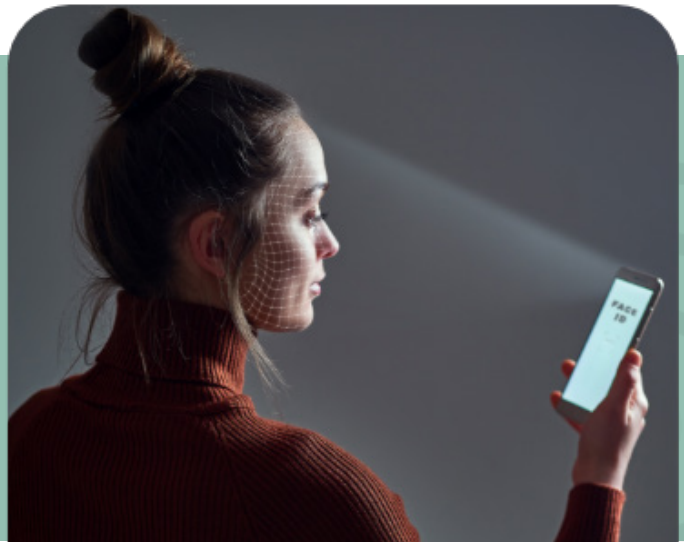
Datasheet

1Kosmos Multi-Factor Authentication

Advanced multi factor authentication to secure users with flexible levels of identity assurance



The Business Challenge

Multi-Factor Authentication (MFA) was developed as a more advanced version of 2FA. In reality, an MFA deployment is very similar to 2FA as users are asked to enter their username, and then a method is evoked to verify the identity. In most cases, these step-up authentication methods are an OTP or SMS. But the security of SMS and OTP is directly dependent on the safety of the receiving device, and just like the device, the OTP may be vulnerable to physical attacks. An attacker – who doesn't have to be miles away – can gain physical access to the device and steal it. In addition, the user's device can be compromised or stolen, making any of the 2FA / MFA methods highly problematic.

Deployment silos are another major fault found in deploying MFA. Implementing siloed and disparate MFA implementations is an exercise in futility. This approach creates security gaps and care needs to be taken to ensure all access points are covered under a single MFA deployment. This also includes all workloads in the cloud. An MFA implementation requires consistency, especially for remote network access for distributed employees and business partners. The focus should be placed on all end-users (including privileged users), cloud and on-premises applications, VPN, server logins and privilege elevation.

The 1Kosmos advantage changes the way users fundamentally authenticate. Our approach binds a user's account to their proofed and validated identity.

The 1Kosmos MFA Advantage

The 1Kosmos advantage changes the way users fundamentally authenticate. Our approach binds a user's account to their proofed and validated identity. In doing so, 1Kosmos BlockID creates an MFA method which is identity-based. The biometric authentication delivers an IAL2 secure passwordless experience meeting the zero trust access controls. Furthermore, by implementing the advanced BlockID solution, each and every access request is completed with a multi-step MFA process that is invisible to the user. The BlockID advanced MFA process includes a user authenticating into their device, the BlockID app, public and private key pairs and LiveID (an advanced biometric). Users will utilize their trusted mobile device for daily authentication and step-up authentication for physical, logical or even offline access.

In addition to 1Kosmos BlockID identity-based biometric authentication, additional authentication methods are available. For instances where passwordless authentication is not possible or to ease users into adoption, BlockID's 2FA and MFA authentication methods can be deployed, unifying all 2FA and MFA into one platform. 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.

