



Navigating the Complexities of Remote Identity Proofing



The Spectrum of Identity Assurance

Contents

- 1** ● **Introduction**
- 2** ● **In-Person Identity Verification to Remote Identity Verification**
 - The Move to Remote
 - The Importance of Remote Identity Proofing
 - Levels of Confidence in Remote Identity Proofing
- 3** ● **Remote Identity Proofing: A Security Inflection Point, Not A Commodity**
- 4** ● **Establishing the Initial Foundation: Identity Verification Technologies**
 - Database Verification
 - Document Verification
 - Biometric Check
- 5** ● **Why Does it All Matter? Chasing the Remote ID Eutopia**
- 6** ● **Conclusion**

Introduction

Identity verification is a critical component of the identity proofing and user onboarding process for many organizations, particularly those in highly regulated industries such as financial services, government, healthcare, border control, and travel. As the world becomes increasingly digital and mobile, the need for secure and reliable remote identity verification methods has grown exponentially.

This paper will focus on the spectrum of identity verification methods and technologies available for remote identity proofing - critical in establishing trust during onboarding for a secure user lifecycle.

The complexity of the onboarding process can vary greatly depending on the industry, the level of risk associated with the product, service, or physical access, and the regulatory requirements that must be met. Factors such as the types of identity documents accepted, the level of assurance required, the need for biometric verification, and the user experience all play a role in determining the appropriate combination of identity verification methods and technologies.



In-Person Identity Verification to Remote Identity Verification

In-person verification, once considered the gold standard for identity proofing, has several limitations that impact its sustainability, effectiveness, and competitiveness in today's digital-first world. It requires individuals to physically present themselves and their identity documents at a designated location, which is often inconvenient, time-consuming, and costly for both the user and the verifying organization. In an era where people expect seamless online experiences, this requirement for physical presence becomes a significant barrier to action and a source of competitive disadvantage.

This method relies heavily on human judgment to detect inconsistencies or signs of fraud, leading to potential identity verification errors. Moreover, in-person verification is not easily scalable, as it requires significant investment in trained personnel and physical infrastructure, resulting in long wait times, reduced accessibility, and a poor user experience. These factors directly impact scenarios like customer onboarding and acquisition, potentially leading to higher drop-off rates and in the case of workforce onboarding, causing unacceptable increases in time-to-value or limited workforce locations. In both cases, the inefficient and time-consuming processes have the potential to cause financial harm to the organization.

Furthermore, in-person verification is limited by geographical locations and operational opening times, restricting availability and convenience. This limitation is particularly problematic in a world where consumers now expect 24/7 access to services and employers want to provide access to extended workforces regardless of location. Organizations relying on in-person verification may find themselves at a competitive disadvantage compared to those offering more convenient, fully digital identity verification solutions.

Given the high costs associated with in-person verification and its potential for disruption it is best used as an exception rather than the norm, reserved for specific situations where its benefits outweigh its limitations and competitive drawbacks.

These factors collectively contribute to the growing shift towards remote identity verification methods, which offer greater flexibility, scalability, and cost-effectiveness while addressing the limitations of traditional in-person verification.

The Move to Remote

Remote identity proofing has become a critical focus for organizations seeking to establish trust and security in online interactions. This whitepaper series emphasizes remote identity proofing solutions rather than in-person verification methods. As well as increased efficiency and reduced cost, remote ID is an opportunity to expand accessibility and convenience for users, enabling secure identity verification from anywhere, at any time, on their preferred devices.

Multiple studies demonstrate the statistically significant effect of trust on economic growth. Countries and organizations with weak institutions and low confidence lack economic development, highlighting the importance of building trust through robust identity verification systems ¹.

1. Zakharov, D., Bezruchuk, S., Poplavska, V., Laichuk, S., & Khomenko, H. (2020). *The ability of trust to influence GDP per capita. Problems and Perspectives in Management.*

By prioritizing the implementation of advanced, secure remote identity proofing techniques, organizations can foster an environment of trust in digital interactions. As we continue to navigate the complexities of digital identity, the focus on robust, reusable identity verification will play a pivotal role in shaping secure, efficient, and user-centric digital ecosystems that drive economic growth, financial inclusion, and social welfare.



The Importance of Remote Identity Proofing

Remote identity proofing forms the cornerstone of trust between organizations and individuals in the digital world. It's important to note that the terms “identity proofing” and “identity verification” are often used interchangeably, which can blur the lines between these concepts.

Identity proofing, broadly speaking, is the process of establishing trust in a person's claimed identity. This can involve various methods and levels of scrutiny, depending on the context and requirements. It verifies a person's claimed identity based on provided evidence and organizational checks. This process is crucial for mitigating risks like identity theft, account takeover, and money laundering.

