



# DAL IDENTITY INTERNATIONAL

Diverse Authentication Library

RESHAPING IDENTITY MANAGEMENT:

The Imperative of Forensic Identity Management  
in the Era of Deepfake Synthetic Identities

2024 White Paper



## Preface

In an age defined by rapid technological advancement and digital transformation, the landscape of Identity Management faces unprecedented challenges. The rise of Deepfake Synthetic Identities has introduced a new frontier of threats, undermining the integrity of personal Identity and exacerbating the risks of Identity fraud and manipulation. DAL Identity International has embarked on a journey to explore and elucidate the imperative of Forensic Identity Management (FIM) in response to these pressing concerns.

This white paper serves as a testament to our commitment to understanding and addressing the critical issues surrounding Identity Management in the era of Deepfake Synthetic Identities. By delving into the intricacies of this phenomenon and examining the limitations of traditional Identity Management solutions, we seek to shed light on the urgent need for a paradigm shift in our approach to safeguarding personal Identity.

Through comprehensive analysis and insightful commentary, we aim to highlight the pivotal role of Forensic Identity Management (FIM) in reshaping the future of Identity security. Drawing upon our expertise and experience in the field, we

endeavor to provide stakeholders with valuable insights and actionable strategies to navigate the complexities of Identity Management in today's digital landscape.

Our exploration will delve into the mechanisms of Deepfake Synthetic Identities, examining their implications for individuals, organizations, and society. We will analyze the shortcomings of current Identity Management practices in mitigating these risks and propose innovative solutions grounded in transparency, accountability, and trust.

As we embark on this endeavor, we invite readers to join us in exploring the challenges and opportunities presented by the era of Deepfake Synthetic Identities. Together, we can pave the way towards a more secure and resilient future for Identity Management, fostering a digital ecosystem where personal Identity remains safeguarded and integrity upheld.

### Co-Founder and CEO

*Dawid Jacobs*

### Co-Founder and CPO

*Gunther Sonnenfeld*

### DAL Identity International LLC

*“Forensic Identity Management (FIM) is a holistic approach to Identity verification and protection that employs forensic principles and methodologies to uphold individuals' identities' integrity, accuracy, and accountability. FIM utilizes scientific techniques to gather, analyze, and interpret Identity-related data, focusing on maintaining the authenticity of digital and physical evidence. By integrating forensic protocols like the Locard Principle and ensuring a secure Chain of Custody, FIM aims to safeguard Identities throughout their lifecycle, including protection during life, maintaining the integrity of digital representations, and respecting deceased Identities. Through rigorous forensic practices, FIM nullifies Deepfake Synthetic Identities and mitigates the risks of Identity fraud, manipulation, and exploitation, instilling trust in Identity verification processes across all sectors.”*

**Dawid Jacobs**



## Table of Contents

Preface .....	2
Introduction .....	4
Challenges with Current Identity Verification (IDV) systems.....	5
Presentation Attack Detection (PAD) and Injection Attack Detection: A Struggle in Identifying Spoof and Deepfake Identities .....	8
Vulnerabilities Exploited by Crime Syndicates in IDV Systems.....	11
Heightened Threats: The Impact of AI on Identity Verification (IDV) Solutions.....	13
Consent: The Ethical, Legal, and Privacy Dimensions of Facial Recognition Technology .....	17
Algorithm Bias in Selfie and Liveness Verification Solutions: A Complex Challenge .....	19
Challenges in Identity Management on Web 2.0 and Web 3.0:.....	23
The Urgent Need to Rethink Remote Onboarding: Mitigating the Escalating Threat of Deepfake Synthetic Identities.....	26
Rethinking IDV: Addressing the Root Cause.....	28
The Emergence of Forensic Identity Management (FIM): Safeguarding Identity Integrity and Accountability .....	31
The Stringency in Forensic Identity Verification .....	34
Certainty in Forensic Identity Verification (FIM).....	37
The Legal Standing in Forensic Evidence.....	40
Role of Forensic Cryptographic Provenance (FCP) in FIM: .....	42
The Role of Forensic Cryptographic Provenance (FCP) in Verifiable Credentials: .....	44
DAL Identity International's Unique Forensic Approach:.....	46
Onboarding Protocol via DAL Identity International Forensic Identity Management (FIM) System.....	49
Compliance and Ethical Standards in Identity Management.....	51
Advancing Forensic Identity Management (FIM) with Web 4.0: A Comprehensive Solution..	54
DAL Identity International: Forensic Identity Management (FIM).....	58
Conclusion: Embracing Forensic Identity Management (FIM) in the Age of Deepfake Synthetic Identities.....	59
About the Authors .....	60
<b>Dawid Jacobs</b> .....	60
<b>Gunther Sonnenfeld</b> .....	61



## Introduction

In an era dominated by digital interactions, safeguarding personal Identity has become an increasingly formidable challenge. Traditional methods of Identity Verification (IDV) are proving inadequate against the rising tide of Deepfake Synthetic Identities. Nowhere is this more apparent than in the realm of biometric authentication, where techniques like "selfie" and "voice" recognition, augmented by "liveness detection," are being exploited with alarming effectiveness.

This white paper aims to explore the inherent shortcomings of current Identity Management and Identity Verification solutions and emphasizes the urgent need for Forensic Identity Management (FIM). As we navigate the complexities of Digital Identity, there arises a critical imperative to reassess existing strategies and embrace a paradigm shift towards more robust, authentic, and resilient frameworks.

DAL Identity International stands at the forefront of this landscape, offering innovative solutions to the contemporary challenges of Identity verification. Through groundbreaking approaches, we aim to redefine the standards of Identity Management and establish new benchmarks for security and trust.

### Key Insights from the Global Deepfake AI Market<sup>1</sup>

- The Global Deepfake AI Market was valued at USD 6.83 Billion in 2023.
- It is experiencing a remarkable growth rate, with a Compound Annual Growth Rate (CAGR) of 33.12% projected from 2023 to 2033.
- The forecast indicates that the Worldwide Deepfake AI Market Size is poised to reach USD 119.34 Billion by 2033.
- North America is expected to witness the fastest growth during the forecast period.

These insights underscore the significance of addressing the challenges posed by Deepfake technology and highlight the growing demand for advanced solutions in Identity Verification and Management.



---

<sup>1</sup> [Global Deepfake AI Market Size, Share, Forecast 2023 to 2033 \(sphericalinsights.com\)](https://sphericalinsights.com)

## Challenges with Current Identity Verification (IDV) systems<sup>2</sup>

### 1. Vulnerability to Deepfake Synthetic Identities:



Figure 1: New Threat Intelligence Report Exposes the Impact of Generative AI on Remote Identity Verification<sup>3</sup>

- The reported 704% increase in face swap attacks, a form of Deepfake, from H1 to H2 2023, highlights a significant vulnerability in current IDV systems. Deepfake technology allows for creation of highly realistic Synthetic Identities, making traditional biometric authentication methods like "selfie" and "voice" recognition susceptible to manipulation.
- **Flaws:** The reliance on static biometric data without robust checks for dynamic liveness verification leaves systems open to exploitation by sophisticated Deepfake techniques.

