



Echidna

AUTHENTICATION PLATFORM

CONTEMPORARY AUTHENTICATION OF USERS, DEVICES & TRANSACTION IDENTITIES

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



Multi-Factor Authenticator for all the organisation's mobile apps supporting multiple methods of sign-in and authentication independent of the service delivery channel



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



High assurance mobile & IoT **Device Identification** for access to the internal APIs of organisation through API Gateways; through authentication of the device rather than the user login credentials

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

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, 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 authentication of the user identity and transaction 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



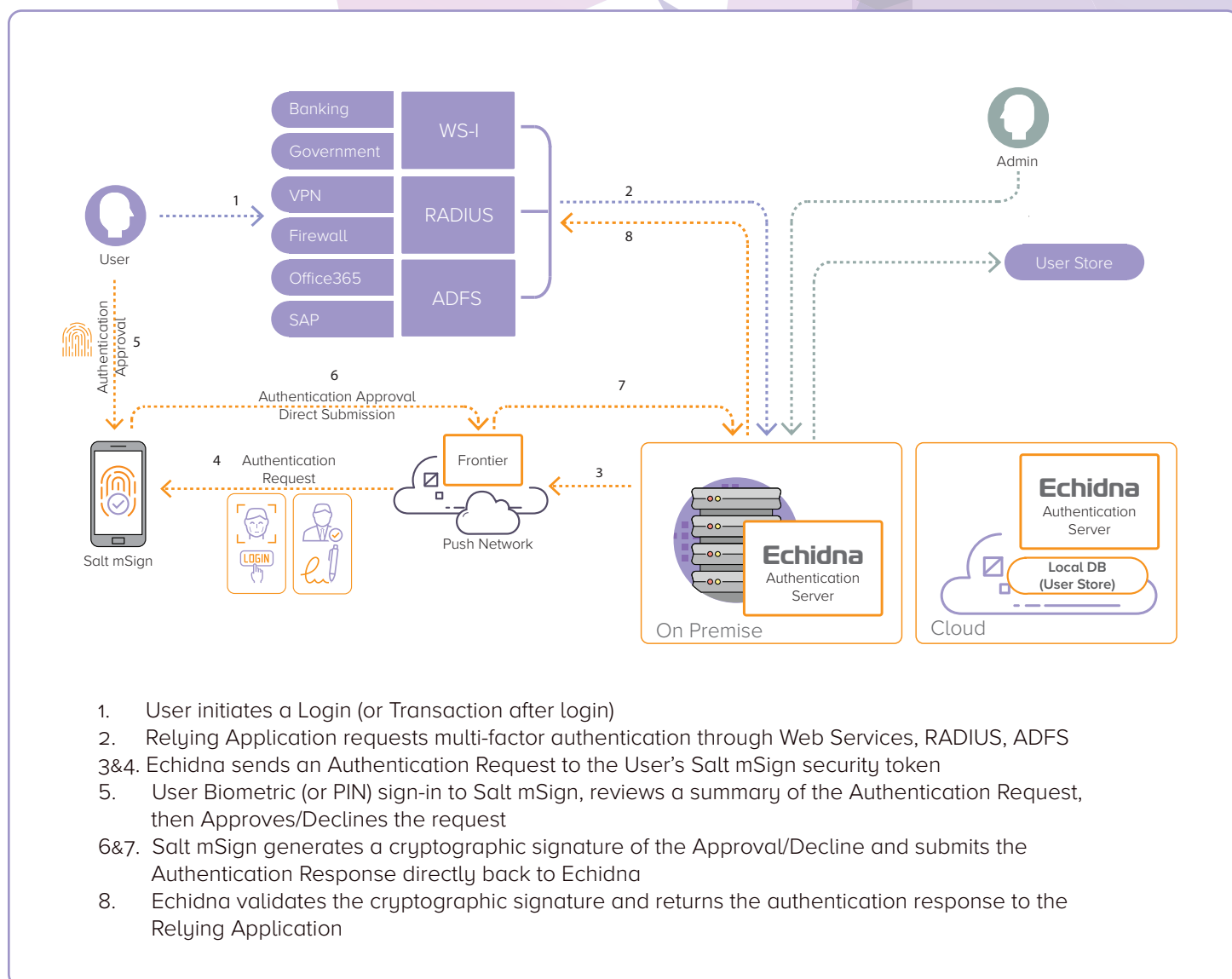
INBOUND CONNECTORS

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

- ✓ **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
- ✓ **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.





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.

Thales 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 JRE 1.6 and JSP 2.1; such as Apache Tomcat, Oracle Weblogic, IBM WebSphere and JBoss. Ubuntu Linux Distribution and VMware Virtualization.
- ✓ **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.

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