IDVerse™

Ver. 1.0 2023

PUBLIC SECTOR\

A Complete Guide to Identify Verification for Government Agencies

BEST PRACTICES
From calculating Return on Investments to managing risks

TRENDS & FORECASTS
The latest face biometric trends impacting governments

ZERO BIAS AI
Frameworks and checklists to address algorithmic bias

Table of Contents

Introduction

This ebook is tailored for government and public sector professionals, aiming to provide a comprehensive understanding of remote identity verification (IDV). It explores key concepts, technologies, and best practices to equip readers with actionable insights for implementing secure and user-friendly IDV solutions.

Identity verification trends include the widespread adoption of biometric authentication and mobile-friendly IDV solutions, the exploration of blockchain for secure identity management, the acceleration of remote and digital IDV due to the COVID pandemic, and the use of generative AI and machine learning to enhance verification processes.

Privacy-enhancing technologies, cross-agency collaboration, and the adoption of international standards are also gaining prominence. Accessibility and inclusivity in IDV processes are receiving increased attention. Finally, the emergence of digital identity wallets and the integration of open banking concepts are transforming how citizens interact with government services.

This paper explores the significance of trusted identity solutions and the increasing need for collaboration between AI-powered IDV companies and the public sector in the following chapters:

1. Why Remote IDV is Crucial for the Public Sector

Identity verification in the public sector differs significantly from the private sector due to distinct legal mandates and responsibilities. Government agencies are bound by stringent laws and regulations, such as privacy and data protection statutes, which private companies may not face to the same extent.

The public sector prioritizes the public interest, accountability, and national security, making robust and inclusive IDV essential to maintain trust and safeguard sensitive information. Moreover, government agencies often deal with critical infrastructure and must ensure data sharing and interoperability across various departments. Resource constraints also play a role, as public sector organizations typically operate within fixed budgets.

In contrast, private companies, while also valuing security and efficiency, have more flexibility in their IDV processes and may not be subject to the same level of regulatory scrutiny and inclusivity requirements.

The significance for the public sector

Below are some of the key reasons why remote identity validation has become an indispensable component of digital governance:

- **Enabling access to government services**: Remote IDV allows citizens to access a wide array of government services from the comfort of their homes or offices. Whether it's filing taxes, applying for benefits, or accessing healthcare services, remote identity verification eliminates the need for physical presence and paper-based processes, ultimately improving citizen access and satisfaction.
- **Meeting regulatory and compliance requirements**: Government agencies must adhere to a multitude of regulatory and compliance requirements related to data

protection, privacy, and security. To do this, they must implement remote IDV solutions that have stringent verification processes and can ensure data privacy, thereby keeping government organizations in compliance with legal and regulatory frameworks.

- **Enhancing security and trust**: Government agencies handle vast amounts of sensitive data and deliver essential services to citizens. Remote IDV acts as the initial gatekeeper, ensuring that only authorized individuals gain access to these resources. Through the implementation of robust ID verification solutions, government entities can significantly reduce the risk of unauthorized access, fraud, and data breaches and bolster trust in their digital services.
- **Streamlining processes and reducing costs**: Remote IDV streamlines government processes by eliminating the need for in-person verifications or cumbersome paperwork. This not only reduces administrative overhead, but also minimizes the time and cost involved in identity verification. Government agencies can therefore leverage digital validation methods to achieve operational efficiencies and allocate resources more effectively.
- **Facilitating digital transformation**: The increasing shift towards digital governance necessitates robust identity verification methods. Remote IDV is at the core of this digital transformation, enabling governments to move towards paperless, online interactions with citizens. It underpins government initiatives and the broader goal of providing seamless, user-centric digital experiences.

Remote identity validation is indispensable for the public sector due to its pivotal role in enhancing security, improving citizen access, streamlining processes, facilitating digital transformation, and ensuring regulatory compliance. Through the effective implementation of remote IDV, government agencies can not only meet the evolving needs of citizens, but also strengthen the overall integrity of their digital services.

Challenges for IDV within the public sector

One of the foremost challenges is ensuring the utmost security while preventing fraud. Government agencies must guard against identity theft, cyberattacks, and fraudulent attempts to gain unauthorized access to sensitive data or government services. Achieving security while also providing a seamless user experience remains an ongoing conundrum, as it requires striking a delicate balance between stringent security measures and user convenience.

Identity verification systems should be user-friendly and accessible to a diverse range of citizens. This inclusivity mandate extends to individuals with disabilities or those with limited access to technology. Designing intuitive and inclusive interfaces that cater to various demographics demands careful attention and consideration.

There are also often laws applicable to the public sector that mandate accessibility for all. For example, the Accessibility Regulations in the UK put a higher burden on public sector websites and apps than the private sector.

The confluence of identity validation with privacy concerns involves navigating the fine line between the necessity for accurate identity validation and an individual's rights to privacy. Stricter regulations, such as the General Data Protection Regulation (GDPR), require organizations to be transparent regarding data collection and usage. This has brought forth questions about data retention, consent mechanisms, and anonymization practices.

Technological advancements represent both opportunities and challenges in identity validation. Rapid progress in fields like artificial intelligence (AI) and machine learning introduces the potential for enhanced validation processes but also raises concerns related to algorithmic bias, accuracy, and the potential for malicious exploitation.

Interoperability and standards adherence are crucial in ensuring that identity validation systems can seamlessly integrate with diverse government services and platforms. However, achieving this level of cohesion can be complex, given that different agencies may employ varying technologies and protocols.

Moreover, building and preserving public trust in identity verification systems impacts public perception and can be significantly affected by high-profile data breaches or misuse of personal information. Government entities must continually communicate their unwavering commitment to security and privacy.

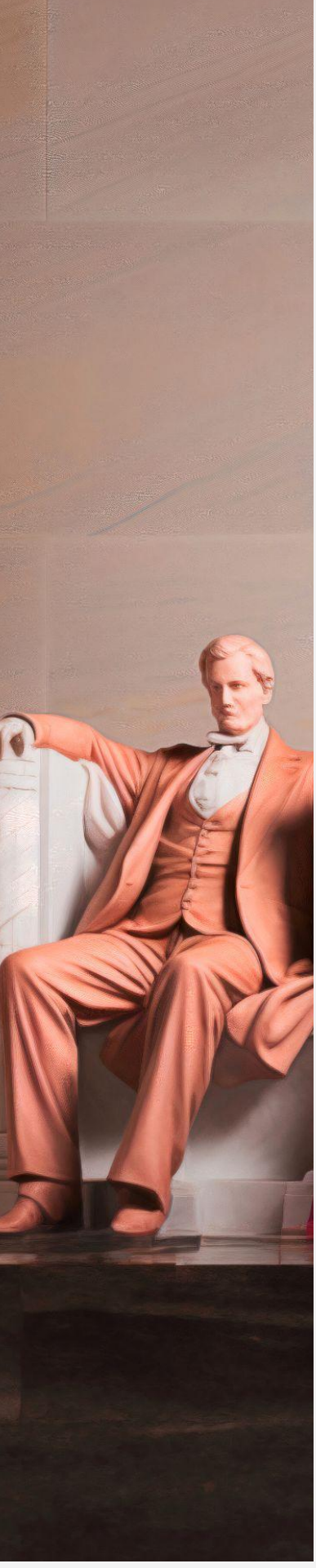
Challenges and Mitigation for Identity Verification in Public Sector

Challenges	Mitigation
Security and Fraud Prevention	Implement robust multi-factor authentication (MFA) and continuous monitoring systems to proactively detect and mitigate security threats, ensuring the integrity of identity verification processes.
User Experience and Accessibility	Design user-friendly interfaces and incorporate accessibility features, such as screen readers and voice recognition, to make identity verification processes inclusive and convenient for citizens of all abilities
Privacy Concerns	Adhere to strict data encryption standards, anonymization techniques, and transparent data handling policies to safeguard user privacy during identity verification, complying with stringent data protection regulations.
Technological Advancements	Embrace emerging technologies like biometric recognition and digital IDs to stay at the forefront of innovation and provide more secure and efficient identity verification solutions.
Interoperability and Standards	Adopt industry-standard protocols and promote interoperability between government agencies

	and systems, ensuring seamless information exchange and consistent identity verification practices.
Public Trust and Perception	Engage in transparent communication with the public about data privacy measures, security practices, and regulatory compliance, fostering trust and positive perception of government identity verification processes among citizens.

Resource constraints, cost considerations, and the evolving threat landscape further compound the challenges in identity validation. Government agencies must find a delicate equilibrium between the imperative for security enhancements and the budgetary constraints that often accompany such endeavors. Moreover, they must remain agile in the face of an ever-evolving array of cyber threats, necessitating regular system updates and a preemptive approach to emerging security challenges–something not always easily done within government agencies.

