



mSign Advanced

OPERATIONAL INTELLIGENCE

Mobile authentication has become a cornerstone of enterprise security. From approving high value financial transactions and corporate payment instructions to validating digital identities, mobile authenticators are increasingly trusted to protect an organisation's most critical business processes.

Selecting the right mobile authenticator has traditionally focused on cryptographic strength, regulatory compliance and user convenience. Features such as biometric authentication, transaction signing and secure Push approvals have become expected capabilities for enterprise deployments.

However, once mobile authenticators are deployed at enterprise scale across thousands of customer devices, a new challenge emerges.

High-Assurance Authentication is Only Half the Story

Security teams know whether a transaction has been approved, but they rarely understand how their authentication fleet is performing in the field. Which mobile operating system versions are deployed? Which devices are failing to receive Push notifications? Which users are migrating to new devices? Which authentication methods are actually being adopted?

As deployments scale across diverse mobile devices, operating system versions and user populations, this lack of operational visibility creates unnecessary support costs, delayed incident resolution and increased operational risk.

Salt mSign Advanced combines the proven high-assurance authentication capabilities of Safetronic and Salt mSign with Concierge operational intelligence, enabling organisations to authenticate users and transactions with confidence while continuously monitoring, managing and optimising their deployed mobile authentication environment.

Enterprise Mobile Authentication Needs Operational Visibility

Enterprise authentication transition from hardware tokens to sophisticated mobile authenticators has improved both security and usability while enabling organisations to standardise on a single mobile authentication experience across multiple digital channels.

Mobile authentication introduces an entirely different operational model. Traditional hardware tokens were predictable. Every token shared identical hardware, firmware and behaviour. Management was relatively straightforward, requiring little more than a serial number and token status.

Mobile authenticators are fundamentally different. Every authentication occurs within a unique combination of mobile hardware, operating system version, manufacturer customisations, biometric capabilities, application permissions, notification services and network conditions.

No two authentication environments are identical. As deployments grow, organisations need to understand how their authentication fleet is behaving in the real world. Organisations require visibility into deployment trends, authentication behaviour, operational health and device lifecycle. They must identify issues before they become support incidents while confidently planning operating system upgrades and application rollouts.



Salt mSign Advanced extends enterprise authentication beyond transaction approval by combining high-assurance authentication with Concierge's operational intelligence.

The result is a mobile authentication solution that not only authenticates transactions and users with confidence, but also enables organisations to operate, support and continuously improve enterprise authentication.

See What Other Mobile Authenticators Can't

Every authentication request contains valuable operational information. Most enterprise mobile authenticators simply validate the transaction, return an authentication response and do not capture the operational context surrounding the event. However, every mobile authenticator operates within an environment that the organisation does not own or control. Device manufacturers introduce customised operating systems, users modify security settings, application permissions change over time, and new operating system releases are deployed continuously. Maintaining operational awareness across this constantly changing ecosystem requires visibility beyond traditional authentication logs.

Salt mSign Advanced takes a fundamentally different approach. Concierge continuously captures and correlates authentication telemetry across the entire authentication lifecycle, transforming individual authentication events into meaningful operational intelligence about real-world deployment behaviour. The organisation's product owners and administrators gain complete visibility into authentication behaviour across users, devices, operating system versions, application releases and enterprise-wide deployment trends. Rather than reacting to authentication problems after they occur, organisations can proactively monitor the health, adoption and performance of their authentication environment.

- ✔ **Fleet Intelligence** — Maintain a complete operational view of every deployed mobile authenticator. Gain comprehensive visibility into device models, operating system versions, application releases, authentication profiles, token lifecycle and device migration history. Track fleet composition over time and understand how the deployment evolves as users upgrade devices and operating systems.
- ✔ **Authentication Intelligence** — Analyse how users authenticate across the organisation. Measure biometric adoption, PIN usage, transaction approval behaviour, authentication methods and user interaction patterns to identify deployment trends and improve user experience.
- ✔ **Operational Health** — Detect emerging operational issues before they become widespread user problems. Monitor device permissions, runtime protection events, operating system compatibility and authentication anomalies across the deployed authentication fleet.
- ✔ **Security Intelligence** — Investigate authentication activity through detailed forensic visibility. Review authentication timelines, profile history, device changes and historical authentication sessions to support incident investigation, fraud analysis and enterprise governance.