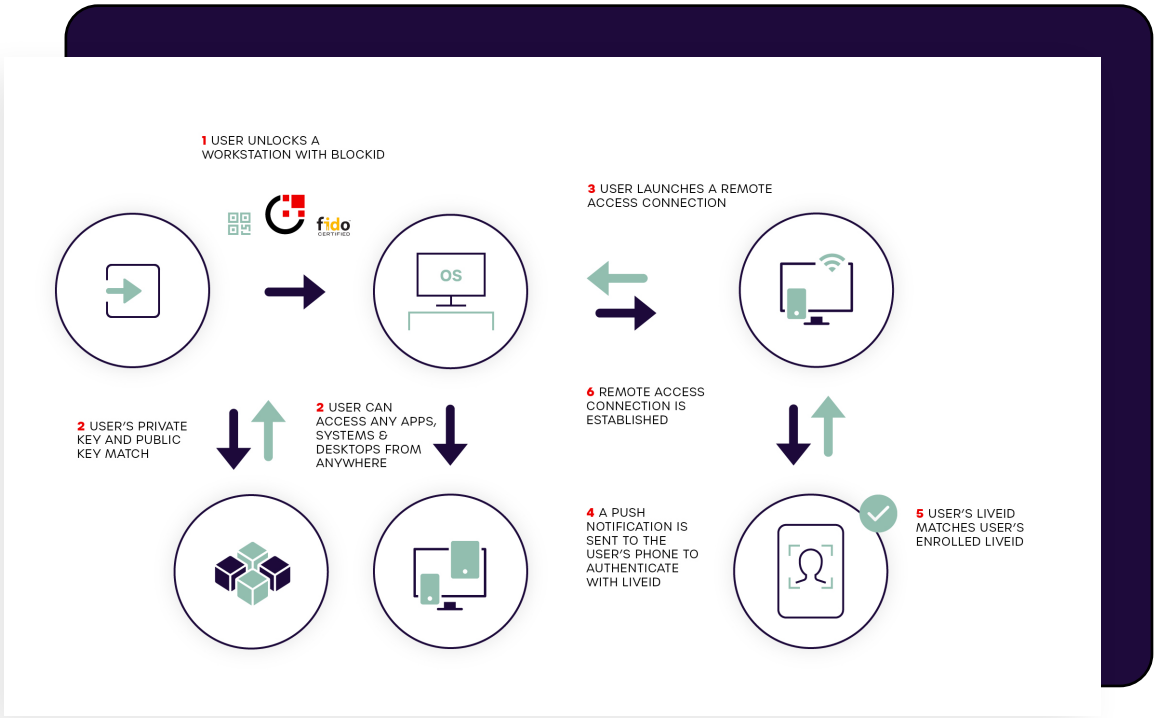
1Kosmos Advanced MFA

MFA for Remote Access, Zero Trust Network Access

The 1Kosmos BlockID platform helps organizations transform how they currently manage identity and access requirements to provide secure remote access. BlockID delivers identity-based passwordless access to users, ensuring that only authorized employees can access data or applications regardless of where they are based. As a result, organizations will authenticate users without usernames, passwords, and one-time codes. Instead,

users will authenticate with their identity. After deploying 1Kosmos, BlockID employees utilize a biometric passwordless experience and completely remove usernames and passwords. Our approach not only secures remote employees but also eliminates all password-based attacks.

BlockID is the only solution that makes Zero Trust and passwordless authentication truly compatible. The use of a password at any point during authentication does not verify the user's identity, making it impossible. Zero Trust is not just zero passwords. NIST-certified, BlockID proofs the user's identity who authenticates up to IAL2 per the NIST 800-63-3 Guidelines.