Effective identity proofing offers multiple benefits:

- Regulatory compliance (KYC, AML)
- Enhanced customer trust
- Improved user experience during onboarding



While the terms often overlap, it can be helpful to distinguish between related concepts:

- **Identity Proofing:** Establishes initial trust through various means
- **Identity Verification:** Often used synonymously with identity proofing, but can specifically refer to confirming the authenticity of a claimed identity
- **Remote Onboarding:** Utilizes these processes for secure digital enrollment

It's worth noting that many factors can contribute to establishing trust in a person's identity, and the specific methods used may vary depending on the organization's needs and regulatory requirements.

Robust identity proofing safeguards organizations from financial losses and reputational damage, often associated with data breaches or imposter attacks. Organizations can build secure, trusted relationships with users in an increasingly digital landscape by prioritizing this foundational step.



Levels of Confidence in Remote Identity Proofing

Remote identity proofing processes can provide varying levels of confidence in the asserted identity. The International Organization for Standardization (ISO) has established standards defining these assurance levels (LoA). Specifically, ISO/29003² (Identity Proofing)

2. <https://www.iso.org/standard/62290.html>

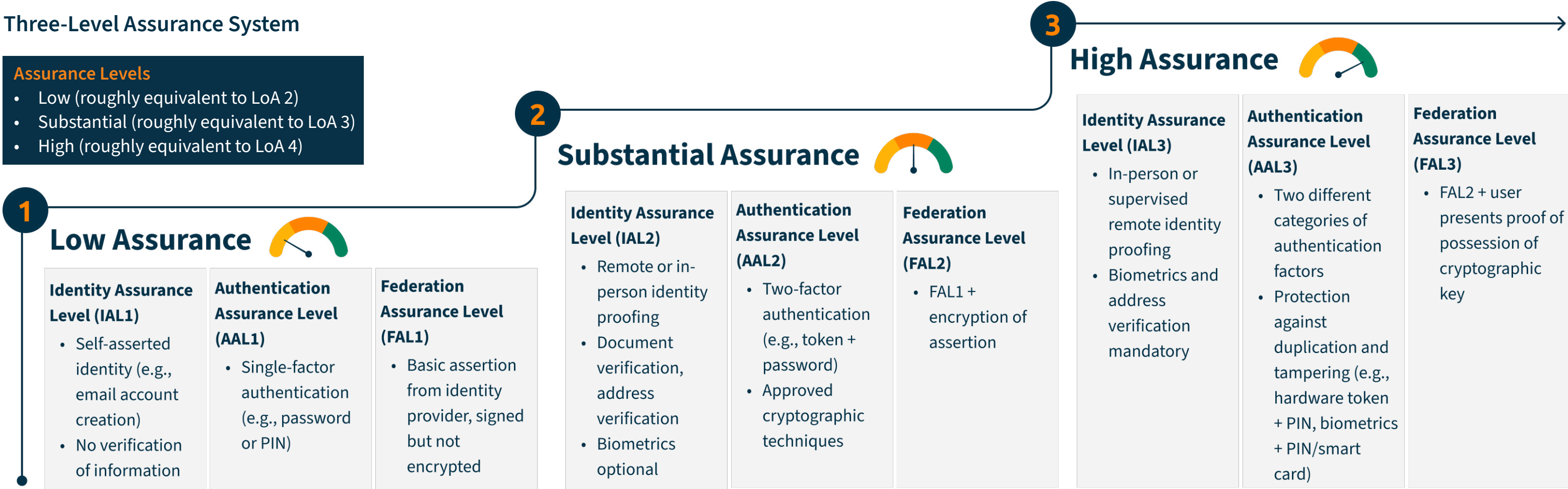
and ISO/IEC 29115 (Entity Authentication Assurance Framework) outline four levels:

- LoA 1:** No/Minimal Confidence
- LoA 2:** Some Confidence
- LoA 3:** High Confidence
- LoA 4:** Very High Confidence

These ISO standards serve as the main guidelines for identity assurance levels. However, various

government and regional standards have adapted these levels to suit their specific needs, sometimes using different labels or not adopting all levels. For example, the European Union’s electronic IDentification, Authentication and trust Services (eIDAS) regulation broadly aligns with the ISO standards but uses a three-level system:

Three-Level Assurance System



The appropriate level of assurance depends on the specific use case and the associated risks. Organizations should conduct a thorough risk assessment to determine the level of assurance required for each scenario. Factors to consider include:

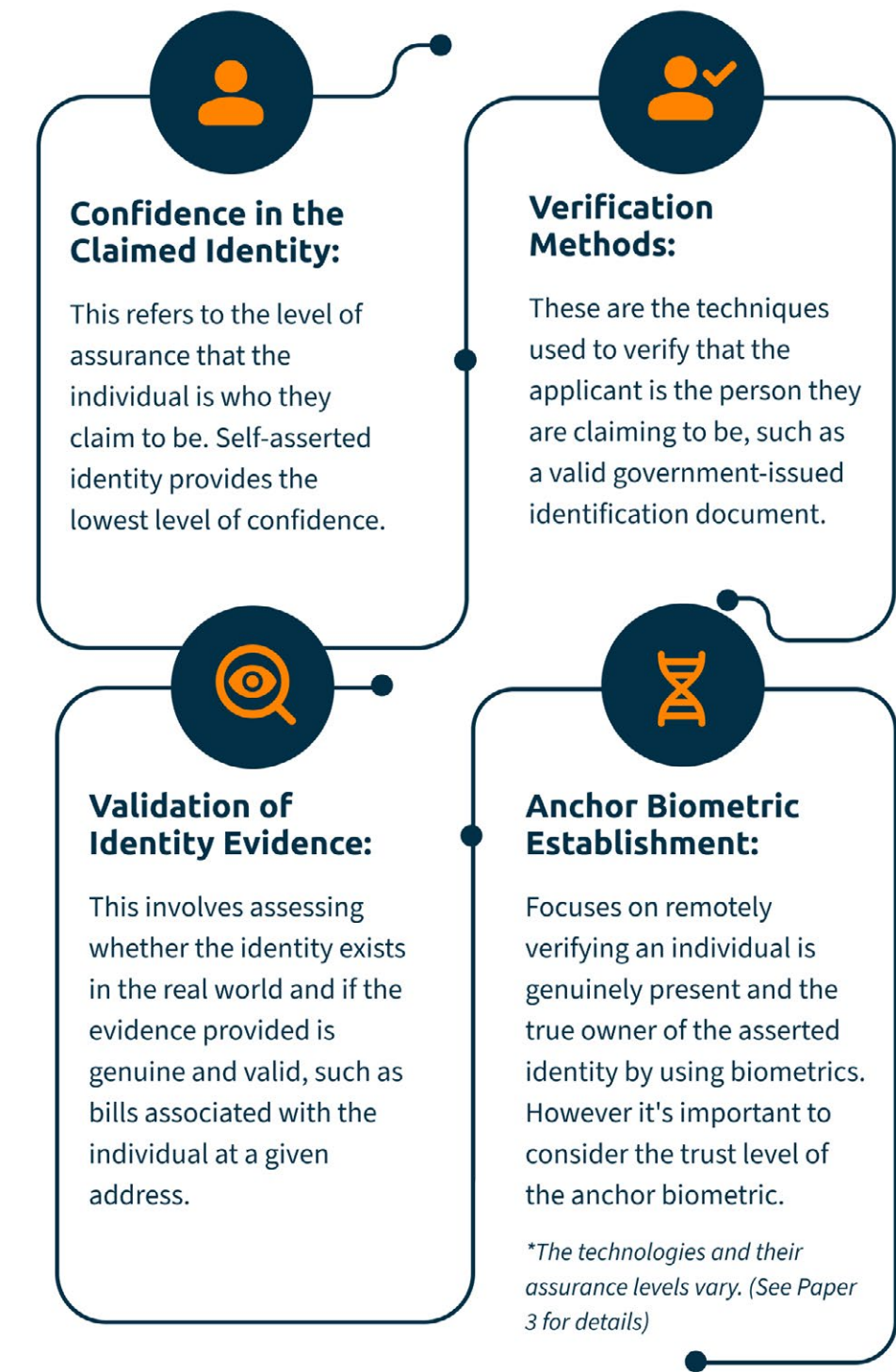
- The potential impact of identity fraud
- The sensitivity of the data or services being accessed
- The contextual knowledge of the individual participating in the use case
- The regulatory requirements applicable to the industry

These levels of assurance are closely tied to identity profiles, which specify the combination of evidence and checks required to achieve a given level of assurance. By aligning their identity proofing processes with the defined identity profiles and corresponding assurance levels, organizations can ensure appropriate security measures to mitigate fraud, maintain consistency, and adhere to best practices, ultimately enhancing their return on investment (ROI).

While these standardized levels aim to bring consistency to identity assurance, the variations in how different regions and regulations adapt them can present challenges for global interoperability in identity verification systems.

Risk-Based Approach: The level of assurance required (LoA) should match the risk associated with the transaction or service. Higher risk scenarios might necessitate stronger evidence and additional security measures.

The Identity Proofing Process



Remote Identity Proofing: A Security Inflection Point, Not A Commodity

As remote interactions become the norm, organizations recognize the critical importance of establishing trust in both consumer and workforce onboarding processes. Trust is key to organizational security and customer confidence, driving productivity, efficiency, and economic growth.

Verifying identities remotely - whether for customers or employees - is crucial for organizational security and customer trust. This trust forms the foundation for secure digital ecosystems. When organizations can confidently verify identities, they're more likely to grant appropriate access, conduct secure transactions, and enable productive interactions. This increased trust leads to greater efficiency across various sectors, contributing to overall economic growth and innovation.

Organizations must carefully assess all facets of identity verification for both consumers and workforce, including the strength of assurance, user experience, and risk mitigation. By selecting the right combination of technologies and processes, such as biometrics, document verification, and secure digital credentials, organizations can create efficient onboarding processes that balance user experience with security and compliance. This balance is crucial for fostering trust, loyalty, and reducing security risks.

A trustworthy digital identity ecosystem enables seamless and secure interactions across various platforms and services, enhancing productivity and opening new opportunities for secure remote engagement. By prioritizing trust in identity proofing, organizations protect themselves, their employees, and their customers, contributing to a more robust, efficient, and productive digital economy.