Enterprise Operations Begin After Authentication

Every successful authentication represents far more than a cryptographic event. Behind every approved transaction is a mobile device operating within a constantly evolving ecosystem of operating system updates, application releases, manufacturer-specific software, biometric services, security settings and user behaviour.

Traditional mobile MFA authenticators perform a single task — they authenticate the transaction and user identity then return a success or failure response. Once authentication is complete, operational visibility effectively ends.

For organisations managing large-scale enterprise deployments of mobile MFA authenticators, this creates a significant operational blind spot. Support teams struggle to diagnose user issues. Security teams lack meaningful visibility into authentication behaviour. Operations teams cannot confidently assess the health of the deployed authentication fleet.

Salt mSign Advanced addresses this challenge by embedding operational intelligence directly into the authentication ecosystem. Rather than relying on generic infrastructure monitoring platforms or building custom reporting solutions, Concierge continuously collects authentication-specific telemetry from deployed Salt mSign tokens and transforms it into actionable intelligence, providing administrators with continuous awareness of their deployed authentication fleet. The result is complete visibility across the authentication environment—from individual authentication sessions through to enterprise-wide fleet trends.

Why Generic APM Platforms Aren't Enough

Application Performance Monitoring platforms such as Dynatrace, Datadog and New Relic provide valuable insight into application infrastructure, server performance and network behaviour. But they were never designed to understand enterprise mobile authentication. They can identify a slow API response or overloaded server. They cannot explain why Push notifications are failing for Samsung devices running a specific Android release. They cannot identify users who have disabled biometric authentication. They cannot trace authentication profiles across multiple device migrations.

Salt mSign Advanced understands authentication because it was designed specifically for enterprise mobile authentication. Purpose-built operational dashboards provide immediate insight into: authentication success and failure trends, device permission blockers, device hardware, device operating system versions, mSign app version adoption, biometric versus PIN user preferences, runtime protection events, device migration history, authentication session analytics, and fleet planning and lifecycle management. Because Concierge understands the semantics of enterprise mobile authentication, organisations receive meaningful operational intelligence immediately without complex telemetry configuration or custom dashboard development.

Generic APM Platforms

Infrastructure Visibility

Designed to answer:
"Is my application healthy?"

- ✓ CPU
- ✓ Memory
- ✓ Network
- ✓ HTTP
- ✓ Database
- ✓ API Response Times
- ✓ Server Availability

Salt mSign Advanced

Authentication Visibility

Designed to answer:
"Is my authentication fleet healthy?"

- ✓ Device details
- ✓ Biometric adoption
- ✓ Token lifecycle visibility
- ✓ Authentication methods
- ✓ Mobile App permissions
- ✓ Runtime protection events
- ✓ Authentication session history
- ✓ Profile history
- ✓ Operating system adoption
- ✓ Mobile App versions

Both are important. They solve completely different problems.

Enterprise monitoring platforms provide excellent visibility into servers, applications, databases and networks. However, they lose visibility at the point authentication leaves the data centre and enters the user's mobile device. For modern mobile authentication deployments, that last mile is where operational uncertainty begins.

Salt mSign Advanced closes this visibility gap by continuously collecting authentication-specific telemetry directly from deployed mobile authenticators, giving operations teams real-time insight into the health, behaviour and lifecycle of their authentication fleet.

Enterprise Mobile MFA Should Deliver More Than Authentication

High-assurance authentication is no longer sufficient on its own. As enterprise mobile authentication deployments continue to expand, organisations require the same level of operational visibility that they expect from every other mission-critical business system.

