1KOSMOS

Secure Your Distributed Workforce: Go Passwordless

The Future of Authentication is Here

Whitepaper

Password Management Unveils Three Groups of Employees

First.

Employees who have no problem remembering different usernames and passwords.

Second.

Employees that give it three tries before they're locked out and start harassing the help desk.

Third.

Employees who choose to rely on the good old post-it note they stick on their monitor, openly and publicly.

And to make matters worse...

IT departments require employees to choose complex formats for their passwords: between 8 and 16 characters long with at least 1 uppercase letter, 1 number, and/or 1 special character. IT also requires that it be changed every 30 or 60 days. For many employees, those requirements, compounded by the number of systems they must access to do their job, can be overwhelming... hence the infamous post-it notes.

This ecosystem creates inefficiencies such as loss of productivity and increased costs. Did you know, for example, that replacing one password can cost up to $70? Yes, that's what it can cost in human capital and machine resources to handle one password reset request.

2FA to the Workforce Rescue?

3 Reasons Why 2FA Solutions Are Vulnerable:

Passwords, the first authentication factor, can be stolen or lost. Second factors such as one-time emails, texts or tokens can also be intercepted or coerced from end-users and also result in a poor user experience. It is the same issue with a security key that can also be forgotten inside the pocket of a pair of jeans and run through the laundry. There are 2FA solutions that use device-based biometrics as a second factor of authentication. But Touch ID and Face ID do not prove a user's identity.

The lack of pertinence, in terms of security, is magnified, when an employee finds himself locked out of an app after losing a factor. Believe it or not, but this employee actually finds himself in the very same position as a hacker, who's trying to gain access to the employee's account. If an account can be reset without an access factor, then a hacker can, too. However, without recovery options, the employee account may be lost forever. To meditate...

Finally, hackers are seasoned criminals. For example, they can set up or reconfigure two-factor authentication to keep the real account holder out of his or her own accounts.

MFA to Plug the Holes?

Replacing 2 with M doesn't necessarily cut it:

MFA solutions are definitely more robust, in terms of security, than 2FA applications. However, the reality is that they add another level of friction to the user's experience.

Besides the added layer of friction, MFA solutions offer several key limitations. To use mobile SMS code MFA, an employee must carry a mobile phone, charged, and kept in-range of a cellular network, whenever authentication might be necessary.

There are MFA solutions that necessitate a piece of hardware like security keys, and that comes at a cost: Pay for each physical token and allocate resources for the hardware's maintenance.

The smartphone and the security key can be lost or stolen.

MFA solutions give the user a sense of added security, however it remains a false sense of security.

MFA + Biometrics: What Kind?

To mitigate the risk, biometrics have been added into the mix: Touch ID, Face ID, iris recognition, etc.

A login page, a QR code to scan from a mobile application, a biometric-based authentication, and the employee is in. No more username and password required. The mobile phone is something the employee has and the biometric data is something the employee is.

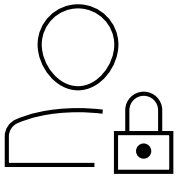
Some levels of biometrics remain ineffective.

Financial Element

Biometric technologies are available commercially in many different forms, but by far the most common devices are fingerprint readers and hand geometry scanners. Now, commercial retina and iris scanners can cost between $2,000 and $10,000, are considered highly invasive by users, and have a slow throughput. Whether fingerprint or iris scanners are required for both physical and logical access, deploying biometrics in the organization is extremely costly.

Biometric Element

Whether it is voice recognition (Voice ID), facial recognition (Face ID), fingerprint scanning (Touch ID) or iris scanning, those types of biometric are falsifiable: Voice can be replicated, fingerprints can be copied, face can be spoofed and iris scanners can be hacked. Biometrics are used by most passwordless solutions is not enough.



Data Storage Element

Most passwordless solutions store their users' biometric data unencrypted inside centralized systems, which are highly prone to cyber attacks.

Compliance With Guidelines Should Mean Something

Per the National Institute of Standards and Technology (NIST), digital identity is the online persona of a subject engaged in an online transaction. Now, accessing a digital service may not mean that the subject's real-life identity is known.

