

SALINA: Rethinking Password-less Multi-Factor Authentication (MFA)

Introduction

The surge in data breaches, insider threats, and sophisticated cyberattacks has placed identity management under intense scrutiny. Weak passwords remain a prime target for hackers, driving organizations to seek stronger credential protection without compromising usability.

A key pain point remains at the individual user level—employees are often overwhelmed by the sheer number of passwords they must create, remember, and securely store. Many revert to poor practices such as reusing passwords, writing them down on sticky notes, or saving them in unsecured digital files. This not only increases the risk of compromise but also creates friction and frustration in day-to-day business operations.



Additionally, password resets and recovery processes significantly increase the total cost of ownership for IT departments—generating help desk tickets, administrative overhead, and delays in productivity. By eliminating the need for traditional passwords, SALINA removes this operational burden, resulting in tangible cost savings and improved user experience.

Therefore, any next-generation IAM solution must address this fundamental usability challenge while offering stronger protections behind the scenes.

What sets SALINA apart is that it delivers the benefits of passwordless MFA while remaining fully compatible with password-dependent infrastructures—such as systems that require passwords for compliance, user authentication fallback, or legacy application integration




To address these challenges, QuantumGate has introduced SALINA, a passwordless MFA solution that ensures **passwords are never exposed — not even to SALINA itself — and cannot be reverse-engineered from stored or transmitted data.**

At the core of this innovation is Oblivious Pseudorandom Functions (OPRFs), an advanced cryptographic technique that enables functions over blinded inputs.

Additionally, SALINA's credential system leverages Multi-Party Computation (MPC), eliminating single points of failure and significantly reducing the risk of user impersonation due to centralized breaches or insider threats.

Going a step further, SALINA integrates a zero-trust approach to support private services. It integrates Anonymous Credentials (ACs), enabling authentication for privacy-sensitive applications such as whistleblower platforms and confidential data access.

Most password management solutions rely on encrypted vaults — centralized databases that store passwords. Even many passwordless MFA solutions ultimately depend on stored passwords to support legacy systems.



Help desk tickets due to forgotten passwords account for a large share of IT support costs. By removing passwords entirely, SALINA eliminates password reset calls, reduces downtime, and cuts administrative overhead — delivering measurable savings.

This white paper explores how SALINA tackles today's identity challenges, delves into the mechanics of OPRF and MPC, and highlights why AC systems will be essential for the next generation of identity and access management (IAM) solutions.



The Password Lockbox Model: OPRF in Action

SALINA's Lockbox model addresses the fundamental weakness of traditional password storage: the existence of a single repository or server process where enough information exists to reconstruct user passwords. Instead, SALINA disperses the process of password derivation through Oblivious Pseudorandom Functions (OPRFs). Though OPRFs are well-known in academic and specialized cryptographic circles, SALINA's innovation lies in making them practical at scale for enterprise IAM.

An OPRF is a cryptographic function that allows a client (the user) to obtain an output from a server without revealing the input. The input is blinded, processed by the server, and unblinded by the client to recover the result.

Even if attackers compromise the SALINA infrastructure, they cannot reverse-engineer the password due to the blinded input and server-side secrets. SALINA ensures that no single party ever sees the full picture.

In SALINA's Lockbox model, the user holds a secret value in its keychain that is "blinded" on the user side by combining it with some random data. This blinded version is then sent to SALINA's authentication server, which after successful user authentication, applies the pseudorandom function with its own secret input. Because the client's input is blinded, the server cannot learn its actual value. It only operates on scrambled data. The server responds with a transformed output, which the client "unblinds" to derive the password—without ever revealing the real password to SALINA authentication service. This approach renders offline cracking nearly impossible for an attacker, because even if an attacker infiltrates SALINA's infrastructure, the data extracted is insufficient to reconstruct passwords. Similarly to the user password derivation flow, SALINA is able to sync with Active Directory to update the users' passwords without seeing those passwords.

SALINA's OPRF was engineered with performance optimizations to ensure that the OPRF does not introduce noticeable latencies for the end-user. The solution easily integrates with existing directory services, SAML/OIDC-based single sign-on (SSO), and multi-factor authentication flows. It also integrates with password-free protocol flows for Windows and MacOS login. Businesses can phase in SALINA's Lockbox model gradually—initially deploying it for high-privilege accounts and then expanding to the entire user base.

SALINA's OPRF system is optimized for performance and integrates with Active Directory, SAML/OIDC-based SSO, and supports login for Windows and macOS. Organizations can start by deploying it for privileged accounts and expand gradually.

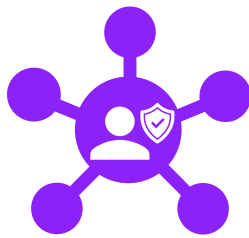
Private Accounts: Anonymous Credentials in action

Private authentication has become a crucial requirement in modern Identity and Access Management (IAM) systems. Emerging services that demand privacy—such as whistleblower platforms, feedback systems, and confidential data access—highlight the need for secure IAM solutions that preserve user anonymity. Traditionally, corporate services requiring anonymous access have relied on trust—users must trust that their interactions, reports, or data access will remain anonymous throughout the service lifecycle. However, stronger privacy guarantees are necessary to drive seamless adoption of confidential services.

