1Kosmos Authenticators

Authentication methods to solve even the most complex identity and authentication challenges

The Business Challenge

Traditional two-factor authentication (2FA) and multi-factor authentication (MFA) methods rely on SMS, push notifications, or email for user verification. This outdated approach creates friction for users and introduces significant security vulnerabilities. Since username and password credentials are still involved, these methods are susceptible to attacks like phishing, push bombing, and man-in-the-middle tactics.

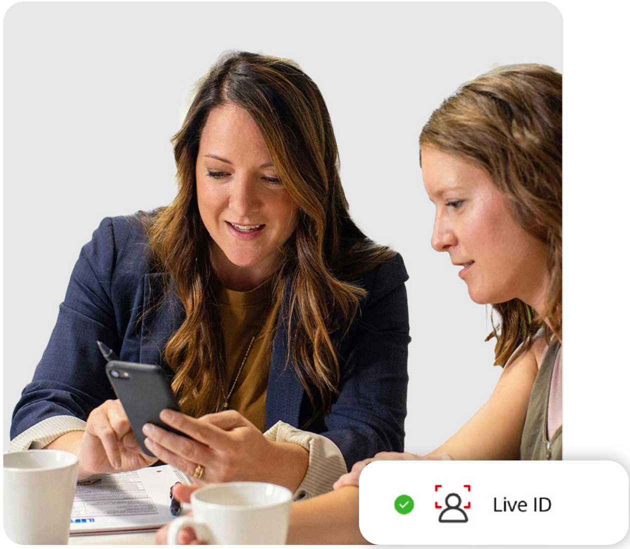
Hackers exploit these weaknesses, often leading to compromised accounts, data breaches, and ransomware attacks.

> Users register once and then can authenticate into devices, environments and applications using verified biometrics. As a result, each access event is associated with a real, verified identity.

The 1Kosmos Authentication Advantage

1Kosmos binds workers, customers, and citizens to their proofed and validated identity. This enables a passwordless login experience.

Users get a reusable digital wallet that is accessible through various modalities. This includes a mobile app, mobile device, web browser, hardware token, and passkey, for online, offline, and in-person authentication. As a result, each access event is associated with a real, verified identity.



Time-Based One-Time Password (TOTP)

1Kosmos supports Time-Based One-Time Password (TOTP) as a secure and efficient method for user authentication. The 1Kosmos app can create a TOTP using a dual key pair value based on the elliptic curve algorithm, ensuring cryptographic security.

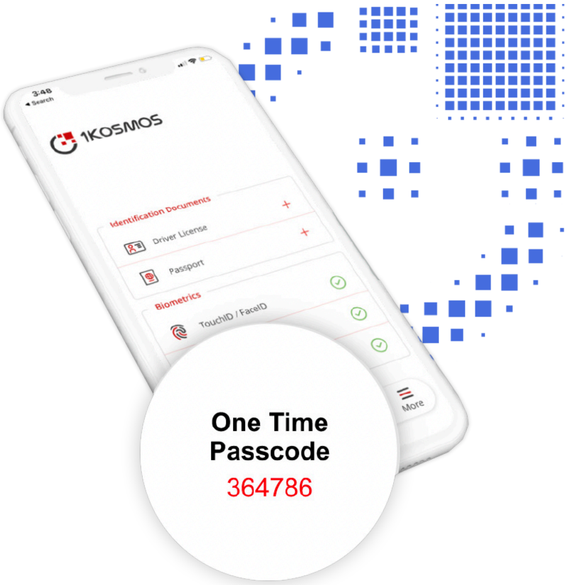
The TOTP is tied to the requesting system, meaning it is generated specifically for the system or application the user is trying to access. The user enters the TOTP to gain access to the system. The TOTP is time-sensitive, adding a layer of security by ensuring that the code expires after a short duration. TOTP is part of the Open Authentication (OAuth) security framework and therefore is based on the OAuth security architecture.

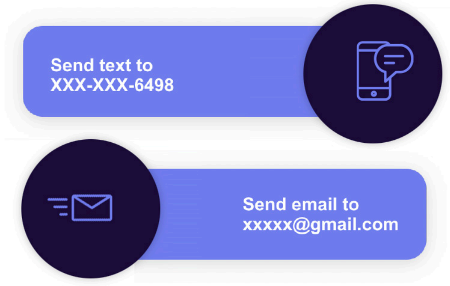
Identity-Based Authentication

With traditional authentication methods, there is a significant chance of risk with employees sharing credentials. The only way forward in proving a user's identity is through biometrics, particularly, real biometrics.

