Safetronic

Authentication Platform

USER IDENTITY, USER TRANSACTION AUTHENTICATION & B2B PAYMENTS ENABLING TRUST ACROSS ALL DIGITAL

Safetronic is an enterprise grade security platform that provides a single trust anchor for organisations to authenticate user identities, transactions and secure high-value B2B payments across a variety of contexts and channels.

Safetronic is a collection of authentication methods that are combined to provide a convenient out-of-the-box solution to cater for different security requirements and application use cases.

Safetronic (formerly known as SafeSign) supports a range of high availability, high volume and high assurance security services in banks, government departments and enterprises globally.

Highlights

Channel Independent Connected **Multi-Factor Authentication** (MFA) through Salt mSign Mobile Tokens enabling Biometric Password-less Login and Transaction Signing that is **PDS2/SCA** Compliant

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)

Protect **High-Value B2B Payments** such as the UK BACS, Faster Payments, CHAPS and Faster Cheques; ensuring traceability of all transactions with robust tamper evident audit trails

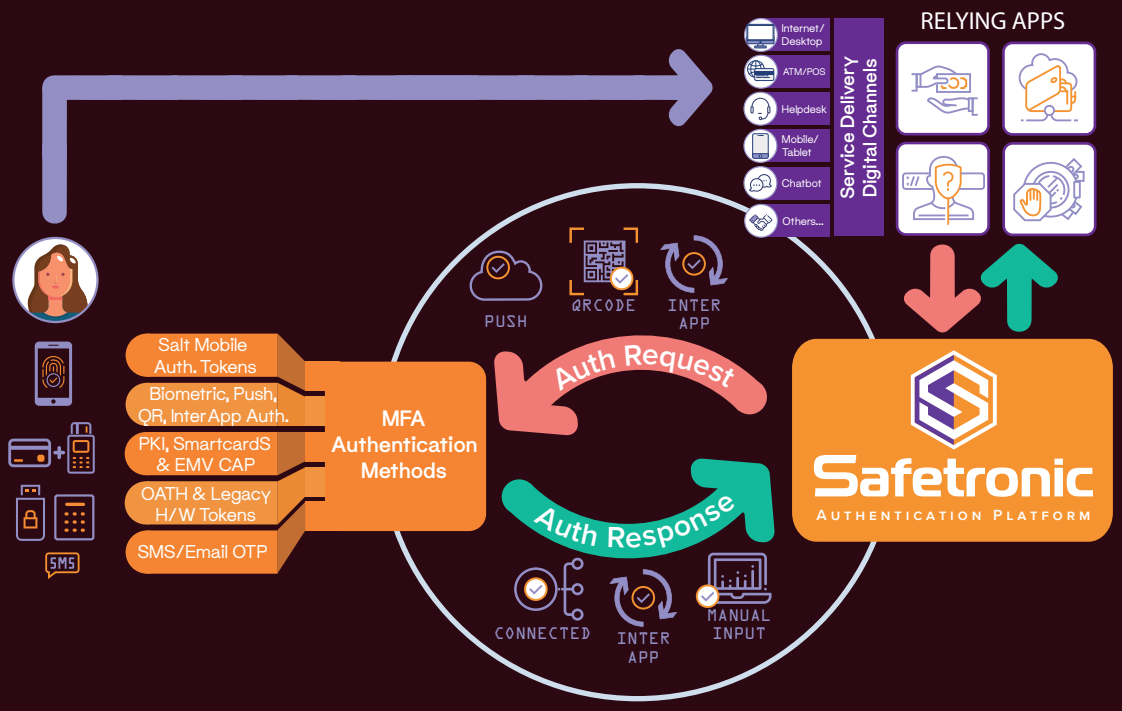
Comprehensive MFA mechanisms and device support, including OATH OCRA/TOTP/HOTP, Vasco DigiPass, EMV CAP, SMS/Email OTP, and contemporary biometric Salt mSign mobile authentication

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

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

Safetronic Authentication

Safetronic 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 MFA methods.



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; including SDK option to embed within existing mobile apps
- **Biometric** user authentication, Push authentication, QR code transaction signing, InterApp mobile app-to-app authentication
- **EMV CAP** authentication including support for verfication of signatures generated by CVN cards
- **PKI** signature generation and validation including certificate status checking against CRLs and OCSPs
- Open Standard **OATH** tokens that are compliant to: OCRA, TOTP, HOTP
- **Legacy**/proprietary hardware token support for Vasco/OneSpan DigiPass and ActivIdentity
- **SMS**/Email OTP provides an entry level solution that enables rapid onboarding of new and occasional users