Salt mSign Advanced bridges this gap by combining enterprise-grade mobile transaction authentication with purpose-built operational intelligence.

The result is a solution that not only authenticates transactions and user identities with confidence, but also enables organisations to understand, optimise and continuously improve the health of their authentication environment throughout its operational lifecycle.

Operational Intelligence That Drives Action

Visibility has limited value unless it enables organisations to make faster, better-informed decisions. Concierge continuously receives operational telemetry directly from deployed Salt mSign mobile authenticators, giving security, operations and product teams an enterprise-wide view of how their authentication fleet is behaving in the field. Rather than relying solely on authentication success and failure logs, teams can identify emerging issues, determine which users and devices are affected, investigate their cause and take informed action before isolated problems develop into widespread service incidents. This changes mobile authentication management from a largely reactive process into a proactive operational capability.

Identify Issues Before They Escalate — Mobile operating systems, device configurations and application permissions change continuously. An issue affecting a particular operating system release, device model or application version may initially appear as a handful of unrelated support incidents. Salt mSign Advanced enables operations teams to correlate these events across the authentication fleet, identify common characteristics and determine the scope of an emerging issue. Instead of waiting for helpdesk volumes to reveal a problem, administrators can understand which users and devices are affected and respond proactively.

Accelerate Support and Incident Resolution — Authentication failures can have many causes outside the authentication platform itself. Push permissions may have changed, a user may have migrated to another device, an operating system update may have altered behaviour, or a particular device and application combination may be experiencing an issue. By providing historical device, profile and authentication context, Salt mSign Advanced gives support teams the information required to investigate these issues without relying entirely on the user to describe their device configuration or authentication history. This reduces investigation time, improves first-call resolution and allows complex issues to be escalated with substantially more diagnostic information.

Plan Change with Greater Confidence — Mobile environments never remain static. New operating system releases, application versions and device generations continuously change the composition of an enterprise authentication fleet. Salt mSign Advanced provides visibility into operating system adoption, application versions, device distribution and authentication behaviour across the deployed population. Product and operations teams can use this intelligence to understand the potential impact of changes, identify affected populations and plan application or operating system transitions with greater confidence.

Strengthen Security and Forensic Investigation — Operational telemetry also provides valuable context during security and fraud investigations. Security teams can examine authentication timelines, device history, profile migrations, authentication methods and runtime security events to reconstruct how authentication activity developed over time. Rather than examining an authentication event in isolation, investigators can understand the wider device and user context surrounding it. This provides a richer operational picture when investigating anomalous authentication activity, suspected account compromise or unusual device behaviour.

Designed for Enterprise Scale — Whether supporting thousands of employees or millions of customers, Salt mSign Advanced provides a consistent operational view across the deployed authentication fleet. Administrators can move from an individual user or authentication session to organisation-wide deployment trends without building custom telemetry pipelines, reporting infrastructure or authentication-specific dashboards.

Enterprise Mobile Authentication Without the Blind Spot

High-assurance mobile authentication protects the transaction. Salt mSign Advanced extends that assurance into the operational environment surrounding it. By combining the proven transaction authentication capabilities of Safetronic and Salt mSign with Concierge operational intelligence, organisations gain visibility beyond the authentication decision and into the real-world behaviour of their deployed mobile authentication fleet. Security, operations and product teams can understand how authentication is being used, identify emerging issues, investigate individual events, assess the impact of technology changes and continuously improve the authentication service delivered to users. For organisations protecting high-value transactions at enterprise scale, this delivers a more complete approach to mobile authentication—one where strong authentication and operational visibility are part of the same solution.

Salt mSign Advanced extends high-assurance mobile authentication beyond the authentication decision itself. It enables organisations to authenticate users and transactions with confidence, understand what is happening across the deployed authentication fleet, and act on that intelligence to improve service availability, user support, security operations and long-term authentication planning.

Authenticate. Understand. Act.

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