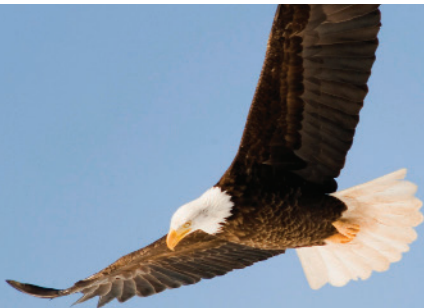


Salt Mobile Tokens

Mobile Phone Authentication



Salt Mobile Authentication Tokens offer organisations a simple and yet reliable solution for online applications including banking, government and internet based payments and transactions.

Key Benefits

- Quick and convenient
- Users can be provisioned instantly
- Introduces a second channel to protect against man in the middle attacks
- Inexpensive to use
- No requirement for additional, dedicated hardware tokens
- Uses a trusted infrastructure

Salt Mobile Token Authentication offers organisations a simple and yet reliable solution for online applications including banking, government and internet based payments and transactions.

It is independent of mobile handset type, network technology and network provider and offers a range of mechanisms to ensure that the most appropriate level of security is applied to transactions based on their assurance level requirements.



- **Salt SMS One Time Password (OTP)** - a text based authentication mechanism introducing a “second channel” to single factor authentication.
- **Salt Push One Time Password (OTP)** - implementing the equivalent functionality of Salt SMS OTP but using Push Technology.
- **Salt mCode One Time Password (OTP)** - implementing the equivalent functionality of existing security tokens onto a mobile handset through the generation of One Time Passwords.
- **Salt mCode Challenge / Response (CR)** - implementing the equivalent functionality of existing security tokens onto a mobile handset through the generation of a “response” derived from a submitted “challenge”.
- **Salt mSign** - enables a user to receive an encrypted authentication request and transaction summary via their handset with a display of the transaction signature code (shown left) generated on the mobile handset.
- **Salt mSign Remote** - implementing the equivalent functionality of Salt mSign but with the signature code transferred to the host via the mobile network.



Salt Mobile Tokens

Mobile Phone Authentication



Supported Networks

Salt Mobile Authentication Tokens have been tested using GSM, CDMA and 3G networks globally including networks in Australia, UK, Europe, Canada, Greater China and Hong Kong, Singapore, Malaysia, Japan, Korea, India, Pakistan, Middle East, South East Asia and South Asia.

Provisioning and transaction processing work is unaffected by physical roaming of handsets.

Supported Handsets

- **Salt SMS OTP** works on all handsets that are capable of receiving SMS text messages.
- **Salt SMS OTP** requires network coverage for operation.
- **Salt Push OTP** supported on iPhone/iPad, Android (version 2.2 and above), BlackBerry devices (OS 5 and above).
- **Salt mCode OTP** and **mCode CR** operate on Java handsets supporting MIDP 1.0 and above.
- **Salt mCode OTP** and **mCode CR** require less than 30K of memory.
- **Salt mCode** Java versions have been tested on a wide variety of handsets and devices from Nokia, Motorola, Sony-Ericsson, Samsung etc along with Symbian and BlackBerry devices.
- **Salt mCode** support for iPhone (version 3.0 and above) and Android (version 1.6 and above) are also provided.
- **Salt mCode** requires network coverage for provisioning only.
- **Salt mSign** operates on Java handsets supporting MIDP 2.0 and above. mSign requires less than 30K of memory.
- **Salt mSign** Java versions have been tested on a wide variety of handsets and devices from Nokia, Motorola, Sony-Ericsson, Samsung etc along with Symbian and BlackBerry devices.
- **Salt mSign** support for native Windows Mobile (version 5 and above) is also provided.
- **Salt mSign** requires network coverage for both provisioning and operation.

Registration

Salt Mobile Authentication Tokens are only deployed to authorised mobile handsets as the result of successful Internet based registration of the user (by the Issuer).

This incorporates user submission of their EOI (evidence-of-identity) along with details of the user's mobile phone number and phone model.

Customisation and Branding

The mCode and mSign application user interface can be fully customised with customer branding, logos, colour schemes, messages and preferred language. The application names can also be changed to reflect customer marketing requirements.

PIN Management

- mCode and mSign applications are both protected by a PIN number that locks after issuer selectable number of attempts.
- The PIN is selected by the user and may be changed by the user. The PIN is local to the handset and not known to the Issuer. The PIN is not stored in clear form within the handset application.
- PIN lengths, weak PIN activation and retry thresholds are Issuer configurable and enforced by the application.
- PIN reset capability is supported through entry of a re-activation code provided from a help desk (or self serve facility). The mCode and mSign PIN can be reset up to five times.
- The mSign application will time out after a period of inactivity, requiring re-entry of PIN.

Cryptographic Modules

- ANSI X9.52 (Triple DES modes of Operation)
- NIST Special Publication 800-67 (Recommendations for Triple DES)
- SO/IEC 18033-3 (Block Ciphers)
- FIPS PUB 46-3 (DES)
- ISO/IEC 9797-2 (MAC)
- FIPS PUB 198, RFC 2104 (HMAC)
- RFC 4226 (OATH HMAC-based OTP)
- FIPS PUB 180-2 (SHA256), FIPS PUB 180-1 (SHA1)
- RFC 1321 (MD5)

Cryptographic Keys

Triple DES using 2 x 56 bit DES keys with randomised parity bits.

Protection Mechanisms

- Cryptographic key material and the user PIN are never held "at rest" in clear form on the handset to protect against black-bag cryptanalysis of handset storage.
- Handset application executables are digitally code signed prior to provisioning and are validated by the user's handset during installation.
- Preventative measures are taken to disallow user choice of "weak" PIN by the handset applications.
- Non-malicious, accidental PIN errors are checked using "modulus 10" Luhn algorithm specified in ISO/IEC 7812-1.

Patents

Patents pending in the U.S. and other countries.

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