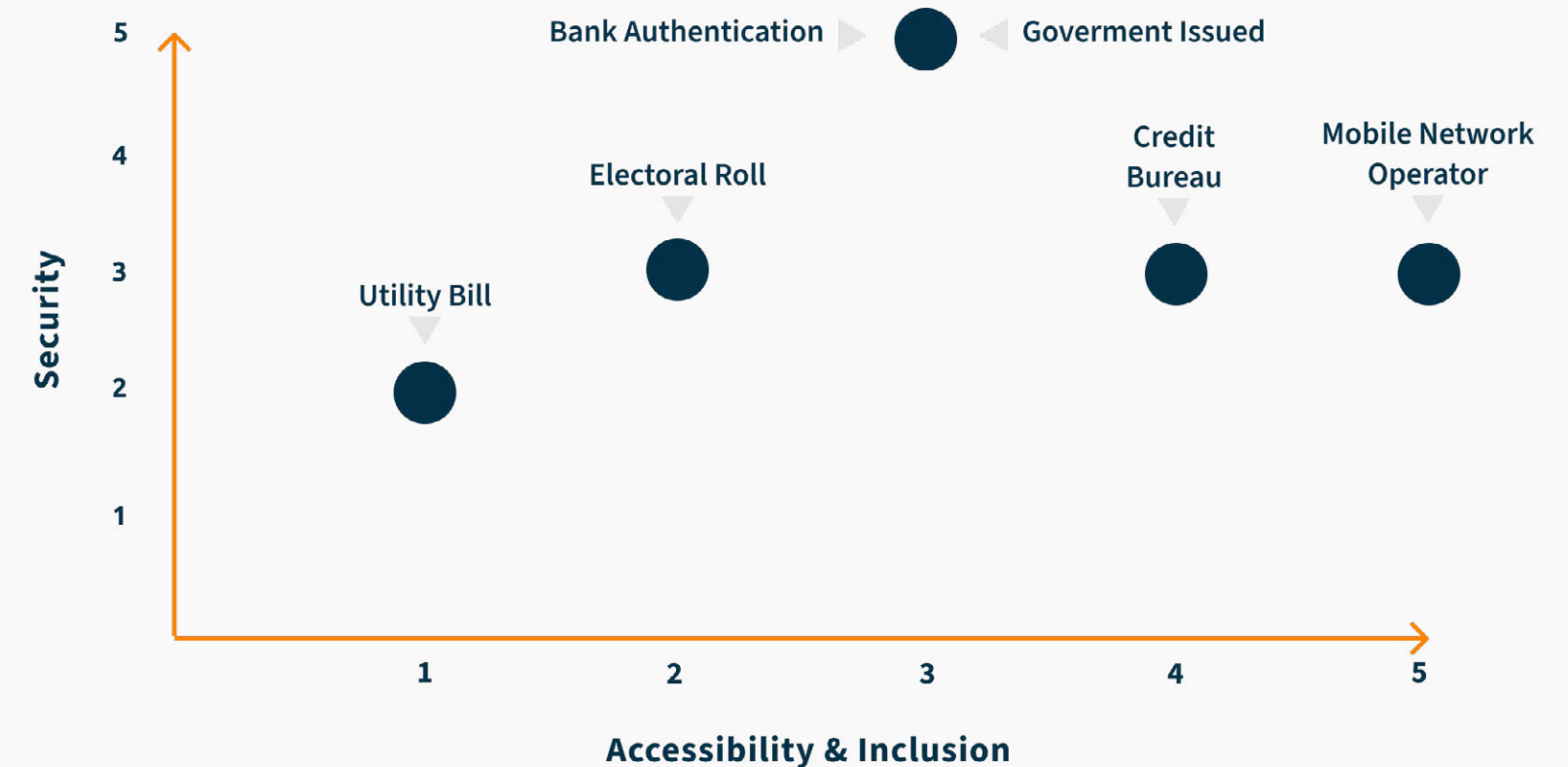


Establishing the Initial Foundation: Identity Verification Technologies

1. Database Verification

Database verification offers organizations the ability to cross-reference user-provided information against trusted databases, such as credit bureaus, government records, and utility providers. This method is often used in combination with other verification techniques to enhance the overall level of assurance, providing a more comprehensive view of an individual's identity. The strengths of database verification lie in its instantaneous nature and its ability to operate seamlessly in the background. This method streamlines the identity proofing process by validating user information against third-party sources without requiring additional actions from the user beyond submitting their initial information.

Security vs. Accessibility & Inclusion - Ranking scale (1-5)



However, it's important to note that this approach typically offers a lower level of assurance than more robust identity verification methods. While it checks submitted data against credit reference agencies or similar databases, it lacks the stronger security measures of linking to a government-issued identity or incorporating the user's biometric data. Moreover, this method can be biased against individuals without sufficient financial credit history, potentially excluding or disadvantaging certain populations. These limitations mean that database verification alone is often insufficient to provide adequate certainty about a user's claimed identity, particularly in contexts requiring higher levels of security or regulatory compliance. A more inclusive and secure approach would combine multiple verification methods to ensure both accuracy and fairness.

