Echidna
MFA Authentication Services

SALT GROUP

Echidna Authentication Services provide a central trust anchor for organisations to provide an additional level of user authentication through Multi-Factor Authentication (MFA) methods such as mobile or hardware security tokens.

Echidna Authentication Services are built on the Echidna Security Platform – an enterprise grade security platform developed by Salt Group – to support a range of high availability, high volume and high assurance security services in banks, government departments and enterprises globally.

Echidna Authentication Services include:

- User Identity Authentication Services during the login process
- General Purpose Authentication Services
- Multi-Method Security Authentication

Echidna Authentication Services support a comprehensive range of authentication methods from Open Standard (OATH) compliant hardware security tokens to Echidna Mobile tokens, enabling a flexible unified Multi-Factor Authentication (MFA) service.

The supported authentication methods can be combined in a flexible manner to support a diverse user base with multiple methods, and even support individual users with multiple available methods.

Echidna interfaces to a range of Identity and Access Management (IDAM) infrastructures and to general-purpose access gateways through either web services or RADIUS to provide user authentication services.

Echidna is available as a virtual appliance which allows an organisation to deploy Echidna in a matter of hours.

Echidna Authentication Services are future proofed through a pluggable architecture that allows an organisation to adopt new authentication methods as they emerge, without expensive retrofit or system remediation.

Echidna Authentication Services supports a seamless migration from exiting MFA solutions which allows an organisation to easily migrate from ageing and expensive token solutions whilst protecting their prior investment during the transition stage.

Key Features

- User Identity Authentication Services
- General Purpose Authentication Services
- Multi-Method Security Authentication
- Rules-based enforcement of authentication methods and user resolution
- Token Lifecycle Management for Echidna Mobile and OATH Hardware Tokens
- Hardware Security Module for secure storage of sensitive assets such as passwords, token keys, shared secrets, SSL cert private keys
- Tamper evident audit logs
- Brokering Authentication requests proxy to 3rd party proprietary servers

Supported Security Tokens

Echidna Authentication Services are agnostic to the user authentication methods and provides wide support for a range of standard, proprietary and brokered methods.

next

Echidna

MFA Authentication Services

Echidna supported security tokens include:

- Open Standard OATH hardware security tokens that are compliant to the OATH HOTP, TOTP or OCRA standards.
- Echidna Mobile tokens to enable MFA through the use of mobile phones and devices to generate OTPs, Challenge/ Responses and Transaction Signing credentials for authentication.
- Proprietary security tokens such as RSA SecurID and Vasco tokens through proxy authentication requests to third party servers.

Inbound Connectors

Echidna Connectors enable standards based interfaces for relying applications to use the Authentication Services. Echidna supports –

- RADIUS – Echidna has a RADIUS interface making it a fully compliant RADIUS Server. Echidna can be used as a cost effective user authentication solution for Virtual Private Networks; Citrix Application Delivery and other RADIUS aware applications.
- WS-I – Echidna has a Web Services interface which supports WSI-SOAP and RESTful web service APIs.
- Customize – Other applications with more specific requirements can request a 'custom' connector to meet their needs.

Token Asset Management

Echidna Authentication Services include console facilities for Administration and User Self-Registration.

Delegated administration is supported to allow administrators to assist end-users in registration and use of their 2FA methods.

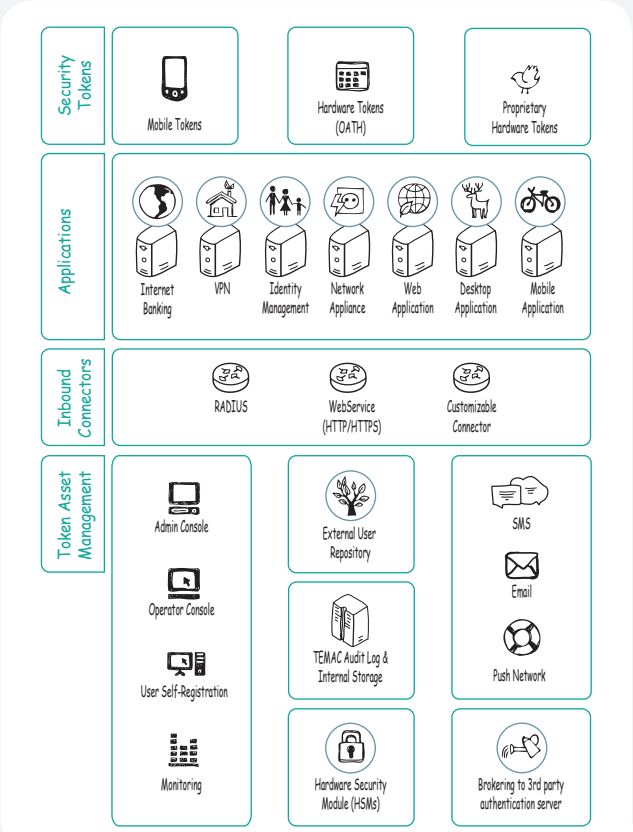
Browsing of the audit records is available through the Admin and Operator console.

Brokering to 3rd Party Authentication Servers

Echidna Authentication Services can delegate authentication requests that match the pre-configured criteria to external servers via either RADIUS or web service calls. This allows support of 2FA mechanisms that are not natively present in Echidna, such as vendor proprietary security tokens.

External User Store

Echidna Authentication Services supports both Active Directory and generic LDAP user directories. While any JDBC based database can be supported with the appropriate driver, compliance testing has been performed for Microsoft SQL



Server (2008), Oracle (11g) and Apache Derby 10.8.2.2.

Echidna Authentication Services do not require a local database, but can use either a local or a remote database for token registration and audit log records.

Hardware Security Modules (HSMs)

Echidna supports Hardware Security Modules (HSMs) for secure storage of sensitive assets such as passwords, token keys, shared secrets, SSL cert private keys, and tamper evident audit logs. Key generation and HSM commissioning is done using the HSMs native toolset.

Thales nShield HSM solutions are fully supported by Echidna.

Tamper Evident Audit Logs & Internal Storage

Echidna's Authentication Services audit records can be sent to flat files and/or a database table. The fields to be logged are configurable, and cryptographic (TEMAC) Tamper-Evident Message Authentication Code protection is available with HSMs.

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
T: +62-21-2965-9377
F: +62-21-2933-9357

Salt Group (Indonesian Office)
APL Tower-Central Park
19th Floor Unit T7 Jl S.
Parman Kavling 28
Jakarta 11470, Indonesia

saltechidna.com