### 2. Ineffective Liveness Detection:



- The rise in threat actors using emulators (353% increase) and digital injection attacks against mobile web platforms (255% increase) from H1 to H2 2023 underscores the inadequacy of existing liveness detection mechanisms. These attacks allow for the

<sup>2</sup> [New Threat Intelligence Report Exposes the Impact of Generative AI on Remote Identity Verification | iProov](#)

<sup>3</sup> [iProov Threat Intelligence Report 2024.pdf](#)





injection of fake video or audio into IDV processes, bypassing traditional security measures.

- **Flaws:** The failure to accurately distinguish between genuine and Synthetic Identities poses a significant risk of Identity fraud. Weak liveness detection mechanisms enable attackers to circumvent authentication processes, leading to compromised security.

### 3. Lack of Comprehensive Protection:

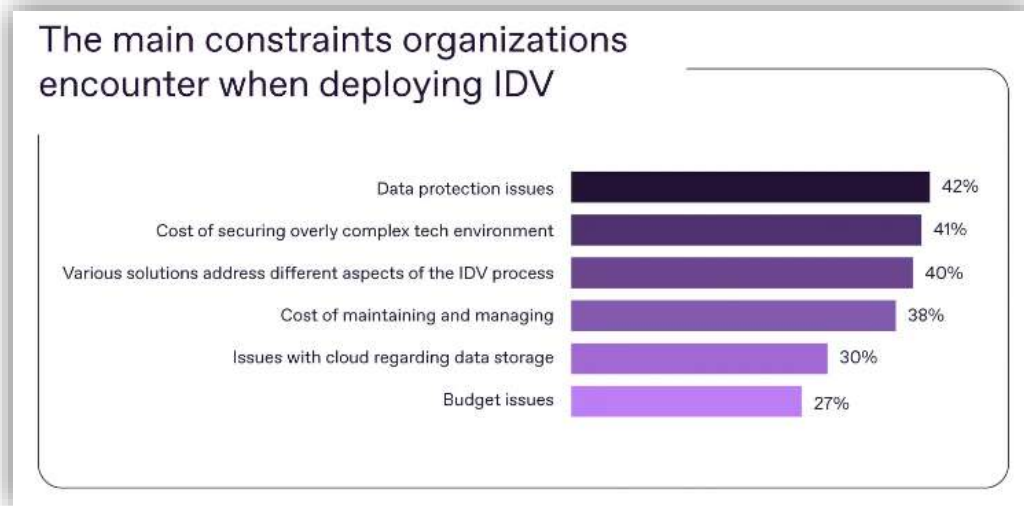


Figure 2: Identity Fraud Statistics: How Businesses Respond to the Issue<sup>4</sup>

- Current IDV solutions often focus on verifying Identity at a single point in time, overlooking the necessity for continuous protection throughout an individual's Identity lifecycle. The creation of information exchange groups in 2023 further complicates this issue, suggesting a lack of holistic Identity Management.
- **Flaws:** The absence of ongoing Identity verification and monitoring leaves systems vulnerable to exploitation over time. Without continuous protection measures, individuals' Identities remain at risk of compromise, potentially leading to unauthorized access and fraud.

### 4. Storing and Reusing of Personal Identifiable Information (PII) Without Consent:

- Instances such as the lawsuit against Jumio<sup>5</sup> for allegedly collecting, storing, and using biometric data without consent highlights a significant privacy concern. Storing and reusing Personal Identifiable Information (PII) without explicit consent violates privacy regulations and exposes individuals to potential Identity theft and fraud.
- **Flaws:** Failure to adhere to consent requirements not only breaches legal obligations but also undermines trust in IDV systems. Improper handling of sensitive biometric data increases the risk of unauthorized access and misuse, posing significant threats to individuals' privacy and security.

<sup>4</sup> [The Cost and Consequences of Identity Fraud | Regula Report \(regulaforensics.com\)](#)

<sup>5</sup> [Jumio named in BIPA lawsuit over crypto ID verification | Biometric Update](#)



## 5. IDV Systems as Potential Enablers of Institutional Fraud:

- Exploitation of IDV systems by crime syndicates to infiltrate and defraud institutions indicates a fundamental flaw in the design and implementation of these solutions. Criminal organizations leverage weaknesses in IDV processes to perpetrate Identity fraud, ultimately undermining the integrity of financial and other regulatory systems.
- **Flaws:** Inadequate authentication methods and vulnerabilities in IDV systems enable criminals to manipulate verification processes, facilitating fraudulent activities. By exploiting these weaknesses, crime syndicates evade detection and perpetrate illicit activities, posing substantial risks to institutions and their clients.

In the realm of Identity Verification (IDV) systems, there persists a prevalent misconception that Human Identity can be reduced to a mere digital artifact. These systems often rely on intricate coding and algorithms, aiming to authenticate individuals' vitality through images or videos. However, addressing the shortcomings within IDV systems goes beyond refining algorithms or embracing further digital augmentations, such as voice recognition. Despite this reality, IDV institutions continue to overlook the fundamental existence of Real-World Human Beings in their pursuit of solutions.

The management of Human Identity and Identity Verification Solutions transcends mere data collection, necessitating profound respect for individual uniqueness. An individual's Identity isn't merely a compilation of data points; it serves as a substantive testament to their real-world existence. Effective Identity Management integrates the core tenets of Records Management seamlessly into every aspect of human Identity.

To effectively combat the rise of Synthetic Identities, a more focused approach to Identity Management is essential, coupled with a cessation of undervaluing the uniqueness of the individual. Recognizing Human Identity as a definitive record of one's physical presence underscores the critical importance of ensuring unquestionable certainty in engaging with real-world individuals, thereby preventing Synthetic Identity infiltration. IDV systems must evolve to embrace this holistic understanding, safeguarding the integrity of identities in an increasingly digital world.



# Presentation Attack Detection (PAD) and Injection Attack Detection: A Struggle in Identifying Spoof and Deepfake Identities<sup>6</sup> *(and approaches to prevent attacks, i.e. presentation attack detection)*

In the domain of biometric authentication, the ability to discern between genuine attempts and fraudulent presentations is paramount. Presentation Attack Detection (PAD) serves as a cornerstone in this endeavor, providing a framework for categorizing and identifying various types of attacks. The categories defined in ISO/IEC 30107 offer a structured approach:

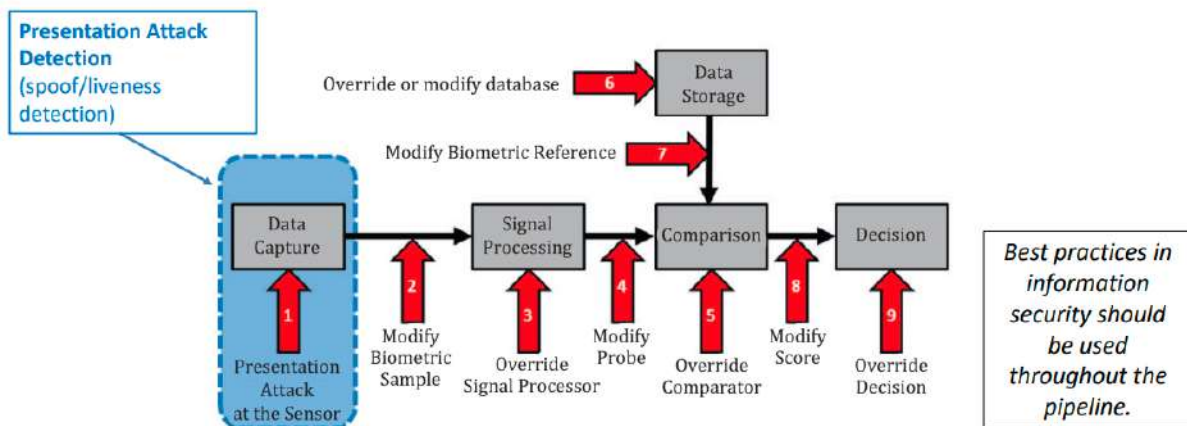


Figure 3: Stephanie Schuckers, Communicating Identity & Overcoming “Corrupted Information”, FedID, September 07, 2023 <https://events.afcea.org/FedID23/Public/SessionDetails.aspx?FromPage=Sessions.aspx&SessionID=10427&SessionDateID=712>

## 1. Liveness not Related to Challenge-Response ("Passive"):

This category encompasses presentations devoid of any indication of response to a challenge. Passive attacks include static images or videos lacking dynamic characteristics associated with live presentations.

