1KOSMOS

Workforce Identity Verification

An Authentication Prerequisite

Password-Based Authentication: The Identity Verification Gap

The staggering statistics that speak for themselves:

Passwords are the weakest form of authentication and do not identify the user who leverages them.

81% **of breaches involve brute force or the user of lost or stolen credential.**

90% **of social engineering attacks are phishing attacks intended to steal users' credentials, including passwords.**

60% **of employees in the U.S. have reported sharing credentials with other employees.**

Passwords are memorized secrets that can be lost, stolen or shared.

For this reason, it is utterly impossible to identity for a fact who is authenticating with a username and a password.

To that effect, passwords only reach the lowest level of identity assurance per the NIST 800-63-3 guidelines, or IAL1. In other words, leveraging a password infers that no user identity evidence is collected in the process.

Identity Service Providers: The Identity Verification Gap

Identity service providers create, maintain, and manage identity information for users and also provide authentication services to relying applications within a federation or distributed network. They bring a level of convenience to employees who needs to access enterprise applications throughout the day to conduct business effectively and without having to enter credentials each time. See it as a "one-click access to all enterprise apps."

Identity service providers are not in the business of proofing the identity of a user

To comply with any level of identity assurance per the NIST 800-63-3 Guidelines is the responsibility of the user. So, what does it mean? The employee who leverages a single sign- on (SSO) platform to access enterprise applications must use a solution that not only verifies in an indisputable fashion his identity but that also integrates with the platform itself. This is why SSO platforms only reach the lowest level of identity assurance per the NIST 800-63-3 guidelines, or IAL1.

When authenticating an employee, SSO platforms do not integrate any details about how the employee can be identified.

Identity service provides that leverage passwords expand the risk of identity compromise

Since there is no certainty about who is on the other side of the communication there is really no security, since there is no way of irrefutably identifying who's truly logging into an SSO platform account. Moreover, the use of a password at any point in time during the authentication process puts the user at risk of being the victim of an identity compromise. After all, 81 percent of data breaches are caused by poor password management. So, password-based single sign-on is a very bad idea.

Identity Service Providers: The Identity Verification Gap

To mitigate the risks of identity compromises and consequently of data breaches, some organizations have eliminated passwords from their authentication processes and gone passwordless.

How truly reliable are passwordless solutions?

To reach the highest levels of identity and authentication assurance to mitigate any risk of identity compromise, passwordless solutions for workforce authentication need to integrate an application that proofs the identity of an employee.

Interestingly enough, when you take a close look at the identity and access management market, you instantly realize that it is extremely siloed. Identity proofing solutions, MFA applications, passwordless solutions, and finally single sign-on platforms operate independently from one another. In other words, those silos do not talk to one another.

