



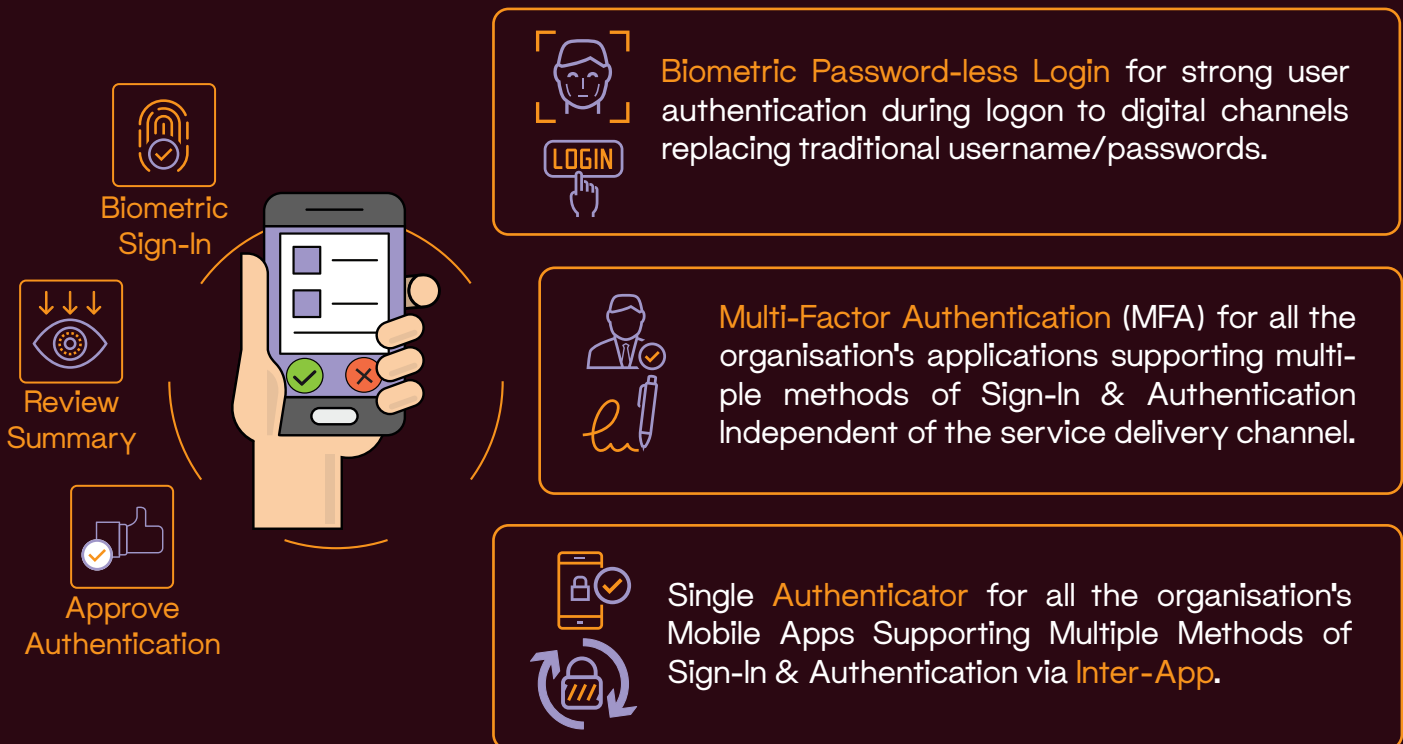
Salt mSign

Connected Token

CONTEMPORARY USER & TRANSACTION AUTHENTICATION
INDEPENDENT & DECOUPLED FROM THE SERVICE CHANNEL

Salt mSign is a contemporary mobile security MFA token for authentication of the user identity during login and authentication/verification of transactions after login. Salt mSign is 'connected' in that the authentication responses are returned directly to the Safetronic authentication platform thereby enabling authentication that is independent of the delivery channel that initiated the request.

What Can Salt mSign Do?