Addressing these multifaceted challenges necessitates a comprehensive approach that encompasses technology, policy development, and proactive engagement with users. Government and public sector organizations must perpetually evaluate and adapt their identity validation strategies to align with the evolving needs and expectations of citizens, all while upholding the highest standards of security and privacy.



2. An Overview of Identity Verification

It is difficult to overstate the importance of implementing trusted identity solutions in contemporary society. With billions of people to support and trillions of dollars to manage, the public sector in particular has a heightened responsibility with identity.

To tackle the complex challenges posed by identity fraud and unauthorized access to sensitive information, a collaborative effort between AI-powered IDV software companies and government agencies has become imperative.

Fundamentals of identity verification

Many countries rely heavily on documents produced by a range of government agencies to help identify their citizens and other residents. Ultimately, there are two key questions that individuals must confidently answer to prove their identity:

1. **Are you a real person?**
2. **Are you the right person?**

Traditionally, governments seeking to verify identities relied heavily on manual processes and physical documents. People seeking verification would present paper-based credentials such as IDs, passports, or driver's licenses. Verification agents then manually compared the presented documents with their physical appearance and information stored in databases. This process, while widely used, was prone to various risks and vulnerabilities.

Forgery was a significant concern, as skilled counterfeiters could produce convincing fake documents. Of course, under these circumstances, identity theft was rampant. Stolen or lost documents could be used by criminals to impersonate others, leading to the defrauding of government programs, illegal entry into the country, and other serious violations.

Unsurprisingly, human error was also prevalent. Mistakes in document examination or database entries were common, frequently resulting in instances of wrongful verification or denial. The reliance on paper documents made the system susceptible to loss or damage, further compromising its reliability. Additionally, the manual nature of traditional identity verification often led to delays and inefficiencies, particularly in high-traffic environments like government offices. Long queues and slow processing times were far from unusual.

As the digital landscape expanded, the need for advanced, secure, and reliable identity verification solutions became paramount to maintain the integrity of online interactions.

The era of generative AI begins

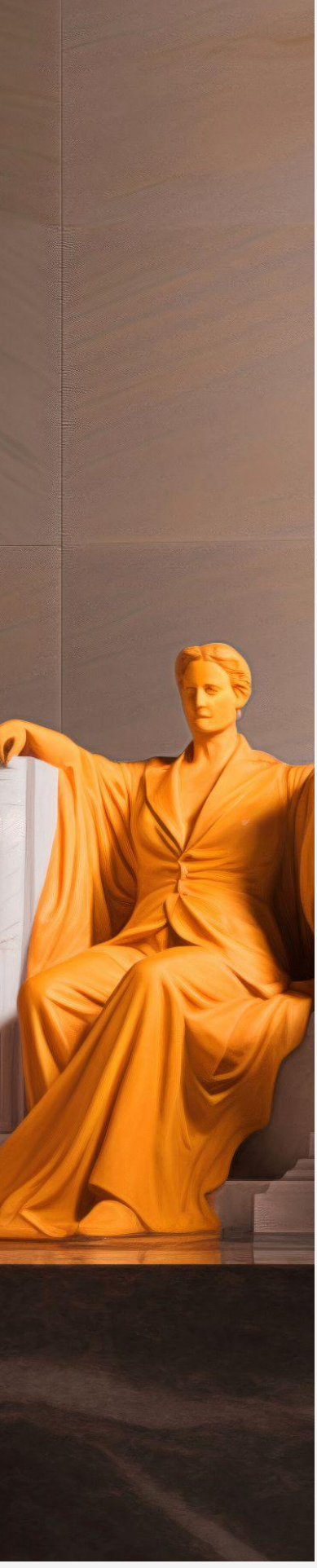
Today, AI-powered identity verification systems are rapidly replacing conventional methods. Unlike paper documents, IDV solutions backed by AI verify identities through methods such as facial recognition, fingerprint scans, and voice analysis. Machine learning algorithms detect anomalies within ID documents, while automation accelerates the process from start to finish. This shift signifies a transformative advancement in identity verification, enhancing trust and safeguarding against modern threats.

The highest-quality modern identity verification systems work using facial biometrics and perform the following key identity proofing steps in an automated manner using AI:

1. **Optical character recognition (OCR)**: The software uses adaptive text recognition and extraction for ID document data validation as well as easy form autofill for the end user.
2. **Document fraud analysis (DFA)**: Dozens of data checkpoints are used to perform an analysis and verify that the ID document is in fact authentic and present at time of verification.

3. **Anti-spoofing**: An automated facial biometrics match is performed on the selfie captured in the liveness video against the face image on the identity document.
4. **Liveness detection**: Advanced, automated checks are made on the face capture mini-video which can detect print attacks, masks, screens, and deepfakes, and which includes depth perception, miniscule movements from heartbeat, and light refraction.

These four key checks make AI-backed IDV solutions indispensable for governments seeking to reliably authenticate the individuals with whom they are interacting—but as we'll see in the next chapter, not all machine learning algorithms are created equally.



3. The Evolution of ID Systems

In an era where digital interactions predominate, verifying identities in real time is critical for ensuring security and building trust. Whether accessing a government tax filing platform, applying for employment benefits, or pre-screening travelers at a border crossing, confirming an individual's identity is essential.

This chapter explores the progression of identity verification solutions, from rudimentary passwords to cutting-edge, automated systems enabling instantaneous identity confirmation.

Passwords' long reign

Passwords were introduced in the 1960s as a means of securing early computer systems, with origins at the Massachusetts Institute of Technology. Computer scientist Fernando Corbató is credited with first using them to protect file access on the large computer systems he was working on at the time.

For decades, passwords remained the primary method for knowledge-based identity verification and access control. Their low implementation cost kept passwords dominant despite security weaknesses like guessability, replay attacks, and phishing. Passwords persist today, but—as Corbató himself acknowledged later in his career—this elementary security measure is no longer equate on its own. Improved technology now augments their security limitations.

In the US, the Social Security numbers (SSN) was also introduced as a knowledge-based solution, used in tandem with passwords. However, the proliferation of SNNs' use as a personal identifier—coupled with security breaches that have exposed most of the confidentiality associated with the numbers—have substantially diminished their reliability.

ID verification emerges

At its core, knowledge-based password authentication represents primitive identity verification—an individual wants to access information, so they must know the right combination of letters, numbers, and symbols that prove they are someone authorized to have that access.

Early identity verification relied extensively on manual processes like in-person verification, physical documents, and knowledge questions. While functional, these methods were inefficient, prone to human error, and provided poor user experiences. Technology innovations soon aimed to enhance identity proofing.

The rise of biometrics

The past thirty years have seen the emergence of attribute verification to enhance identity verification. A person's personal attributes, such as one's fingerprints or face, are generally regarded as the most secure verification method subject to maintaining strong presentation attack defenses in the technology to avoid hack attempts. Fingerprint recognition gained prominence in the 1990s as one of the earliest biometric authentication methods. Face recognition followed in the 2000s, relying on facial structure analysis for identification. Mobile devices accelerated the adoption of attribute biometrics to manage control over personal data in the event of a lost or stolen device.

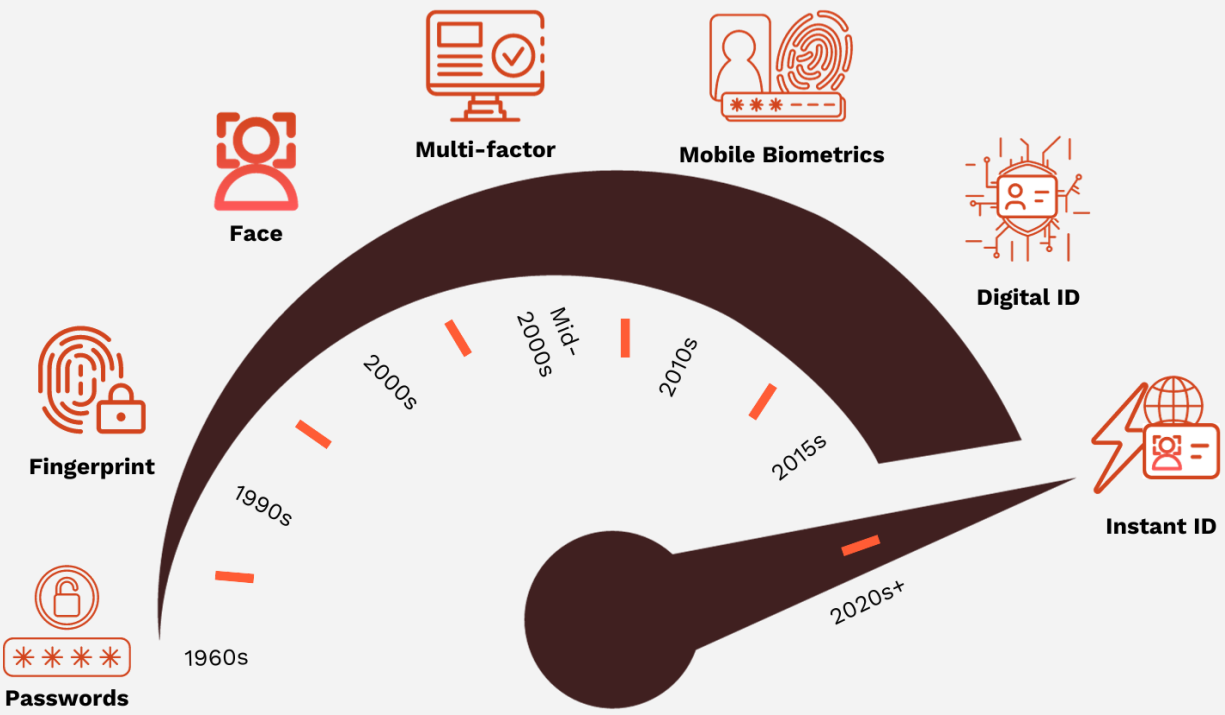
Today, the Australian government's cyber team advises all government websites to use biometrics rather than username and password for logging in. (See Principle 5 in this link.)