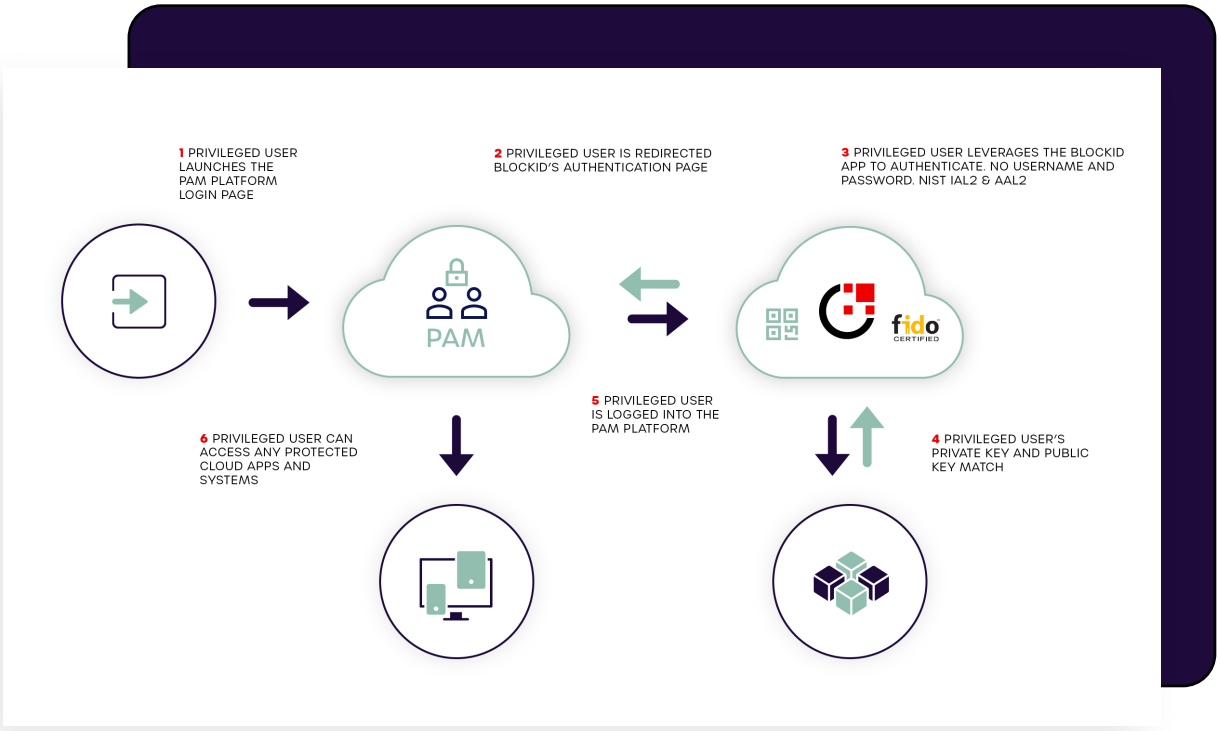
MFA for Remote Access, Zero Trust Network Access

MFA for Privileged Account Login

BlockID allows PAM solutions to identify who accesses sensitive systems and applications, whether the privileged user is on-premise or working remotely. Under a single application, BlockID combines indisputable NIST-certified digital identity proofing

with advanced non-spoofable biometrics for passwordless authentication. In addition, BlockID is FIDO2 and iBeta PAD2 certified for biometric passwordless access.

The privileged user experience is greatly improved since BlockID allows your admins and DevOps users to authenticate with our LiveID via their smartphone, laptop, or workstation in seconds, without passwords, with high assurance (AAL2) to remotely access key systems and applications wherever they are installed and deployed. The elimination of a password, as well as the utilization of advanced biometrics for authentication, rules out any risks related to password sharing and therefore insider threats.



MFA for Privileged Account Login

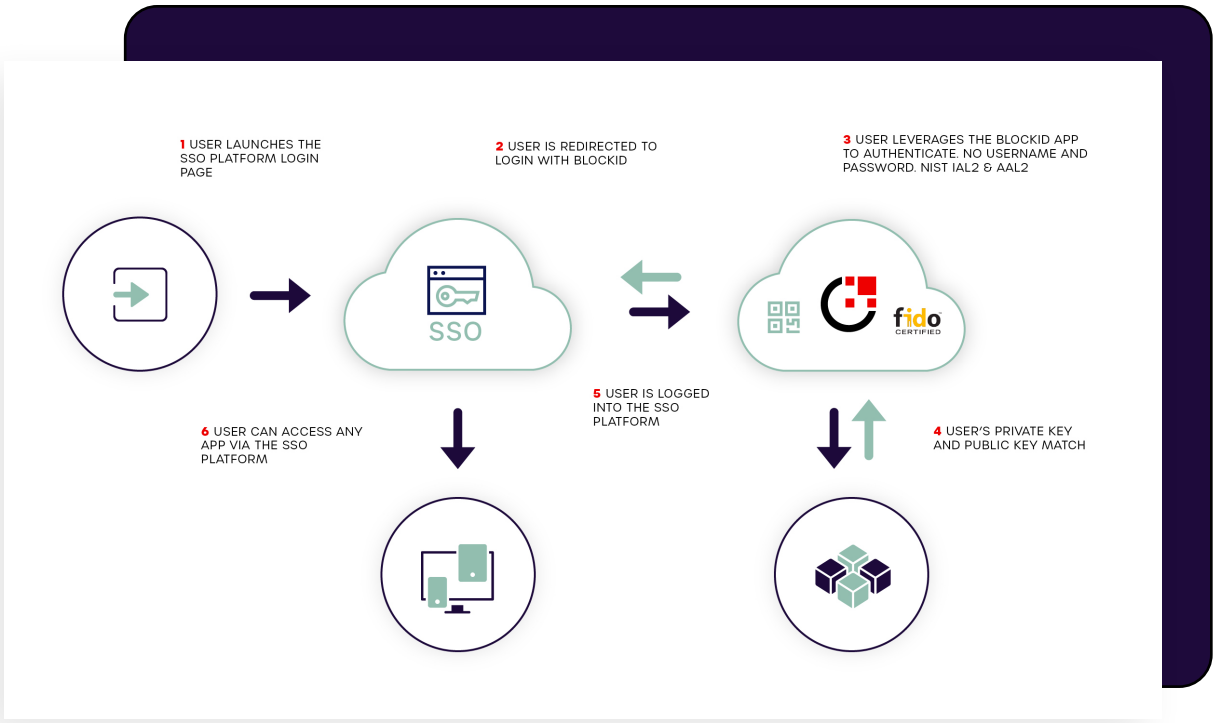
MFA for SaaS, Webapp, Client/Server Application Login