- LiveID: Verifies identity using live facial biometrics, ensuring only the legitimate user can authenticate—no passwords, no shared credentials.
- 1Key: Provides a seamless authentication experience with or without a phone, making identity verification accessible in any scenario.

The path to identity-based authentication can be a long one, hence at 1Kosmos, we supports legacy methods, ensuring a seamless transition and gradual migration.



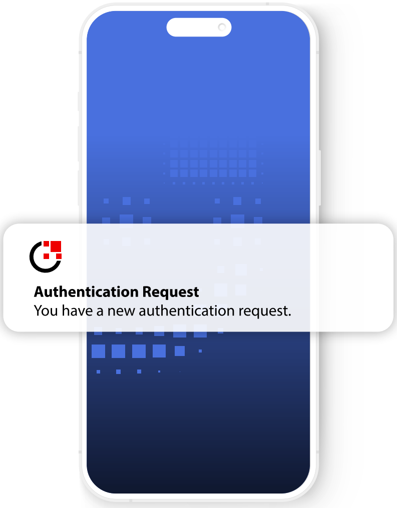


SMS and Email

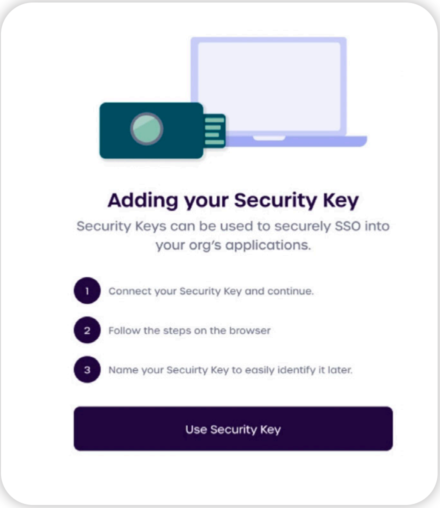
SMS and email authentication are one-time passwords (OTP) tied to a session. This approach requires users to validate that they have access to the email or phone number associated with the account. SMS and email authentication methods rely on a security code sent to a user via traditional text or email messaging with an expiration time set. Like the TOTP authenticator, this method also generates a unique device ID and a seed using a dual key pair value based on the elliptic curve algorithm for the time-based token generation. Administrators can configure the tenant session expiration to meet internal parameters. This code is entered into the requesting application, and access is granted.

Push Notification

Push notification is similar to SMS but not reliant on the device connected to a SIM card. The experience for push authentication is straightforward. When logging in, the user receives a notification on the trusted devices (either mobile or desktop) associated with the user account. The push notification prompts open the 1Kosmos mobile application. Then the application asks for consent from a privacy standpoint. Then, the user is presented with a simple "accept" or "deny" message to allow or prevent the login. Accompanying this action is information about where the request comes from, such as the location, application, or device type. And like the TOTP, SMS, and email authenticators, this method also generates a unique device ID and a seed using a dual key pair value based on the elliptic curve algorithm for the time-based token generation.



Authentication Request
You have a new authentication request.



Adding your Security Key

Security Keys can be used to securely SSO into your org's applications.

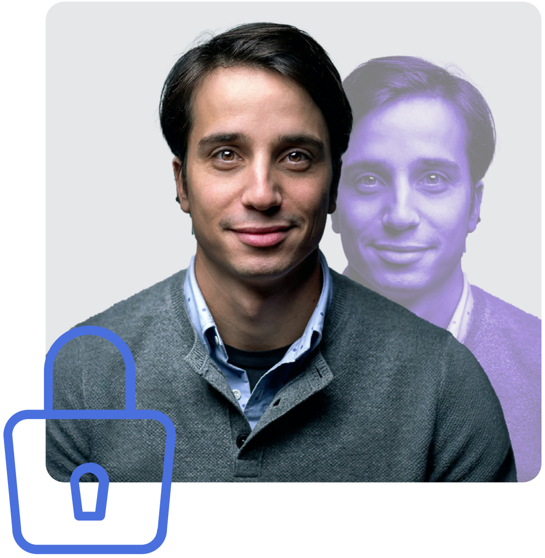
1. Connect your Security Key and continue.
2. Follow the steps on the browser
3. Name your Security Key to easily identify it later.