Multi-factor and decentralized identity

By the 2000s, multilayered security became best practice. Multi-factor authentication (MFA) combines different layers of

authentication, including knowledge, device, and attribute methods.

Biometrics are considered the strongest form of MFA, with additional factors like passwords and tokens for layered security. The 2010s saw major advancements in decentralized digital identity via blockchain and self-sovereign identity solutions to increase user control.



Instant identity starts now
The evolution of computer vision technology has changed the identity verification landscape and simplified user experience.

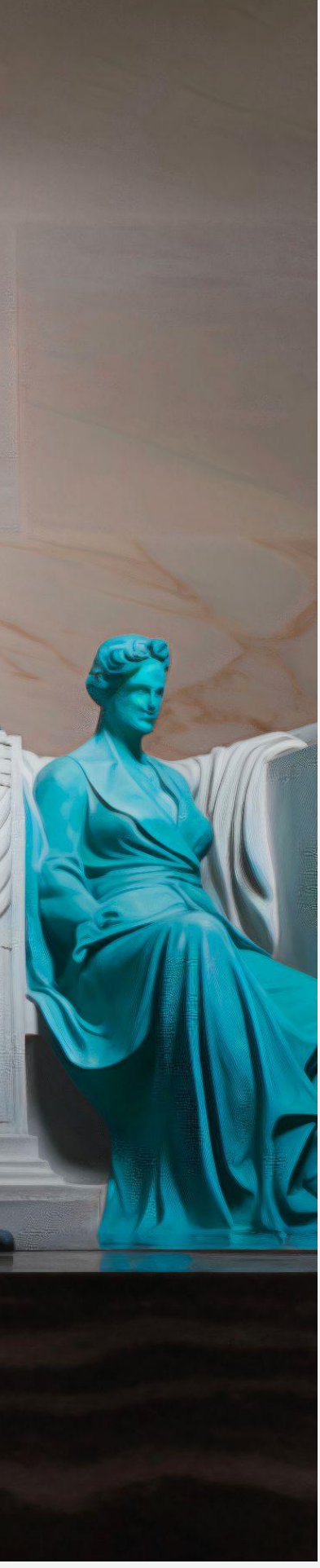
The future is Instant ID

More recently, the COVID-19 pandemic accelerated the use of remote identity verification and digital IDs for access to services. The automated IDV solutions of the present day use

state-of-the-art tech like artificial intelligence (AI) and machine learning (ML) to verify identities in seconds.

Contemporary leading identity verification techniques converge passwords, biometrics, multi-factor authentication, and integration with authoritative identity data sources into instant, seamless verification that is both highly secure and universally interoperable.

Instant identity is the result of this convergence—made possible through advancements in the underlying technologies—and has not only simplified the user experience, but increased the overall security of identity verification. As the technology progresses, instant identity verification will likely become ubiquitous across digital interactions, powering frictionless, trusted authentication.



4. Eliminating Bias, Embracing Inclusion

As the guarantors of rights for all who live within their jurisdictions, governments must prioritize inclusion and the development of identity systems that work for everyone. Ensuring that biometric and document verification technologies function effectively for users regardless of ethnicity, sex, gender identity, age, national origin, disability, broadband speed, or the quality of their mobile device is vital.

In the United States, Executive Order 13985 on Advancing Racial Equity and Support for Underserved Communities Through the Federal Government specifically directs the federal government to revise agency policies to account for racial inequities in their implementation. The order is intended to protect "historically underserved communities," including persons of color, members of religious minorities, LGBTQ+ persons, persons with disabilities, persons experiencing homelessness, persons who live in rural areas, and persons otherwise adversely affected by persistent poverty and inequality.

Removing bias, in its myriad forms, from the IDV procedure should be a top concern for governments everywhere.

Bias here and there

Identity verification processes can be marred by various biases, undermining their fairness and accuracy. The four key sources of bias within verification systems are: system bias stemming from unequal access to technology; algorithmic bias; data bias, influenced by skewed datasets; manual screening bias, arising from human judgments; and language bias, driven by linguistic nuances. Let's examine each one in a bit more detail:

1. **System bias**: If an identity verification solution only works on the latest smartphone model with a superior camera spec or with a high speed internet connection, then any users who do not meet these requirements will be forced to rely on manual methods of verification or be excluded from accessing a service altogether.
2. **Algorithmic bias**: When improperly designed, the coded rules embedded within an algorithm itself can inherently favor or discriminate against certain groups. Mitigating this bias involves addressing programming decisions to prevent unjust outcomes independent of training data.
3. **Data bias**: If biased data is used to train the algorithm, it is likely the system will exhibit those same biases when making decisions. This has become the AI industry's Achilles heel. Advancements in generative AI, also known as synthetic media, combined with ethically-sourced synthetic datasets for training shows that developers are using this tech to make their products better.
4. **Manual screening bias**: Automated IDV systems that are available at all times, day or night, and require no manual human intervention are far more inclusive to a wider customer base. For example, offering account opening services during business operating hours, when human analysts are available, excludes low-income customers who can't afford to take time off of work.
5. **Language bias**: The onboarding process often represents a major hurdle to users, who are prepared to drop off if this stage is too difficult or can't be completed. Removing the barriers that prevent users from comprehending the actions they need to successfully advance through each stage requires catering to a range of accessibility needs.

Countering bias

To face these challenges head on, IDVerse has introduced the Code Zero Bias Oath, inspired by the enduring principles of the Hippocratic Oath, but tailored to the unique challenges and

opportunities of the field of AI-powered biometric identity verification technology. This oath embodies a commitment to reducing algorithmic bias, promoting fairness, and upholding the highest ethical standards in AI software development:

Code Zero Bias Oath

I, as a software engineer, solemnly swear to uphold the principles and practices outlined in this Code Zero Bias Oath. In my pursuit of designing, developing, and deploying software, I commit to the following:

1. ***Do No Harm**: I shall prioritize the well-being of individuals and communities who may be affected by the software I create. I will strive to ensure that my work does not cause harm or perpetuate bias, discrimination, or inequality.*
2. ***Equity and Fairness**: I will actively seek to identify and rectify biases in algorithms and data sets. I pledge to promote fairness and impartiality, striving to create software that treats all individuals equally regardless of their background, race, gender, or any other characteristic.*
3. ***Transparency and Accountability**: I will be transparent about the decision-making processes and data sources used in my software. I accept responsibility for the consequences of my work and will be accountable for any biases or ethical lapses that may arise.*
4. ***Inclusivity**: I will advocate for diverse and inclusive teams, recognizing that different perspectives lead to more robust and ethical solutions. I will actively work to create an environment where underrepresented voices are heard and valued.*
5. ***Continuous Learning**: I understand that technology evolves rapidly, and I commit to staying informed about emerging best practices, guidelines, and regulations related to algorithmic bias and ethical software development.*
6. ***User Privacy and Consent**: I will respect user privacy and seek informed consent for data collection and usage. I will implement strong data protection measures to safeguard user information.*

*7. **Mitigation and Remediation**: If I discover bias or ethical concerns in software I have developed, I will take immediate steps to mitigate harm and rectify the issues. I will report such concerns to relevant stakeholders and take corrective action.*

*8. **Community Engagement**: I will actively engage with the communities impacted by my software, seeking their feedback and addressing their concerns. I will be open to criticism and commit to improving my work based on community input.*

*9. **Regulatory Compliance**: I will adhere to all relevant laws, regulations, and industry standards related to algorithmic fairness and data ethics in software development.*

*10. **Advocacy for Ethical Technology**: I will advocate for the responsible and ethical use of technology within my organization and the broader industry. I will use my influence to promote ethical practices and raise awareness about the importance of reducing algorithmic bias.*

I acknowledge that my work as a software engineer has a profound impact on society, and I accept this oath as a solemn commitment to ethical software development. I will strive to uphold these principles throughout my career, recognizing that my actions can shape the future of technology and its impact on humanity.

