1KOSMOS

Charting an Enterprise Passwordless Authentication Strategy with Entra ID

Adding Verified Identity to Entra ID and Extending Passwordless Multifactor Authentication to All Apps and Environments

Whitepaper

Executive Summary

Organizations moving from Active Directory to Entra ID gain many advantages, including unified identity management, enhanced security features such as conditional access, and improved integration to cloud-based apps.

However, support for identity verification is still lacking. IT Support Desks still struggle with heavy workloads to rapidly onboard users at scale. And passwordless access for apps and environments outside the scope of Windows 11 is missing. This includes Mac, iOS, Android, Linux, and Unix as well as legacy Windows OS, VPNs, and niche cases such as domain controllers and virtual machines.

This leaves organizations vulnerable to identity-based attacks, and users clumsily cycling passwords and juggling multiple authenticators across disparate systems. The result: hundreds of millions in losses rooted in social engineering attacks (most recently targeting the Service Desk) and millions more in wasteful spending on administrative overhead.

Onboarding users at scale is still an administration-heavy process because IT Service Desks lack tools for remote identity verification and account and password recovery.

1Kosmos provides high-assurance identity verification, passwordless MFA, and a universal authenticator to enhance Entra ID for improved cybersecurity and user convenience.

Through self-service workflows that are easily tailored to different use cases and levels of risk, 1Kosmos serves as an onramp for users to Entra ID, reducing administration overhead related to new account origination and account recovery/password reset.

A standards-based architecture, off-the-shelf APIs, and software development kit enable 1Kosmos to be easily embedded into mobile apps and integrated into legacy systems for convenient, passwordless access to systems not supported by Entra ID.

What is 1Kosmos?

1Kosmos provides identity verification and passwordless access for all systems, not simply a siloed approach for the most modern ones. Around a dozen identity verification mechanisms can be deployed to tune assurance levels for various types of users, use cases, and levels of risk. This helps stop social engineering and phishing attacks at the source.

By replacing passwords with verified digital identities and hardened, live biometrics, 1Kosmos shifts the traditional balancing act between security and convenience.

Through a privacy-by-design architecture based on a private, permissioned distributed ledger 1Kosmos eliminates centralized user stores or "honeypots," and all administrative access to user personal identifiable information (PII).

This gives users sole access and control over their information and sets up permission-based sharing of that information with online services at the point of access. If an administration account gets compromised, there is no risk of a PII breach. It also sets up an immutable record of every update and access attempt, creating tamper-evident identity and verified credentials.

As an artifact of identity verification, 1Kosmos creates a passwordless MFA (Multi-Factor Authentication) credential that is certified to multiple industry standards, including FIDO, NIST 800-63-3, UK DIATF IDSP & ASP, and iBeta ISO/IEC 30107-3. This ensures against AI presentation and injection attacks, giving users an exit from old-fashioned codes and security keys to a consistent passwordless login experience for Active Directory, Windows, Mac, iOS, Android, Linux, Unix, and most legacy systems.

By replacing passwords with verified digital identities and hardened, live biometrics, 1Kosmos shifts the traditional balancing act between security and convenience. It gives IT (Information Technology) and Security teams the flexibility to adjust identity assurance levels for different users and systems based on business needs without adding significant friction to the user experience.

Why 1Kosmos?

1Kosmos solves the Trust on First Use or "TOFU" problem which happens when users transition to new systems and must provide a username and password. This is a problem because the user's identity cannot be known with high assurance any time a password is leveraged.

The outdated but familiar approach also creates a complicated and costly mix of people, processes, and IAM (Identity & Access Management) technology to support a perpetual cat-and-mouse game with red versus blue teams vying to prevent and gain access to knowledge, inherence, and possession factors.

This leaves organizations reeling from social engineering, phishing, and deepfake attacks. Hackers have become adept at push bombing and SIM swaps to defeat MFA.

The idea behind 1Kosmos is to:

One.

Create a durable and tamper-evident digital identity replacing the user ID and password

Two.

Make this identity as private and independent as the users themselves

Three.

Use the attributes that comprise the digital identity to authenticate the individual into online service

Instead of relying on usernames and passwords, 1Kosmos creates a durable artifact at enrollment using Decentralized Identity (DCI)—a unique identifier and digital wallet for the user.

