1KOSMOS

Solution Brief

1Kosmos Authenticators

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

The Business Challenge

Identity management has gone essentially unchanged since the introduction of the password nearly 60 years ago.

Additional means of access verification were developed to mask the issues with passwords – second factor (2FA) and multi-factor authentication (MFA) are prominent examples. These solutions rely on SMS, push notifications, or email to verify who the user is and what the user has. These present friction to the user and come with well-known security gaps that still lead to compromise, as user name and password credentials always remain part of this process. Hackers use phishing attacks as they routinely send emails, SMS messages, and phone calls, trying to trick them into disclosing account credentials, personal information, or downloading malware. Organizations need to eliminate the password and move to a strong, identity-based authentication model, to eliminate the weak link in the security chain: the password.

Users will utilize their trusted mobile device for daily authentication and step-up authentication for physical, logical, or even offline access. As a result, each access event is associated with a real, verified identity.

The 1Kosmos Authentication Advantage

The 1Kosmos advantage changes the way users fundamentally authenticate. Our approach binds workers, customers, and citizens to their proofed and validated identity. In doing so, 1Kosmos BlockID creates an identity-based biometric authentication and a passwordless experience. Users will utilize their trusted mobile device for daily authentication and step-up authentication for physical, logical, or even offline access. As a result, each access event is associated with a real, verified identity.

In addition to 1Kosmos BlockID identity-based biometric authentication, additional authentication methods are available through our SDK and can be easily integrated into any custom app or through the 1Kosmos BlockID app. The identity-based 2FA and MFA authentication methods available can be deployed for workforce, consumer, or citizen use cases. These users can authenticate via any of our identification methods depending on the business need, risk profile of the activity, and security requirement for each access request. By implementing 1Kosmos BlockID, you will consolidate several types of methods into one experience. 1Kosmos BlockID fully supports industry authentication standards such as OAuth, OIDC, SAML, and FIDO.

The 1Kosmos advantage is adding to or replacing the authentication method with LiveID to enhance the security and identity assurance levels of any access request. This is a significant enhancement to any MFA capability.

Identity-Based Access

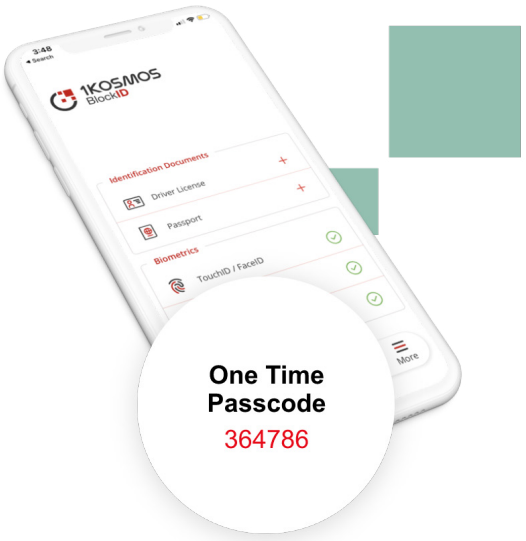
The 1Kosmos BlockID platform offers several forms of built-in identity-based authentication:

- "LiveID" advanced biometric authentication
- Device biometrics such as TouchID and FaceID
- U2F – Universal Second Factors such as Universal Serial Bus (USB) and near-field communication (NFC) These methods vary in their security level. Still, each of them will protect against man-in-the-middle (MITM) attacks.

The 1Kosmos BlockID platform is a flexible and customizable platform, so you'll be able to find the best adaptive authentication method that meets the unique needs of your diverse application ecosystem.

Time-based One-Time Password (TOTP)

Once the 1Kosmos BlockID app is installed, a time-based Device Identifier (DID) is generated. This method 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. The DID is unique to the installation on the mobile device. Once a user scans the QR code with the 1Kosmos BlockID mobile app, the user will receive a TOTP from the requesting system to gain access. TOTP is part of the Open Authentication (OAuth) security framework and therefore is based on the OAuth security architecture.

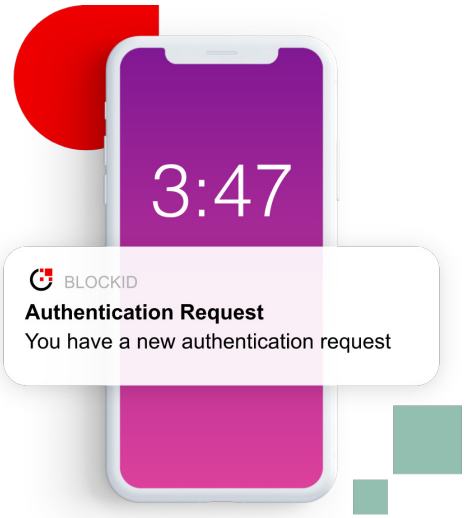


SMS and Email

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. And 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 Simcard. Upon registration, 1Kosmos BlockID registers the DID (Distributed Identifier) and is now bound to the user. 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. 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.



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 BlockID 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

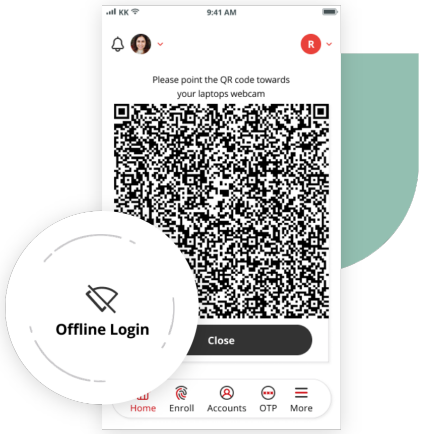
The Web Authentication API is a specification that enables strong, public-key cryptography registration and authentication. WebAuthN was created by the FIDO (Fast IDentity Online) Alliance and W3C. Third parties like 1Kosmos can tap into built-in biometric authenticators on laptops and smartphones, letting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

Desktop Agent

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

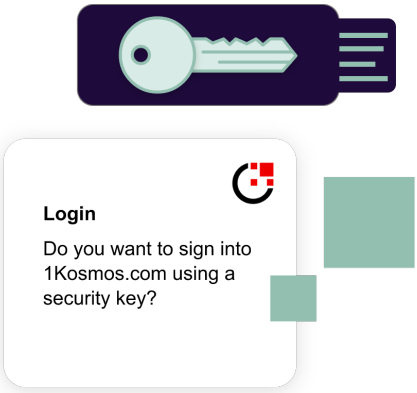
Offline Access

For accounts that are set for offline access, the 1Kosmos BlockID 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 to allow offline access are quick, secure, and seamless to the user.



Appless

1Kosmos appless authentication was developed for organizations or instances where a mobile app is unavailable. Users will still scan a QR code with their mobile camera, and they will be directed to a website where they will use device biometrics such as Face ID. The 1Kosmos appless capability can also be used on laptops. A user can authenticate using his or her laptop biometrics capabilities, like a camera or a fingerprint reader.



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 where strong authentication is required.

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.