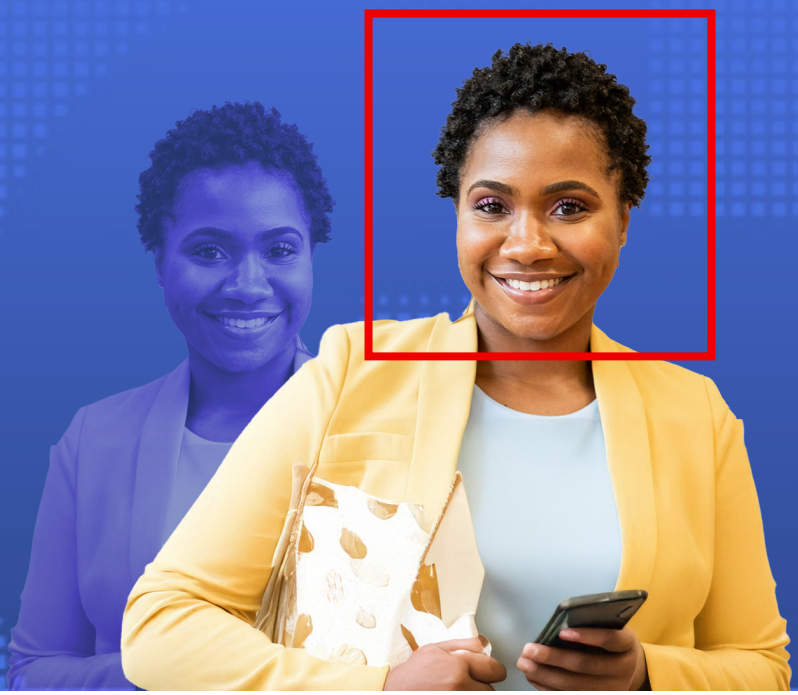
1Kosmos Customer



Use identity-based biometric authentication with flexible levels of identity assurance

The Business Challenge

Organizations are continuously dealing with fraudulent customer activities. The issue is a direct result of an inability to verify, secure, control, and manage customer identities at scale. To address this, businesses must confidently determine whether a person is real and who they claim to be—without compromising user experience during onboarding or service access.

While the CIAM digital transformation has integrated security controls with customer experience, it has yet to fully address customer enrollment journey, improve privacy controls or advance the customer experience by delivering identity-based biometric passwordless access.

By binding customers to their proofed identity, 1Kosmos Customer creates an identity-based biometric authentication and a passwordless experience.

The 1Kosmos Customer Advantage

1Kosmos Customer is built with specific capabilities for the onboarding, verification and authentication of customers. The CIAM approach was intended to eliminate barriers to user engagement and improve the user experience. Unfortunately, this opened the door to fraudulent activities as identities are not fully verified. 1Kosmos Customer eliminates this gap. We deliver a quick and convenient way for customers to self-verify their identity using physical documents such as a driver's license and passport. We can also leverage the nonphysical, such as a telco ID account and banking credentials to further improve identity assurance.

Combined with 1Kosmos Verify, 1Kosmos Customer digitally transforms the standard onboarding process for customers, delivering the highest degree of end-user assurance. This transformation securely automates the entire onboarding process for new and existing customers.

Our approach binds the device not only to an identity but to a verified and validated identity. This creates identity-based biometric authentication and a strong passwordless experience. Customers will utilize their trusted device for daily authentication and step-up authentication for account access and high-risk transactions. As a result, each access event is validated against a real, verified identity that meets the KYC (Know Your Customer) guidelines. This provides users with a frictionless experience and organizations with a flexible level of assurance for the identity on the other side of the digital engagement.

New Customer Onboarding

1Kosmos Customer and 1Kosmos Verify bind 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 customers. Once a customer begins their account setup, a process starts to verify the new identity remotely. 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.

Once the identity is validated and verified, the customer account is generated and enrolled in a passwordless experience. 1Kosmos Customer provides the option of using a much stronger identity-based MFA during this flow. 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.

Existing Customer Onboarding

Onboarding existing customers into the 1Kosmos Customer identity-based biometric passwordless experience is simple and takes less than a minute to complete. Moving customers to a passwordless experience can be achieved in one of three ways:

- An invitation sent to the user through the 1Kosmos administration portal.
- An invite to join is added to the standard login page.
- Or within your organization's custom app (our mobile app can be white labelled or embedded into your own via our API / SDK.
- Users choose to accept the invitation and onboard themselves to start their passwordless journey.

First, the enrollment begins by prompting the user to enroll their identity, either in an existing app or via an existing webpage. The user is then guided to use their mobile phone to complete the onboarding process. Depending on the business need, the customer may enroll in an optional biometric to increase their access assurance level. If the organization requires a higher identity assurance level, the customer may enroll up to two forms of government-issued ID. The user's LiveID is validated against the picture extracted from the provided documents. The data is encrypted with the user's private key and stored in the 1Kosmos private and permissioned blockchain. The customer will now use their enrolled identity or identity-based biometric to complete a transaction or to authenticate into their account without a username and password.