It has several unique characteristics and advantages:

1. **Public-Private Key Encryption** ensures all data related to an identity remains confidential, tamper-proof, and accessible only upon user consent.
2. **Decentralized Private Ledger (i.e., Blockchain)** shards and stores data, eliminating user data lakes and creating a transparent immutable log where every entry is time-stamped and linked to ensure and prove data integrity (i.e., tamper evidence).
3. **W3C Verifiable Credentials (VCs)** which are verified digital attestations about a holder such as a qualification, certification, level of authority, etc

4. **Smart Rules and Protocols** manage data and enable peer-to-peer network interactions without human administration. Backed by W3C-DID and W3C-VC standards, this enables automated, intelligent workflows and privacy-preserving sharing of user information after consent is obtained.

5. **Identity-Backed Biometrics** certified against deepfake presentation and injection attacks (ISO/IEC 30107-3) and verified to various levels of identity assurance up to NIST (National Institute of Standards and Technology) Identity and Authentication Assurance Level 2 (IAL2 / AAL2) by Kantara.

6. **Off-the-Shelf APIs and a Software Development Kit (SDK)** to connect with any system or easily embed into mobile apps.

7. **Flexible Deployment Options** to ensure broad coverage for technologies and user cases. This includes over 50 out of the box connectors and an API framework to provide passwordless security for more use cases beyond Entra coverage up to and including on-prem active directory.

How Does 1Kosmos Enhance Microsoft Entra ID?

Self-Service User Onboarding and Verified Identity

With 1Kosmos, organizations can digitally transform user onboarding with convenient self-service identity verification into Entra ID. Through self-service enrollment, users can remotely verify their identity and complete new account origination with minimal manual reviews. This can involve any of the familiar mechanisms (e.g., physical keys, OTPs, smart links) or can accommodate the highest levels of remote identity verification recognized by NIST (i.e., IAL2) by using government-issued documents and live biometrics.

Organizations can easily configure custom user journeys to include automatic validation of government-issued documents, significantly reducing the risk of synthetic identities, stolen identities and identity impersonation as is common, for example, in contractor hijacking.

Upon successful verification, users are provided with a digital wallet that securely stores their identity information and credentials. Most importantly, the verified identity is bound to the user and creates an identity-based biometric authentication, enabling a modern, convenient passwordless experience. This comprehensive approach ensures a high degree of identity assurance for the verified user while maintaining a user-friendly onboarding process.

By integrating 1Kosmos self-service onboarding with Entra ID, organizations can:

- Rapidly onboard new employees, partners and contractors at scale
- Eliminate manual reviews and administration by HR, IT Operations, and Service Desk
- Enhance security by verifying user identities before granting access
- Deploy an identity verification, authentication and data retention certified platform

Passwordless Access for Unsupported Environments

While Entra ID is effective for Microsoft-centric environments, 1Kosmos provides a consistent passwordless experience across legacy on-premises technologies, Active Directory, and various operating systems, including Windows, Mac, iOS, Android, Linux, and Unix - plus, coverage for VPN, PAM, virtual machines, and servers. This extends passwordless authentication capabilities beyond Microsoft Entra ID and significantly reduces the number of authenticators required to support daily user activities.

With the addition of 1Kosmos, organizations can deploy any of the 12 authentication methods, including a phishing-resistant biometric – LiveID, and 1Kosmos 1Key (a biometric security key), plus device biometrics, push message, email/SMS/Token, 3rd party hardware token and more. These can be deployed depending on the business need, the risk profile of the activity, and the security requirement for each access request.

By integrating 1Kosmos into Entra ID, organizations can:

- Provide a consistent user authentication experience across disparate systems
- Deliver passwordless authentication, reducing the risk of password-related vulnerabilities
- Utilize biometric authentication, delivering high identity assurance
- Support MFA login by default with FIDO-compliant authentication methods
- Match authentication methods to activity risk
- Manage users with multiple accounts, for example, those with user accounts, admin accounts, and privilege accounts

Password Resets and Account Recovery with Live Biometrics

A limitation to Microsoft Entra ID, even in a passwordless approach, is the username and password requirement. For instance, enrolling in Microsoft Authenticator and Windows Hello for Business requires the user to enter their username and password. The issue when going passwordless is - users will forget their passwords when needing to transition to a new device or accessing infrequently used applications and services, locking users out of their accounts and requiring time consuming support requests.

The issue when going passwordless is - users will forget their passwords when needing to transition to a new device or accessing infrequently used applications and services, locking users out of their accounts and requiring time consuming support requests.

1Kosmos addresses common password-related challenges, even in a Microsoft Entra ID environment, with an integrated solution for secure password resets and account recovery. The reset password feature allows users to reset an account with their mobile device and live biometrics. With this capability, users can reset their password for Entra ID, on-premise Active Directory, or any other account for those rare occasions when they need to use it, such as enrolling Windows Hello for Business on a new system or accessing systems that have not been migrated to a passwordless experience. This approach reduces Service Desk burden, minimizes user disruption, and maintains strong security standards.

