Safetronic Echidna Edition

Authentication Platform

CONTEMPORARY AUTHENTICATION OF USER IDENTITIES & TRANSACTIONS

Safetronic “Echidna Edition” (Echidna) is an enterprise grade security platform that provides a single trust anchor for organisations to authenticate users, transactions and device identities across a variety of contexts and channels.

Echidna is a collection of Authentication Services, Inbound Connectors, Salt Mobile Tokens, and OATH Security Tokens that are combined to provide convenient out-of-the-box solutions to cater for different security requirements and application use cases.

Highlights

Connected **Biometric** 2FA **Login** for User access via RADIUS, Microsoft ADFS, SAML Federated Login for cloud, Shibboleth and Browser-based Web Applications

Payment **Card PIN Validation** for identity verification and card PIN management. ISO-9564 Format-0 compliant with support for interface into Interchange AS2805 (ISO8583 equivalent)

Support HSMs (Hardware Security Modules) for secure storage of sensitive assets, token keys, shared secrets, SSL cert private keys and database protection

Legacy Token Replacement using brokering to delegate to 3rd Party authentication servers, enabling a non-disruptive migration

Token **Lifecycle Management** through an operator console and user self-service console for Salt Mobile tokens and other user security methods such as OATH hardware tokens

Operate as **Identity Provider** (IdP) to enable Access Management products to delegate their user authentication to Echidna as a Federated Identity Provider

Echidna is an enterprise grade authentication 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
- Device Authentication for access into API Gateways
- General Purpose Authentication Services
- Transaction Signing Authentication
- Multi-Method Security Authentication
- Payment Card PIN Validation for identity verification and PIN management

Echidna supports a comprehensive range of authentication methods 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 Web Services, OIDC, RADIUS or ADFS to provide user authentication services.

Echidna's Token Lifecycle and User Management Console capabilities are also available as APIs to enable interfacing with the organisation's User Management Systems.

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 existing MFA solutions which allows an organisation to easily migrate from ageing and expensive legacy token solutions whilst protecting their prior investment during the transition stage.

Security Tokens

- **Salt mSign** mobile security MFA token for biometric authentication of the user identity and transaction signing independent of the delivery channel that initiated the request
- **Salt mCode** traditional 2FA mobile token combined with contemporary biometric methods for verifying user access to online services
- **Salt Mobile SDK** to embed the capability of Salt mSign and mCode standalone security tokens within existing mobile apps
- Open Standard **OATH hardware tokens** that are compliant to: HOTP, TOTP, OCRA. And OATH compliant soft tokens such as Google Authenticator
- **SMS/Email OTP** provides an entry level solution that enables rapid onboarding of new and occasional users
- **Legacy**/proprietary token support via delegated authentication to existing authentication servers during token migration while new security tokens or other 2FA methods are introduced, allowing the existing legacy tokens to be gradually replaced as they expire