By taking this Code Zero Bias Oath, software engineers demonstrate their dedication to ethical software development, with a focus on reducing algorithmic bias and promoting fairness, transparency, and accountability.

Table of identity verification certifications

The table below covers key identity verification and security certifications from government entities, international standards bodies, and industry organizations. These trustmarks validate compliance with best practices for protecting sensitive personal

data, managing risk, ensuring reliability of biometric systems, minimizing bias, and providing assurance through independent auditing.

Certifications for IDV Companies

Certification body	Basic certifications	Advanced certifications
NIST	NIST SP 800-171	NIST SP 800-53 NIST IAL 2
iBeta/BixeLab against ISO 30107-3	Liveness PAD Level 1	Liveness PAD Level 2 Liveness (bias testing)
Government entities	CPRA GDPR	TDIF L3 DIATF
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

5: Use Cases in the Public Sector

Identity verification technology, now backed by the power of Zero-Bias AI™, has solidified its place as a paradigm-shifting force within the public sector. Its applications extend far beyond mere identity confirmation, permeating diverse domains and enhancing public service delivery, electoral integrity, national security, and other governmental functions.

Below, we take a deeper dive into how governments are harnessing the potential of IDV software to create a more efficient, secure, and equitable future for all.

Citizen services use cases

Streamlining access to benefits and services

One of the most compelling use cases of IDV technology is its role in ensuring efficient access to social benefits and public services. In an environment where government resources are limited, the verification of individuals' identities becomes crucial in making sure they're dispersed in a responsible manner.

IDV software comes into play by accurately validating the identities of applicants, preventing fraudulent claims and ensuring that resources are directed to those who genuinely need them. Implementing a reliable identity verification solution not only reduces the strain on public finances but also promotes a fair distribution of benefits, building trust in the system.

Protecting payments in real time

IDV helps secure real-time payment systems (such as the FedNow Service launched by the US Federal Reserve) by verifying identities to reduce fraud, protecting sensitive account data through encryption and tokenization, meeting KYC requirements for compliance, and creating an audit trail for accountability.

Overall, effective identity proofing techniques provide reassurance about the safety of real-time payments from initiation to settlement, and serve as key enablers for preventing fraud and ensuring trust in the integrity of real-time payment systems.

Certifications for IDV Companies

Use Case	Description
CITIZEN SERVICES	
Streamlining access to benefits and services	IDV technology ensures efficient access to social benefits and public services by accurately verifying the identities of applicants during the enrollment and service disbursement phases. This prevents fraudulent claims and directs resources to those genuinely in need, promoting fair distribution and trust in the system.
Protecting payments in real time	IDV secures FedNow real-time payments by verifying identities, reducing fraud, protecting sensitive account data, meeting KYC compliance, and creating an audit trail for accountability. It ensures the safety of real-time payments and builds trust in the FedNow system.
Improving quality of care	Government-operated healthcare organizations adopt identity verification software for patient identification, reducing medical identity theft and improving data integrity. This ensures correct patient records and enhances continuity of care based on medical history.
Allocating public housing	IDV solutions validate the eligibility of public housing applicants, reducing fraud and promoting fair allocation of resources. Agencies use document verification and government database checks to confirm identities, income status, and occupancy, preventing identity deception.
Facilitating tax filing	During tax season, IDV plays a critical role in e-filing by implementing robust identity proofing to verify taxpayers' identities, reducing fraudulent filings. It protects citizen data, ensures proper tax revenue allocation, and allows for smooth e-filing operations.

Ensuring equitable access to disaster relief	IDV technology can help address concerns about inclusivity and promote fairness and accessibility in disaster relief financial aid processes, especially for vulnerable populations and underserved communities.
NATIONAL SECURITY & LAW ENFORCEMENT	
Enhancing border security	IDV plays a pivotal role in enhancing border security and expediting immigration processes. Utilizing advanced biometric technologies like facial recognition, border control agencies can accurately verify travelers' identities, improving border surveillance and deterring illegal entries. A robust IDV solution optimizes both security and the flow of legitimate travel.
Securing mobile drivers license	IDV solutions provide protection for mobile driver's licenses (mDLs) across their entire lifecycle. During enrollment, IDV verifies identities to prevent fraudulent issuance, and ongoing authentication protections secure access to mDL apps and data. Generative AI-powered facial biometric IDV prevents spoofing and unauthorized usage, making mDLs trusted and resistant to fraud.
Keeping criminals at bay	Law enforcement agencies adopt identity verification technologies to identify suspects and criminals accurately, leading to expedited case resolution and a reduction in wrongful arrests. Multimodal biometrics, document verification, and cross-checking against government databases provide rapid, reliable suspect identification in the field, enhancing public safety through faster case closure and upholding civil rights. These use cases demonstrate the versatile applications of IDV technology in enhancing security, efficiency, and trust in various contexts.
GOVERNMENT OPERATIONS & EMPLOYEE MANAGEMENT	
Simplifying government hiring	Government agencies deploy IDV solutions in public sector hiring to validate candidates' identities and qualifications. By checking identities and credentials against authoritative sources, these systems prevent identity-related hiring fraud and ensure that hired candidates meet background check requirements, building public trust in government employees.

Upholding electoral integrity	To maintain the integrity of electoral processes, governments use IDV software during voter registration to authenticate voters' identities. This eliminates the risk of multiple registrations or impersonation, enhancing the credibility of elections and reinforcing citizens' trust in the democratic process.

Improving quality of care

Identity verification software is being adopted by government-operated healthcare organizations to aid in patient identification, which helps to reduce medical identity theft and improve patient data integrity.

Workers are able to confirm patient identities during appointments and procedures, thereby preventing fraudsters from illegally obtaining treatment using stolen medical identities. Accurate identification also ensures patient medical records are assigned to the correct individuals, a critical step for appropriate continuity of care based on medical history.

Allocating public housing

Millions of people apply for public housing assistance every year, and agencies are turning to IDV solutions to validate the eligibility of applicants. Incorporating identity verification into the process reduces the potential for fraud and also promotes fair allocation of limited public resources.

The technology helps public housing agencies confirm identities, income status, and occupancy using document verification and government database checks, ensuring that only qualified applicants receive aid. Eliminating identity deception prevents ineligible individuals from unlawfully occupying subsidized housing units and receiving benefits.

Facilitating tax filing

As tax season arrives, identity verification takes on critical importance in the e-filing process. IDV solutions implement robust identity proofing to affirm taxpayers are who they claim, reducing incidence of fraudulent filings.

These systems verify identities upfront, allowing tax authorities to uphold the integrity of revenue collection and preventing thieves from illegally obtaining refunds. Implementing IDV checks as a key gatekeeper allows e-filing to operate smoothly while protecting citizen data and ensuring proper tax revenue allocation.

National security & law enforcement use cases

Enhancing border security

Border security is a critical concern for nations across the globe. In this context, IDV technology plays a pivotal role in bolstering security measures while expediting immigration processes.

Utilizing advanced biometric technologies like facial recognition, border control agencies can accurately verify travelers' identities, thereby enhancing border surveillance and deterring illegal entries. Implementing a robust IDV solution not only improves security, but also optimizes the flow of legitimate travel.

Securing mobile credentials

Identity verification solutions provide protection for mobile driver's licenses (mDLs) across the entire credential lifecycle. During enrollment, IDV verifies identities to prevent fraudulent issuance, and ongoing authentication protections enabled by the technology secure access to mDL apps and data.

Furthermore, generative AI-powered facial biometric IDV prevents spoofing and keeps bad actors from unauthorized usage of the credential. By tying identity to each step, from issuance to daily use to data handling, sophisticated identity verification software helps make mDLs a trusted mobile credential resistant to fraud.

Keeping criminals at bay

Law enforcement agencies are increasingly adopting identity verification technologies to accurately identify suspects and criminals during investigations, leading to expedited case resolution and a reduction in wrongful arrests.

The combination of multimodal biometrics, document verification, and cross-checking against government databases provide rapid, reliable suspect identification in the field. Instant access to identity records aids officers in confirming identities, checking for warrants, and connecting suspects to crimes, thereby enhancing public safety through faster case closure while also upholding civil rights by avoiding mistaken arrests.

Government operations & employee management use cases

Simplifying government hiring

Government agencies are deploying IDV solutions within public sector hiring processes to validate candidates' identities and qualifications. By checking identities and credentials against authoritative sources, these systems ensure candidates are who they claim to be and help prevent identity-related hiring fraud.