NIST has created the NIST 800-63-3 guidelines to establish 3 levels of assurance for ID-proofing and authentication:

Identity Assurance Levels

IAL1:

There is no requirement to link the applicant to a specific real-life identity.

IAL2:

Evidence supports the real-world existence of the claimed identity and verifies that the applicant is appropriately associated with this real-world identity. IAL3: Physical presence is required for identity proofing (address verification).

Authentication Assurance Levels:

AAL1:

Requires either single-factor or multi-factor authentication using a wide range of available authentication technologies.

AAL2:

Proof of possession and control of two distinct authentication factors is required through secure authentication protocol(s). Approved cryptographic techniques are required at AAL2 and above.

AAL3:

Based on proof of possession of a key through a cryptographic protocol. Authentication must use a hardware-based authenticator and an authenticator that provides verifier impersonation resistance. The same device may fulfill both these requirements. Approved cryptographic techniques are required.

Federated Assurance Levels:

FAL1: IAL1 + Any AAL, IAL2 + AAL1, IAL3 +AAL1 FAL2: IAL2 + AAL2, IAL2 + AAL3, IAL3 + AAL2 FAL3: IAL3 + AAL3

Employee Data: Two Major Storage Issues

Most passwordless solutions store their users' data in such a way that it represents a cybercriminal's dream for 2 main reasons:

Users' data stored unencrypted

Did you know what major organizations are still storing passwords in plain text? Unfortunately, there are multi-billion dollar companies out there that continue to minimize the importance of security. Some actually choose to compromise security in the name of (financial) convenience. Others do everything right when storing their employees' password. They might add overzealous logging capabilities, which record passwords in plain text... Encryption is standard during the data transmission process, but many enterprises have failed at implementing the same for information held within their databases. That's a hacker's dream, because they are able to easily use stolen data in its rawest form.

Data storage falls way below what is required to ensure users' data security.

Users' data stored in centralized systems

First, the user of a centralized database has access to four data functions: Create, Read, Update, Delete. Logically, anyone with access credentials can utilize the Create, Update and Delete functions to compromise data. Read is only as good as the data which is read. Then, a centralized system represents a single point of failure. Naturally, the bigger firms which is associated with centralized systems can afford redundancy, but it is inherently expensive.

The 1Kosmos platform fundamentals

Identity Should Be Your Number One Focus At All Times

1Kosmos is the only passwordless solution that verifies a user's identity. 1Kosmos reaches IAL2, AAL2 and FAL2 per the NIST 800-63-3 guidelines, and store users' data encrypted in a decentralized ledger.

Enrolling Your Workforce

During the enrollment process, 1Kosmos creates a credential safe and the private key always stays with the employee.

Enrollment process:

Triangulating a given claim with a multitude of company or government-issued documents as well as sources of truth, including biometrics like a liveness test.

Each enrolled document is validated in the background:

AAMVA for driver's licenses, issuing country for passports.

By enrolling a driver's license and a passport, for example, 1Kosmos validates the employee's first and last name, address, date of birth, and ensure, to the extent possible, that the photos on both documents actually match.

1Kosmos adds an extra source of truth to our ID proofing process:

A liveness test to verify if the biometric traits of an individual are from a living person rather than an artificial or lifeless person.

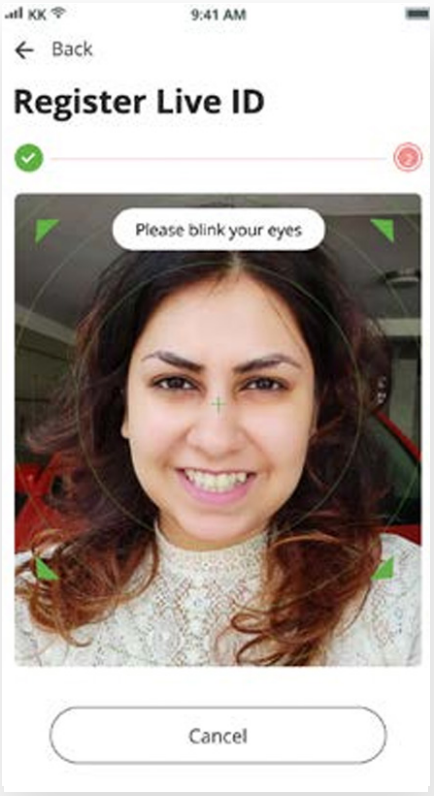
1Kosmos accesses even more sources of validation:

A passport's chip to validate the fact that the passport scanned during the enrollment process matches digitally signed data, for example. or external sources of truth like a credit card, a bank account or a loyalty program.

