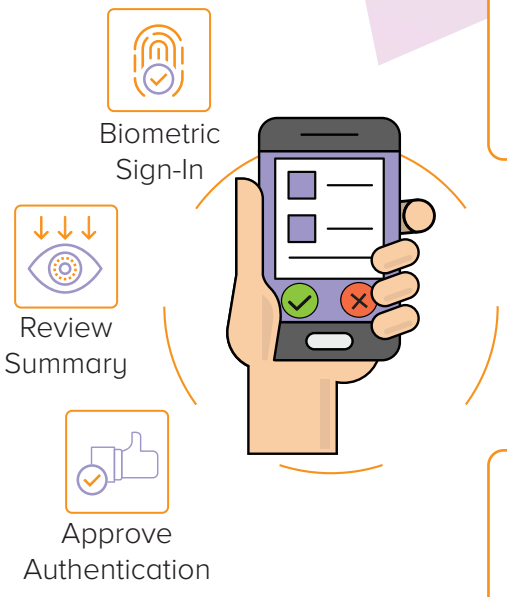
Salt mSign

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 Echidna Authentication server thereby enabling authentication that is independent of the delivery channel that initiated the request.

What Can Salt mSign Do?



Connected **Biometric** 2FA **Login** for User access via RADIUS, Microsoft ADFS, SAML Federated Login for cloud, Shibboleth and Browser-based Web Applications.

Multi-Factor **Authenticator** for all the organisation's Mobile Apps Supporting Multiple Methods of Sign-In & Authentication Independent of the service delivery channel.

Single **Authenticator** for all the organisation's Mobile Apps Supporting Multiple Methods of Sign-In & Authentication via **Inter-App**.

Typical Uses

- Mobile Soft Token used for 2FA 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)
- Biometric MFA Login for Remote Network Access: RADIUS, ADFS, Shibboleth
- Authentication for other Mobile Apps on the same device
- Quorum Approvals and Advanced Work-flows 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 market-place.
- 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

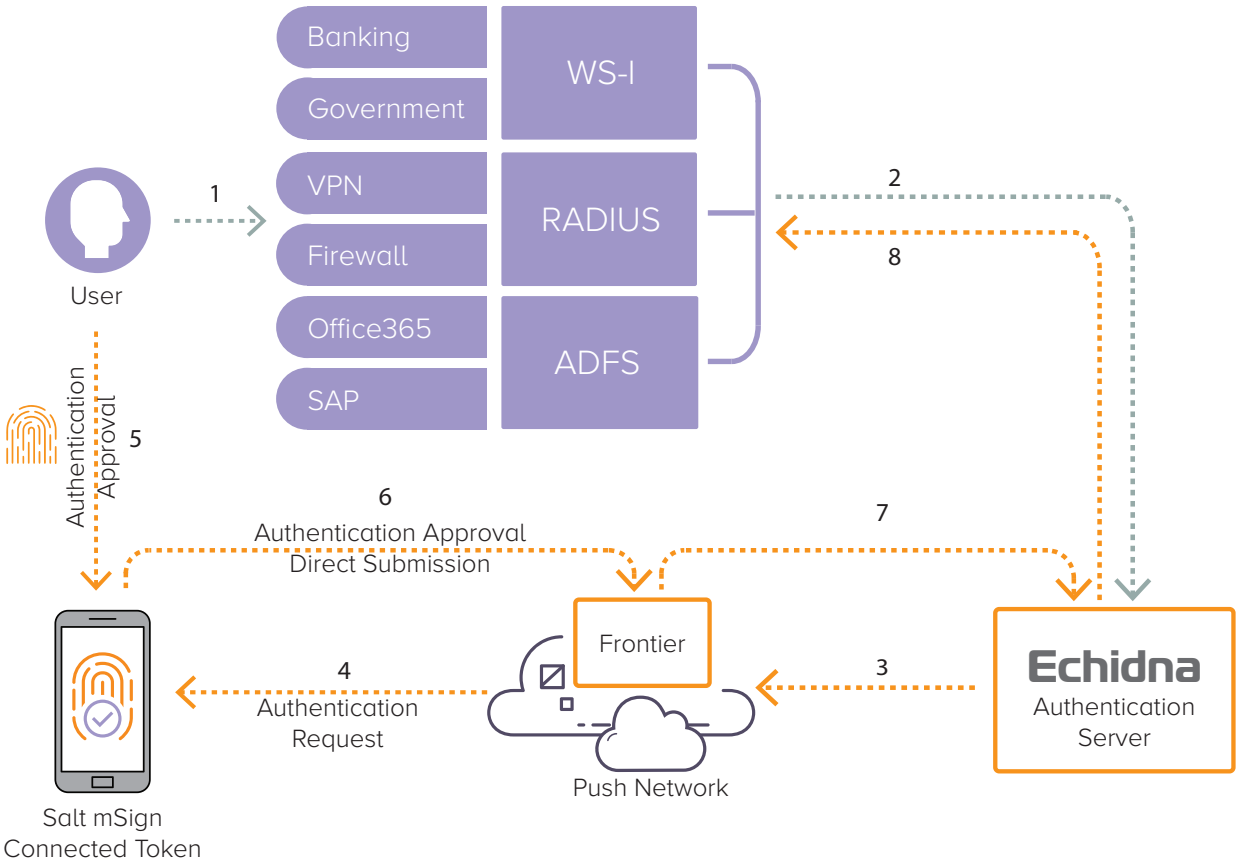
- Use of contemporary cryptographic services based on NIST endorsed standards
- Cryptographic keys generated within hardware cryptographic modules (HSMs) and distributed securely to the token. Each token has a unique set of keys
- Cryptographic keys are secured within the token in a manner that protects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

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 Echidna Authentication Server addresses multi-factor authentication needs across the enterprise.

How Does Salt mSign Work?

The following diagram shows a typical deployment architecture addressing VPN and ADFS multi-factor authentication for user access; and multi-factor transaction authentication.



1. User initiates a Login (or Transaction after login)
2. Relying Application requests multi-factor authentication through Web Services, RADIUS, ADFS
3&4. Echidna sends an Authentication Request to the User's Salt mSign security token
5. User Biometric (or PIN) sign-in to Salt mSign, reviews a summary of the Authentication Request, then Approves/Declines the request
6&7. Salt mSign generates a cryptographic signature of the Approval/Decline and submits the Authentication Response directly back to Echidna
8. Echidna validates the cryptographic signature and returns the authentication response to the Relying Application

Benefits of Salt mSign

- Salt mSign provides a single security token per user which can be used identically across all the Enterprise's digital channels; mobile apps, ADFS, VPNs, PAMs and web applications
- 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 multi-factor authentication. Salt mSign has been reviewed independently by Trusted Labs in France

Technical Info

- Supported on Android and iOS
- Symmetric and public key signature capability
- Supports multiple methods of receiving authentication request: Push Notification, QR Codes and Inter-App
- Biometric and PIN support
- Dynamic Linking, WYSIWYS (What You See Is What You Sign)
- Strong User & Transaction Authentication: Knowledge, Possession, Inherence
- Anti-cloning and Jailbreak/Root detection
- Advanced electronic signatures uniquely linked to the signer

Salt Group Pty Ltd
Level 30, 459 Collins Street
Melbourne VIC 3000
Australia

Australia & Asia Pacific
T: +61-3-9614-4416
F: +61-3-9614-2992
E: sales@saltgroup.com.au