At the same time, identity verification provides assurance that those ultimately hired meet background check requirements, which in turn improves public trust in government employees.

Upholding electoral integrity

The integrity of electoral processes is one of the most fundamental principles of a functional democracy. Governments around the world are turning to IDV software to ensure that the electoral process is carried out fairly and accurately.

By employing these solutions during voter registration, authorities can authenticate voters' identities, eliminating the risk of multiple registrations or impersonation. These practices bolster the credibility of elections and ensure that every vote counts, thereby reinforcing citizens' trust in the democratic process.

Instilling trust among the people

In each of these scenarios, IDV technology emerges as a cornerstone for the credibility of public sector operations. Its role goes beyond mere identity confirmation; it safeguards the principles of efficiency, transparency, security, and trustworthiness in governance. Put another way, governments are investing in IDV solutions not merely as a technological tool, but as a means to ensure equitable access to protect the very core of democracy.

As AI's role in evolving the digital landscape continues to grow, it is difficult to overstate the significance of the role IDV software will play in shaping the public sector's future. By responsibly harnessing the potential of this groundbreaking technology, governments can enter a new era of efficiency, fairness, and accountability, ultimately building a better future for citizens around the world.

6. Government Management of Artificial Intelligence

Government involvement in eliminating AI bias is essential to ensure fairness and societal trust in the technology. As machine learning systems increasingly impact critical sectors like healthcare, finance, and law enforcement, mandating unbiased outcomes—and holding accountable those who fail to properly develop bias-free solutions—becomes imperative.

Effective regulation ensures that AI technologies serve humanity's best interests while preventing the propagation of inequitable practices.

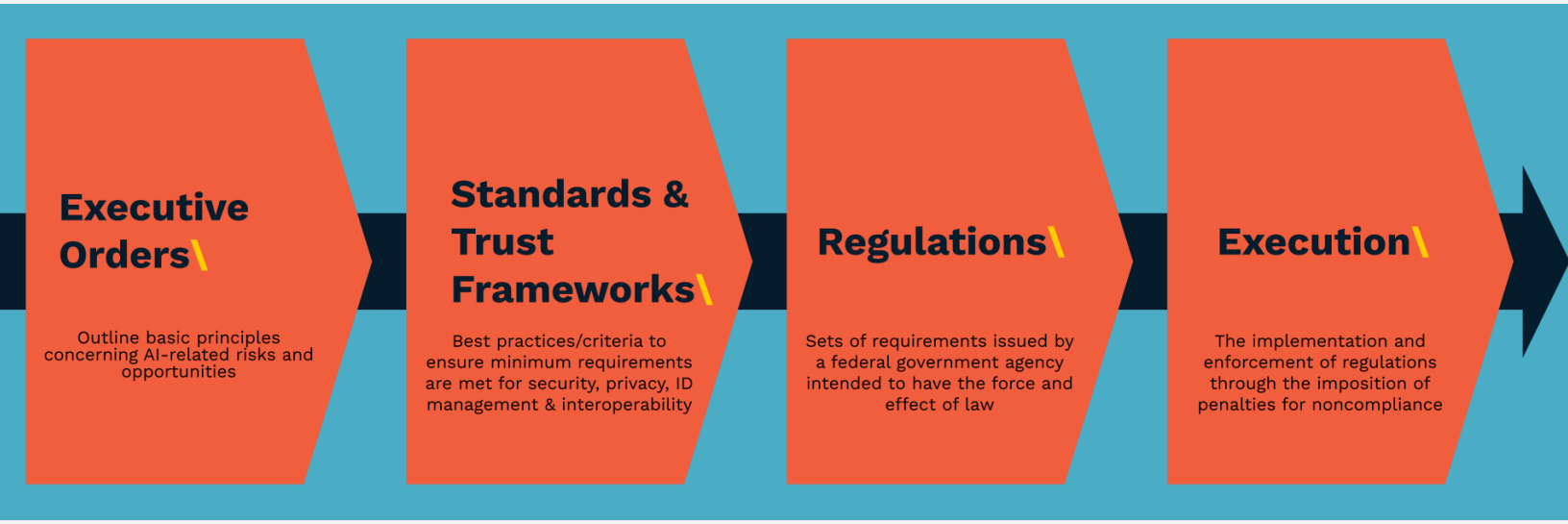
Means of management

Governments around the world are using a number of approaches to put pressure on private companies to eliminate bias from AI. Ideally, they deploy a multi-pronged strategy that includes the following:

- **Legislation**: Some governments have passed or are considering passing legislation that would regulate the development and use of AI. For example, the European Union's proposed Artificial Intelligence Act would require companies to assess the fairness of their AI systems and take steps to mitigate bias.
- **Regulation**: Governments are also issuing regulations that govern specific applications of AI. The US Department of Housing and Urban Development, for instance, has issued regulations that prohibit the use of AI in housing discrimination. An increasing number of global regulators are asking entities to carefully select if they use human-in-the-loop, human-out-the-loop, or human-over-the-loop AI systems to ensure that the

models' decisions have the right level of human involvement depending on the use case.

- **Trust frameworks**: The Australian Trusted Digital Identity Framework (TDIF) and UK Digital Identity Assurance Trust Framework (DIATF) outline requirements and standards for digital identity services to securely verify identities online. They aim to enable trusted digital identity transactions between government, businesses, and individuals through certified identity providers and authenticated credentials.
- **Guidance**: Additionally, governments are issuing guidance to businesses on how to develop and use AI in an ethical way. In one such example, the US National Institute of Standards and Technology (NIST) has published guidelines on managing bias in AI. In addition, the Federal Trade Commission has published guidelines on biometric information and Section 5 of the Federal Trade Commission Act.
- **Public awareness**: Governments are running campaigns to raise public awareness of the issue of bias in AI. This can help to encourage businesses to adopt bias-mitigating measures when developing AI systems.



Ideas that carry weight
Principles alone cannot be enforced—they must be codified into regulations to truly compel compliance and enable oversight.

A look around the world

Globally, government entities in various jurisdictions are proactively addressing AI bias through strategic measures. What follows are some specific examples of what governments are doing to address bias in AI.

The **European Union** is developing a new AI regulation that would require companies to assess the fairness of their machine learning systems and take steps to mitigate bias. The regulation would also prohibit the use of AI for certain applications, such as social scoring and mass surveillance.

The **United Kingdom** has published a set of ethical guidelines for the development and use of AI. The guidelines call for AI systems to be developed in a way that is fair, transparent, and accountable.

Australia has had several governmental agencies, including the Australian Human Rights Commission and the Department of Industry, Science, Energy, and Resources, collaborate on developing AI ethics guidelines to ensure machine learning systems are built and deployed in ways that respect human rights, fairness, and transparency.

New Zealand established the Algorithm Charter for Aotearoa New Zealand, which aims to promote ethical and transparent government use of algorithms. This charter emphasized fairness, transparency, and accountability in the use of AI.

In the **United States**, in January 2021, the White House issued guidelines stating that automated systems should be designed and used equitably, with proactive measures to promote fairness and prevent unjustified discrimination based on protected characteristics.

In April 2023, joint guidelines were issued by the Consumer Financial Protection Bureau, the Department of Justice's Civil Rights Division, the Equal Employment Opportunity Commission,

and the Federal Trade Commission on enforcement efforts against discrimination and bias in automated systems.

More recently, in October 2023, the White House unveiled the Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence, which was followed swiftly by the Office of Management and Budget (OMB) release of Implementation Guidance in response. These guidelines will directly impact major tech companies as well as smaller tech vendors that serve the Federal system, ultimately percolating into the broader market.

Bypassing Congress, the order focuses on accountability and responsible innovation in AI systems. Its two major aspects are mandating the watermarking of AI-generated content and mitigating AI-driven discrimination.

The watermarking mandate, to be spearheaded by the Commerce Department, will require labeling of all AI-generated audio, visual, and text content. This enables consumers to discern what is human-created versus machine-created, combating deceptive deepfakes. It also promotes transparency and accountability in the AI industry to disclose the data used to train models.

The order also tackles AI-driven discrimination by providing guidance to minimize biased outcomes. It emphasizes inclusivity and fairness in AI applications. This aligns with the concept of Zero-Bias AI™ discussed in Chapter 1 of this ebook, where engineers adhere to an ethical framework for transparency, consent, data security, and compliance.

The executive order signifies how the White House is taking a proactive approach to managing the risks and opportunities of AI, by enacting meaningful regulations on key areas like content labeling and non-discrimination. Oversight and responsibility are critical as AI capabilities rapidly advance.

The order also marks a pivotal moment—we have reached a technological threshold where meaningful oversight and

governance are vital. Executive orders alone are insufficient; they must be codified into laws to have enforceable impact.