Typical Uses

- ✓ Password-less Biometric Login to Internet Banking, e-Government Portals and Corporate Online Services
- ✓ High Value Transaction Signing with WYSIWYS (What You See Is What You Sign)
- ✓ Improved security and mitigation of common MitM/MitB attacks
- ✓ Single Authentication for other Mobile Apps on the same device
- ✓ Quorum Approvals and Advanced Workflows with separation of duties where the Initiator of Payment Instruction is not authorised to approve; with multiple Authorisers
- ✓ Hardware Token replacement

The Challenge

Organisations are rapidly expanding their use of electronic delivery channels such as the Internet beyond static information services to provide higher value transaction services for their customers and trading partners. These facilities enable users to make purchases, effect payments or bank transfers, and generally manage their commercial or personal affairs online.

With this increase in "value" of services delivered via electronic channels comes an increase in the risk that these channels may be compromised through malicious attack, potentially resulting in financial, privacy and reputational losses for one or both parties.

At greatest risk is the integrity and authenticity of authorisation instructions for the payments received via these channels, many of which are inherently insecure and subject to a range of malware and interception attacks.

The high transaction volumes supported by modern online channels and the time criticality of processing necessitates higher assurance and more automated and scalable approaches to out-of-band authentication.

Critical requirements of a contemporary out-of band authentication are:

- The authentication request must be sent to the authoriser via an independent channel to the original instruction submission.
- The authentication request should not rely upon the authoriser being at a particular location; the party could be anywhere in an electronic marketplace.
- The authentication request must be sent and received in real-time and the mechanism must support real-time responses.
- The authentication request and the resultant response must be high assurance such that in combination with controls over the original request, there is high trust in the integrity and veracity of the instruction.
- The authentication request should be unstructured and not bound to static layouts or content requirements, thereby enabling ongoing serviceability of the mechanism even in the event of changes in the underlying instruction structures.

TECHNICAL REQUIREMENTS

- Use of contemporary cryptographic services based on NIST endorsed standards
- Cryptographic keys generated within hardware cryptographic modules (HSMs) and distributed securely to the token. Each token has a unique set of keys
- Cryptographic keys are secured within the token in a manner that protects against cloning and brute force attack of the token
- Token is protected against unauthorised use through a PIN or biometric
- Runtime App Self-Protection (RASP)