The effectiveness of database verification relies heavily on the accuracy and security of the databases being accessed. Incomplete, outdated, or compromised data, as well as differences in the quality of data depending on locality, can lead to false rejections or potential identity fraud.

2. Document Verification

Document verification is a crucial component of remote identity proofing, offering organizations a reliable means of verifying an individual against their government-issued identity. This method involves capturing an image of a passport, driver's license, or other official ID and subjecting it to rigorous analysis. The key strength of document verification lies in its ability to provide a higher level of assurance compared to database checks alone.

By verifying a person against their government-issued ID, businesses can more confidently establish the authenticity of a user's claimed identity. This is particularly valuable in contexts requiring stringent identity verification, such as financial services, travel, and other regulated industries. The distinguishing factor is the higher level of assurance it provides by linking the verification process directly to government-issued identification. This enables organizations to meet regulatory requirements and mitigate fraud risks while providing a convenient process for users in today's digital landscape.

The effectiveness of this method relies heavily on the security features and integrity of the identity document itself. Document verification remains a powerful tool in the identity proofing toolbox, providing a strong foundation for establishing trust in remote interactions when combined with other verification techniques and ongoing fraud monitoring.



Optical Character Recognition (OCR)

OCR technology extracts data from a captured image of a document, such as a passport or driving license. This includes personal information and the machine-readable zone (MRZ), a core security feature of identity documents containing a string of characters. The document authenticity can be verified manually or using machine learning techniques. The document image is extracted and matched to the selfie captured during the user session.



Near-Field Communication (NFC)

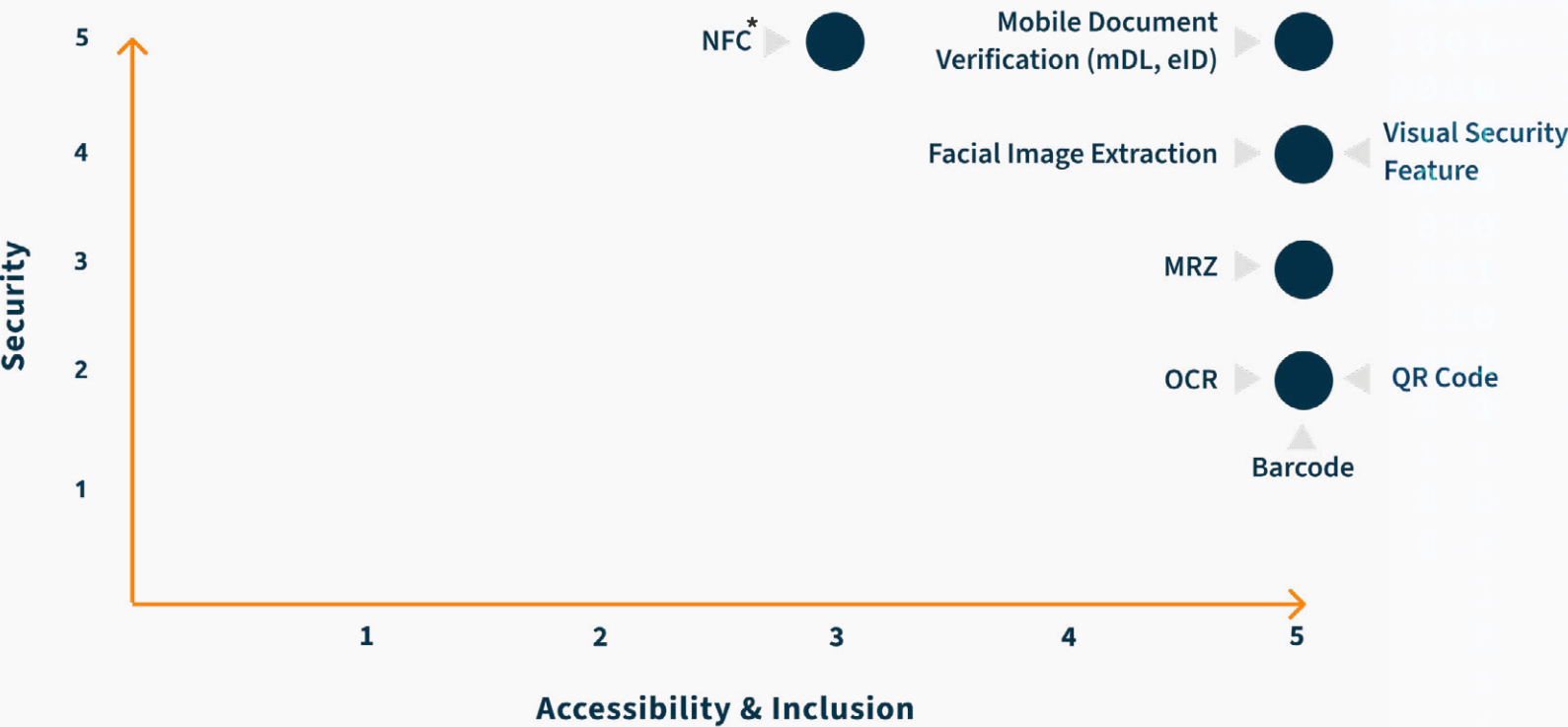
Documents with an electronic chip can be verified and validated using the NFC reader in a smartphone. With a quick tap, data is extracted and cryptographically verified. Advanced security features are unlocked to detect forged or manipulated documents. The chip also includes biometric data, such as a photo or fingerprint, which can be matched against the biometrics captured during the user session.