Public-private collaboration

There exists a shared responsibility among governments, private enterprises, and individuals to shape a future where artificial intelligence is a force for good for all. As discussed above, governments must craft robust strategies that prioritize ethical AI deployment to safeguard against biases and ensure maximum transparency.

Meanwhile, private businesses hold the duty to design and develop AI technologies that adhere to these principles, meshing their drive for innovation with accountability. And individual humans, as the ultimate protectors of their own interests, must be strong advocates for unbiased AI and take it upon themselves to understand the implications of putting machine learning algorithms in charge of making critical decisions.

7. Legal and Regulatory Framework for IDV

A legal and regulatory framework allows government and public sector agencies to conduct identity verification in a manner that is lawful, secure, and respectful of individuals' rights. It sets the rules of the game, fosters trust, and promotes responsible and effective governance.

The essential aspects of the legal and regulatory framework governing identity validation are:

1. **Privacy laws and data protection**: Government agencies must navigate a complex landscape of privacy laws when handling personal data for identity validation. This includes compliance with regulations such as the General Data Protection Regulation (GDPR) in the European Union, the Health Insurance Portability and Accountability Act (HIPAA) in the United States, and various regional data protection laws. Understanding these regulations is critical to safeguarding citizen data and maintaining trust.
2. **Identity verification laws**: Different regions and countries may have specific laws and regulations pertaining to identity verification for various purposes, including financial transactions, access to government services, and more. It is crucial for government entities to stay informed about and comply with these laws to ensure the legitimacy of their identity validation processes.
3. **Digital signature laws**: In many jurisdictions, digital signatures carry legal weight, enabling individuals to sign documents electronically. Government agencies need to understand the legal status and requirements surrounding digital signatures to implement secure and legally valid remote identity validation methods.
4. **Interoperability standards**: Governments often collaborate with other entities, both domestically and internationally.

Interoperability standards, such as those outlined by the World Wide Web Consortium (W3C) and the International Organization for Standardization (ISO), play a vital role in ensuring that identity validation systems can work seamlessly across different platforms and organizations.

5. **Accessibility and inclusivity regulations**: Accessibility and inclusivity regulations ensure that all citizens, including those with disabilities, can access government services. Laws such as the Americans with Disabilities Act (ADA) in the U.S. emphasize the need for digital services, including identity validation processes, to be accessible to all.

Navigating this legal and regulatory landscape to develop identity verification systems that are not only secure but also compliant with the law will avoid legal repercussions and the erosion of public trust.

The framework serves to promote compliance with laws, protection of data privacy, enhances security, fosters trust, and enables fair and equitable access to government services while providing a structured approach to risk mitigation and accountability. It serves as the foundation for responsible and effective governance of identity verification systems.

8. Best Practices

Adopting these best practices will help to ensure robust security, safeguard data privacy, and maintain compliance with evolving regulatory standards. To streamline these best practices, we categorize them into key areas:

Regulatory compliance

Stay current with an ever-changing landscape of data protection regulations. Adhere to legal frameworks such as GDPR, HIPAA, and government-specific guidelines. Additionally, ensure that identity verification solutions meet compliance requirements set by relevant regulatory authorities.

Ethical and fair practices

Maintain ethical considerations throughout the verification process. Implement policies and safeguards to ensure responsible and fair use of identity verification technology. To address concerns of bias in AI models, check if vendors use fair-sourced training data for AI models, promoting equity in verification processes.

Vendor due diligence

Vet identity verification vendors carefully. One crucial best practice is to check for certifications and standards that vendors adhere to. Ensure that vendors have undergone and maintained relevant certifications to guarantee the quality and security of their services. A thorough evaluation of vendor practices can be instrumental in securing the most reliable and ethical solutions for your identity verification needs. Refer to the Vendor Due Diligence Checklist for more information.

Security and data protection

Implement robust security measures to protect sensitive user data. Employ strong forms of multi-factor-authentication (MFA) to fortify verification processes, combining something the user knows (e.g. a password) with something they have (e.g. a mobile device) and something they are (e.g. a face). Furthermore, use encryption both for data in transit and at rest, ensuring that collected data is minimal, necessary, and well-protected.

User-centric design

Prioritize the user experience to enhance accessibility and efficiency. Design user-friendly interfaces with real-time feedback, facilitating a seamless journey through the verification process. Empower users with clear instructions and offer readily accessible support channels. Furthermore, educate staff on identity verification processes to ensure consistent, effective user assistance.

Best Practices in Remote Identity Verification

Category	Best Practice
Regulatory Compliance	• Stay current with data protection regulations • Adhere to GDPR, HIPAA, and government guidelines
Ethical and Fair Practices	• Implement policies and safeguards for ethical use • Check if vendors use fair-sourced training data for AI models
Vendor Due Diligence	• Vet vendors based on certifications and standards
Security and Fraud Prevention	• Implement strong multi-factor-authentication (MFA) • Use encryption for data in transit and at rest. • Collect only necessary data and protect it
User-Centric Design	• Prioritize the user experience with clear instructions. • Design user-friendly interfaces with real-time

	feedback • Empower users with accessible support channels. • Train staff to ensure effective user assistance

By adopting these best practices in each of these five categories, government and public sector agencies can establish secure, compliant, and user-centric remote identity verification processes. This not only safeguards user data but also fosters trust and confidence in government services, ultimately leading to more efficient and effective operations.

9. ROI: Return on Identity

The public sector faces unique considerations when assessing Return on Investment (ROI) due to its distinct mission, objectives, and accountability to taxpayers and citizens. The key considerations to factor into ROI analysis in the public sector:

Nature of public sector projects

In the public sector, the assessment of Return on Investment (ROI) goes beyond financial considerations. Public value and outcomes are central, emphasizing societal benefits such as enhanced quality of life, safety, and environmental sustainability. This extends to a long-term perspective, recognizing that projects often span extended timeframes, necessitating analysis of evolving costs and benefits. Transparency in funding sources, typically taxpayer or government-funded, is crucial for maintaining public trust. Additionally, the complex stakeholder landscape and sustainability goals in the public sector demand a multi-objective approach in ROI analysis to effectively balance various interests and objectives.

Summary of public sector ROI considerations:

- **Public value and outcomes**: Public sector initiatives prioritize outcomes that benefit society, including improved quality of life, enhanced safety, or environmental sustainability. ROI assessments must quantify and evaluate these non-financial benefits.
- **Long-term perspective**: Public sector projects often have extended time frames, and ROI analysis should account for both short-term and long-term impacts. This includes considering how benefits and costs may evolve over time.
- **Funding sources**: Public sector projects are funded by taxpayers or government budgets, necessitating a high degree of transparency and accountability in ROI

assessments. The public has a vested interest in understanding how their money is being used.

- **Complex stakeholder landscape**: Public sector initiatives involve diverse stakeholders, each with their own interests and priorities. ROI analysis must navigate these complexities, considering the needs and expectations of various groups.
- **Sustainability and environmental impact**: Many public sector projects have sustainability and environmental goals. Evaluating the environmental impact and ensuring long-term sustainability are integral aspects of ROI analysis.
- **Multi-objective analysis**: Public sector initiatives often serve multiple objectives concurrently, such as economic development, social equity, and environmental preservation. ROI analysis may require a multi-objective approach to assess and prioritize these diverse goals effectively.

ROI considerations for the public sector

This comprehensive framework underscores the multifaceted nature of ROI analysis in the public sector, encompassing considerations related to project nature, governance, and the challenges associated with risk, non-financial benefits, and accountability:

Considerations	Examples
1. Nature of Identity Verification Projects	
Public value and outcomes:	Assessing an identity verification system's impact on reducing fraudulent access to government services (financial) and enhancing citizen data security (non-financial).
Long-term Perspective	Evaluating the ROI of implementing a biometric-based identity verification system over several years, considering system maintenance,

	evolving technology, and societal trust.
Funding sources	Transparently disclosing the allocation of government funds for developing and maintaining an online identity verification portal.
Complex stakeholder landscape	Balancing the interests of citizens, cybersecurity experts, and privacy advocates in designing identity verification protocols.
Sustainability and environmental impact	Assessing the environmental sustainability aspects of identity verification hardware and data centers.
Multi-objective analysis	An identity verification initiative addressing both security enhancements and improved citizen convenience through digital access to government services.
2. Governance and Accountability:	
Political and stakeholder influence	Adjusting the design of an identity verification project based on input from government officials and privacy watchdogs.
Legal and regulatory frameworks	Ensuring that the identity verification process complies with data protection laws (e.g. GDPR, CPRA, BIPA) and national privacy regulations.
Accountability and transparency	Maintaining a public-facing dashboard that provides real-time information on how citizen data is handled and secured during identity verification.
Public input and engagement	Gathering public feedback through surveys and consultations to shape the policies and procedures governing identity verification.
3. Risk and Uncertainty	
Risk and uncertainty	Considering potential data breaches, cyberattacks, and evolving threats when assessing the risks associated with implementing a new identity verification system.
Non-monetary Benefits	Recognizing that improved identity verification not only prevents financial fraud but also enhances citizens' trust in government services, leading to increased civic engagement and satisfaction.

