Echidna
Remote Network Access

SALT GROUP

Echidna Authentication Services in conjunction with Echidna Mobile and OATH hardware 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 communication 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 user ID / password based authentication methods used within 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 mobile phone, to address the risk of common attacks through malware or man in the middle intercepts.

Echidna for Remote Network Access is an Echidna Packaged Solution that combines pre-configured components of the Echidna security platform to provide a standalone and scalable out-of-the-box RADIUS compliant authentication server enabling enterprises to leverage their existing directory to secure remote network access using strong two-factor authentication via Echidna Mobile tokens, SMS OTP or OATH compliant security tokens, as the remote user's 2FA credentials.

Echidna Remote Network Access is positioned as a cost effective user authentication solution for Virtual Private Networks; Citrix Application Delivery and other RADIUS aware applications.

Echidna Remote Network Access 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. Echidna is configured via onboard web pages with template configurations also provided for leading VPN and gateway services.

Key Benefits

- **Echidna** is able to directly leverage common user stores such as Active Directory and databases for retrieval of user's authentication credentials.
- **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 security token for authentication is inconvenient and unwarranted.
- **Echidna Mobile** is a handset resident token which provides all the features of a specialised security token with the convenience of operation available through the user's mobile handset.
- **Echidna Mobile** 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.
- **Echidna Mobile** 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.

next

Echidna
Remote Network Access

- **Echidna Mobile** tokens can be deployed on a broad range of mobile handsets and tablet devices, and are independent of network technology or service provider.

User Store

In a typical deployment, Echidna connects to a User Store to validate user ID / password credentials and retrieve user mobile numbers. Echidna 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, Echidna can store and manage user information locally if the deployment environment does not have an appropriate User Store.

Simplified Token Provisioning & Registration

Echidna supports two simple registration and provisioning models for Mobile tokens.

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 the Echidna Mobile app 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 alpha-numeric "Registration Code"
- The user then enters the Registration Code into the Echidna self-service User Registration pages

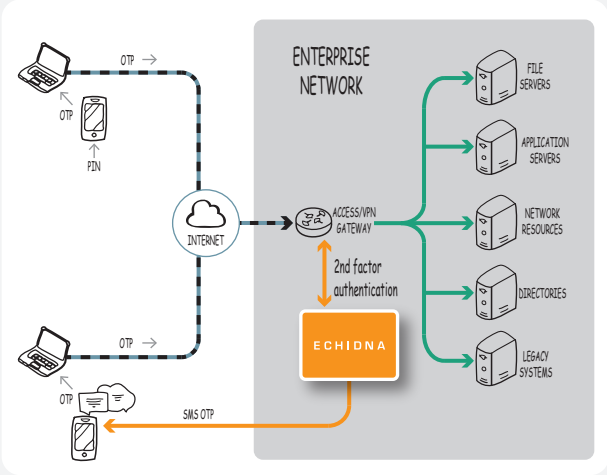
For remote users with traditional user ID / password access to a VPN seeking to upgrade to higher assurance levels, the same procedure can be followed with the final activation of the Echidna Mobile token completed by an Administrator after validation (by phone or email with the user) that the deployment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

SMS OTP Registration

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

OATH Token Support

- **HOTP** HMAC-Based One-Time Password (RFC 4226)
- **TOTP** Time-Based One-Time Password (RFC 6238)
- **OCRA** OATH Challenge-Response (RFC 6287)



Cryptographic Keys

128-bit AES

RADIUS Profile Support

- Password Authentication Protocol (PAP)
- Challenge-Handshaking Authentication Protocol (CHAP)*

Web Services Interoperability Support

- Simple Object Access Protocol (SOAP)
- Representational State Transfer (REST)

Compliance & Interoperability Testing

- AT&T Global Network Service
- CheckPoint Firewall-1
- Citrix XenApp 5.0 and Citrix Netscaler Gateway
- IBM Tivoli Access Manager (TAM)
- Microsoft Forefront Treat Management Gateway (TMG) and Unified Access Gateway (UAG)

Platform Support

- Any J2EE container supporting JRE 1.6 and JSP 2.1; such as Apache Tomcat, Oracle Weblogic, IBM WebSphere, JBoss
- VMware Virtualization
- Ubuntu Linux Distribution

**CHAP not supported with LDAP User Stores*

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

Indonesia
APL Tower-Central Park
19th Floor Unit T7 Jl S.
Parman Kavling 28
Jakarta 11470, Indonesia

Salt Group (Indonesian Office)
T: +62-21-2965-9377
F: +62-21-2933-9357

saltechidna.com