The 1Kosmos platform fundamentals

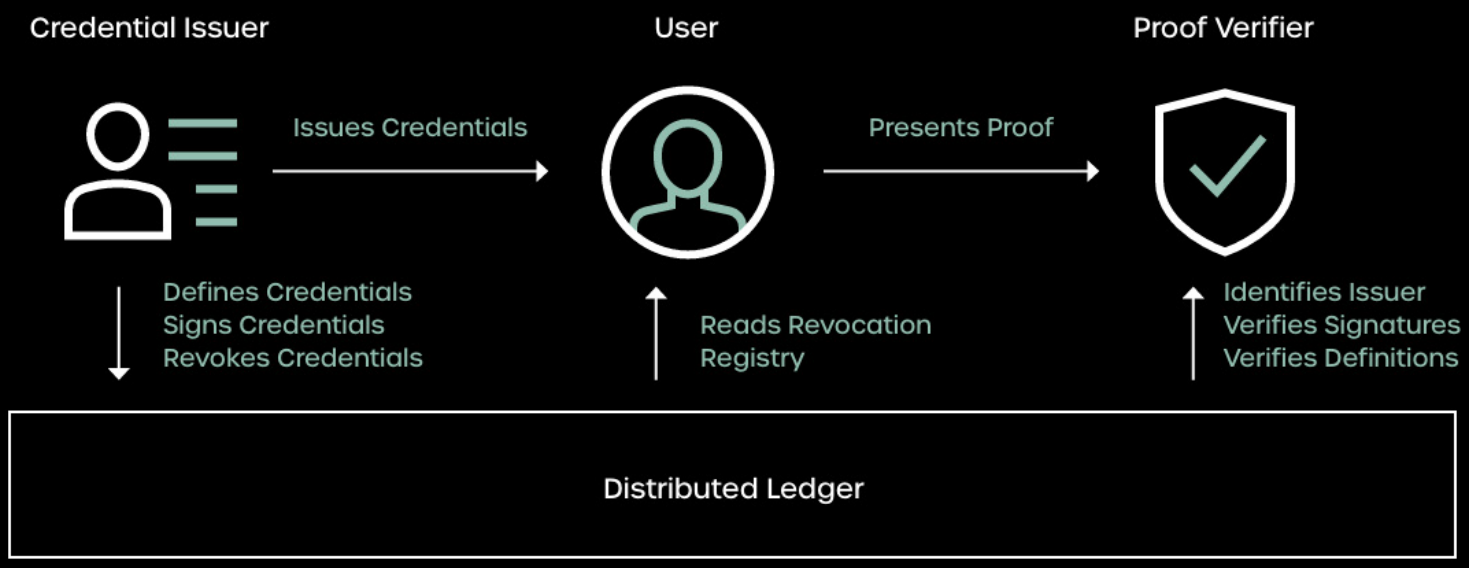
Authenticating Your Workforce

1Kosmos uses advanced, unspoofable biometric authentication as a security process that relies solely on the unique biological characteristics of a user to verify that he is who he says he is.



Authentication process:

A liveness test to eliminate any risk of facial spoofing, which is the task of creating false facial verification by using a photo, video, mask or a different substitute for an authorized person's face.



Including Verifiable Credentials

The verification process leverages the attributes 1Kosmos triangulates during the enrollment phase and digital verifiable credentials employees can share with third-parties and with explicit consent.