10. Future Trends

Government and public sector agencies are navigating a dynamic terrain shaped by emerging identification technologies and shifting priorities, all while taking into account an increasing focus on regulations and laws addressing algorithmic bias.

The future trends and opportunities that are reshaping remote verification processes include:

Permanently altered behaviors

The COVID-19 pandemic has accelerated the adoption of remote verification. Even as the pandemic subsides, remote verification will remain integral to government operations, with citizens expecting digital-first, contactless services. Governments will prioritize user-centric design and increasingly focus on creating intuitive, accessible, and user-friendly interfaces to enhance the citizen experience.

Harnessing AI and ML for enhanced verification

Artificial intelligence (AI) and machine learning (ML) will continue to revolutionize remote verification. These technologies will not only analyze vast datasets and patterns, but will increasingly also focus on addressing and mitigating algorithmic bias. Expect to see AI-powered facial recognition, voice recognition, and behavior analysis becoming standard features in remote verification systems, with a heightened emphasis on fairness and equity.

Balancing innovation with ethics

As remote verification technologies advance, governments will grapple with ethical and regulatory challenges. Striking the right balance between innovation and ethics, while ensuring adherence to data protection laws, will be an ongoing concern.

Empowering citizens with control

Decentralized identity solutions, often based on blockchain technology, will empower citizens to have more control over their digital identities. Citizens have the most to lose and gain, especially in addressing and preventing algorithmic bias, ensuring fairness and transparency in identity verification.

Mobile devices as identity hubs

The ubiquity of smartphones will continue to drive the adoption of mobile-centric verification. Mobile IDs, digital wallets, and authentication apps will prioritize fairness in algorithms, ensuring that verification processes are equitable and unbiased.

Elevating security posture

Zero trust architecture will gain prominence, placing a heightened focus on addressing and eliminating algorithmic bias within the verification process. Governments will emphasize continuous identity verification for all users and devices, and combined with Zero Bias AI™, will strengthen fairness and equity.

Balancing security and privacy

Privacy-preserving technologies, such as secure multi-party computation and homomorphic encryption, will enable secure verification while actively addressing and mitigating algorithmic bias.

Facilitating global interactions

Cross-border verification solutions promote international collaboration, trade, and diplomacy. Governments will work on standardizing cross-border verification protocols, enabling seamless interactions and transactions across national boundaries.

Table of Future Trends in Public Sector IDV

Topic	Key points
Permanently altered behaviors	• Remote verification remains integral to government operations post-covid • Citizens expect digital-first and contactless services • Governments prioritize user-centric design • Focus on intuitive, accessible, and user-friendly interfaces to enhance the citizen experience
Harnessing AI and ML for Enhanced Verification	• AI and ML revolutionize remote verification. • Analyzing vast datasets and patterns • Addressing and mitigating algorithmic bias • AI-powered facial recognition, voice recognition, and behavior analysis becoming standard • Emphasis on fairness and equity
Balancing Innovation with Ethics	• Ethical and regulatory challenges as remote verification technologies advance • Striking the balance between innovation and ethics • Ensuring adherence to data protection laws
Empowering Citizens with Control	• Decentralized identity solutions, often based on blockchain • Empowering citizens with control over digital identities • Addressing and preventing algorithmic bias • Ensuring fairness and transparency in identity verification
Mobile Devices as Identity Hubs	• Ubiquity of smartphones driving mobile-centric verification • Prioritizing fairness in algorithms for mobile IDs, digital wallets, and authentication apps • Ensuring equitable and unbiased verification processes
Elevating Security Posture	• Zero trust architecture gaining prominence • Focusing on addressing and eliminating algorithmic bias • Emphasizing continuous identity verification for all users and devices

	• Strengthening fairness and equity with Zero Bias AI™
Balancing Security and Privacy	• Privacy-preserving technologies like secure multi-party computation and homomorphic encryption • Enabling secure verification while addressing and mitigating algorithmic bias
Facilitating Global Interactions	• Cross-border verification solutions promoting international collaboration, trade, and diplomacy • Governments standardizing cross-border verification protocols • Enabling seamless interactions and transactions across national boundaries

11. Conclusion

Remote identity verification is an indispensable tool enabling governments and public sector agencies to thrive in a world that's becoming more and more digital with each passing day. As explored throughout this paper, IDV solutions backed by artificial intelligence strengthen security, combat fraud, optimize processes, and facilitate digital transformation across diverse public sector use cases.

To fully harness the potential of this technology, however, government entities must prioritize privacy while eliminating bias and embracing inclusion. Through responsible development and deployment of IDV systems, the public sector can enter an era of efficient, user-friendly services that engender trust among citizens—but this requires selecting partners who are also committed to mitigating algorithmic bias via techniques like diverse data sourcing, regular audits, and transparent development practices.

Ultimately, remote identity verification represents a pivotal innovation shaping the public sector's digital future. Yet its full promise will only be realized through a shared commitment by governments, vendors, and citizens alike to uphold principles of accessibility, security, privacy, and fairness.

By working together proactively, the immense possibilities of IDV can be channeled to benefit all members of society equitably. This collaborative vision will enable remote identity solutions to strengthen public sector operations today and for decades to come.

Appendix

States of data and data management

Organizations must navigate a delicate balance between using customer data for business purposes and respecting individuals' privacy rights—or else risk significant financial and reputational harm. Among the sundry items a business must take into account are obtaining informed consent for processing of biometrics, being transparent about data collection and usage practices, implementing robust security measures to protect customer data, and providing individuals with control over their own data.

Understanding the different states of data is crucial for maintaining its security and integrity. We can categorize data into three distinct states: data at rest, data in transit, and data in use. Each state represents a unique phase in the lifecycle of information, with its own set of considerations and risks. By understanding these states, companies can effectively implement measures to safeguard data throughout its journey.

Questions to ask a provider about their handling of data at rest:

1. Does your platform allow us to set automated data deletion rules?
2. What is the shortest period that we can set?
3. How long is the data retained in your engines themselves? (Data is often held in engines separately to the main platform.)
4. What is your data deletion policy for Illinois residents, including any backups?
5. Can you prove that you do delete when you say you do?
6. Can we delete all biometric and photo data from the records you keep for us?
7. Is data held in backup, and for how long? (In order for an organization to recover data and the results of checks in the event of a severe incident, the organization will need to

make copies of data into backup. Typically the data resides in backup for a set period, say 30 or 60 days. When you delete data from the main platform, the backup data will not usually be deleted. So you need to ask how long that backup retention period is. The risk of storing data in backup is much lower because the backup data cannot be accessed via the platform, which from a security perspective is normally the weakest link, but you still need to ask the questions.)

8. Is data held in your training database? If so, for how long?

Questions to ask a provider about their handling of data in transit:

1. In which jurisdiction will the data of my end users be hosted?
2. Can we select different jurisdictions for data hosting depending on where the data originated?
3. At any point in the IDV process, is any data transferred from the UK or the EU into the US?
4. If yes to Q3, what is the lawful mechanism the transfer is made under?
5. Is my end user data used in any fraud signal sharing database? If so, please share your Data Protection Impact assessment so we can understand the legality of this processing.

Questions to ask a provider about their handling of data in use:

1. Please show me your consent screen and show me your legal advice that it complies with BIPA and CUBI (the Capture or Use of Biometric Identifier Act, Texas' less scary version).
2. Where can I read your public "biometric processing statement"?
3. Do you use the data of Illinois residents in any form of training?

4. Can you send me your Data Protection Impact Assessment (DPIA) covering the service you are selling to me?
5. How have you trained your algorithms?
6. Will you be reusing personal data from our end users to train your algorithms, and if so, what is your lawful processing ground?
7. From where do you source your training data?
8. How have you, or the source of your data, collected express consent from the data subjects?
9. Can you prove to us that you have that consent?
10. How can a person withdraw consent if they later change their mind?