For instances where help desk and service desk support is required, 1Kosmos offers a high assurance identity verification process where agents initiate a secure session via the user's phone or email. Once the caller's identity is verified, via an ID and live biometric check, the agent can safely proceed with password resets or account recovery, maintaining high identity assurance throughout the process.

By integrating 1Kosmos Password Resets and Account Recovery with Live Biometrics into Entra ID, organizations can:

- Deliver self-service account and password recovery options reducing dependency on IT support or VPN access
- Reduce IT Service Desk workload
- Provide self-service identity verification for users with multiple accounts
- Ensure high identity assurance levels for the legitimacy of the credential reset request
- Provide users a consistent passwordless user experience

Extending Passwordless to Restricted Environments

The 1Kosmos platform provides passwordless deployments in diverse environments like call centers, manufacturing floors, kiosks, clean rooms, SCIFs (Sensitive Compartmented Information Facilities), kiosks, shared workstations, and healthcare facilities where multiple users may login to the same device.

These use cases do not allow mobile devices, preventing organizations from deploying Microsoft Authenticator, and due to the limitation of the number of enrolled users per device and lack of support for desk "hoteling," Windows Hello for Business can be rendered unsuitable.

The 1Kosmos 1Key biometric security key supports multiple users per device with one-to-one, one-to-many, or many-to-one configurations. One device can support multiple logins while maintaining individual accountability.

The approach is simple – install the 1Kosmos 1Key on the protected device, providing a biometric passwordless login for any user onboarded within the control plane. Users register once and can then authenticate on any device.

IT and security teams can continue to leverage conditional access policies in Entra ID while leaving the authentication to 1Kosmos. This approach also contains costs because users do not need their own keys, so fewer keys and replacements are needed. It also prevents security vulnerability from unauthorized key sharing

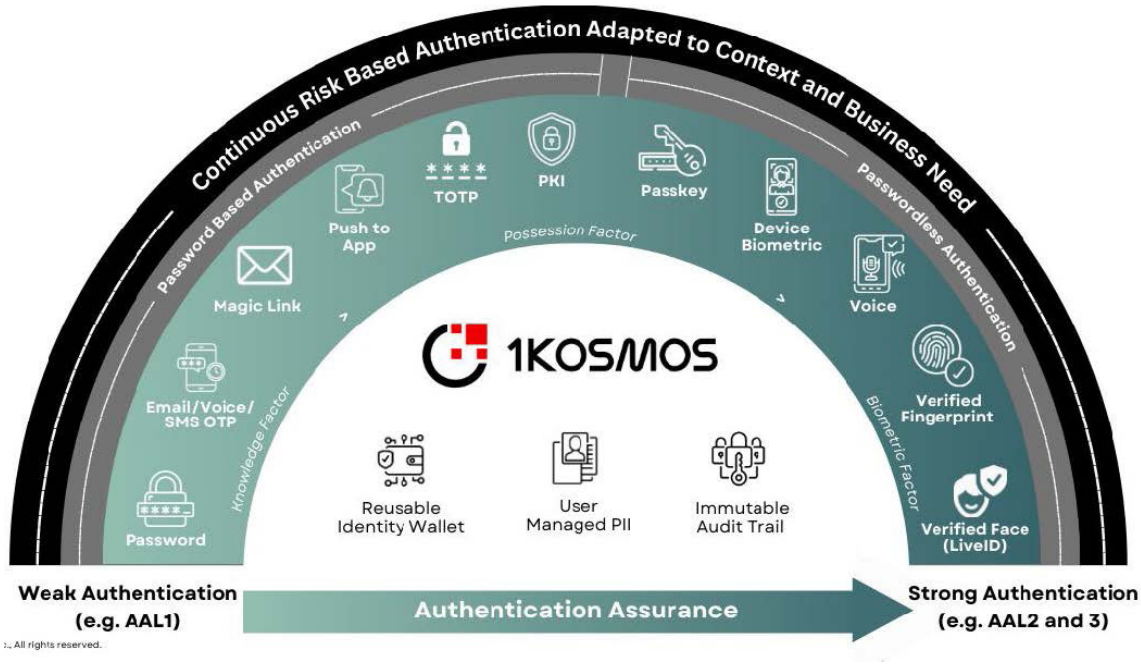
By integrating the 1Kosmos 1Key Biometric Security Key into Entra ID, organizations can:

- Deliver passwordless authentication to restricted areas
- Reduce the risk of password-related vulnerabilities
- Utilize biometric authentication with high identity assurance
- Support MFA login by default with a FIDO-compliant authentication method
- Reduce cost with a register-once-use-anywhere, workstation independent strategy
- Simplify management as users will no longer be required to carry an assigned authenticator

1Kosmos as an Entra ID External Authentication Method (EAM)

Microsoft's External Authentication Method (EAM) is a new feature in Microsoft Entra ID that allows organizations to satisfy multifactor authentication (MFA) requirements using external providers, and not rely on native Microsoft authenticators. Organizations can deploy 1Kosmos and, therefore, utilize verified identity and passwordless multi-factor authentication (MFA) for every login.

