1Kosmos Zero Trust Access

Proof of identity and advanced biometrics to meet zero trust access requirements

The Business Challenge

With the dramatic rise in remote work, previous IT security default options, like using a virtual private network (VPN), were quickly proved insufficient and unsecure for many companies. Organizations need to be able to establish trust relationships in order to securely enable access for various people (employees, partners, contractors, supply chain, etc.) regardless of their location, device, or network. Unfortunately, traditional IT security perimeters framed around weak, password-based access credentials have proven ineffective for protecting your remote workforce, API ecosystem, and digital transformation initiatives.

Zero Trust is a security framework requiring all users, whether inside or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. Zero Trust assumes that there is no traditional network edge. Networks can be local, in the cloud, or a combination or hybrid with resources anywhere as well as workers in any location.

The 1Kosmos Zero Trust Access Advantage

1Kosmos identity based authentication authenticates users into an organization's environment with cryptographic proof that they are who they say they are, with an immutable audit trail.

1Kosmos provides identity-based authentication by proofing a user's identity and reaching IAL2 per the NIST 800-63-3 guidelines and binding that to the user's account. This makes credential sharing and identity impersonation impossible. The cost of deploying 2FA and MFA solutions that require hardware is also eliminated. The 1Kosmos app installed on the user's smartphone will be the primary means for physical and logical access to whoever authenticates successfully.

When a user downloads the 1Kosmos app and enrolls, they will take a live selfie – This is part of our LiveID biometric. Then, we ask the user for that selfie and compare it to their photo on government- issued documents like a passport or a driver's license. 1Kosmos matches the selfie with the captured image(s) and gives the user a digital certificate that verifies their identity and it binds the account to the proven identity. When users authenticate through LiveID we compare the live selfie with the one taken at enrollment to prove identity and grant access. This is how 1Kosmos meets the Zero Trust access requirements.

1Kosmos identity based authentication authenticates users into your environment with cryptographic proof that they are who they say they are, with an immutable audit trail.

1Kosmos Zero Trust Access
Establish Identity

1Kosmos binds the user's mobile device to a verified and validated identity. Our solution provides organizations with the ability to complete a mobile-first onboarding journey for any user. First, the new user will download your custom app integrated with the 1Kosmos mobile SDK or, the 1Kosmos app. Then, depending on the level of assurance required, the user will be guided to enroll their identity. For those instances where high identity proofing assurance is required, the user must enroll one or more forms of government-issued ID. The captured data is encrypted with the user's private key and goes through another level of encryption before being stored in the 1Kosmos private and permissioned blockchain.

1Kosmos identity proofing will utilize a user's driver's license, passport, or National ID to validate a user's identity. With the user's consent, 1Kosmos will extract the content from the ID and verify the document's validity. 1Kosmos supports document verification for 150 countries. The extracted data, including the picture, is used to verify the user's identity and is encrypted with the user's private key and stored in the 1Kosmos private and permissioned blockchain protecting the user's data and privacy.

Our identity proofing technology can:

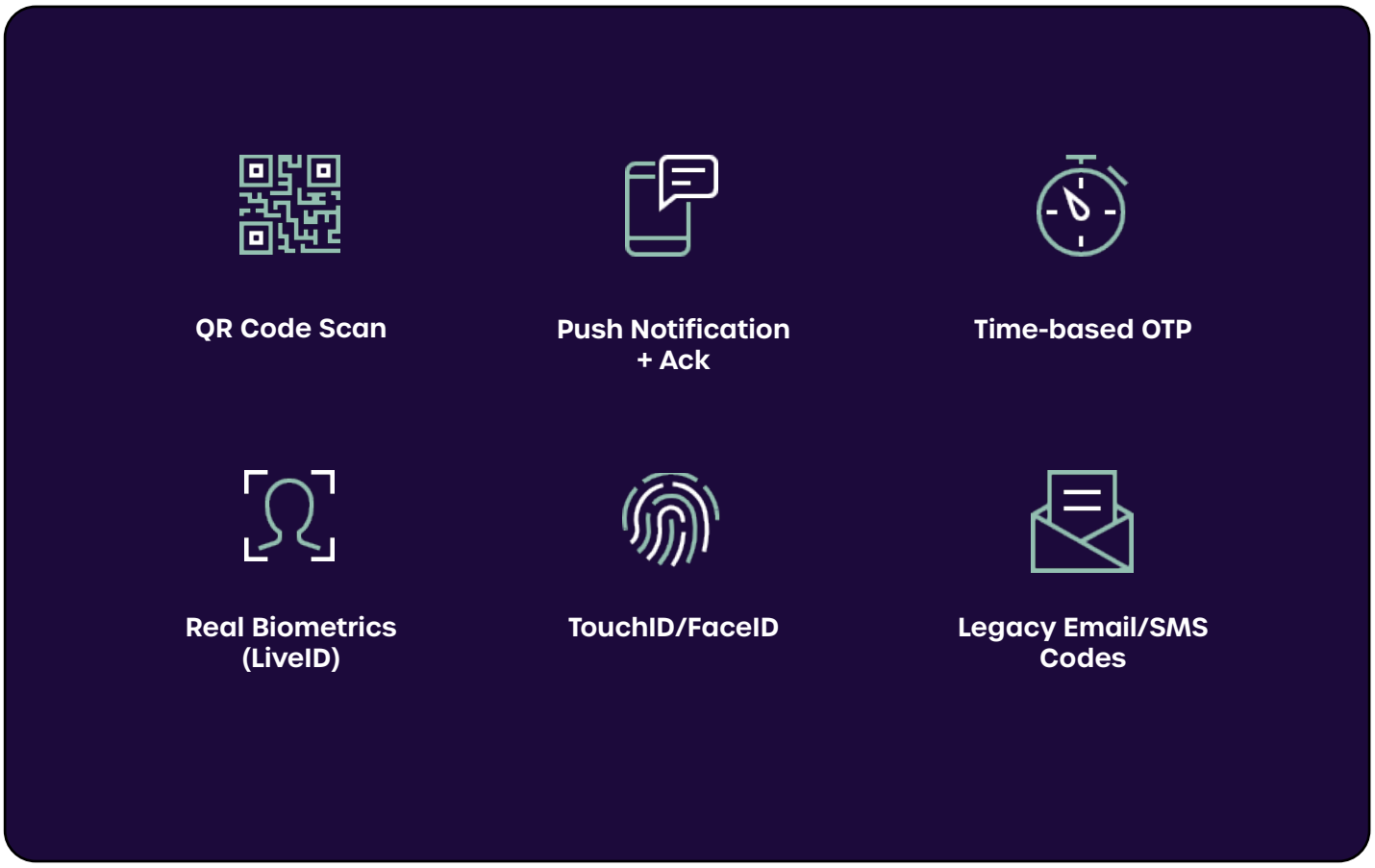
- Read barcodes defined by PDF 417 standard that has data encapsulated in it
- Read the data stored in an MRZ code on both passports and National ID's
- Read and extract the secure data located in passport RFID chips
- Provide a certified identity assurance level 2 (IAL2)

Enforce Authentication

Once the identity is validated and verified, synthetic ID fraud is prevented and the user account is generated and enrolled in a passwordless experience. 1Kosmos provides the option of using a much stronger identity-based MFA during this flow, 1Kosmos LiveID. The user will never need (or know) their credentials (username and password) and can now access their account or service through an identity-based biometric and a strong passwordless experience.

For low-risk authentication 1Kosmos can authenticate users to a lower identity assurance. By implementing 1Kosmos, organizations can consolidate, or now deliver, several types of methods into one experience.

We offer native support for:



LiveID Liveness Verification

1Kosmos performs a liveness verification when capturing the user's picture and gesture and then leverages AI to validate the identity record upon access attempt. The process is certified (by the Kantara Initiative) to NIST Identity Assurance Level 2 and compliant with Identity Assurance 3, as per the NIST 800-63-3 digital identity guidelines.

LiveID Authentication

The authentication is a two-step process. The first is validating that it is a real-life person and not a spoofing attempt. Using the expressions and a true-depth camera functionality 1Kosmos verifies that a live person is present. Second, a selfie is taken, compared to the picture taken at enrollment, and access is granted if they match.