Verification process:

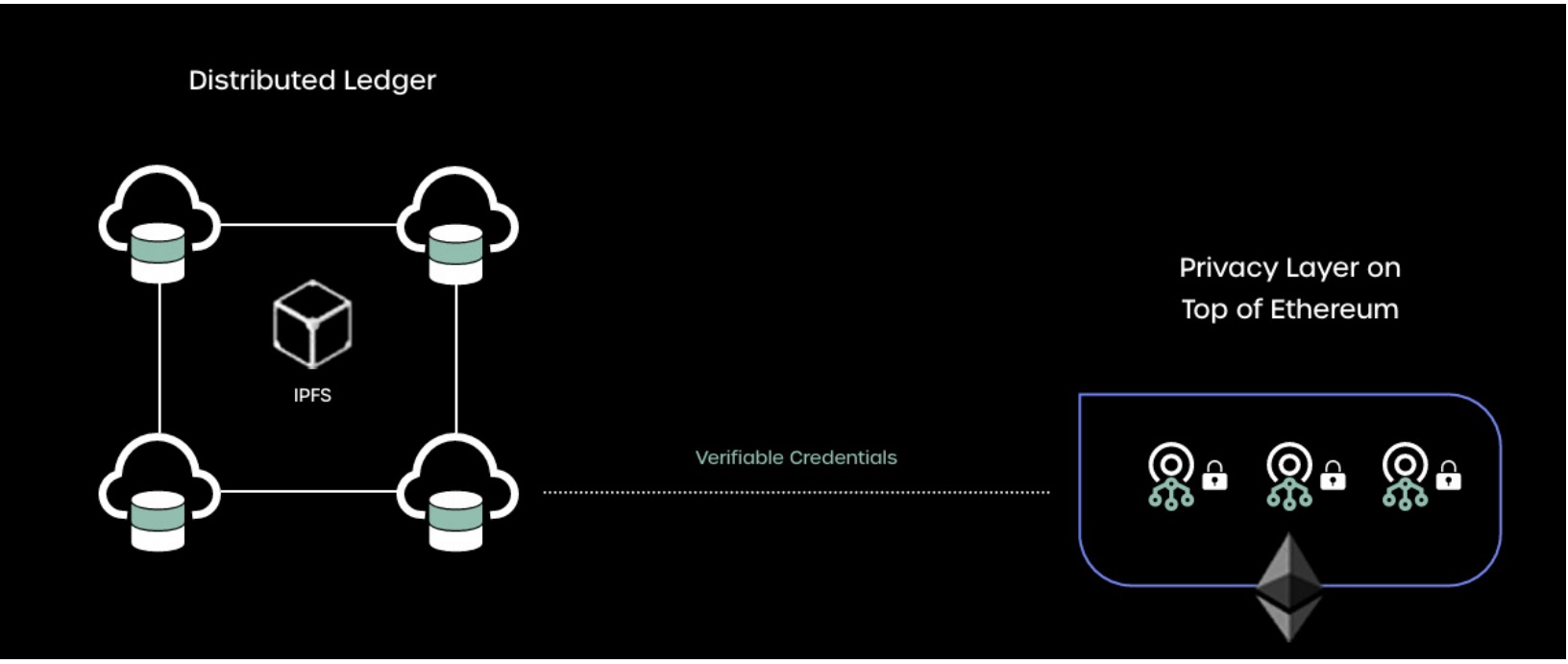
Issuers create verifiable credentials, users can store some of them, and verifiers ask for proof based upon them. When identity needs to be verified, the user chooses those credentials that must be verified. The process involves data the user initially enrolled in the 1Kosmos platform, verifiable credentials in their digital form through API calls, or a mix of both. The attestations that verifiable credentials make are backed by the Decentralized Identifiers (DIDs), a technology that enables verifiable, decentralized digital identity.

Securing Employee Data: The Blockchain Ecosystem

1Kosmos leverages a Distributed Ledger to securely store employees' identity information, with access controlled by the employee (GDPR compliant) as well as a layer of privacy built around Ethereum to execute smart contracts. This is the 1Kosmos Private Blockchain ecosystem.

Each user's information is encrypted using their own unique cryptographic key pairs, with their private key stored securely on their own mobile devices. That means there are literally thousands of separate and unique encryption keys and mobile devices protecting the identity data, which makes it impervious to hacking (W3C compliant).

1Kosmos solutions automatically and seamlessly handle all interactions with the Blockchain — No Blockchain knowledge or expertise is required by anyone on your team to enjoy all of its benefits. It couldn't be any easier.



The 1Kosmos platform is the only passwordless solution to store users' data encrypted in a decentralized ledger.

The 1Kosmos platform reaches FAL2 per the NIST 800-63-3 guidelines. 1Kosmos is also fully W3C compliant.

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