Certifications

The various certifications from table x explained:

NIST: National Institute of Standards and Technology (U.S. Dept. of Commerce)

Basic certification(s):

- NIST SP 800-171: Cybersecurity standards for protecting controlled unclassified information

Advanced certification(s):

- NIST SP 800-53: Cybersecurity framework that provides guidelines for federal information systems
- NIST SP-800 63 IAL 2: Cybersecurity standard that provides identity assurance in digital and online transactions

iBeta/BixeLab against ISO 30107-3 (Biometric testing lab)

Basic certification(s):

- Liveness PAD Level 1: Basic presentation attack detection for biometrics

Advanced certification(s):

- Liveness PAD Level 2: Enhanced presentation attack detection for biometrics
- Liveness (bias testing): Testing for bias in biometric systems

Government entities

Basic certification(s):

- CPRA: California Privacy Rights Act for data privacy rights
- GDPR: EU's General Data Protection Regulation for data privacy rights

Advanced certification(s):

- TDIF L3: The Australian Government's Trusted Digital Identity Framework
- DIATF: The UK Government's Digital Identity Authentication Trust Framework

ISO (International Organization for Standardization)

Basic certification(s):

- ISO 9001: Quality management systems
- ISO 22301: Business continuity management
- ISO 29100: Privacy framework

Advanced certification(s):

- ISO 27001: Information security management
- ISO 27017: Cloud security
- ISO 27018: Cloud privacy
- ISO 27701: Privacy information management
- ISO 19795: Biometric performance testing
- ISO 30107-3: Biometric presentation attack detection

AICPA SOC (System and Organization Controls)

Basic certification(s):

- SOC 1: Financial controls audit

Advanced certification(s):

- SOC 2: Security, availability, processing integrity, confidentiality and privacy controls audit

Vendor Due Diligence Checklist for Remote Identity Verification
☐ Verify Vendor Credentials
☐ Check for relevant industry certifications and standards. ☐ Ensure the vendor has a history of reliable service and a positive reputation. ☐ Review vendor financial stability and long-term viability. ☐ Assess vendor experience with similar projects or government contracts.
☐ Data Security and Privacy
☐ Review the vendor's data security measures, including encryption protocols for data in transit and at rest. ☐ Evaluate the vendor's disaster recovery and data backup procedures. ☐ Inquire about the vendor's incident response and breach notification processes. ☐ Assess data minimization practices and the extent of data collected.
☐ Regulatory Compliance
☐ Ensure the vendor complies with data protection regulations (e.g., GDPR, HIPAA). ☐ Check for government-specific guidelines and mandates the vendor must adhere to. ☐ Verify that the vendor can provide audit trails and compliance reporting as required. ☐ Assess the vendor's track record for responding to regulatory inquiries or audits.
☐ Ethical and Fair Practices
☐ Inquire about the vendor's ethical guidelines for AI model development and deployment. ☐ Request details on the vendor's data anonymization practices and transparency measures.

Vendor Due Diligence Checklist for Remote Identity Verification
☐ Verify the presence of a clear and accessible appeals process for users facing verification issues. ☐ Assess the vendor's commitment to addressing bias and ensuring fairness in identity verification.
☐ Technology and User Experience
☐ Evaluate the technology and features offered by the vendor for compatibility and scalability. ☐ Assess the user-friendliness of the vendor's interfaces, including real-time feedback and clear instructions. ☐ Inquire about the vendor's accessibility features for users with disabilities. ☐ Verify that the vendor's technology aligns with your organization's existing infrastructure.
☐ Support and Training
☐ Confirm that the vendor provides accessible customer support channels for assistance. ☐ Inquire about vendor-provided training for your staff to ensure they can effectively assist users. ☐ Assess the vendor's user documentation and knowledge base for self-service support. ☐ Verify the responsiveness and availability of the vendor's support team.
☐ Vendor Contracts and SLAs
☐ Review vendor contracts thoroughly to understand terms, conditions, and obligations. ☐ Ensure SLAs specify service levels, response times, and escalation procedures. ☐ Verify that the vendor has a clear dispute resolution process defined in the contract. ☐ Assess contract provisions related to data ownership, exit strategy, and vendor liability.
☐ Security Audits and Penetration Testing
☐ Verify if the vendor conducts regular security audits, vulnerability assessments, and penetration testing. ☐ Inquire about the results of these audits and any measures taken to address vulnerabilities. ☐ Assess the vendor's incident response procedures and post-incident reporting.

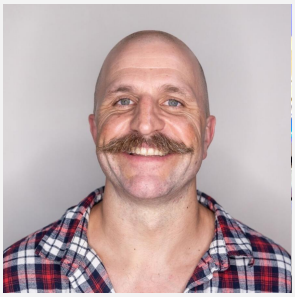
Vendor Due Diligence Checklist for Remote Identity Verification
☐ Verify that the vendor follows best practices for secure coding and software development.
☐ Data Retention and Disposal Policies
☐ Understand the vendor's data retention and disposal policies, ensuring they align with your organization's data management practices. ☐ Inquire about mechanisms for data deletion, especially upon user request or contract termination. ☐ Verify that the vendor has secure data disposal procedures in place to prevent data breaches or leaks.
☐ Compliance Reporting
☐ Request documentation or reports from the vendor that demonstrate their compliance with regulatory requirements and security standards. ☐ Inquire about the frequency and detail of compliance reporting provided by the vendor. ☐ Assess the accessibility of compliance reports for internal and external audit purposes. ☐ Verify that the vendor maintains a record of previous compliance audits and remediation actions.
☐ Cost and Pricing Structure
☐ Clarify the vendor's pricing structure, including any hidden costs or fees. ☐ Ensure that the pricing aligns with your budget and needs. ☐ Inquire about flexibility in pricing to accommodate potential changes in usage or requirements. ☐ Assess the transparency and predictability of billing and invoicing processes.
☐ Redundancy and Failover
☐ Inquire about the vendor's redundancy and failover measures to ensure continuity of service in case of system failures. ☐ Verify the effectiveness of these measures in maintaining system availability and reliability. ☐ Assess the geographical diversity of data centers and servers for disaster recovery. ☐ Inquire about failover testing and backup power solutions in place.
☐ Exit Strategy

Vendor Due Diligence Checklist for Remote Identity Verification
☐ Establish an exit strategy in the contract to ensure a smooth transition if you need to change vendors in the future. ☐ Ensure that the exit strategy includes data migration, data ownership, and contract termination procedures. ☐ Verify that the vendor provides support during the transition period, including data transfer assistance. ☐ Inquire about any associated costs, such as data retrieval or termination fees.
☐ References and Case Studies
☐ Request references from other organizations that have used the vendor's services. ☐ Review case studies and success stories to understand the vendor's track record in similar projects. ☐ Inquire about any challenges or obstacles faced by clients in the past and how the vendor addressed them. ☐ Verify the vendor's flexibility and adaptability to meet diverse client needs.

About the authors

Terry Brenner *is Head of Legal, Risk & Compliance, Americas, for IDVerse. Previously he has served in executive office and general counsel roles, in both start-up and mature businesses, across a range of diverse industry sectors. His focus at IDVerse is to lay the path for the successful integration of IDVerse's remote ID verification technology into the Americas market, heeding to the sensitivities around data and privacy protection. From a commercial perspective, he drives towards supporting disciplined growth of the business whilst reinforcing the ethics and compliance mission of IDVerse to be the industry benchmark from a compliance perspective and to build trust in the brand.*

Peter Violaris *is Global DPO and Head of Legal EMEA and APAC for IDVerse. Peter is a commercial technology lawyer qualified in England and New South Wales with a particular focus on biometrics, privacy, and AI learning. Peter has been in the identity space for 6 years and before that worked for London law firms.*



Paul Warren-Tape *is IDVerse's SVP Risk and Compliance. He has over 20 years of global experience in governance, operational risk, privacy, and compliance, spending the last 10 years in pivotal roles within the Australian financial services industry. Paul is passionate about helping organizations solve complex problems and drive innovation through encouraging new ideas and approaches, whilst meeting their legislative requirements.*

About the imagery

IDVerse's dedication to pushing boundaries in the realm of identity verification with generative AI has led us to explore the applications of this technology in other contexts. Hence, we made the choice to incorporate the artificially produced visuals in this document.

For this report, we colorfully reimagined the Lincoln Memorial, one of the world's most recognizable symbols of steadfast and honorable leadership. Like many other monuments around the globe, it represents the connection between the government and the governed—As well as freedom and dignity for all people, which can only be achieved through inclusion and fairness.

About IDVerse

IDVerse, an OCR Labs company, is the leading automated identity verification platform to onboard and re-authenticate trusted users at scale.

What sets us apart? Our commitment to Zero Bias AI™ means that we are pioneering the use of machine learning to protect against discrimination on the basis of ethnicity, age, and gender. We build software capable of authenticating tens of thousands of ID document types and verifying the liveness of billions of real people without manual human intervention—all underpinned by generative AI that achieves maximum inclusion and fairness.

IDVerse can recognize over 16,000 ID types in 142 languages from more than 230 countries and territories. The world's leading companies like Amex, HSBC, and Hertz trust us to help their users prove their identity in seconds.

The IDVerse solution has been tested and certified to meet the most stringent standards in the industry, including NIST, ISO, iBeta, and algorithmic Zero Bias AI™ specifications.

Want to learn more? Book a demo today, or get in touch with us at hello@idverse.com.