LiveID Accuracy

When implementing 1Kosmos' Identity Based Authentication, organizations can choose to verify the user via LiveID as one of their options. The stored LiveID image must match the user's enrolled LiveID image before access is granted. The LiveID biometric authentication is certified iBeta PAD2 and is over 99% accurate to deliver the assurance needed for zero trust access requirements.

Document Verification

Identity proofing is only as sound as the ID used. 1Kosmos identity proofing technology captures the information in the ID and looks to ensure the ID is valid. For instance, 1Kosmos checks for common characteristics of the entered document to identify if a photocopy is used. The RFID chip in a passport is another example, where if the chip can not be read, then the data is not validated.

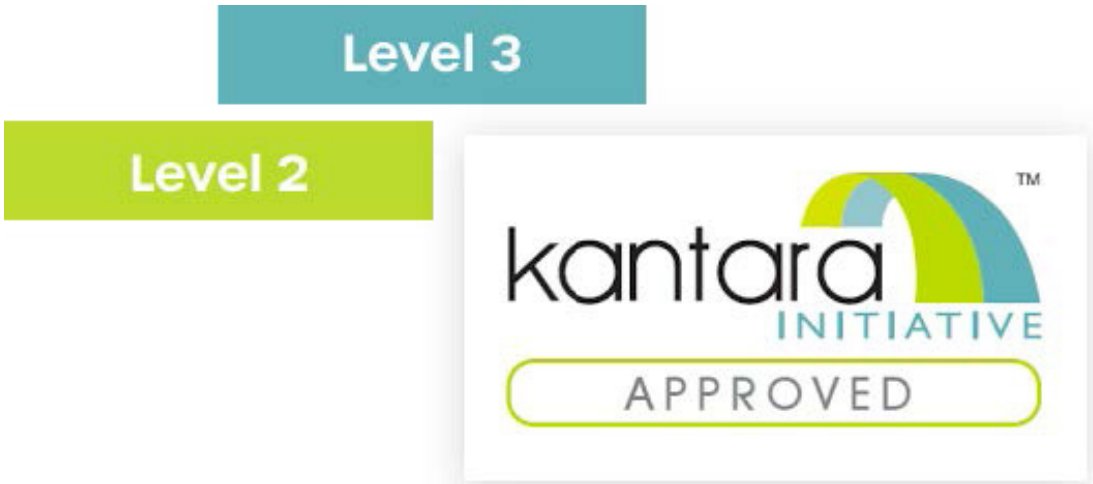
In cases where a visual check of the data is required, 1Kosmos will work with third parties to validate the captured data and the ID document. Or, if organizations would prefer, 1Kosmos can activate an API to verify the data from the Country Signer Certificate Authority (CSCA) or from an issuing authority such as AAMVA for US drivers licenses, to validate the document and the data.

Certification

1Kosmos unifies identity proofing and authentication for employees, customers and citizens to enable secure passwordless access to sensitive applications, data and resources.

1Kosmos is the only platform in the industry to be certified for iBeta, NIST 800-63- 3 and FIDO which allows organizations and government agencies to onboard users with certainty on who they say they are in the digital world.

It also performs an instant IAL2 certified identity verification without requiring the individual to be present at a physical location, and stores user data encrypted in a private, permissioned blockchain.



Blockchain Backend

To manage identity attributes and user privacy, 1Kosmos utilizes a W3C Decentralized Identifier standard - a private and permissioned blockchain distributed ledger. The 1Kosmos backend eliminates the central storage database of usernames and passwords and removes any risk of lost, borrowed, or stolen credentials. This backend is immutable, highly secure and designed to support rapid transaction execution that often cannot be achieved when using a public blockchain. Each user's information is encrypted using their own unique cryptographic key pairs, with their private key stored securely on their mobile device.

Once users enroll their attributes and biometrics with 1Kosmos, the data is pushed to the 1Kosmos private and permissioned blockchain network. A smart contract inside the blockchain is triggered and executed, and once validated, the user's data is stored inside the blockchain. The clear benefit of the blockchain approach is eliminating a single identity repository, so hackers will not be able to access a "honey pot" of identity data that traditional vendors support.

Identity Proofing SDK

Our Identity Proofing functionality is available through our customizable SDK and is easily integrated into any custom app. Whether you are using the 1Kosmos app or a custom integration, you can implement a mobilefirst automated identity proofing workflow.

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.