SALINA is at the forefront of IAM innovation, integrating an Anonymous Credential (AC) system that enables authentication while safeguarding identity privacy.



ACs allow users to access anonymous services through unlinkable pseudonyms, i.e. pseudo-identities. Users can generate multiple pseudonyms, ensuring that all activities within confidential corporate services remain untraceable. At the same time, organizations can authenticate users anonymously, ensuring that only legitimate users gain access—preventing impersonation and Sybil attacks.



Decentralized Credential protection: MPC in Action

Passwordless authentication typically relies on credentials, keys, or passkeys stored on the user's device, enabling authentication via a mobile app, hardware device, or browser extension. These secret keys are generated and managed by the user, ensuring no other entity has access to them, thus preventing impersonation. However, in corporate environments, a more controlled credential management approach is often desirable.

To address this, SALINA leverages Secure Multi-Party Computation (MPC) to generate and back up key material securely. MPC distributes the credential generation process across multiple servers or entities, ensuring no single point of compromise. Within SALINA's architecture, several distributed components each hold partial cryptographic keys. When a user enrolls, these components collaboratively generate the credentials without revealing their individual secret shares to one another. As a result, even if one server is compromised, it cannot reconstruct the full credential set.

Centralized storage creates a single point of failure—if breached, all user credentials may be compromised. SALINA's distributed model ensures no one party ever has enough information to reconstruct the credentials.



This approach allows organizations to maintain control over credential generation and backups while ensuring that only the user ever holds the complete secret. There is no centralized vault storing user credentials—eliminating a single target for attackers or malicious insiders. In practice, this system is both highly secure and remarkably efficient.

SALINA's Multi-Party Computation system is also a fundamental part to ensure anonymous credential generation to grant private access while maintaining full privacy compliance. This ensures organizations can enforce authentication policies without ever compromising user anonymity.

Multiple SALINA components each hold a share of a secret. When generating credentials, they collaboratively compute without revealing their shares. If one server is compromised, it cannot recreate the secret.



SALINA Use Cases

The SALINA mobile app enables passkey creation and login, supports BLE and FIDO2-compliant devices, and offers a seamless experience across Windows and macOS. Admins can enforce policies for onboarding, backup, and revocation.

With SALINA, whistleblowers authenticate anonymously while proving legitimate access. The system meets EU and SOX whistleblower regulations without maintaining audit trails that could reveal identities.

SALINA's Lockbox solution, powered by OPRFs and MPC, is a flexible, scalable approach that can be tailored to meet the security demands of various industries. It effectively bridges the gap between legacy systems that rely on traditional password or nickname authentication and more modern software services. SALINA is equipped to handle password management for legacy systems, Single Sign-On (SSO) for web services, password-free access for Windows and macOS, and even provides dedicated APIs for seamless software integrations.

From the moment a new user is onboarded, SALINA automatically generates the necessary passwords and updates internal corporate systems. Once set up, users can securely access all services through SALINA's mobile authenticator app. The app, compliant with FIDO standards, allows users to generate their own passkeys and is compatible with Yubikeys and Bluetooth Low Energy (BLE) devices. For scenarios demanding higher levels of authentication, where credential generation and backup cannot be delegated to users, SALINA offers a distributed credential generation model for added security.

Moreover, for organizations that support internal whistleblower programs, SALINA ensures a secure and anonymous reporting mechanism. Employees can report misconduct without fear of retaliation while still verifying their status as legitimate corporate users. With SALINA's Lockbox, whistleblowers authenticate privately, ensuring their true identities are never exposed to the system. This enables anonymous yet verifiable access, meeting key regulatory requirements such as the EU Whistleblower Directive and the Sarbanes-Oxley Act (SOX), all while eliminating the risks associated with centralized authentication logs or forensic tracking.

Conclusion



In a landscape where credential theft remains a leading cause of data breaches, SALINA delivers a fundamentally different approach to IAM, redefining how passwords are derived, stored, and verified. By harnessing OPRF to blind passwords and employing MPC to distribute cryptographic operations across multiple servers, SALINA's system ensures that passwords and credentials are protected at every stage—even against insider threats and advanced external attackers. This zero-trust methodology goes beyond incremental improvements, offering a transformative framework for how organizations handle their most sensitive information.

As industry regulations tighten and attackers become more resourceful, the benefits of a robust, cryptographically grounded IAM solution are not only about reducing risk but also about staying competitive in an environment that demands resilience and trustworthiness. With proven deployments in healthcare, education and defense, SALINA stands as a frontrunner in the next generation of password-less authentication—one where neither the provider nor the attacker can see or steal the keys that protect an organization's data. Adopting SALINA is not just about upgrading security and privacy; it's about embracing a fundamentally new standard that may well define the future of IAM.

For further details on how the Lockbox model can be implemented within your organization, including proof-of-concept trials and custom integration guidance, please reach out to the QuantumGate team. We look forward to hearing from you



 quantumgate.ae

 contact@quantumgate.ae