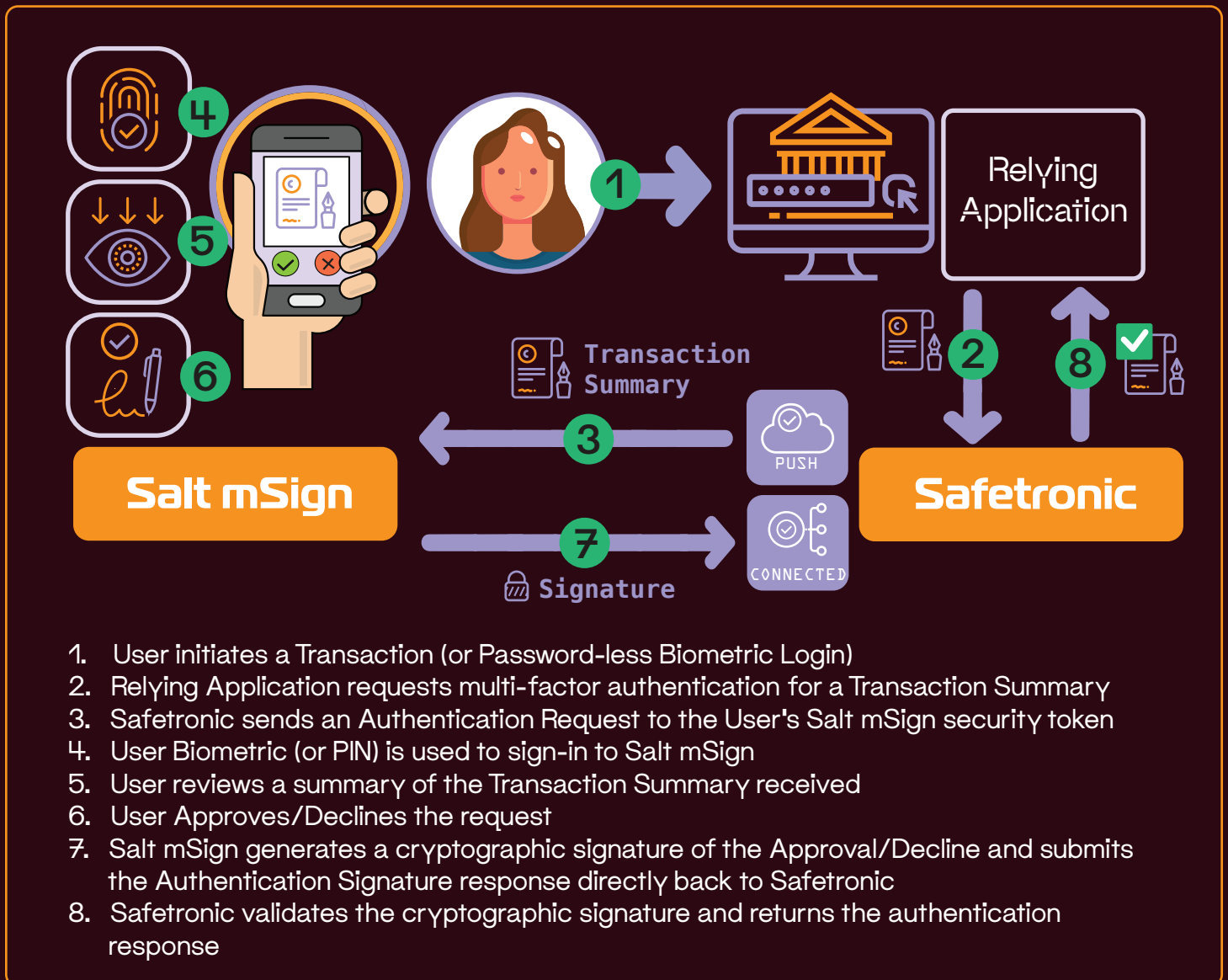
The Answer – Salt mSign

Salt mSign Connected Token is a mobile app that provides a convenient, high assurance solution that addresses all of the critical requirements of a contemporary electronic out-of-band authentication. Salt mSign Connected Token in conjunction with Safetronic Authentication platform addresses multi-factor authentication needs across the enterprise.

Salt mSign meets the requirements for Strong Customer Authentication (SCA) within the European Payment Services Directive (PSD2) authentication.

How Does Salt mSign Work?

The diagram below outlines Salt mSign multi-factor authentication for transaction signing (or Password-less Biometric Login) through an independent channel for authentication.



Benefits of Salt mSign

- ✓ Salt mSign mobile tokens operate as a single authenticator that can be used identically across all digital services to create an independent channel for authentication whereby the authentication requests and responses are direct with the user's Salt mSign token
- ✓ The use of Salt mSign's unique Inter-App capability enables mobile apps to leverage the authentication capabilities of Salt mSign with minimal changes to their mobile apps. This avoids significant app re-engineering to accommodate a security SDK, and moreover provides a consistent and frictionless authentication workflow, regardless of the channel being used. Salt mSign will seamlessly accommodate situations where Salt mSign is resident on the same device as the app or on an alternate device
- ✓ Salt mSign provides a cryptographically based authentication service that utilises internationally recognised and approved standards for signature generation that provide surety that the authentication signature was generated on the registered device; and through biometric or PIN based authorisation, that the user was in charge of the device at the time of signature generation and submission to the authentication service
- ✓ Salt mSign tokens comply with contemporary standards and specifications as prescribed by NIST. This applies to the use of particular cryptographic and related algorithms, cryptographic key usage and e-Authentication assurance guidelines in respect to multifactor authentication. Salt mSign has been reviewed independently by Trusted Labs in France

Technical Info

- ✓ Supported on Android and iOS
- ✓ On-device cryptographic signature generation using a protected unique key
- ✓ Supports multiple methods of delivering authentication requests: Push Network, Encrypted QR Codes and Inter-App
- ✓ Biometric (Face, Fingerprint) and app PIN with central policy Biometric enforce-
- ✓ Dynamic Linking, WYSIWYS (What You See Is What You Sign)
- ✓ Strong User & Transaction Authentication: Knowledge, Possession, Inherence
- ✓ Runtime App Self-Protection (RASP) Anti-cloning and Jailbreak/Root detec-
- ✓ Advanced electronic signatures uniquely linked to the signer

Salt mSign authentication method is protected by patents in the U.S. and other countries.

- U.S. Patents: 11/665,719
- Publication: US2008/0046988 A1
- Classification 726007000

Salt Cybersecurity
Office 4, 219 Kensington High Street,
London W8 6BD, UK

UK/EU & Australia/AsiaPac
T: +44-20-3966-1686 (UK/EU)
T: +61-3-9614-4416 (AU/AsiaPac)
E: sales.uk@saltgroup.com.au