

1Kosmos ensures we meet the compliance requirements necessary to protect you and your identity.

BlockID NIST 800-63-3 Compliance

SP 800-63-A: Enrollment and Identity Proofing

IAL1 - When a user initially registers with **BlockID Safe**, the name identifier is based on the name registered on the device. It could be a "mickey mouse" account. **BlockID Safe** DOES NOT validate or verify any of the attributes (name, and CSP's can request 0 or more attributes from **BlockID Safe** (name & "did"). All requested attributed from any CSP would require the user to consent to it using biometrics.

IAL2 - BlockID Safe collects two pieces of STRONG evidence (i.e., Driver's License AND Passport). Both these documents are verified in real time directly with the issuing source (*via an identity hub*) to be valid and not reported lost or stolen. Additionally **BlockID Safe** validates that the data collected between the two pieces of identity documents are an exact match including the photographs.

IAL3 - Can be achieved only if the user is IAL2. **BlockID Safe** validates the user's current address is done with direct integrations with backend address validation services to ensure that the user actually lives at the address as stated in the proof of identity document. The addresses themselves are not self-asserted, but rather extracted via the valid documents presented for IAL2.



SP 800-63-B: **Authentication Assurance Level**

AAL1 - BlockID Safe does a complete out-of-band authentication using biometrics in adherence to Section 5.1.3, Section 5.1.4, Section 5.1.6, Section 5.1.7, Section 5.1.8, Section 5.1.9 as the distributed ID itself is generated based on BIPS39 standard mnemonic phrase based identifiers linked to its own private and public keys.

AAL2 - BlockID Safe uses multi-factor biometric authentication. Factor 1 is the biometrics used to unlock and use the app. Factor 2 would be the CSP requested biometric mechanism (face, voice, thumbprint or pin).

BlockID Safe does a complete out-of-band authentication using biometrics in adherence to Section 5.1.5 and Section 5.1.8. Section 5.1.9, as the distributed ID itself, is generated based on BIPS39 standard mnemonic phrase based identifiers linked to its own private and public keys.

AAL3 - BlockID Safe uses multi-factor biometric authentication. Factor 1 is the biometrics used to unlock and use the app. Factor 2 would be the CSP requested biometric mechanism (face, voice, thumbprint or pin).

BlockID Safe does a complete out-of-band authentication using biometrics in adherence to Section 5.1.4, Section 5.1.6, Section 5.1.7, Section 5.1.9, Section 5.1.8 and Section 5.1.9 as the distributed ID itself is generated based on BIPS39 standard mnemonic phrase based identifiers linked to its own private and public keys.

SP 800-63-C: Federation Assurance Level

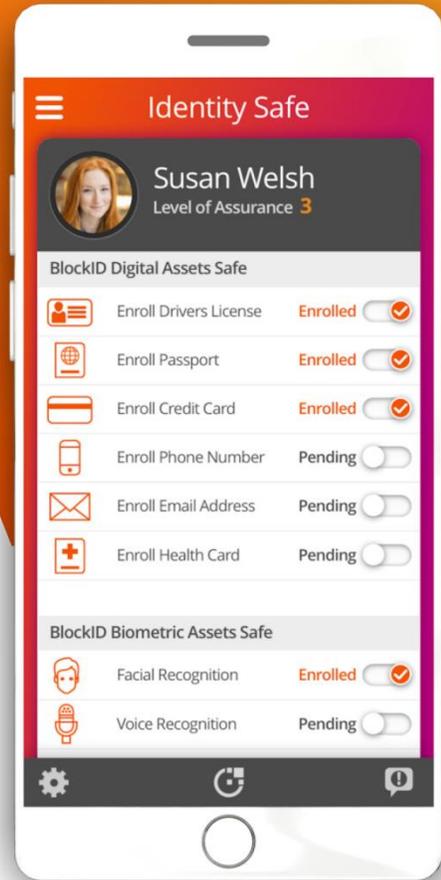
FAL1 - BlockID Safe encrypts all data transmitted using the public key of the service provider thus ensuring that only the intended service provider could decrypt the assertion. This encrypted data is signed by **BlockID** to enable service providers to verify the authenticity of the sender of the assertion

FAL2 - BlockID Safe encrypts all data using RsaSignatureAuthentication2018

FAL3 - BlockID Safe ensures that only the user in possession of the identity credentials is able to decrypt the identity data and could share elements of identity data or attributes as requested by the service provider.

In addition to the above, the FAL (*for additional security & compliance*) is dynamically calculated and is typically a lower of the 2 assurance levels for IAL and AAL (*as indicated in the table.*)

For further detail on NIST standards for SP 800-63-3 visit <https://pages.nist.gov/800-63-3/>



IAL1 + AAL1 = FAL1
IAL1 + AAL2 = FAL1
IAL1 + AAL3 = FAL1
IAL2 + AAL1 = FAL1
IAL2 + AAL2 = FAL2
IAL2 + AAL3 = FAL2
IAL3 + AAL1 = FAL1
IAL3 + AAL2 = FAL2
IAL3 + AAL3 = FAL3

Contact Us

1Kosmos, LLC

 www.1kosmos.com

 info@1kosmos.com