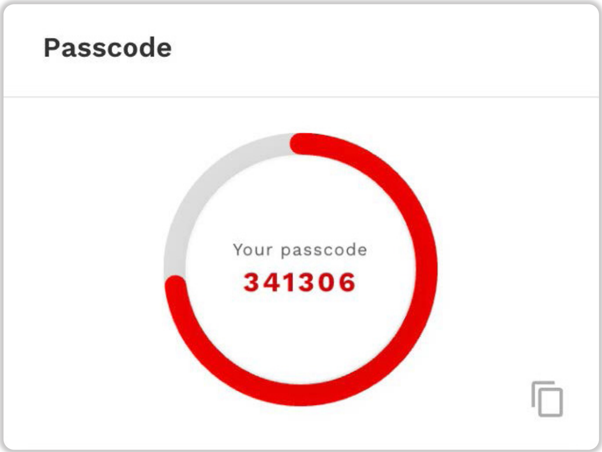
FIDO2 Tokens

FIDO2 is a further development of the U2F protocol with an expanded version of CTAP (Client to Authenticator Protocol), now called CTAP2. 1Kosmos supports the cryptographic capabilities U2F tokens provide. Where organizations require U2F tokens to secure access from multiple devices, 1Kosmos links the FIDO2 token to the user account for access requests. Universal 2nd Factor (U2F) is an open authentication standard that strengthens and simplifies two-factor authentication using specialized USB or NFC (Near-Field Communication) devices.

WebAuthn

The Web Authentication API is a specification that enables strong, public key cryptography registration and authentication. WebAuthN was created by the FIDO (Fast IDentity Online) Alliance and W3C. 1Kosmos can tap into built-in biometric authenticators on laptops and smartphones, letting users authenticate quickly and with the tools they already have at their disposal.





Passcode

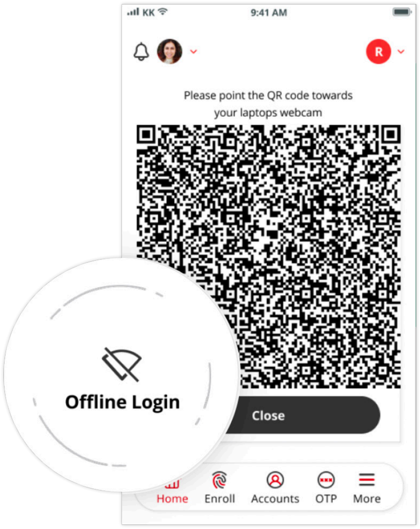
Your passcode
341306

Desktop Agent

The desktop agent is tied to the user's account and unique device ID. An OTP is generated, and linked to the device ID, so only that device can use that OTP at the time of request.

Offline Access

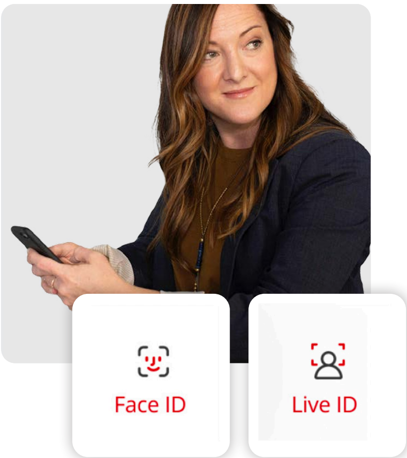
For accounts that are set for offline access, the fully brandable 1Kosmos app generates a QR Code that a user would scan with their webcam. To work, both the laptop and mobile device need to be offline. The connection and decryption process for offline access is fast, secure, and seamless for the user.



Please point the QR code towards your laptops webcam

Appless Authentication

1Kosmos appless authentication was designed for organizations or instances where phones are unavailable. Users can authenticate with or without a phone — simply scan a QR code with a mobile camera or access a website directly on a laptop. From there, they can use built-in biometrics like Face ID, a fingerprint reader, or a camera for secure authentication. No phone required.



Face and Touch ID

1Kosmos can leverage the built-in Face ID or Touch ID identity technologies available on today's devices. While Face ID or Touch ID are commonly used to authenticate users into their devices, 1Kosmos does not recommend this for use cases for use cases where proof of identity is required.

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.