IGAMING/GAMBLING

IDV CERTIFICATIONS

IDVerse is the most certified & compliant identity infrastructure system on the market, providing secure access to your players at scale — wherever in the world they are.

16,000+
ID documents supported

220+
Countries & territories

142
Languages & typesets

The Importance of External Validation

Endorsement from independent organizations plays a crucial role in **establishing credibility and trustworthiness** of IDV vendors. As the demand for robust identity verification solutions grows, certifications from reputable third-party validators like NIST, ISO, SOC, and iBeta/BixeLab serves as a beacon of assurance, instilling **confidence in the reliability, accuracy, and compliance** of authentication systems.

Dependability: External validation enhances the credibility of IDV solutions, signaling adherence to rigorous standards and best practices as well as providing assurance to partners.

Compliance: Third-party certification ensures that IDV vendors and their solutions align with industry regulations, mitigating compliance risks and affirming a dedication to data protection and privacy.

Accuracy: Validation from independent organizations substantiates the precision and dependability of identity verification solutions in authenticating identities and detecting fraudulent activities.

Innovation: By seeking endorsement from reputable external organizations, vendors demonstrate a commitment to continuous improvement, ensuring their solutions remain innovative and effectively address emerging threats.

Certification body	Basic certifications	Advanced certifications
NIST	NIST SP 800-171	NIST SP 800-53, NIST 800-63 IAL2
iBeta/BixeLab against ISO 30107-3	Liveness PAD Level 1	Liveness PAD Level 2, Level B Bias testing
Government entities	CPRA, GDPR	TDIF L3 (Australia), DIATF (UK), DocAuth
ISO (International Organization for Standardization)	ISO 27001, ISO 9001, ISO 19795	ISO 22301, ISO 27017, ISO 27018, ISO 27701, ISO 29100, ISO 30107-3
AICPA System and Organization Controls (SOC)	SOC 1	SOC 2

GET IN TOUCH hello@idverse.com www.idverse.com

WHAT DO OUR CERTIFICATIONS MEAN?

Certifications	Notes	Compliant?
ISO 19795	Biometric performance and testing. Sets testing and grading guidelines for 1:1 face matching algorithms. OCR Labs was tested on this ISO by BixeLabs, a NIST accredited testing laboratory. Achieved accuracy of 99.997% (with False Match Rate of 0.003%, False Non-Match Rate of 0.0%, Failure to Acquire 0.0015% and Failure to Enroll 0.0%).	
ISO 27001:2022	Information security management. Sets out requirements for establishing, implementing, maintaining and continually improving a company's information security management system. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the company.	
ISO 27017:2015	Cloud service providers. Guidelines for information security and controls applicable to the provision and use of cloud services by providing additional controls with implementation and management guidance that specifically relate to cloud services.	
ISO 27018:2019	Protection of personally identifiable information (PII) in the cloud. Establishes commonly accepted control objectives, controls and guidelines for implementing measures to protect PII for the public cloud computing environment. Applicable to all types and sizes of organizations that provide information processing services as PII processors via cloud computing under contract to other organizations. Controls include user, access, information classification and physical environment management, among others.	
ISO 27701:2019	Extension to ISO 27001 for PII management. Specifies requirements and provides guidance for establishing, implementing, maintaining and improving a Privacy Information Management System (PIMS), in the form of an extension to ISO 27001. Specifies PIMS-related requirements and provides guidance for PII controllers and PII processors holding responsibility and accountability for PII processing. Extends an organization's PII management compliance in line with global privacy regulations. Includes requirements for PII consent, conditions for collection, and privacy by design.	
ISO 22301:2012	Business continuity management system (BCMS). Specifies requirements to implement, maintain and improve a BCMS to protect against, reduce the likelihood of the occurrence of, prepare for, respond to and recover from disruptions when they arise. Also applicable to the need to be able to continue to deliver products and services at an acceptable predefined capacity during a disruption and to ensure security and resilience of the system.	
ISO 30107-3	Biometric presentation attack detection (PAD). Tested by iBeta. Liveness PAD Level-1 using high quality photos and videos of likeness with equipment readily available in a home or office environment. Test time for each PAD = 8 hours "per species". 100% success for OCR Labs, with 0% presentation attack success rate. Completed Sep. 2019. Liveness PAD Level-2 using high resolution photos and latex masks with more expensive equipment. Test time for each PAD = 48-96 hours "per species". 100% success for OCR Labs, with 0% presentation attack success rate. Completed Jun. 2020 and re-assessed in March 2023.	
ISO 9001:2015	Quality management systems. Specifies requirements for a quality management system (a) to demonstrate a company's ability to consistently provide products and services that meet customer and statutory and regulatory requirements, and (b) to enhance customer satisfaction through the effective application of the system, including processes for improvement of the system and the assurance of conformity to customer and statutory and regulatory requirements.	
NIST 800-63A	Digital identity. Guidelines for identity proofing as set out by the US National Institute of Standards and Technology (NIST). BixeLabs has confirmed that OCR Labs conforms with these Guidelines to the IAL2 level relating to remote identity verification.	
BixeLab Level Bias Evaluation Assurance	Demographic differentials. A new test protocol developed by BixeLab to evaluate the demographic differentials, or bias, in biometric liveness detection systems. Bias is not limited to biometric matching algorithms. It also applies to PAD or "liveness detection". Includes testing of the OCR Labs liveness algorithm to validate it is equally accurate for all demographic groups varying by gender, age, and geographic origin.	
FIDO	FIDO Biometrics Requirements. Biometric performance certification administered by the Fast Identity Online (FIDO) Alliance. Includes reference in part to ISO 19795 definitions and guidelines.	
SOC 2, Type 2	Service Organization Controls (SOC) audit framework. SOC for Service Organizations reports are designed to help service organizations build trust and confidence in the service performed and controls related to the services through a report by an independent CPA. The standards were developed by the American Institute of CPAs (AICPA). SOC 2 - Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy – includes an assessment of the oversight of the organization, internal corporate governance and risk management processes, and regulatory oversight.	
NIST 800-53	Risk Management Framework that sets a US government standard for security and privacy controls. We are compliant (though not certified) against NIST 800-53.	