Technologies and methods used in document verification:

There are several methods to validate the genuineness of an identity document during verification. For example, US Driver’s Licenses have a barcode on the rear containing much of the same biographical data printed on the front of the license, which can be validated using barcode reading. So, in addition to OCR, the data can be validated using barcode reading. Some passport issuers, on the other hand, rely on NFC chips while others have added a QR code too.

Security vs. Accessibility & Inclusion - Ranking scale (1-5)



*NFC accessibility is currently rated at 3 due to adoption, but is expected to increase as it becomes more widely available across regions

3. Biometric Check

The final check is to verify that the remote person asserting that identity is real. NIST³ defines two remote ways of achieving this; ‘Remote Attended’ and ‘Remote Unattended’:

3. Temoshok D, Proud-Madruga D, Choong YY, Galluzzo R, Gupta S, LaSalle C, Lefkovitz N, Regenscheid A (2024) Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-4 2pd. <https://doi.org/10.6028/NIST.SP.800-63-4.2pd>

Remote Attended:

‘Remote Attended’ relies on human interaction and judgment, namely that the person on the screen is an actual human being. This is typically done via video conference. It provides a personal touch but potentially introduces vulnerabilities. For instance, video conferencing is vulnerable to deepfake technology to impersonate a real person^{4&5}. It can also be compromised by poor network conditions, leading to unclear images or audio that make accurate verification difficult⁶. Additionally, human verification is inherently biased, as agents may become fatigued or distracted during long sessions, potentially missing crucial details in the verification process^{7&8}.

3. Temoshok D, Proud-Madruga D, Choong YY, Galluzzo R, Gupta S, LaSalle C, Lefkovitz N, Regenscheid A (2024) Digital Identity Guidelines. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-63-4 2pd. <https://doi.org/10.6028/NIST.SP.800-63-4.2pd>

4. Groha, M., et al. (2021). Deepfake detection by human crowds, machines, and machine-informed crowds. The Proceedings of the National Academy of Sciences (PNAS).

5. Yang, X., Li, Y., & Lyu, S. (2018). Exposing deep fakes using inconsistent head poses. ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP). IEEE, 2019.

6. Davis, J. P., & Valentine, T. (2015). Human verification of identity from photographic images. Forensic Facial Identification: Theory and Practice of Identification from Eyewitness, Composites and CCTV.

7. Weatherford, D.R., Roberson, D. & Erickson, W.B. (2021). When experience does not promote expertise: security professionals fail to detect low prevalence fake IDs. Cogn. Research 6, 25.

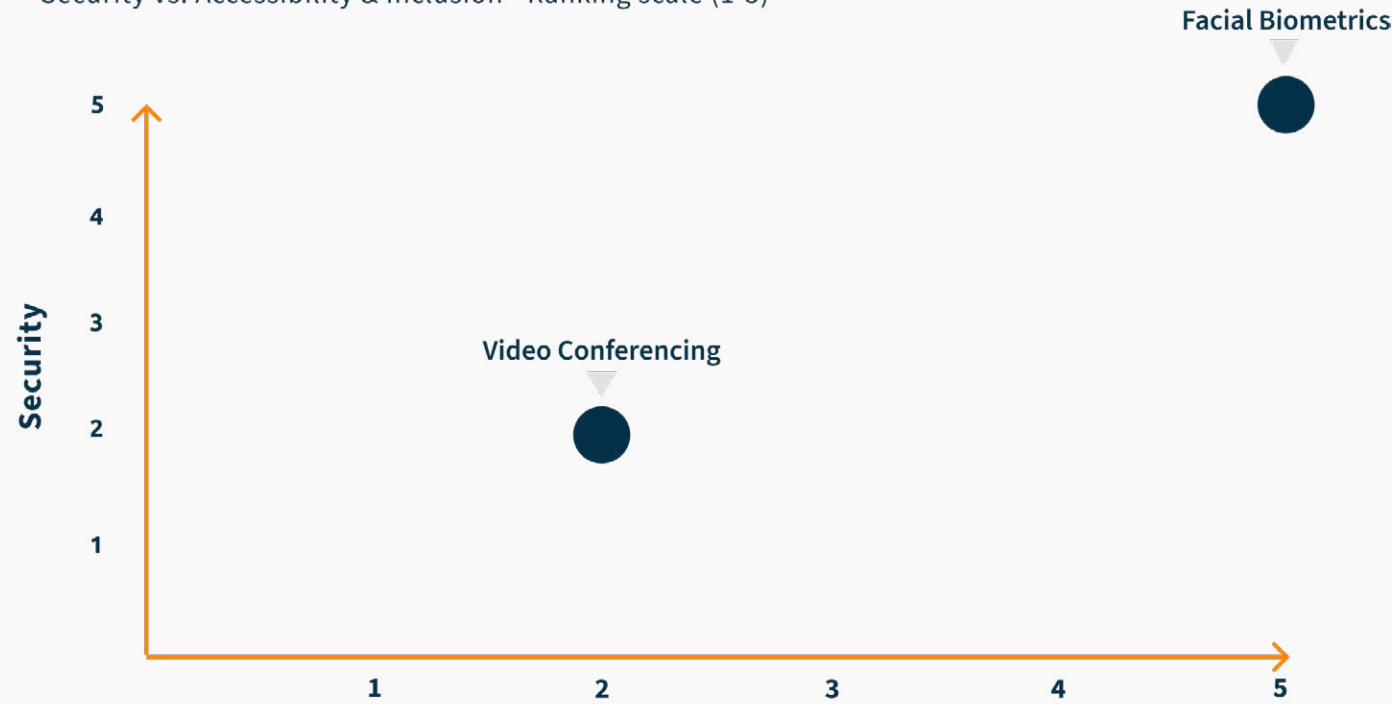
8. Drew, T., Vo, M. L. H., & Wolfe, J. M. (2013). The invisible gorilla strikes again: Sustained inattentional blindness in expert observers. Psychol Sci. 2013 September; 24(9): 1848–1853.