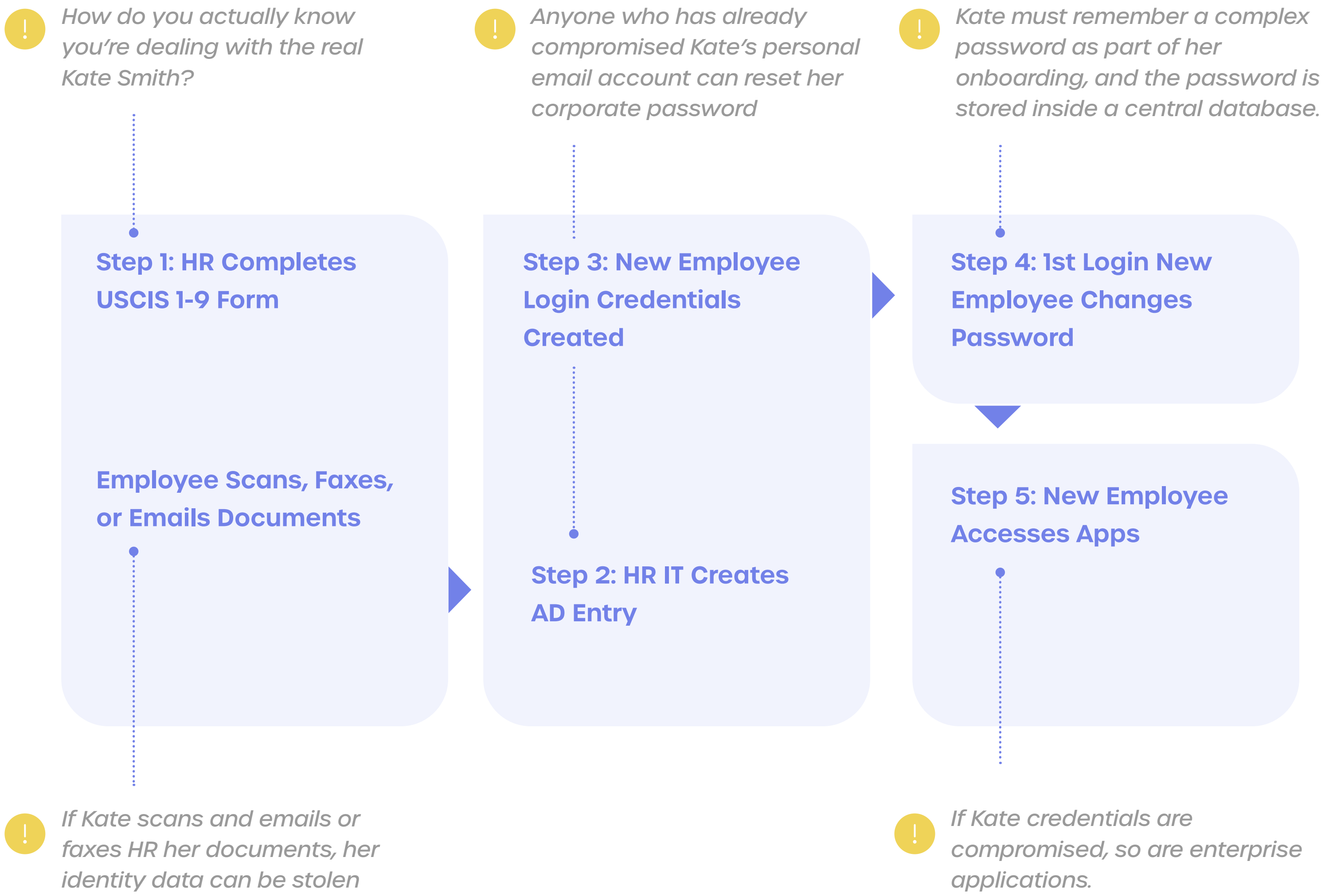
So, as much as password mismanagement related issues are not a concern any longer for a company that has gone passwordless, passwordless authentication is only reliable if, and only if, the process also includes identity proofing.

And a great majority of passwordless authentication solutions do not verify a user identity, which prevents organizations from knowing who is on the other side of the communication, when there is a request to access their systems and enterprise applications.

Most passwordless solutions for workforce authentication, including those that leverage basic user biometrics like Touch ID and Face ID, do not verify the identity of the users.

New Employee Onboarding: The Identity Verification Gap

Risk of identity compromise during the onboarding of a new employee



How do you actually know you're dealing with the real Kate Smith?

Step 1: HR Completes USCIS 1-9 Form

Employee Scans, Faxes, or Emails Documents

If Kate scans and emails or faxes HR her documents, her identity data can be stolen as it travels unencrypted over the Internet or sits in an HR mailbox.

If Kate documents are processed in person, then sensitive PII is being exposed creating a privacy liability for the employer.

Step 2: HR IT Creates AD Entry

Step 3: New Employee Login Credentials Created

Anyone who has already compromised Kate's personal email account can reset her corporate password

Step 4: 1st Login New Employee Changes Password

Kate must remember a complex password as part of her onboarding, and the password is stored inside a central database.