## 2. Involuntary Challenge Response:

Attacks in this category elicit involuntary responses from the subject, such as changes in pupil dilation due to exposure to random stimuli or variations in light colors.

## 3. Voluntary Challenge Response:

Here, the presentation prompts voluntary responses from the subject, like specific gestures or utterances in response to predefined challenges.



<sup>6</sup> [CommunicatingIdentity&Overcoming“CorruptedInformation”.pdf](#) - Communicating Identity & Overcoming “Corrupted Information” September 2023 Dr. Stephanie Schuckers Director, Center for Identification Technology Research (CITeR) Professor, Clarkson University



While PAD primarily focuses on detecting presentation attacks, including Deepfake Identities, Injection Attack Detection addresses threats like Deepfake injection into the authentication process. Although not explicitly covered by ISO/IEC 30107, Injection Attack Detection is crucial for bolstering the security of biometric systems.

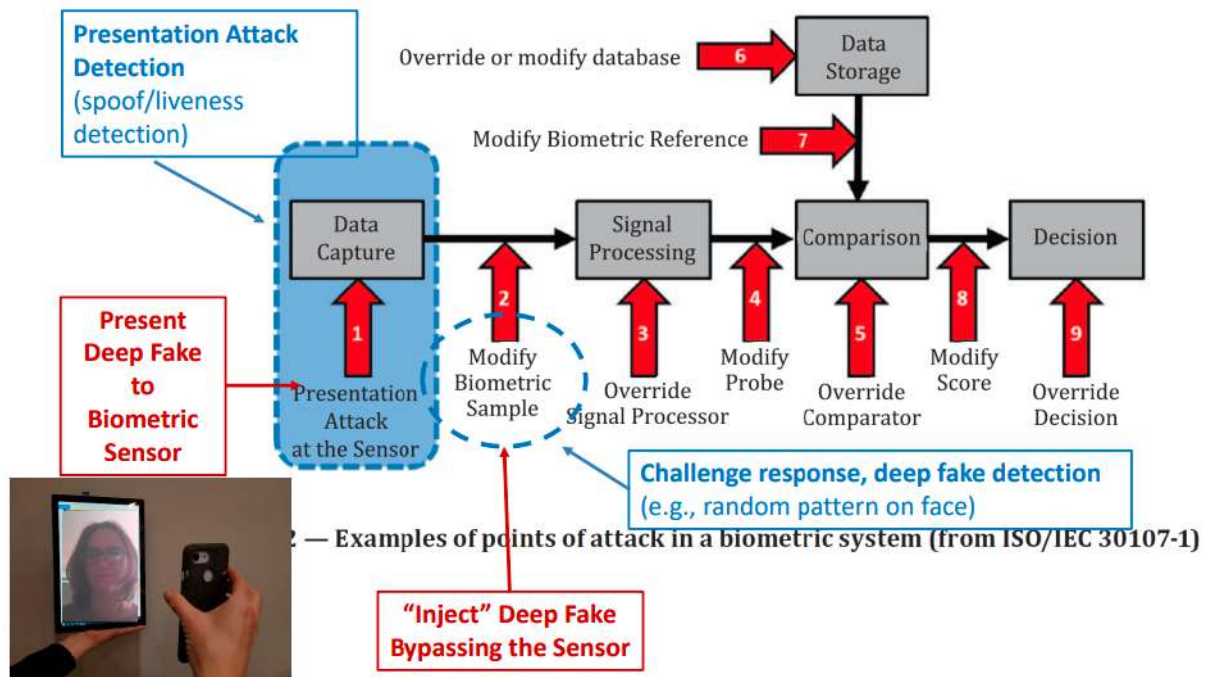


Figure 4: Stephanie Schuckers, *Communicating Identity & Overcoming "Corrupted Information"*, FedID, September 07, 2023 <https://events.afcea.org/FedID23/Public/SessionDetails.aspx?FromPage=Sessions.aspx&SessionID=10427&SessionDateID=712>

Potential solutions for Injection Attack Detection include:

**1. Deepfake Detection not Related to Challenge-Response ("Passive"):**

Techniques to Identify Deepfakes without relying on explicit challenges or responses.

**2. Involuntary Challenge Response:**

Detection of physiological responses like changes in pupil dilation or light colors due to random input.

**3. Voluntary Challenge Response:**

Solutions prompt specific responses from users to verify their authenticity.

**4. Best Practices in IT Security:**

Implementation of measures such as detecting virtual cameras, browser scripts, etc., to thwart injection attacks.

The advent of Deepfake technology exacerbates the challenge faced by biometric recognition systems. While certifications exist for PAD solutions, there's a noticeable gap concerning certifications specific to injection attacks. Standards such as ISO and frameworks like FIDO play a crucial role in addressing these challenges by considering security and other detection methods.



## Summary:

### 1. PAD:

Understanding the three categories of PAD is crucial for Identifying and mitigating presentation attacks. Independent testing is necessary for evaluating performance, with multiple certification programs available.

### 2. Deepfakes:

Deepfakes pose dual threats as both presentation and injection attacks. While ISO 30107 focuses on PAD, solutions for Deepfake detection and best practices in IT security are essential in combating these threats.

### 3. Certification:

Certifications for biometric solutions addressing injection attacks are lacking, emphasizing the need for standards and evaluation frameworks tailored to these specific threats.

In conclusion, the struggle to Identify spoof and Deepfake Identities persists, necessitating comprehensive solutions that encompass both PAD and Injection Attack Detection to safeguard biometric authentication systems effectively.



## Vulnerabilities Exploited by Crime Syndicates in IDV Systems

In an Identity Verification (IDV) system, Presentation Attack Detection (PAD) and Injection Attack Detection are critical for ensuring the authenticity and integrity of the Identity verification process. However, crime syndicates and bad actors exploit vulnerabilities in the system, manipulating the onboarding process and exploiting weaknesses at various stages to perpetrate fraudulent activities within the institution to be defrauded or manipulated.

