

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 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 Connected Token** - 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



Registration

Salt Mobile Authentication Tokens are only deployed to authorised mobile handsets as the result of successful registration of the user by the Issuer. This incorporates user submission of their EOI (evidence-of-identity).

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 the 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.
- The mSign application will time out after a period of inactivity, requiring re-entry of PIN.

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 can be configured to be checked using "modulus 10" Luhn algorithm specified in ISO/IEC 7812-1.

Supported Networks

Salt Mobile Authentication Tokens have been tested using GSM, CDMA and 3G/4G 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.





Salt mSign Mobile Token



Salt mCode Mobile Token



SMS OTP

Description	Salt mSign Mobile Token	Salt mCode Mobile Token	SMS OTP
Description	Transaction request is sent to the Customer's registered phone to authenticate by Signature generation.	Generate OTPs and Challenge/Response codes with Salt mCode mobile application.	OTPs delivered via SMS.
Platforms			All phones.
Available Offline?	<input checked="" type="checkbox"/> QR Code Delivery.	<input checked="" type="checkbox"/>	
Additional Cost?	Free download. Salt Mobile tokens are free mobile applications available for download from App Stores.		SMS Charges Apply.

Legacy Handset Support

- **Salt mCode** is supported on legacy Java handsets running (MIDP 1.0 and above) and requires less than 30K of memory.
- **Salt mSign** is supported on legacy Java handsets running MIDP 2.0 and above.
- **Salt mCode & mSign** requires less than 30K of memory. 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.

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.

Patents

- Patents in the U.S. and other countries.
- U.S. Patents: 11/665,719
- Publication: US2008/0046988 A1
- Classification 726007000

