

# Salt RADIUS<sup>+</sup>

## Remote Network Access



*Salt RADIUS<sup>+</sup> in conjunction with Salt Mobile authentication tokens provides a convenient out-of-the-box solution for high assurance authentication of remote users connecting to enterprise networks via VPNs, Citrix gateways or other RADIUS aware access points.*

Through the use of the shared network structure of the Internet, companies are able to greatly reduce communications costs, whilst enabling an increasingly mobile workforce to stay in constant touch with the home office from anywhere in the world.

With this evolution to a remote workforce, and the opening up of access to enterprise resources, there is an increasing need to more strongly authenticate users than is possible with traditional userid/password based authentication methods used within the enterprise's secured internal environment.

The industry response to this requirement is the use of strong "two factor" authentication, where the authentication process is supplemented through the use of a second factor credential such as a security token, or second channel such as a mobile phone, to address the risks of common attacks through malware or man in the middle intercepts.

Salt RADIUS<sup>+</sup> is a standalone and scalable out-of-the-box RADIUS compliant server enabling enterprises to leverage their existing directory to secure remote network access using strong two-factor authentication via Salt mCodeXpress mobile tokens or SMS OTP (one time password) as the remote user's credential.

Salt RADIUS<sup>+</sup> is positioned as a cost effective user authentication solution for Virtual Private Networks; Citrix Application Delivery and other RADIUS aware applications.

### **Key Benefits**

- **Salt RADIUS<sup>+</sup>** is designed for rapid deployment as an appliance making it ideal for SMEs and others seeking low complexity but high trust solutions to their user authentication needs. Salt RADIUS<sup>+</sup> is configured via onboard web pages with template configurations also provided for leading VPN and gateway services.

- **Salt RADIUS<sup>+</sup>** is able to directly leverage common user stores such as Active Directory for retrieval of user's token identifiers to be used within the Salt RADIUS<sup>+</sup> server.
- **Salt SMS OTP** provides an entry level solution that enables rapid onboarding of new users and a cost effective authentication mechanism for occasional users where carrying a specialised device for authentication is inconvenient and unwarranted.
- **mCodeXpress** handset resident token provides all the features of a specialised security token with the convenience of operation available through the user's mobile handset.
- **mCodeXpress** provides a lower total cost of ownership compared with traditional specialised one time password generators or security tokens. Savings accrue through over the air provisioning, simple replacement of lost or stolen tokens, and through utilising the user's existing mobile phone.
- **mCodeXpress** tokens are provisioned over the air, to anywhere in the world, with users up and running in minutes rather than days as experienced with physical token distribution.
- **mCodeXpress** tokens can be deployed on a broad range of mobile handsets and are independent of network technology or service provider.



# Salt RADIUS+

## Remote Network Access



### User Store

In a typical deployment, Salt RADIUS+ connects to a User Store to validate userid|password credentials and retrieve user mobile numbers. Salt RADIUS+ will work with any LDAP or JDBC User Store, including: Active Directory, MS SQL Server, Oracle, Novell Directory Server, Novell eDirectory, and IBM Tivoli Directory Server.

Alternatively, Salt RADIUS+ can store and manage user information locally if the deployment environment does not have an appropriate User Store.

### Protection Mechanisms in mCodeXpress

mCodeXpress incorporates a range of security measures designed to reduce the risks of contemporary attack scenarios.

- Unlike many specialised OTP tokens, mCodeXpress is PIN protected and will lock after a configurable number of successive bad PIN entries.
- To protect against black-bag cryptanalysis of the handset's storage, neither cryptographic key material nor the user PIN will be held "at rest" in clear form on the handset. Even with access to the handset data, a PIN precision mechanism prevents brute-force attack of the PIN.
- The mCodeXpress application binary is digitally signed prior to provisioning and is validated by the user's handset during installation. This protects against inadvertent loading of corrupted or maliciously constructed applications.

### Simplified mCodeXpress Provisioning and Registration

Salt RADIUS+ supports two simple registration and provisioning models for mCodeXpress.

User self service whereby a user who is already authenticated to a LAN accesses LAN based web registration pages which lead the user through:

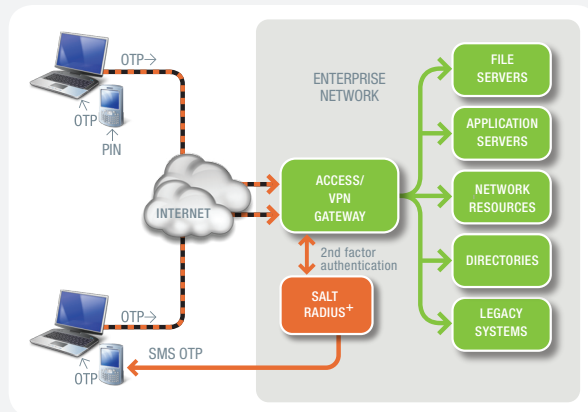
- Download of a generic mCodeXpress application to the user's handset.
- Initiation of the application on the handset which requests the user to select a PIN and then generates a 128-bit AES key, and displays a 16-digit alphanumeric "Registration Code".
- The user then enters the Registration Code into the Salt RADIUS+ self-service User Registration pages.

For remote users with traditional userid|password access to a VPN seeking to upgrade to higher assurance levels, the same procedure can be followed with the final activation of the mCodeXpress token completed by an Administrator after validation (by phone or email with the user) that the deployment is in fact to the identified user's handset.

### Salt SMS OTP Registration

Registration for SMS OTP service is through inclusion of the user's mobile handset within the external or local user store as appropriate, and activation of the user for SMS OTP validation.

As for mCodeXpress, this can be completed via Salt RADIUS+ web based registration pages by the user or the Administrator.



### Cryptographic Keys

128-bit AES

### Cryptographic Modules

- FIPS PUB 197 (AES)
- ISO/IEC 9797-2 (MAC)
- FIPS PUB 198, RFC 2104 (HMAC)
- FIPS PUB 180-2 (SHA256), FIPS PUB 180-1 (SHA1)
- RFC 1321 (MD5)

### RADIUS Profile Support

- Password Authentication Protocol (PAP)
  - Challenge-Handshaking Authentication Protocol (CHAP)\*
- \* Not supported with LDAP User Stores

### Compliance & Interoperability Testing

- AT&T Global Network Service
- CheckPoint Firewall-1
- Citrix XenApp 5.0

### Platform Support

- Any J2EE container supporting JRE 1.5 and JSP 2.1; such as Apache Tomcat, Glassfish, Oracle WebLogic, IBM WebSphere, JBoss
- VMware Virtualization
- Sun VirtualBox
- Ubuntu Linux Distribution

### mCodeXpress Handset Support

- Salt mCodeXpress will operate on a wide variety of handsets and devices from Nokia, Samsung, Sony-Ericsson, LG, Motorola, and other Symbian devices
- iPhone, BlackBerry and Android devices are also supported
- Network Coverage is only required for OTA provisioning