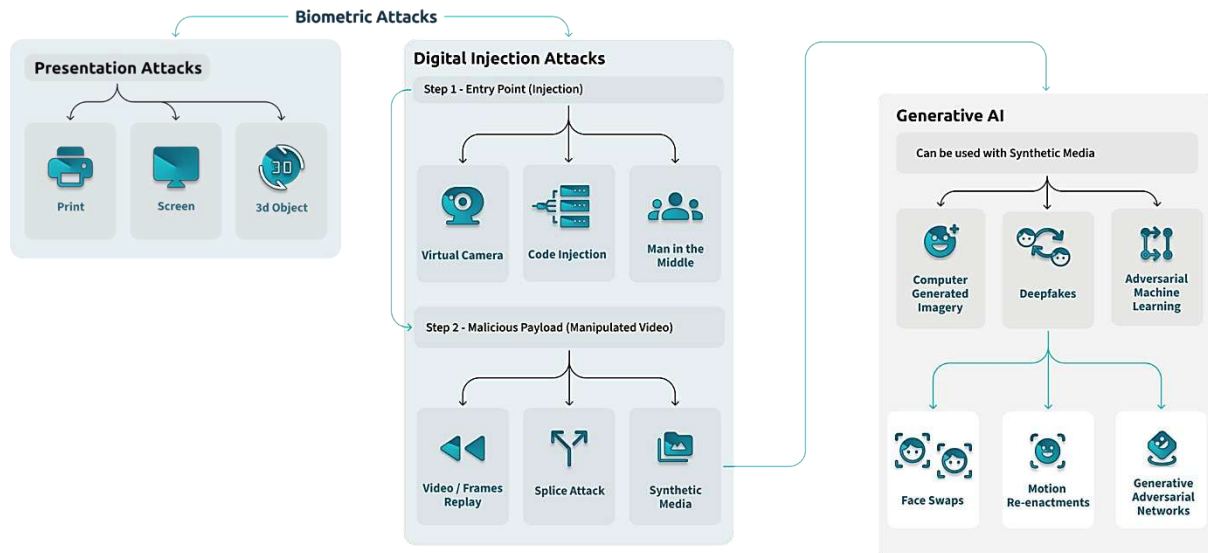


Figure 5: The iProov Taxonomy of Threats<sup>7</sup>

### Easiest Targets for Manipulation:

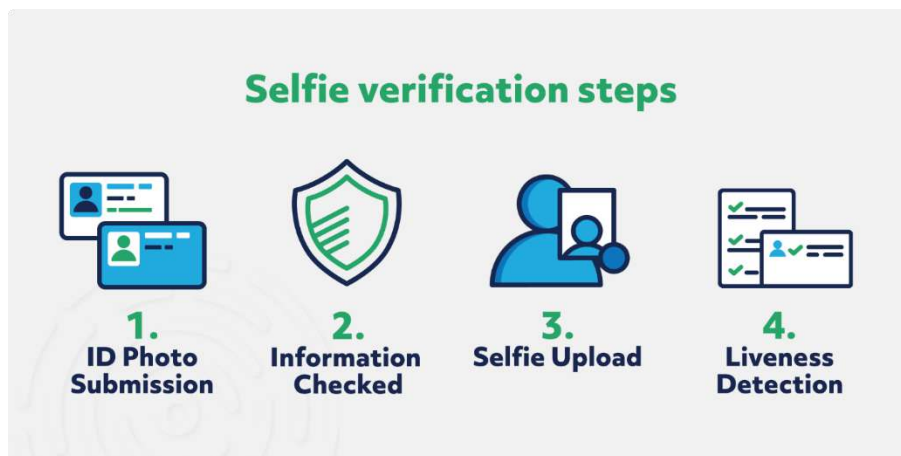


Figure 6: What is Selfie Identity Verification?<sup>8</sup>

#### 1. Onboarding or Verification Stage:

During the onboarding or verification process, individuals submit their Identity documents and biometric data to the IDV system for verification. This stage is particularly vulnerable to manipulation by crime syndicates and bad actors. Criminal organizations use stolen or forged Identity documents to create Synthetic Identities, which can then be onboarded

<sup>7</sup> [iProov Taxonomy of Threats-compressed.pdf](#)

<sup>8</sup> [What is Selfie Identity Verification? \(truststamp.ai\)](#)



onto the IDV system. Additionally, Deepfake technology allows for the creation of realistic synthetic biometric data, such as facial images or voice samples, which can be used to pass Identity verification checks.

## 2. Initial Data Collection and Presentation Capture:

Once onboarded, individuals provide additional biometric presentations (e.g., facial images, and voice samples) during authentication attempts. Crime syndicates already use advanced Deepfake technology to generate synthetic presentations that closely mimic genuine biometric data, making them difficult to detect during the presentation capture stage.

### Most Difficult Attacks to Detect:

#### 1. Injection Attack Stage:

Injection attacks involve manipulating or injecting fraudulent data directly into the IDV system, bypassing traditional presentation capture stages. This can be particularly challenging to detect because the injected data may closely resemble genuine biometric presentations, making it difficult to differentiate between legitimate and fraudulent Identities.

#### 2. Post-Authentication Stage:

Once an Identity has been authenticated, it may be challenging to detect manipulation or fraudulent activity, especially if the system lacks continuous monitoring capabilities. Crime syndicates may exploit vulnerabilities in the system's data handling processes to manipulate or inject data post-authentication, compromising the integrity of the IDV solution.

### Reasons for Exploitation by Crime Syndicates:

#### 1. Complexity of Detection:

The difficulty of detecting presentation and injection attacks at various stages of the IDV process makes these systems attractive targets for crime syndicates. The sophistication of Deepfake technology and the ability to create Synthetic Identities make it challenging for IDV solutions to distinguish between genuine and fraudulent presentations.

#### 2. Reliance on IDV Solutions:

Institutions and organizations often rely heavily on IDV solutions for Identity verification purposes, making them lucrative targets for infiltration by crime syndicates. Bad actors exploit this reliance by exploiting vulnerabilities in IDV systems to gain unauthorized access or commit fraudulent activities.

The vulnerability of the onboarding process, combined with the complexity of detecting presentation and injection attacks at various stages of the IDV process, provides ample opportunities for manipulation by crime syndicates and bad actors. To mitigate these risks, IDV solutions must implement robust security measures, including advanced detection algorithms, continuous monitoring, and thorough verification processes, to safeguard against fraudulent activities and protect the integrity of the Identity verification process.





## Heightened Threats: The Impact of AI on Identity Verification (IDV) Solutions

The integration of Artificial Intelligence (AI) into Identity Verification (IDV) solutions brings about significant concerns and challenges, particularly in the realm of security and fraud prevention.



Figure 7: One-Third of Global Businesses Already Hit by Voice and Video Deepfake Fraud<sup>9</sup>

Some negative impacts AI is already having now and is likely to exacerbate in the future:

### 1. Emergence of Deepfake Synthetic Identities:

AI technologies are increasingly utilized by sophisticated crime syndicates to generate Deepfake Synthetic Identities. These Identities are incredibly realistic and difficult to detect using traditional verification methods. As AI algorithms continue to advance, the creation of Synthetic Identities will become even more sophisticated and prevalent.

### 2. Struggle to Stay Ahead:

IDV solutions are facing an uphill battle to stay ahead of the rapid advancements in AI-driven Deepfake technology. Despite efforts to enhance fraud detection algorithms, the

<sup>9</sup> The rise of AI-generated identity fraud like deepfakes is alarming, with 37% of organizations experiencing deepfake voice fraud and 29% falling victim to deepfake videos, according to a survey by Regula, a global developer of forensic devices and identity verification (IDV) solutions. The increasing accessibility of artificial intelligence technology for creating deepfakes is making the risks mount, posing a significant challenge for businesses and individuals alike. [One-Third of Global Businesses Already Hit by Voice and Video Deepfake Fraud | Business Wire](#)





pace of AI innovation often outstrips the ability of IDV solutions to adapt. This results in a constant game of catch-up, leaving vulnerabilities in the verification process.