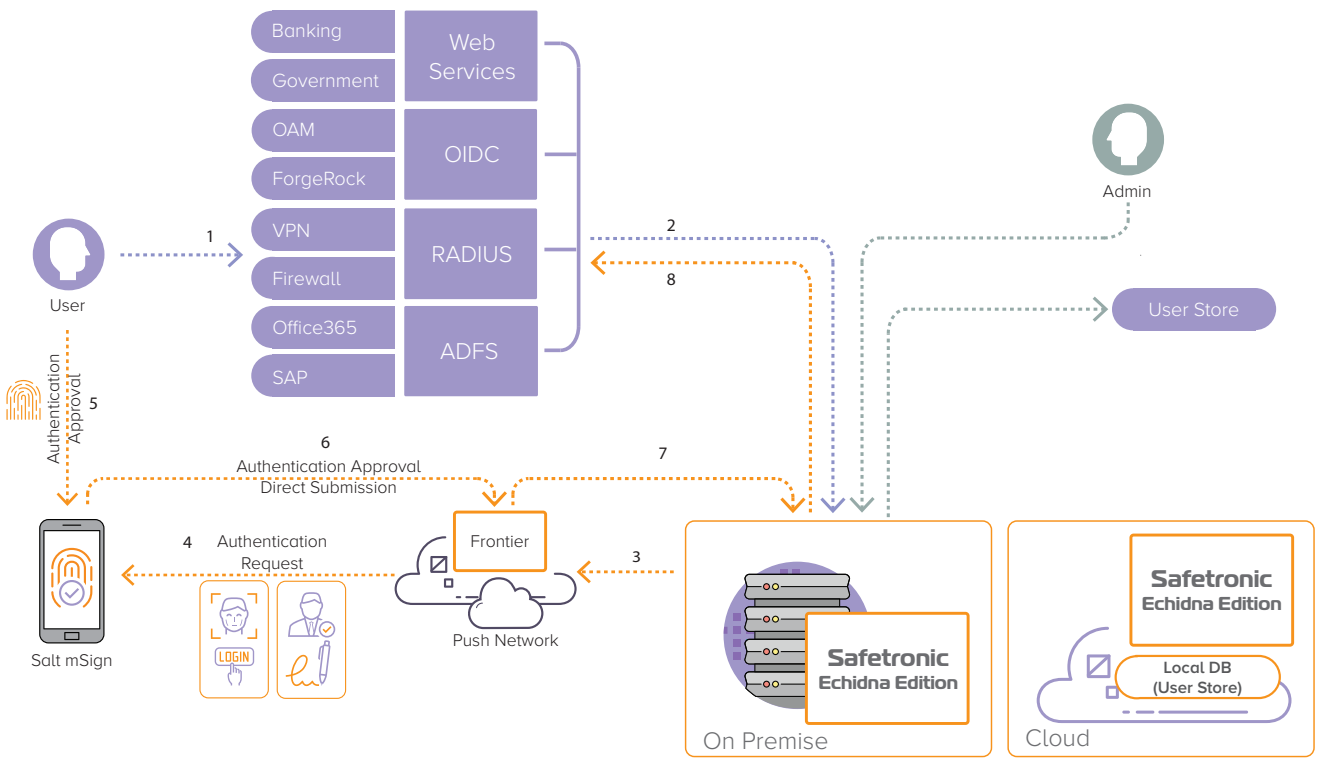
Inbound Connectors

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

- **OIDC** – Echidna has an OpenID Connect (OIDC) interface and can operate as an Identity Provider (IdP) to enable Access Management products to extend their authentication to Federated Identity Providers to delegate user authentication
- **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
- **Web Services** – Echidna has a Web Services interface which supports RESTful (JAX-RS) and SOAP web service APIs
- **ADFS** – Echidna has an ADFS Plug-In to enable 2FA for Windows Server, Office365, Google Drive, Salesforce, SAP Fiori

How Does Echidna Work?

The following diagram depicts a typical Echidna implementation supporting user biometric login and transaction authentication with Salt mSign connected token.



1. User initiates a Login (or Transaction after login)
2. Relying Application requests multi-factor authentication through Web Services, RADIUS, ADFS, OIDC
3&4. Echidna sends an Authentication Request to the User's Salt mSign security token
5. User Biometric (or PIN) sign-in to Salt mSign, reviews a summary of the Authentication Request, then Approves/Declines the request
6&7. Salt mSign generates a cryptographic signature of the Approval/Decline and submits the Authentication Response directly back to Echidna
8. Echidna validates the cryptographic signature and returns the authentication response to the Relying Application

HSM Support

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.

nCipher nShield HSM solutions are fully supported by Echidna.

Echidna's 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.

Technical Info

- **User Store** - In a typical deployment, Echidna connects to a User Store to validate username / password credentials and retrieve user mobile numbers. Echidna will work with any LDAP or JDBC User Store, including: Active Directory, MS SQL Server, Oracle, MySQL, 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.
- **Platform Support** - Any J2EE container supporting Java 1.8, JSP 2.3 + Servlet 3.1; such as Apache Tomcat, Oracle Weblogic, IBM WebSphere and JBoss. Distribution options include VMware Virtualization, Linux (Ubuntu, RHEL) and Windows.
- **Cloud Deployment** - Echidna can be deployed into a Private Cloud such as Amazon AWS and Microsoft Azure.
- **RADIUS Compliance & Interoperability** - AT&T Global Network Service, CheckPoint Firewall-1, Citrix XenApp 5.0 and Citrix Netscaler Gateway, IBM Tivoli Access Manager (TAM), Microsoft Forefront Threat Management Gateway (TMG) and Unified Access Gateway (UAG). RADIUS Password Authentication Protocol (PAP) profile support and limited support for RADIUS CHAP.
- **ADFS Plug-In Interoperability** - ADFS 3 on Windows Server 2012 R2 , ADFS 4 on Windows Server 2016, and ADFS 5 on Windows Server 2019.

Salt Group Pty Ltd
Level 30, 459 Collins Street
Melbourne VIC 3000
Australia

Australia, UK/EU & Asia Pacific
T: +61-3-9614-4416 (AU/AsiaPac)
T: +44-20-3966-1686 (UK/EU)
E: sales@saltgroup.com.au