1Kosmos BlockID easily integrates into SaaS and web applications and complies with the strictest GDPR, SOC2, ISO 27001 certification standards for handling and retention of sensitive data. In addition,

BlockID can also integrate into systems via industry authentication standards such as OAuth, OIDC, SAML, and FIDO and offers legacy support via RADIUS.

MFA for SSO Login

1Kosmos BlockID modernizes MFA to improve the security of your SSO environment by eliminating password-based attacks and meeting zero trust access requirements.



MFA for SSO Login

What 1Kosmos brings to SSO is a more secure access environment by eliminating password-based attacks and meeting zero trust access requirements. Our identity-based authentication ties a proofed and verified identity to the access request. Meaning the user's biometric is the authentication method. By implementing 1Kosmos users will login into their Windows, Mac, or Unix desktop

with a passwordless experience using real biometrics. The authentication will verify, with high assurance, that the user is who they claim to be. Our authentication assurance is certified by NIST, FIDO and PAD2 and delivered with a distributed identity architecture. Our architecture delivers an immutable audit trail and meets the Zero Trust requirements for user authentication. 1Kosmos BlockID elevates your SSO deployment so organizations will know exactly who is accessing the network meeting zero trust access standards that are otherwise unattainable.

Mobile Authenticator

1Kosmos Block MFA and password reset functionality is available through our SDK and is easily integrated into any custom app. Whether you are using the BlockID app or a custom integration, you can implement a mobile-first MFA passwordless experience, including the advanced biometric LiveID feature.

BlockID complies with the strictest GDPR, SOC2, ISO 27001 certification standards for handling and retention of sensitive data. In addition, BlockID can also integrate into systems via industry authentication standards such as OAuth, OIDC, SAML, and FIDO and offers legacy support via RADIUS.

Once integrated, organizations will eliminate passwords and add advanced biometrics for authentication or other MFA factors as the business and use cases require.

1Kosmos MFA Capability Comparison

	1KOSMOS	Windows Hello	SSO	Legacy 2FA	Legacy MFA	Legacy Token
Identity Verification	✓					
Identity Based Passwordless Access	✓					
LIveID Biometric	✓					
Face and Touch ID	✓	✓	✓		✓	
TOTP	✓	✓	✓	✓	✓	
SMS	✓	✓	✓	✓	✓	
Email	✓	✓	✓	✓	✓	
Push Notification	✓	✓	✓	✓	✓	
FIDO for Desktop Logon	✓					
FIDO2 Token	✓	✓	✓	✓	✓	✓
WebAuthN	✓	✓	✓	✓	✓	
Device App	✓	✓	✓	✓	✓	
Desktop Agent	✓	✓	✓	✓	✓	
App-less	✓					
Offline Access	✓					
Self-Service	✓		*Additional*	*Additional*	*Additional*	
Windows	✓	*(Windows 10)*	✓	✓	✓	✓
MacOS	✓		✓	✓	✓	✓
Linux	✓					
Unix	✓					
NIST	✓					
IAL1, IAL 2	✓					
AAL1, AAL2	✓					
Authentication Persona Capabilitiy	✓					
OAuth	✓					
OIDC	✓					
SAML	✓				✓	✓
FIDO	✓					
Distributed Identity	✓					

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.

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