### 3. Futility of Detection Methods:

As AI capabilities evolve, the methods employed to detect Synthetic Identities may become increasingly ineffective. In particular, techniques relying on AI to detect AI-generated Deepfakes may prove futile shortly. This could render current detection mechanisms obsolete, leaving IDV solutions vulnerable to exploitation.

### 4. IDV Prediction:

[Replying to @Time VS Journey Artificial Intelligence will be able to e... | Artificial Intelligence | TikTok](#) (In the TikTok video, the commentator suggests that the quality of fabricated photos, videos, and voices of individuals will reach a point where discerning whether you're interacting with an actual Human Being will become increasingly challenging, even impossible - Dawid Jacobs)

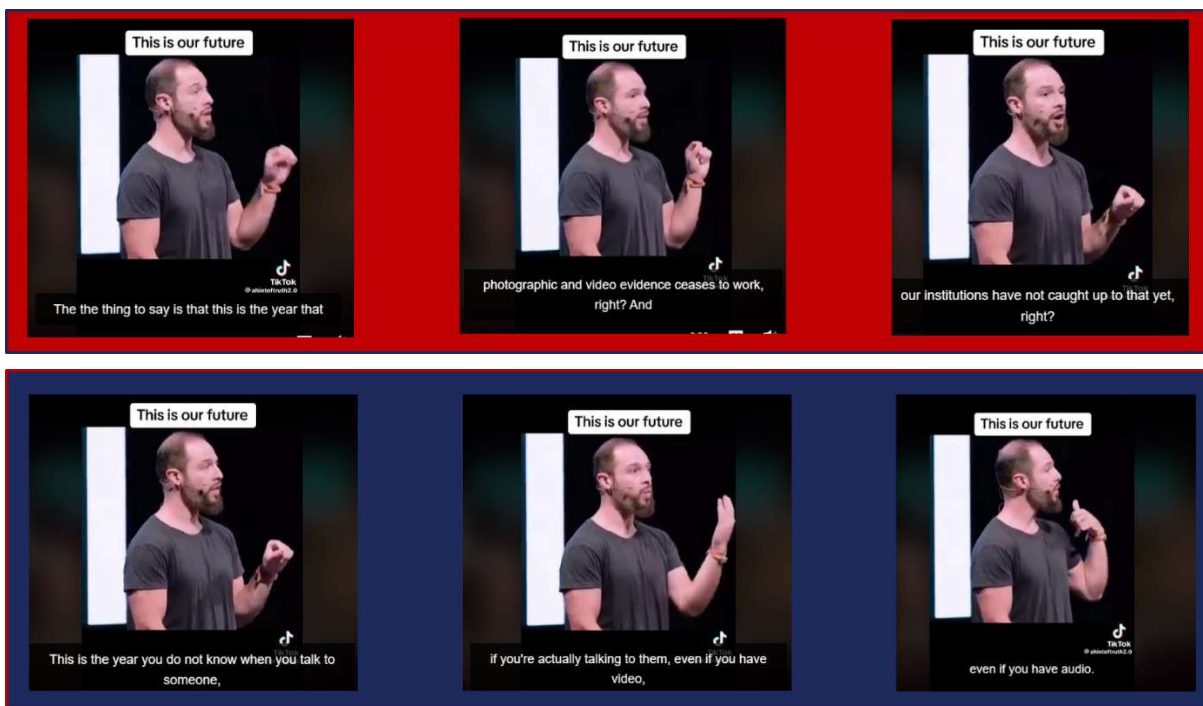


Figure 8: Images from: [Replying to @Time VS Journey Artificial Intelligence will be able to e... | TikTok](#)

Furthermore, the issue amplifies when even a single Synthetic Identity infiltrates any system, opening the door to considerable data, financial, and reputational losses. While present Identity Verification Solutions may prove lucrative for providers, viewing Synthetic Identity as solely a data problem that can be resolved through digital comparisons disregards the fundamental issue—Synthetic Identities are intrinsically rooted in human manipulation. The problem escalates when unprepared buyers invest in solutions that fail to address the underlying challenges, thereby exacerbating the imminent challenges of the situation.

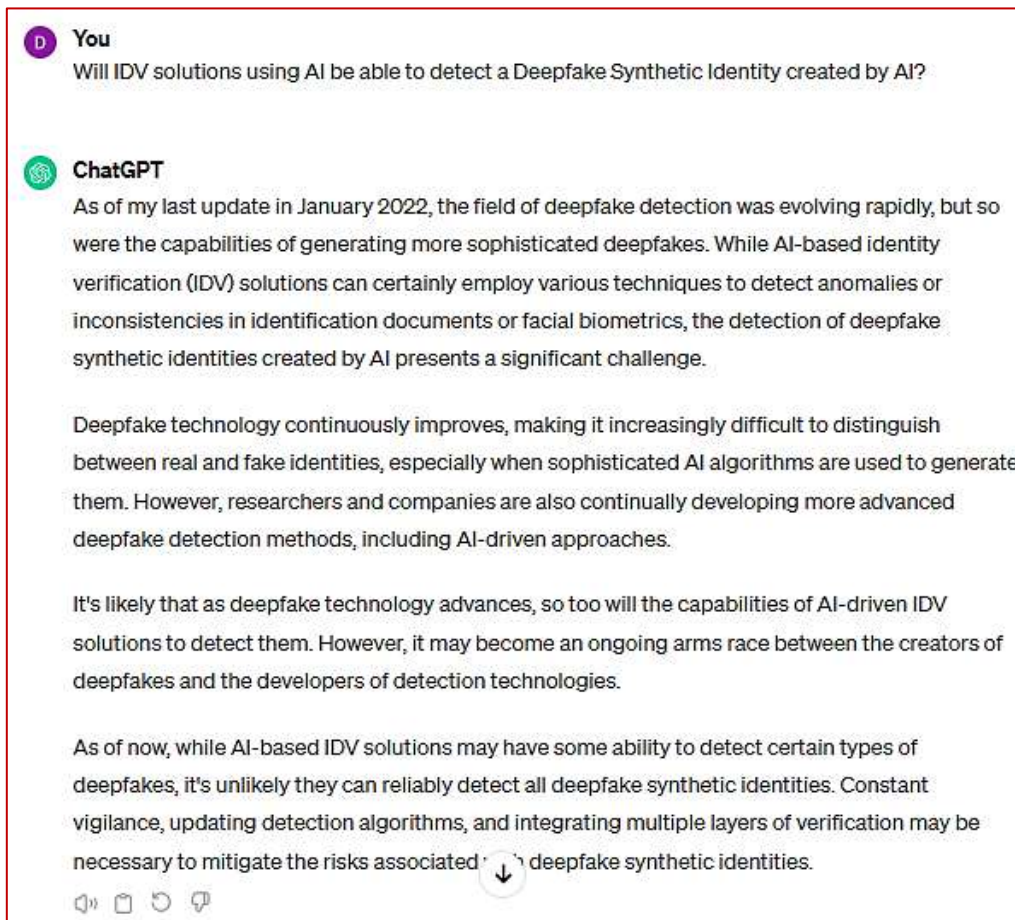


## 5. Disregarding Warnings<sup>10</sup>:

Warnings about the escalating risk posed by Synthetic Identities have been issued for years. Financial institutions, in particular, were alerted to this threat, emphasizing that criminal syndicates would exploit and manipulate Identity verification (IDV) solutions to infiltrate institutions. Their aim is not solely to defraud individuals but primarily to defraud the institutions themselves, notably traditional banks and FinTech entities. This threat has now materialized into actual attacks. Once again, the imperative is clear: **Take Identity Management Seriously**<sup>11</sup>. Recognize that you are, fundamentally, a Human Being before you are anything digital.

