the law enforcement agency in terms of the number of users or functionality and ideally provide for a seamless migration from their existing fleet of RSA SecurID hardware to a more flexible and scalable 2FA authentication service.

The option needed to be superior to the SecurID solution in terms of deployment, security, manageability, and total cost of ownership.

The Client had a clear vision for much greater flexibility and improved staff satisfaction.

Key Objectives

☑ Increase security

☑ Find a more cost effective 2FA solution

☑ Incorporate a greater number of users at a lower cost to close security gaps

☑ Provide integrity across the full range of the Client's systems

☑ Seamless migration to the new solution

The Solution – Salt Group's Echidna with Salt Mobile Tokens & OATH Token Authentication

Salt Group pioneered the development of mobile device based authentication tokens and back-end processes and holds important patents around mobile token authentication. Our Salt Mobile products leverage the connectivity of a mobile device for both provisioning of the token and for Multi-Factor Authentication (MFA).

The advent of smart devices offered even greater capabilities that could be utilised to improve the user experience and security management, with fingerprint and face biometrics now providing integral components to Salt's technology suite. Cameras and GPS capabilities further expanded the palette which we could use to construct and deliver truly user focused authentication solutions.

Once introduced to Salt Mobile authentication and Echidna's capabilities as a security platform for multiple authentication methods, the Client quickly appreciated the benefits offered and after POC testing a number of use cases, adopted Salt Group's solution to deploy Echidna with Salt Mobile security tokens for 2FA.

Echidna's support for OATH compliant hardware tokens meant that the Client could also deploy hardware tokens alongside Salt Mobile tokens. OATH being an open standard meant that the Client was not locked in to a particular hardware token manufacturer.

The migration to the Echidna authentication service from the existing RSA SecurID was facilitated through Echidna's brokering feature which, for existing users, enabled continued use of legacy SecurID tokens until they expired at which time new Salt Mobile or OATH hardware tokens would be assigned. In this way the Client protected their investment in SecurID tokens whilst avoiding a big-bank conversion.

Benefits of Echidna & Salt Mobile tokens over RSA SecurID

☑ Salt Mobile enabled personal mobile devices to be used to authenticate staff identities for remote systems access; instead of requiring staff to carry a SecurID hardware token.

☑ Increased security as Salt Mobile tokens support both PIN and Biometrics user authentication.

☑ Salt Mobile tokens enable a broader rollout to staff and officers as the mobile token is well-priced and cost effective, with no replacement costs as they do not expire.

☑ Echidna's support of OATH hardware tokens meant that the Client could deploy a mixed fleet of mobile and hardware tokens based on user preference or operational needs.

☑ Echidna's support of the OATH standard gave the Client the ability to source tokens from a range of hardware vendors as the OATH standard is implemented widely.