Step 5: New Employe Accesses Apps

If Kate credentials are compromised, so are enterprise applications.

Employee onboarding in the digital age is a true identity security nightmare, which has been compounded with the sharp increase in remote hires since the beginning of the COVID-19 pandemic. The onboarding of a new employee includes key phases, from the verification of the new hire's identity for USCIS compliance purposes to the new employee's first login and corporate password reset, and during this journey there are five main opportunities for identity compromise.

Workforce Identity Verification

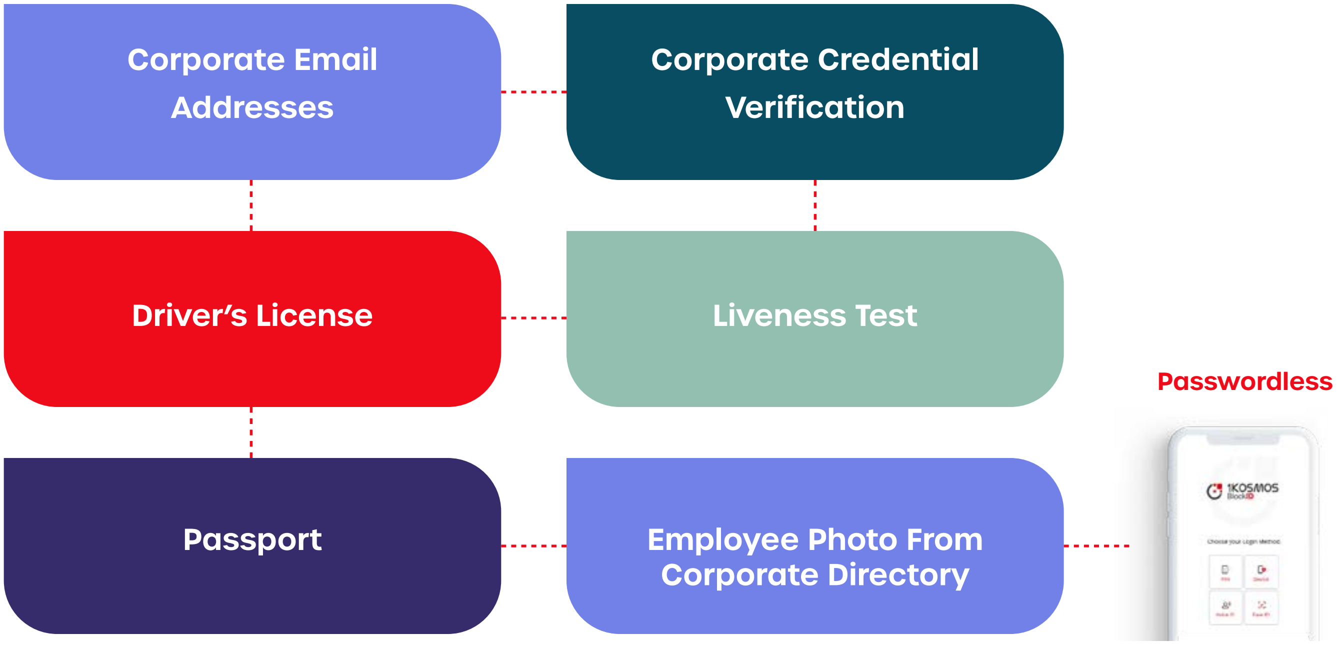
The Solution to Fill The Identity Verification Gap

Fully integrated to BlockID Workforce

BlockID Verify for Workforce

Workforce Identity Verification: The Steps

To reach a higher level of identity assurance per the NIST 800-63-3 Guidelines, or IAL2, it is imperative for employers to verify the validity of an employee's corporate information, the validity of his or her government-issued documents and leverage a form of advanced, unspoofable biometrics called a liveness test. The latter proves that the individual indeed exists.



