Ensuring Trustworthy Digital Identities:

A Primer on Ensuring Secure and Reliable Remote Biometric Identity Verification & Onboarding

BixeLab

Testing, compliance, and certification for identity and biometric solutions.

3/16 Bentham Street, Yarralumla, ACT 2600, Australia.

www.bixelab.com

info@bixelab.com

Executive Summary

Trust has become a fundamental component in how we negotiate our personal and business relationships in a fast-paced, highly linked world. Making online payments, accessing government services, completing property deals, and establishing businesses are only achievable when the individuals undertaking these transactions can trust each other. Connecting digital identities to those in the real world is foundational to this trust.

How can we increase trust over the internet? By having sound advice from world-leading experts when selecting and implementing biometrics for digital identity. By getting independent validation of performance by an organization accredited to meet international standards of security, accuracy and usability. By understanding risk through this advice and testing. This is the mission of Bixelab: to be the global leader in the assurance and trust of digital identity products and services through standardised testing and evaluation.

From passing through borders to paying your taxes, the binding of biometrics to identity credentials to prove an individual's identity is now a critical part of the global trust ecosystem. The trustworthiness of this connection between digital and real-world identity underpins everything else that uses digital identity to transact. Further, these connections should be underpinned by technology making it easier to access services, not harder for certain groups due to technological restrictions or biases.

This primer provides valuable insights into key threats and effective strategies for biometric risk management in remote ID verification. By implementing comprehensive testing approaches, technology providers and users can ensure accurate results and manage risk while maintaining a balance between security and usability.

info@bixelab.com
www.bixelab.com

Understanding key remote digital identity verification processes

The Remote Identity Proofing process generally requires an applicant to:

- Use their electronic device to provide a photograph of a government-issued identity document to attest their identity which is:
  - to be validated by the service provider and/or,
  - to be validated for authenticity using an automated detection system (aka 'Automated Document Verification' for Driver Licenses, passports etc.).
- Use their electronic device to provide a definitive proof that the applicant is physically present with the device and their identity document.
- Receive a high confidence match between their verification photo or video and their photo, present on their identity document or in the NFC chip.
- Prove that they are a live person and not an attack instrument presented to the data capture sensor (aka 'Presentation Attack Detection').

Some of the key processes involving remote digital identity verification include:

- Automated Document Verification
- Optical Character Recognition
- Biometric Matching
- Presentation Attack Detection

The probabilistic nature of machine learning and artificial intelligence aspects of such electronic digital identity verification systems, along with continuous improvements in sophistication of attacks on these systems, require extensive and continual testing to ensure that they deliver good outcomes that meet the balance of security and usability requirements.

info@bixelab.com
www.bixelab.com

Key threats to the process:

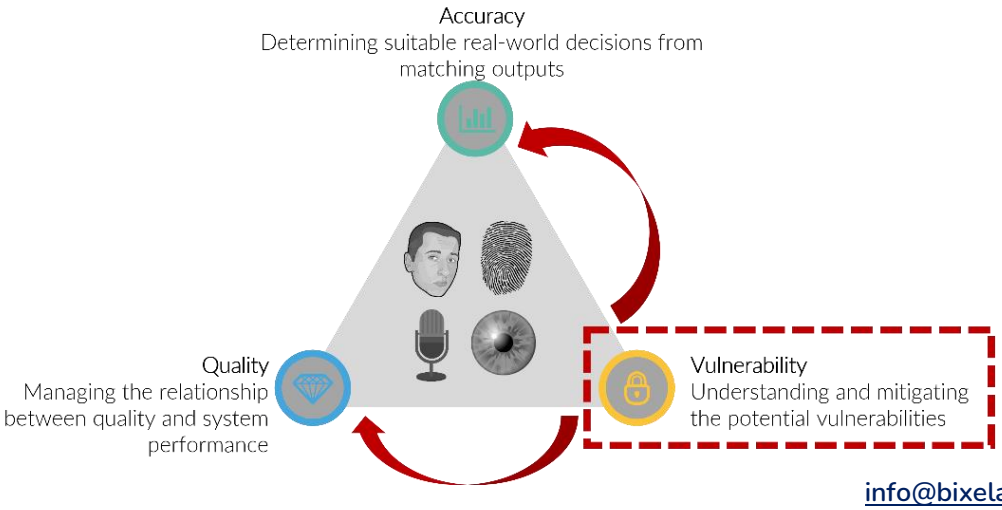
Understanding and addressing key threats to the remote digital identity verification process is essential for maintaining security and reliability.