## 6. Infiltration of Institutions:

IDV solutions, particularly those utilizing "selfies" and "voice" with liveness detection, are not merely at risk of exploitation by organized crime syndicates and AI; they likely have already been compromised. These syndicates are actively preparing for attacks that could dismantle any institution within days. While these technologies were designed to bolster security, they may unwittingly offer pathways for fraudsters and malicious entities to infiltrate institutions. Such infiltration could result in a range of fraud schemes, manipulation of individuals, and potential compromise of voting systems.



**You**  
Will IDV solutions using AI be able to detect a Deepfake Synthetic Identity created by AI?

**ChatGPT**  
As of my last update in January 2022, the field of deepfake detection was evolving rapidly, but so were the capabilities of generating more sophisticated deepfakes. While AI-based identity verification (IDV) solutions can certainly employ various techniques to detect anomalies or inconsistencies in identification documents or facial biometrics, the detection of deepfake synthetic identities created by AI presents a significant challenge.

Deepfake technology continuously improves, making it increasingly difficult to distinguish between real and fake identities, especially when sophisticated AI algorithms are used to generate them. However, researchers and companies are also continually developing more advanced deepfake detection methods, including AI-driven approaches.

It's likely that as deepfake technology advances, so too will the capabilities of AI-driven IDV solutions to detect them. However, it may become an ongoing arms race between the creators of deepfakes and the developers of detection technologies.

As of now, while AI-based IDV solutions may have some ability to detect certain types of deepfakes, it's unlikely they can reliably detect all deepfake synthetic identities. Constant vigilance, updating detection algorithms, and integrating multiple layers of verification may be necessary to mitigate the risks associated with deepfake synthetic identities.

Figure 9: Direct question to AI

<sup>10</sup> [Synthetic identity "creation" - a tsunami of problems for financial institutions | LexisNexis South Africa](#)

<sup>11</sup> [Taking Identity Management Seriously – Preventing Identity Theft | LexisNexis South Africa](#)



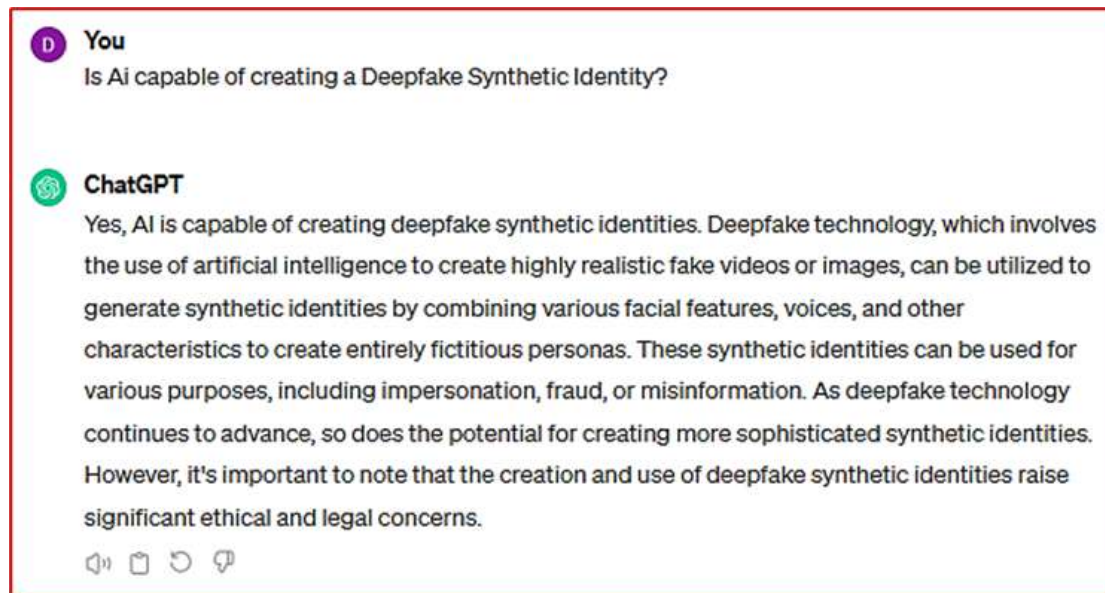


Figure 10: Direct question to AI

The integration of artificial intelligence (AI) into Identity Verification (IDV) solutions has raised serious concerns about the emergence of Deepfake technology. Deepfakes, Synthetic Identities created using advanced algorithms blending facial features, voices, and other traits, present diverse challenges, from impersonation to the spread of misinformation and fraud, raising ethical and legal dilemmas.

As Deepfake technology evolves, the ability to generate highly convincing Synthetic Identities grows. This underscores the urgent need for proactive action from stakeholders, including regulatory bodies, technology developers, and society as a whole. While robust safeguards like authentication mechanisms and detection algorithms are essential to curb the misuse of Synthetic Identities, their implementation seems inadequate. Additionally, increasing awareness about Deepfakes is crucial to empower individuals and organizations in discerning reality from digitally manipulated content.

Responsible and ethical use of AI-driven Deepfake technology is paramount to preserving Identity integrity and trust in digital interactions. Achieving this requires navigating the ethical complexities of this rapidly advancing field through collective action and a commitment to ethical principles. Neglecting these challenges could have severe consequences for individuals and institutions, highlighting the urgent need for proactive measures to safeguard against the evolving threats of AI-driven Deepfake technology.





# Consent: The Ethical, Legal, and Privacy Dimensions of Facial Recognition Technology



Figure 11: Facial Recognition Technology: Threat to Personal Privacy and Security<sup>12</sup>

The utilization of digital images, particularly facial recognition technology, for identifying potential criminals has sparked intense debate and scrutiny. While promising enhanced law enforcement and public safety, this technology also raises ethical, legal, and privacy concerns that warrant careful consideration. Achieving a balance between leveraging facial recognition's benefits and safeguarding individual rights is a complex challenge, demanding exploration of various facets. In this discussion, we delve into the key dimensions of this debate, shedding light on the ethical dilemmas, legal frameworks, and privacy implications associated with facial recognition technology in criminal identification.

## 1. Effectiveness of Facial Recognition

Facial recognition technology serves as a tool for law enforcement, enabling the identification of individuals in surveillance footage or public spaces swiftly. Its capacity to scan and compare faces against extensive databases holds promise for crime-solving, locating missing persons, and enhancing public safety. Quick face matching against vast datasets provides law enforcement a significant advantage in investigations.

## 2. Data Privacy and Consent

The ethical quandary arises from collecting and storing facial data without explicit informed consent. Consent, a foundational principle in data protection regulations like GDPR, is essential for respecting individuals' privacy rights. Individuals must be fully informed about facial data usage and granted the choice to opt in or out.