Corporate Email Addresses

Corporate Credential Verification

Driver's License

Liveness Test

Passport

Employee Photo From Corporate Directory

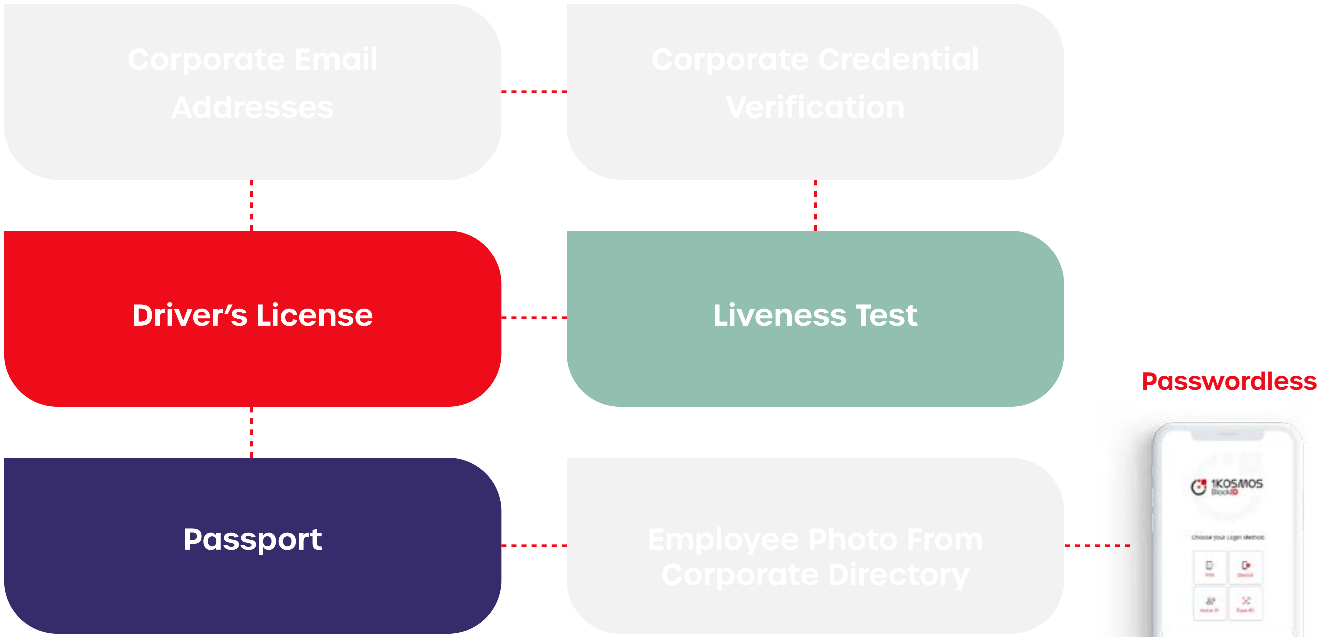
Passwordless

The employee's corporate information to verify can include Kate's corporate email address, the credentials associated to her Active Directory entry, and whether the result of her liveness test does indeed match the photo her employer has on file. Government-issued documents can include the employee's driver's license and passport, which must be verified against the proper issuing administration. Finally, the liveness test is performed to verify if the biometric traits of the employee are from a living person rather than an artificial or lifeless person.

BlockID Verify for Workforce

New Employee Onboarding: Eradicate Identity Compromises

To make sure that the new hire is who she says she is, it is imperative to follow a process that not only proofs the identity of the new recruit, while protecting her personally identifiable information (PII), but that also offers the new hire a frictionless experience.


Corporate Email Addresses
Corporate Credential Verification
Driver's License
Liveness Test
Passwordless
Passport
Employee Photo From Corporate Directory
1KOSMOS
BlockID
Choose your Login Method

The new hire performs a liveness test that is then matched with enrolled government-issued documents and also leveraged for authentication, once the enrollment process is complete.