- Attacker bypasses automated document authenticity checks when using a fake/counterfeit ID document to enrol e.g., photo substitution.
- Attacker bypasses the liveness/PAD detection mechanisms when using a digital or physical artefact for impersonation e.g., deepfakes.
- Attacker bypasses the matching by getting incorrectly accepted as a different person e.g., twins.

Testing Approaches:

Effective evaluation and maintenance strategies are key for ensuring a high degree of confidence in the overall performance and security of remote digital identity verification systems.

- Validate the accuracy and reliability of the automated document verification process by subjecting it to a wide range of genuine and forged identity documents, covering evolving forgery techniques.
- Evaluate the accuracy and reliability of biometric matching algorithms by testing diverse sets of images, considering various demographics, and comparing the applicant's verification photo or video with their identity document or NFC chip.
- Assess the effectiveness of presentation attack detection mechanisms by conducting comprehensive testing with different types of attacks, including printed photos, videos, masks, and other spoofing techniques.
- Perform vulnerability assessments and penetration testing to identify and mitigate potential software and hardware vulnerabilities, ensuring the system's security and integrity.
- Ensure compliance with privacy regulations, evaluate data anonymization, encryption, access controls, and secure transmission protocols to safeguard user data appropriately.
- Conduct fairness assessments to identify and address algorithmic biases, ensuring equitable treatment across different demographic groups and minimizing discriminatory outcomes.
- Complete these assessments and testing process to international standards, performed by an independent party accredited to do the job.



info@bixelab.com
www.bixelab.com

Managing Remote ID Verification Risks:

- Assess the stand-alone performance as well as the end-to-end performance of the completed solution to manage risks associated with each individual line of defense (quality/ID authenticity/Liveness and Matching).
- Gain insights on the impact each component's settings and configurations have on the overall success rate.
- Assess the performance of the people performing manual back-office biometric processes in support of automation failures.
- Understand the residual risks associated with complete system working with these subcomponents which each work on their own individual configurations.

Use of Biometrics to support digital identity requires addressing the following key aspects:

- Biometric performance testing
- Ongoing performance management
- Usability
- Manual Face Comparison and Document Examination
- Privacy
- Data security

To assist organisations in obtaining reliable digital identity services, global initiatives are underway to establish industry best practices and technical requirements. Interoperability among multiple frameworks is being prioritized. Although it may take time for various standards and frameworks to converge, this indicates a positive movement towards establishing a shared basis for dependable digital identity services. These frameworks offer valuable guidance for securely implementing digital identity services in diverse scenarios. Notable among these frameworks are:

NIST SP 800-63 provides technical requirements for US federal agencies implementing digital identity services and covers identity proofing and authentication of users interacting with government IT systems over open networks.

eIDAS Regulation provides a common foundation for secure electronic interaction between citizens businesses and public authorities in the EU.

FIDO Identity Verification and Binding will have testing requirements and specifications for remote, possession-based techniques including biometric "selfie" matching and government-issued identity document authentication.

Trusted Digital Identity Framework (TDIF) is an accreditation framework for Australian digital identity services and currently addresses biometric accuracy and presentation attack detection (automated document fraud detection testing requirements to come in future iterations).

UK Trust Framework provides accreditation framework for identity services in the UK. Currently covers aspects of performance testing and bias reduction based on ISO/IEC 19795.

Digital Identity: Standardisation Efforts

Where biometrics testing for matching and liveness system subcomponents has gained national and international standardisation, work is ongoing to establish international standards and best practices relating to assessment of Automated Document Verification systems.

As a leading independent laboratory specialising in biometric and identity testing, certification, and compliance for ISO/IEC, NIST, and FIDO, BixeLab is committed to driving innovation and advancing the field of biometrics. Our formal lab accreditations from NIST/NVLAP [Lab Code: 600301-0] and FIDO have allowed us to provide services to government and private sector clients around the world. We would be delighted to assist your organisation navigate the challenges of digital identity and biometric solutions with confidence.

Reach out to us on info@bixelab.com for more information.