Remote Unattended:

‘Remote Unattended’ is performed by Facial biometric verification (FBV) with liveness detection. Liveness detection is a critical security feature that determines whether the biometric sample (in this case, a face) is from a live person present at the point of capture, rather than a photo, video, or mask. Leveraging advanced algorithms, liveness detection, and 3D mapping, FBV offers enhanced security, accuracy, and inclusion compared to traditional methods. As an anchor point in digital identity ecosystems, FBV provides robust protection against spoofing attempts, especially when combined with ongoing threat management.

Regardless of whether it’s attended or unattended, remote identity proofing must rely on strong evidence.

Security vs. Accessibility & Inclusion - Ranking scale (1-5)



Why Does it All Matter? Chasing the Remote ID Eutopia

As our world becomes increasingly digital, there's a growing need for reusable identity proofing processes. The strength of initial verification processes is crucial for the integrity of the entire digital identity ecosystem. This approach creates trust across digital wallets and various applications, eliminating repetitive identity verifications and laying a foundation for ongoing digital interactions.

Electronic ID (eID) systems, including physical digital identity cards, have marked significant progress in this domain. They offer enhanced security through features like biometrics and encryption, provide convenience for both online and offline scenarios, reduce fraud through tamper-resistant designs, and streamline access to government services.

Building on eID systems, verifiable credentials take digital identity further by offering:

- Interoperability across different systems and jurisdictions
- Reusability for multiple purposes
- Enhanced privacy control for users
- Selective disclosure of specific attributes
- Reduced reliance on central authorities

However, it's crucial to note that the challenge with verifiable credentials and reusable digital identity lies in building an ecosystem of organizations that accept these credentials. For digital identities to be truly reusable, there must be a network of entities willing to recognize and trust these credentials across various contexts and transactions. This requires extensive collaboration, standardization efforts, and often, regulatory support.

While blockchain has been proposed for decentralized identity systems, it faces challenges in scalability, energy consumption, and regulatory compliance. Alternative technologies like decentralized identifiers (DIDs) and zero-knowledge proofs may offer similar benefits without these drawbacks.

The importance of establishing trust at the outset of the user lifecycle is paramount. Creating high-assurance verified credentials for continued use is vital in the eID ecosystem, especially as we transition into an era dominated by digital identity ecosystems. The security methods employed during remote onboarding must be of the highest caliber, as they form the foundation for all subsequent digital interactions.

eID, with facial biometrics and liveness detection at its core, has emerged as a game-changer in digital identity proofing. This foundation ensures that the person presenting the digital identity remotely is genuinely present and matches the registered biometric data. The integration of liveness-based facial biometric verification with pre-existing, rigorously proofed digital identities reduces the need for repetitive verifications while maintaining robust security.

A key advantage of eID and verifiable credentials is selective disclosure. For example, if an organization only needs to verify a person's age, this is the only information they will receive. This approach, rooted in facial biometric verification, reduces over-sharing of personal identifiable information (PII) and minimizes “honeypots” of identity information. Even if fraudsters manage to circumvent a link in the chain, the potential use of this information becomes negligible.

As we navigate the complexities of digital identity, focusing on robust, reusable identity verification will be crucial in shaping secure, efficient, and user-centric digital ecosystems. It's essential to thoroughly vet third-party facial biometric vendors to ensure the resilience of their technology, a topic that will be covered in more detail in the third paper of this series, “Spectrum of Identity Assurance: Navigating Facial Biometrics.”