<sup>12</sup> [Facial Recognition Technology: Threat to Personal Privacy and Security | LinkedIn](#)

### 3. Data Security

Ensuring the security of facial data is paramount. Any compromise or unauthorized access can lead to severe privacy breaches and misuse of sensitive information. Robust security measures, including encryption and stringent access controls, are vital for safeguarding this data.

### 4. Bias and Accuracy

Concerns arise regarding biases inherent in facial recognition algorithms, especially concerning race and gender. Biased algorithms may lead to wrongful identification and profound consequences. Rigorous testing and bias mitigation strategies are crucial to address these concerns.

### 5. Legislation and Regulation

Countries and regions have initiated legislation and guidelines governing facial recognition technology usage. GDPR, for instance, regulates biometric data collection, processing, and storage, aiming to balance security and individual privacy.

### 6. Transparency and Accountability

Transparency in law enforcement and organizational practices employing facial recognition is indispensable. Clear protocols and mechanisms for accountability are necessary to rectify misuse or identification errors, ensuring individual rights protection.

### 7. Public Opinion and Debate

Facial recognition deployment has sparked substantial public debate. Engaging the public and stakeholders in discussions is crucial for evaluating technology's benefits and risks. Balancing individual rights and public safety is a dynamic challenge requiring ongoing dialogue.

### 8. Alternatives and Oversight

Investing in alternatives, like community policing or enhanced surveillance oversight mechanisms, may offer less invasive solutions than sole reliance on facial recognition.

The use of facial recognition in criminal identification requires balancing potential law enforcement advantages with individual rights and privacy protection. Upholding principles of informed consent, data security, fairness, and accountability is essential for ethical and effective technology use. Navigating evolving legislation, public opinion, and security-privacy considerations remains a challenging task demanding careful consideration and regulation.





## Algorithm Bias in Selfie and Liveness Verification Solutions: A Complex Challenge



Figure 12: What is Selfie Identity Verification?<sup>13</sup>

Algorithm bias in "selfie and liveness verification solutions poses a critical concern due to its potential for discrimination or inaccuracies in the verification process. While these solutions offer benefits such as good security and user convenience, they are susceptible to bias, which can have profound implications for individuals and institutions. Here's an in-depth examination of this complex challenge:

### 1. The Nature of Algorithm Bias

#### a. Data Bias:

Algorithm bias can arise from biased training data. If the data used to train these algorithms is not representative of the entire population, it can lead to skewed results. For example, if training data primarily includes images of certain racial or gender groups, the algorithm may perform less accurately for individuals from underrepresented groups.

#### b. Algorithm Design Bias:

Bias can also result from flawed algorithm design or inadvertent prioritization of certain characteristics. This bias can affect how algorithms analyze facial features or assess liveness, potentially leading to disparities in verification outcomes.

### 2. Impact on Different Groups

#### a. Racial Bias:

Concerns about racial bias are significant, as some facial recognition algorithms exhibit higher error rates for people with darker skin tones. This bias can result in

<sup>13</sup> [What is Selfie Identity Verification? \(truststamp.ai\)](https://truststamp.ai)



discriminatory outcomes, where certain racial or ethnic groups face more verification failures.

#### **b. Gender Bias:**

Gender bias can also be problematic, with algorithms sometimes struggling to accurately verify individuals whose gender presentation does not conform to binary norms. This can disproportionately affect transgender or non-binary individuals.

### **3. Legal and Ethical Implications**

Algorithm bias in Identity verification solutions raises legal and ethical questions. Discriminatory outcomes can lead to unfair treatment, privacy violations, and breaches of anti-discrimination laws.

### **4. Mitigation Efforts**

Addressing algorithm bias requires a multi-faceted approach:

- a. Diverse Training Data:** Ensuring training data represents diverse populations can help reduce bias.
- b. Algorithm Audits:** Regular audits of algorithms for bias can identify and rectify issues.
- c. Transparency:** Solution providers should be transparent about their algorithms and update them regularly to improve fairness and accuracy.
- d. User Education:** Educating users about the limitations and potential biases of these solutions is crucial.

### **5. Evolving Regulatory Landscape**

As concerns about algorithm bias in facial recognition and Identity verification grow, various regions are implementing or considering regulations to address these issues. Compliance with evolving regulations is becoming critical for solution providers.

Algorithm bias in selfie and liveness verification solutions presents a multifaceted challenge, with the potential to unfairly impact diverse demographic groups. Solution providers must remain vigilant, continuously striving to reduce bias through diverse data, transparency, and algorithmic enhancements. However, the advent of AI-generated Deep Fakes and Synthetic Identities poses a significant threat, potentially overwhelming traditional IDV methods. Institutions and governments must navigate this complex terrain, embracing emerging technologies like Forensic Identity Management (FIM) to defend against these evolving threats and ensure the resilience of Identity verification systems. Failure to adapt could have far-reaching consequences, emphasizing the need for flexibility and innovation in this critical domain.