The 1Kosmos platform offers flexible authentication options with 11 different authentication methods through which organizations can match conditional access policies and tailor to risk levels.



These same methods can be deployed to environments not natively supported by Entra ID, such as legacy on-premises technologies and various operating systems, ensuring a consistent login experience no matter the platform, application, or service. This will also benefit security teams as this integration will significantly reduce the number of authenticators required for day-to-day business.

By integrating the 1Kosmos as an EAM to Entra ID, organizations can:

- Improve user experience across systems
- Continue to leverage conditional access policies
- Match authenticator to activity risk
- Reduce management cost by eliminating additional authenticators

Interoperability

Interoperability and extensibility are key features of 1Kosmos, which gives organizations using Entra ID a safe and secure way to get new users and new organizations rapid access to digital services. Out of the box, 1Kosmos comes with over 50 connectors, an open API framework, and a flexible SDK.

The integration of 1Kosmos with Microsoft Entra ID offers organizations a solution to prevent identity-based attacks while facilitating convenient passwordless authentication across disparate IT systems.

This allows for rapid integration with Entra ID and all other technologies and legacy systems that fall out of scope for Entra ID passwordless, plus easy embedding of 1Kosmos into mobile apps.

Our solution also provides authentication resiliency and interoperability, where organizations can deploy 1Kosmos as the primary authenticator and leverage Microsoft Authenticator as a backup.

By leveraging the 1Kosmos interoperability capabilities in conjunction with Entra ID, organizations can:

- Improve coverage across a wide variety of applications and services
- Swap underlying technologies without impacting the authentication user experience
- Improve user experience with a consistent passwordless experience
- Provide a consistent, passwordless authentication experience across systems
- Continue to leverage conditional access policies

Conclusion

The integration of 1Kosmos with Microsoft Entra ID offers organizations a solution to prevent identity-based attacks while facilitating convenient passwordless authentication across disparate IT systems. As discussed, the combination of 1Kosmos and Entra ID addresses critical security gaps, preserving the Entra ID investment while improving user experience across diverse environments.

1Kosmos + Microsoft Entra ID Highlights:

- Streamlined self-service user onboarding and identity verification: reducing administrative overhead, so security teams can leverage verified identities for authentication, password resets, and account recovery.
- Extended passwordless authentication beyond Microsoft Entra ID: covering legacy systems, various operating systems, and critical infrastructure – VPN, PAM, virtual machines, and more.
- Secure password reset and account recovery options using live biometrics: minimizing IT support costs while providing user convenience and maintaining high identity assurance.
- Provide passwordless access for edge use cases: extending passwordless to eliminate identity-based attacks for one-to-many and many-to-one use cases.
- Flexible authentication methods: tailored to risk levels, ensuring consistent login experiences across all platforms and applications with minimal transaction friction.
- Improved interoperability: with systems through numerous out-of-the-box connectors and industry-standard protocols including 1Kosmos as an EAM via WS Fed and WS-Trust.

This integration delivers high identity assurance, self-service identity verification, and a passwordless approach to cover all use cases. The result is a safe and efficient way to onboard, authenticate, and verify new and existing users for access to digital services, password resets, and account recovery requests.

As cyber threats continue to evolve, this combined approach offers a flexible forward-thinking solution that improves the balance between security requirements and user convenience, making the combination an invaluable asset for security teams looking to eliminate identity-based attacks and minimize non-value-added administrative overhead related to user onboarding and account / password recovery.

About 1Kosmos
1Kosmos enables remote identity verification and passwordless multi-factor authentication for workers, customers and residents to securely transact with digital services. By unifying identity proofing, credential verification and strong authentication, the 1Kosmos platform prevents identity impersonation, account takeover and fraud while delivering frictionless user experiences and preserving the privacy of users' personal information. 1Kosmos performs millions of authentications daily for government agencies and some of the largest banks, telecommunications, higher education, and healthcare organizations in the world.

1KOSMOS