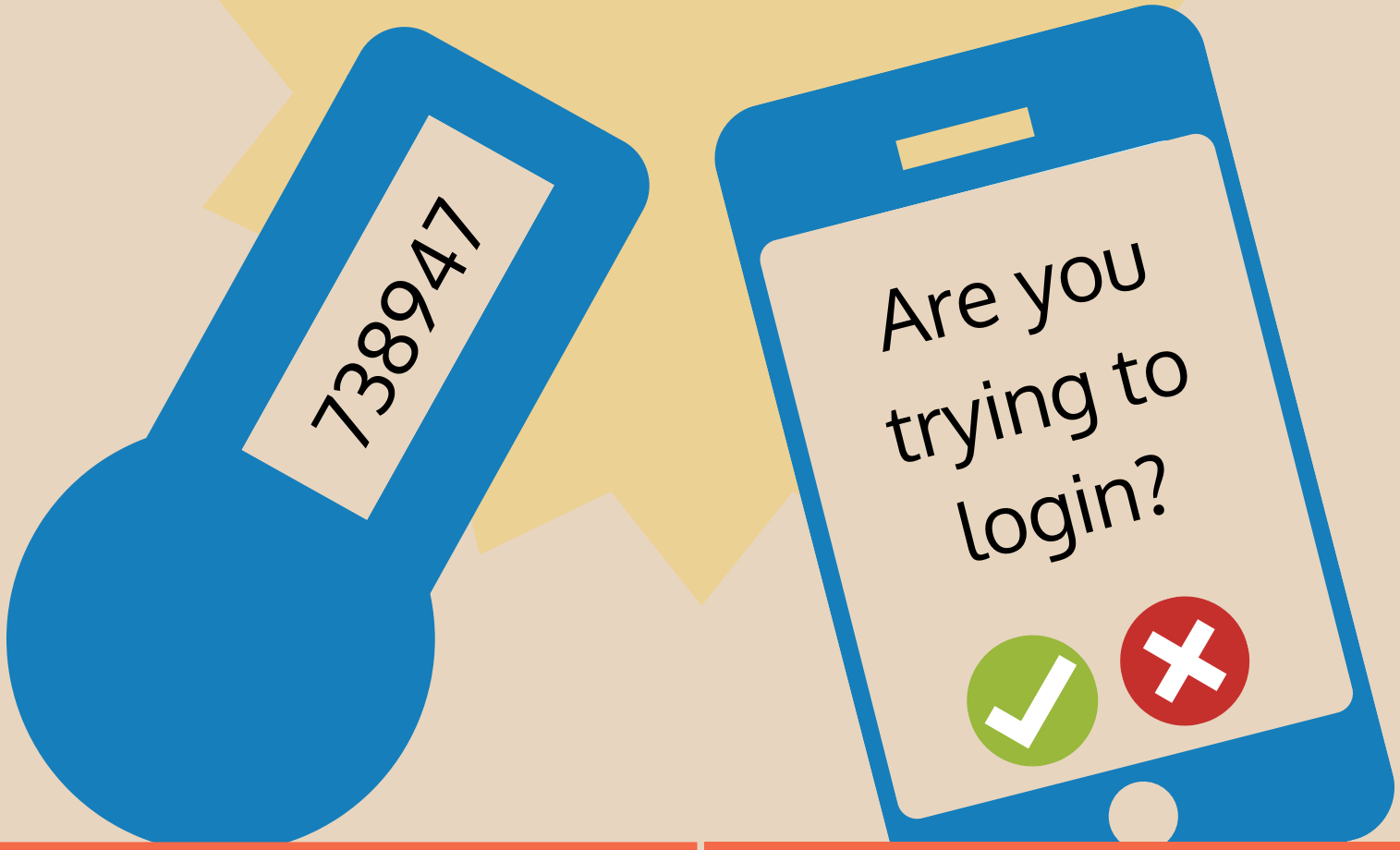
★ ★ ★ RIVALS AS OLD AS TIME ★ ★ ★

SecurEnvoy
A Shearwater Group plc Company

PRESENTS



HARDWARE TOKENS

- The Originator -

VS

SOFTWARE TOKENS

- The Innovator -

A comparative guide between hardware and software token options when using and implementing a multi-factor authentication solution

☆ ☆ ★ FORM FACTOR ★ ★ ★

Hardware tokens are small plastic units, sometimes with a button to power them on or enter a PIN. Broken tokens or tokens with empty batteries must be replaced at a cost to the owner.

Software tokens are intangible and reside on a mobile phone or laptop. Due to this very nature, they cost very little and have no cost associated with loss or damage.

☆ ☆ ★ SEED SECURITY ★ ★ ★

Hardware tokens arrive with their seed files pre-built into the unit. This means that the hardware token vendor knows your seed file and ultimately how to reverse engineer OTPs. Risk is higher with a third-party holding your seeds.

Software tokens are function-less until enrolled with an MFA solution. This means there is no need to pre-provision seed files. Instead most software token vendors create a seed file at the point of installation, unique to that organisation and never known to the vendor.

☆ ★ ★ TOKEN SECURITY ★ ★ ★

Hardware tokens can have additional security added by way of a keypad on the token. This keypad will use a PIN as part of the OTP calculation process. Incorrect entries will result in an incorrect OTP.

Software tokens can also include the requirement for entry of a PIN. In addition, software tokens can often include the requirement for a fingerprint to be produced by the owner before displaying an OTP.

☆ ★ ★ USABILITY ★ ★ ★

A tried and test method of OTP delivery, the hardware token has changed very little in 20 years. People are familiar with it and require almost no training to use it.

Software tokens come in a variety of types dependent on the preference of the owner. Innovation has been strong with the software token. Today, push-notification which verifies a user's identity by answering a simple yes or no question is making software tokens increasingly simple to use.

ENROLMENT

Hardware tokens are often enrolled by an administrator prior to being sent to the assigned user. This is time-consuming for administration teams but ensures tokens are correctly set up before use.

Software tokens are downloaded and enrolled directly by the user. This typically involves some form of enrolment portal. This method requires the least effort from the administration team but can result in support calls from users.

OFFLINE AUTHENTICATION

As hardware tokens have no direct communication back to their administrative MFA server, they require no connectivity to WiFi or cellular networks, this means they can function in an offline state.

Some software token types, such as SMS or push-notification require some form of connectivity in order to receive an OTP or request. In the event of there being no connectivity, the token will revert to an offline mode to allow authentication.

TOTAL COST OF OWNERSHIP

Implementing a hardware token solution has an initially higher cost due to purchasing the tokens. The ongoing cost is difficult to predict due to the cost of replacing faulty, broken or lost tokens and those which require a battery change.

Software token solutions have no comparative initial costs as there is no physical equipment. Total cost of ownership for the lifetime of the solution is easier to predict as the tokens are on mobile devices not associated with the cost of the solution.

FUTURE INNOVATION

There has been little innovation from the hardware token over the years outside of the YubiKey, a one button USB or NFC token which can inject an OTP into a field of focus. The YubiKey is patented and unavailable to other hardware token providers.

Software token vendors continue to innovate and produce new tokens for the changing mobile landscape. For example, software tokens on wearable technology and the use of NFC chips on mobile phones to transmit the OTP and open the relevant application.