Then, the new employee enrolls government-issued documents, like her driver's license and passport, which must be verified against the proper issuing administration.

Once validated, the information is used to fill the USCIS Form-I9.

The new hire's first name, last name and unique identifier are transmitted from the HR application into the account provisioning (IGA) system.

BlockID Verify for Workforce

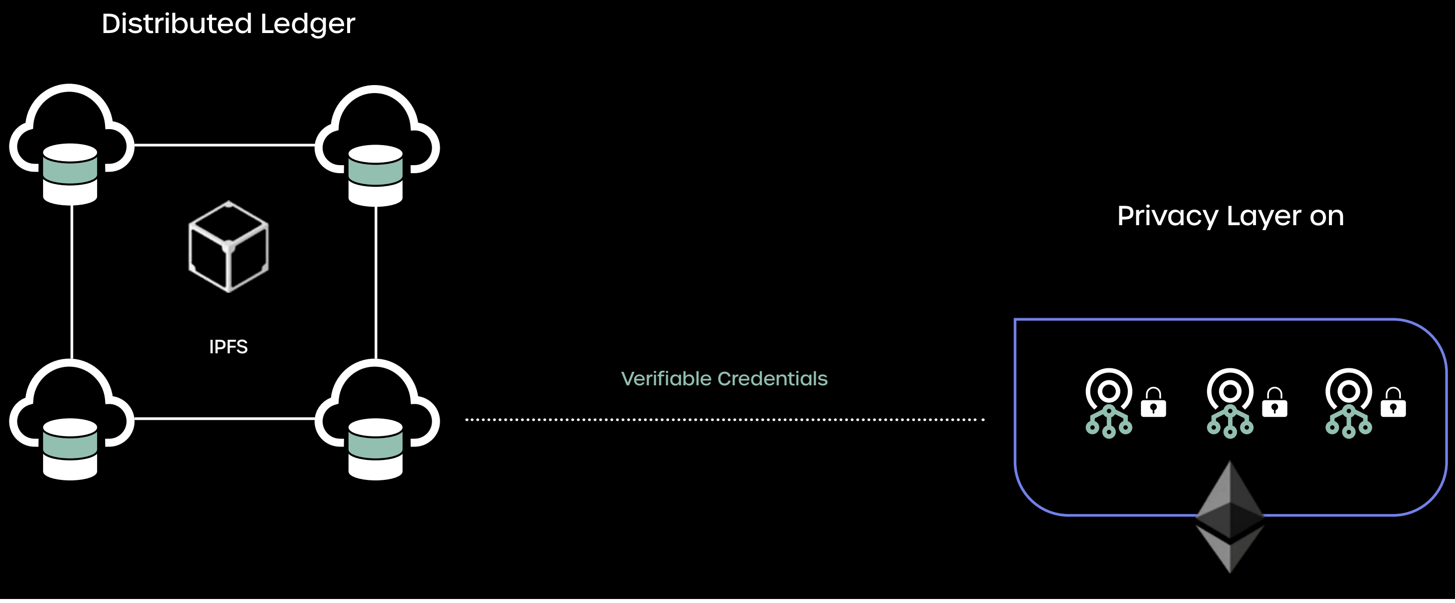
Securing Identity Employee Data: The Blockchain Ecosystem

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

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 BlockID 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).

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



About 1Kosmos

1Kosmos BlockID is a distributed digital identity platform supporting both business-to-employee and business-to-consumer services that easily integrates with existing operating systems, applications, and IT security infrastructure to perform strong, verified identity-based authentication – eliminating the need for passwords, one-time codes, and more. By simplifying identity infrastructure, 1Kosmos drives both cost savings and user convenience while securing businesses and individuals from the harm and inconvenience of identity fraud. The company is headquartered in Somerset, New Jersey.

For more information, visit www.1kosmos.com or follow @1KosmosBlockID on Twitter.