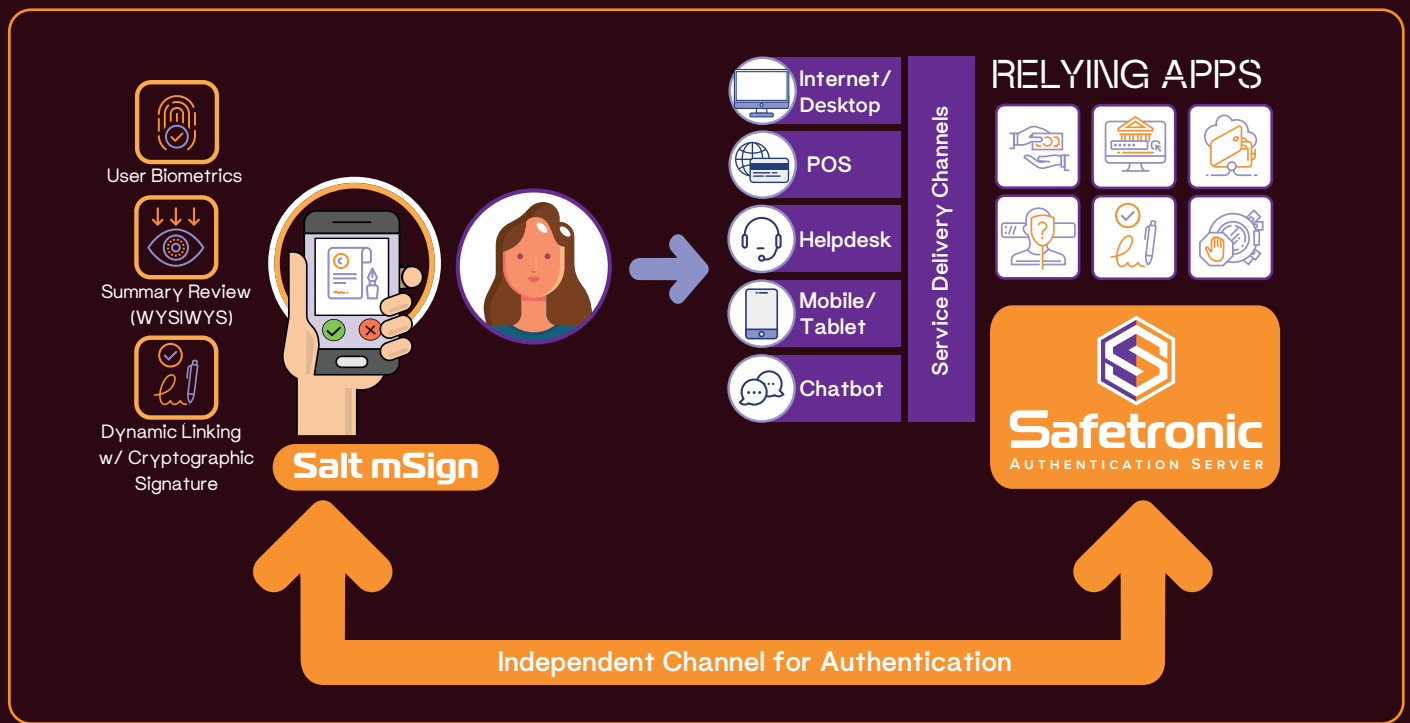
Strong Customer Authentication

- Heterogeneous MFA - mobile, biometric, smartcard, OATH, EMV CAP, soft & hard tokens
- Support omni-channel authentication with a consistent frictionless customer authentication experience across all digital channels
- End-to-end workflows to securely verify the identity of your customers
- Consolidate multiple authentication services onto a single platform to realise cost benefits and efficiencies, and to protect your investment

Comply with the regulator requirements such as the European Payment Services Directive (PSD2) for Strong Customer Authentication (SCA), whilst retaining a flexible customer focused approach to authentication. The directive requires that customer and transaction authentication across digital channels be implemented by a compliant multi-factor mechanism that incorporates knowledge, possession and inherence which ensures that both the originator of the transaction and the transaction content can each be strongly authenticated and bound to each other.

Safetronic has been designed to support a diverse range of PSD2/SCA compliant authentication mechanisms simultaneously. The scalable Safetronic architecture future proofs your authentication investment and enables you to expand your existing security platform to accommodate new or additional authentication mechanisms as they emerge.

Safetronic when used with Salt Group's PSD2/SCA compliant Salt mSign Connected mobile token enables organisations to utilize a single authentication method across all digital channels and abstracts the authentication layer from the business logic.



Payment System Innovation

Safetronic has been at the core of the UK payments network since the inception of BACS-TEL-IP in 2002. The Banker's Automatic Clearing System (BACS) selected the Safetronic platform to authenticate payment transactions, ensure traceability of all transactions and provide robust audit trails. Safetronic provides a unique multi-channel signing and validation capability to support simultaneous connection to the 20+ member banks that form BACS. This removes the complexity of securely supporting and managing multiple PKIs from the applications themselves and separates the application logic from security functions, ensuring compatibility with all relevant PKI standards and the required levels of compliance and governance for each scheme.

To minimize time to market and reduce project risks, Salt Group works closely with the schemes to keep abreast of roadmaps, standards and ensure Safetronic is ready for the everchanging payments landscape.

Safetronic for securing payment submissions is a tried and tested platform that is at the heart of the UK payments infrastructure. Flexible deployment models are available: a rich set of service-based APIs to incorporate Safetronic into existing applications, and turnkey applications providing an out-of-the-box payment solution.

HSM Support

Safetronic supports Hardware Security Modules (HSMs) for secure storage of sensitive assets such as PKI private keys, passwords, token keys, shared secrets, SSL keys and keys used for Tamper Evident (TEMAC) Audit Logs. Entrust nShield HSM solutions (formerly known as Thales nCipher) are fully supported by Safetronic.

Encryption keys handled outside the cryptographic boundary of a certified HSM are significantly more vulnerable to attack, which can lead to compromise of critical keys. HSMs are the only proven and auditable way to secure valuable cryptographic material. nShield HSMs integrate with Safetronic to protect high value payment keys in tamper resistant hardware certified to recognized industry standards. Mandated by a number of schemes, a FIPS 140-2 device is essential to protect critical key material against attack and compromise.

Safetronic uses HSMs to enforce key usage policies and separation of security functions from administration. HSMs allow Safetronic to support bulk unattended 'lights out' authentication submissions, centralised key management and operational redundancy and resilience.

Salt Cybersecurity
Office 4, 219 Kensington High Street,
London W8 6BD, UK

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