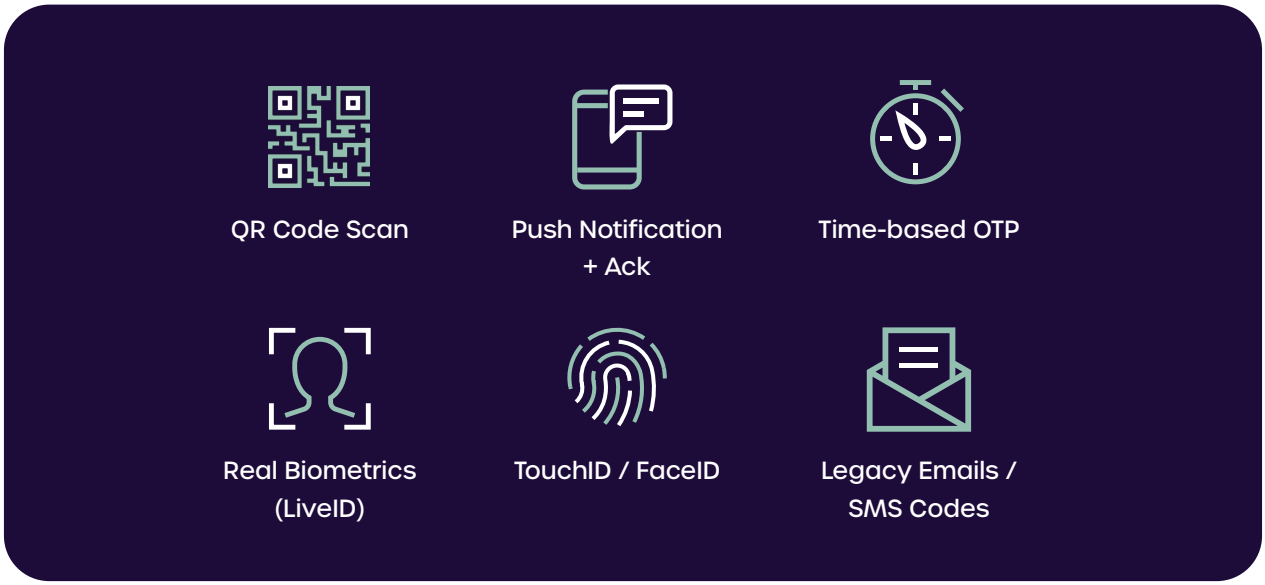
Appless Access From the Desktop

If a mobile device is not needed or available, 1Kosmos Customer can still deliver a strong passwordless experience from the desktop. To do this, we leverage the platform authenticators available on the desktop, like a fingerprint reader, or through a security key. To enroll in the passwordless experience, the customer would log in as normal. Then, the customer will be asked to provide their biometric or supply their security key to enroll in a passwordless experience. This process binds the device or security key to the user, and from then on, the user will have a passwordless access experience.

Employee and Contractor Identity Based-Authentication

1Kosmos Customer authentication methods are built into the 1Kosmos app and customers can authenticate via any of our identification methods. By implementing 1Kosmos Customer, you will consolidate, or now deliver, several types of methods into one experience.

We offer native support for:



We also support industry authentication standards such as Auth0, OIDC, SAML and FIDO.

Blockchain Backend

To manage identity attributes and user privacy, 1Kosmos Customer 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 Customer, 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 CIAM vendors support.

Mobile App and Mobile SDK

The 1Kosmos mobile app can be white labelled, so you can easily customize the look and feel to fit in with your brand identity and improve the customer experience.

Alternatively, by implementing our mobile SDK/API, you can integrate functionality into your existing app or service. This approach allows you to eliminate silos created when managing multiple apps and services.

Administration Portal

For administrators, the portal is a centralized hub that allows for easy management of users and applications and is the starting point to enroll the customer into passwordless access.

Our administration portal delivers:

Visibility. Review a user's identity profile, their access and usage (but not their private identity information).

Policy-based authentication. Define authentication policies based on rules.

Policy enforcement. Challenge users, based on defined rules and "strength of identity."

Strong identity. Begin the user's identity lifecycle based on strong identity proofing.

Dashboard to monitor threats. Receive alerts on unauthorized access and unusual behavior patterns.

User Portal

For customers, the portal is a centralized hub that allows for easy control of their identity data and how it is shared.

Visibility. Customer will have visibility into their identity profile, applications and devices.

Portfolio of devices. Enroll a portfolio of devices allowing seamless access to applications.

Avoid helpdesk. Manage and recover account(s), sign-up for passwordless access, link & unlink devices.

Protect against fraud and identity theft. Customer will be alerted when unusual behavior is detected on their device.

Continuous Verification

It's not enough to just authenticate and let users do what they please once access is granted. The 1Kosmos Customer approach continuously validates identity assurance and offers a configurable journey to map user authentication requirements. Traditional "allow or deny" responses are replaced by more fine-grained options such as "allow, but step up the authentication level with biometrics."

1Kosmos can ingest behavioural and peripheral risk signals. For example, we have partnered with organizations like Behaviosec and RSA to track user behavior (desktop, mobile and environmental factors). This capability will detect attacks including session hijacking or credential loss on an access attempt. This combination of technologies improves your overall security posture as you can detect potentially fraudulent activities in real-time and step-up authentication if something out of band is noted with the least impact to the user.

Transactional Authentication

Based on your domain and risk level, 1Kosmos provides schematics to increase every session's assurance level. As customers transition to higher-risk activities, they can be asked to re-authenticate to ensure identity. To ensure the highest level of compliance, 1Kosmos supports the NIST AAL3 and eIDAS "HIGH" level of authentication.

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