Challenges

The success of verifiable credentials and eID systems will ultimately depend on widespread adoption and the development of trust frameworks that enable seamless, secure transactions across various sectors and jurisdictions. A primary challenge is the prerequisite for users to possess a pre-existing digital identity from a trusted issuer. This requirement may impede regions or demographics with limited access to such trusted authorities.

Moreover, the security and availability of the issuing authority's systems are paramount to the reliability of eID. This underscores the critical need for robust infrastructure and continuous monitoring to ensure the integrity and accessibility of these systems.

Despite these considerations, the benefits of eID in terms of enhanced security, privacy, improved user experience, and reduced identity fraud make it a compelling solution for organizations seeking to establish trust in digital interactions.



Trust Frameworks and Digital Identity Ecosystems

As we have established, the success of eID is intrinsically linked to the existence of trust frameworks and digital identity ecosystems. These ecosystems involve the collaboration of multiple stakeholders, including governments, financial institutions, and service providers. Together, these entities work to define common standards, policies, and processes for issuing, managing, and using digital identities.

These frameworks serve several crucial functions:

- They establish a common language and set of expectations for all participants in the digital identity space.
- They define the levels of assurance required for different types of transactions or services.
- They outline the technical and operational requirements for identity providers and relying parties.
- They provide mechanisms for dispute resolution and liability allocation.

Several notable examples of such frameworks exist globally

- 1** The eIDAS (electronic IDentification, Authentication, and trust Services) regulation in the European Union provides a standardized framework for electronic identification and trust services across EU member states.
- 2** The NIST (National Institute of Standards and Technology) Digital Identity Guidelines in the United States offer comprehensive guidance on digital identity verification, authentication, and lifecycle management.
- 3** The Pan-Canadian Trust Framework in Canada aims to develop a national, interoperable system for digital identity and authentication.

These frameworks play a vital role in fostering trust, interoperability, and standardization in digital identity ecosystems. They provide the necessary structure and governance to support the growth and adoption of eID systems while also addressing critical issues such as privacy, security, and user rights.

The importance of these trust frameworks will be instrumental in realizing the full potential of verifiable credentials and reusable digital identities, enabling seamless, secure, and trusted digital transactions across various domains and jurisdictions.

Conclusion

In the rapidly evolving digital landscape, organizations must navigate the complex spectrum of identity assurance to establish trust, mitigate fraud, and deliver secure, user-friendly experiences. As remote onboarding becomes the norm, biometric technologies have emerged as the essential anchor for robust identity verification systems.

By leveraging innate characteristics tied to government-issued documents, biometrics provide a level of assurance that is difficult to replicate or forge. However, the other factors must not be dismissed. Adopting a risk-based, multi-layered approach to identity proofing is essential to establish the right level of assurance for the organization's use case, creating a comprehensive security ecosystem.

Identity verification (IDV) is often implemented as a one-time process during user onboarding. However, best practices suggest incorporating periodic re-verification to ensure the identity remains valid over time. This is where biometrics and verifiable credentials can play a crucial role, allowing for more seamless and secure ongoing verification.

Some organizations, particularly in regulated industries like banking, implement continuous monitoring in the form of Anti-Money Laundering (AML) checks, screening customers against watchlists on an ongoing basis.

It's important to distinguish between the ongoing nature of these security measures and the continuous improvement efforts of identity verification technology providers. While the end-user may not experience constant identity checks, the underlying systems and algorithms are typically subject to regular updates and enhancements to address emerging threats and improve accuracy.

While identity verification itself may not always be a continuous process for the user, maintaining the security and effectiveness of the system requires ongoing attention and adaptation from the service provider.

Organizations must remain vigilant about the data quality used in their processes and conduct regular security audits, penetration testing, and timely updates to their remote identity proofing technologies. By staying attuned to the latest developments, organizations can transform remote identity verification from a necessary burden into a competitive advantage. The path to success lies in navigating the spectrum of identity assurance with trusted face biometrics as the cornerstone, keeping a keen eye on risk, compliance, user experience, and cost factors. Ultimately, this approach turns remote identity verification into a powerful enabler of digital transformation, with biometrics leading the way toward a more secure and user-friendly digital future.

To learn more about the Spectrum of Identity Assurance, and for supporting information to the series, please visit the Spectrum hub.

Find Out More About

The Spectrum of Identity Assurance





SOLUTIONSABOUT USRESOURCESDEMO →

The Spectrum Of Identity Assurance

In today's digital landscape, organizations face the critical challenge of ensuring online users are genuinely who they claim to be. Robust identity verification processes are essential across industries to prevent fraud, protect sensitive data, and maintain digital ecosystem integrity.

To address these challenges, we developed the three-part Spectrum of Identity Assurance series. This comprehensive guide provides insights to help organizations select appropriate assurance levels for various use cases when designing and implementing identity verification processes.

 understanding the spectrum of identity assurance,

SEARCH

DEMO

CONTACT

QUOTE