## Addressing the Fragmentation in Identity Verification and Management Systems:

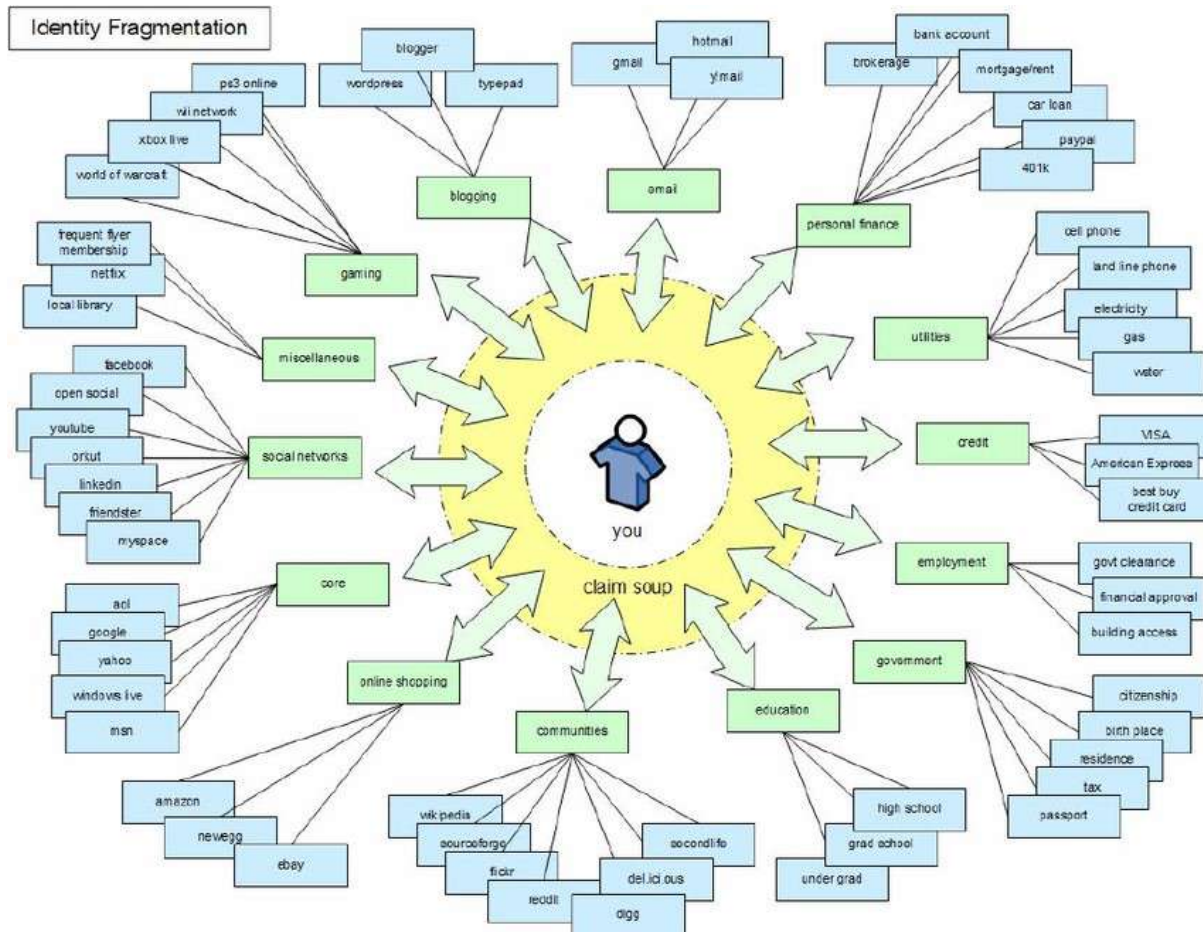


Figure 13: [\(PDF\) How Can a Person's Digital Identity be Managed and Protected? \(researchgate.net\)](#)

The fragmented nature of Identity verification (IDV) solutions and Identity Management systems is indeed a significant global issue. This fragmentation stems from several factors, including the diversity of stakeholders involved, varying technological standards, and differing regulatory environments across regions.

### 1. Lack of Standardization:

One of the primary reasons for the fragmentation in IDV and other Identity solutions is the absence of standardized protocols and frameworks for Identity verification. Different hardware and software suppliers may adhere to their proprietary standards, making interoperability between systems difficult if not impossible.

### 2. Silos of Information:

Identity solutions often operate in silos, where each system stores and processes Identity data independently. This lack of integration results in duplication of efforts and inefficiencies when attempting to verify Identities across multiple platforms.

### 3. Regulatory Challenges:

Compliance with regulatory requirements such as GDPR in Europe or HIPAA in the United States adds another layer of complexity to Identity Management systems. Different



regions have their regulations regarding data privacy and security, making it challenging to develop a one-size-fits-all solution. Moreover, the lack of adherence to standards like ISO 15489 Records management further complicates the situation.

#### **4. Forensic Protocols:**

The absence of forensic protocols in basically all IDV and other Identity solutions exacerbate the problem by providing fertile ground for the creation of Synthetic Identities and Deepfake technology. Forensic protocols are necessary to ensure the authenticity and integrity of Identity data, but their implementation is often overlooked in favor of more immediate verification needs.

#### **5. Limited Collaboration:**

Collaboration between Identity solution providers, hardware suppliers, software developers, and regulatory bodies is limited, further exacerbating the fragmentation issue. Without cooperation and communication among these stakeholders, it's challenging to develop comprehensive Identity Management systems that address the evolving threats posed by Deepfake technology and Synthetic Identities.

**To address these challenges and move towards a more cohesive Identity Management ecosystem, several steps must be taken:**

##### **1. Standardization Efforts:**

Industry-wide efforts to establish standardized protocols for Identity verification can promote interoperability between different systems and suppliers.

##### **2. Regulatory Alignment:**

Regulatory bodies should work towards harmonizing data privacy and security regulations to facilitate the development and adoption of unified TRUE Identity Management solutions.

##### **3. Investment in Forensic Technologies:**

Prioritizing the development and integration of Forensic Identity Management (FIM) into IDV solutions can mitigate the risks associated with Deepfake technology and Synthetic Identities.

##### **4. Collaborative Partnerships:**

Encouraging collaboration and partnerships between Identity solution providers, hardware suppliers, software developers, and regulatory bodies can foster innovation and drive the development of more comprehensive Identity Management systems.

By addressing these issues and implementing collaborative solutions, the industry MUST work towards overcoming the fragmentation in Identity verification and management, thereby enhancing security and trust in digital Identities.



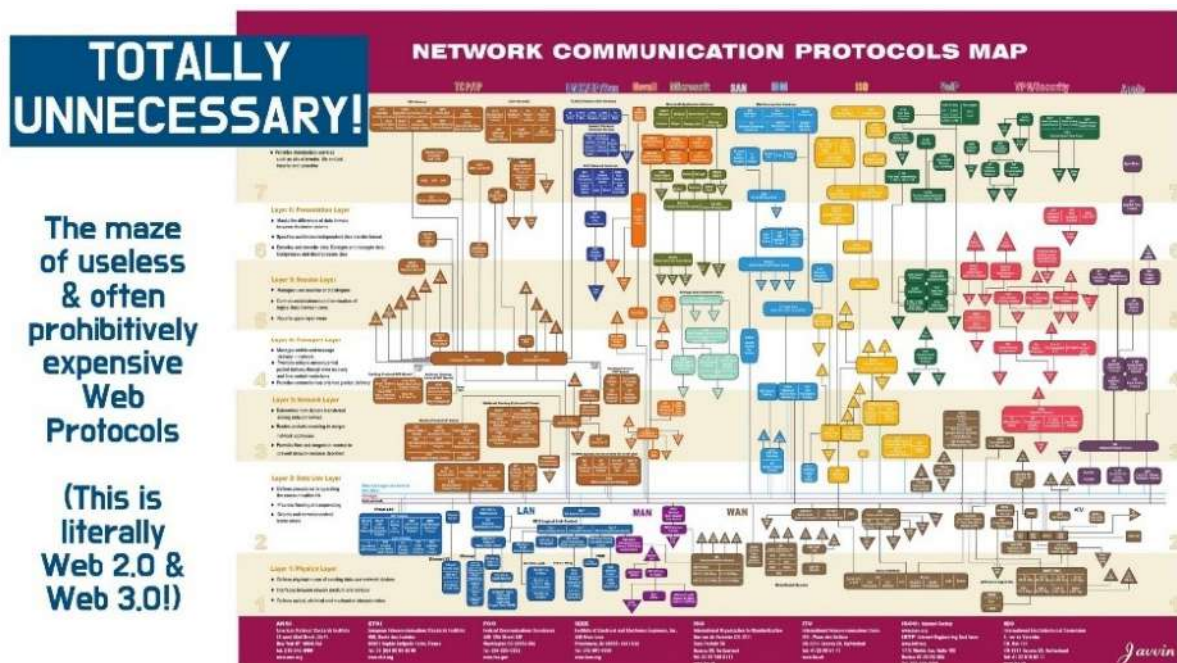


## Challenges in Identity Management on Web 2.0 and Web 3.0:

Identity Management, including the creation of Digital Twins or Digital Identities, faces significant challenges on both Web 2.0 and Web 3.0 due to the inherent flaws in these paradigms.

### 1. Overreliance on Protocols

- **Web 2.0:** The reliance on HTTP and other protocols in Web 2.0 makes it challenging to establish secure and reliable Identity Management systems. These protocols lack robust security features, exposing Digital Identities to vulnerabilities such as man-in-the-middle attacks and data breaches.
- **Web 3.0:** While decentralized protocols like blockchain offer promising features for Identity Management, they also introduce new complexities. Smart contract vulnerabilities and the pseudonymous nature of blockchain transactions raise concerns about the security and privacy of Digital Identities in Web 3.0 environments.



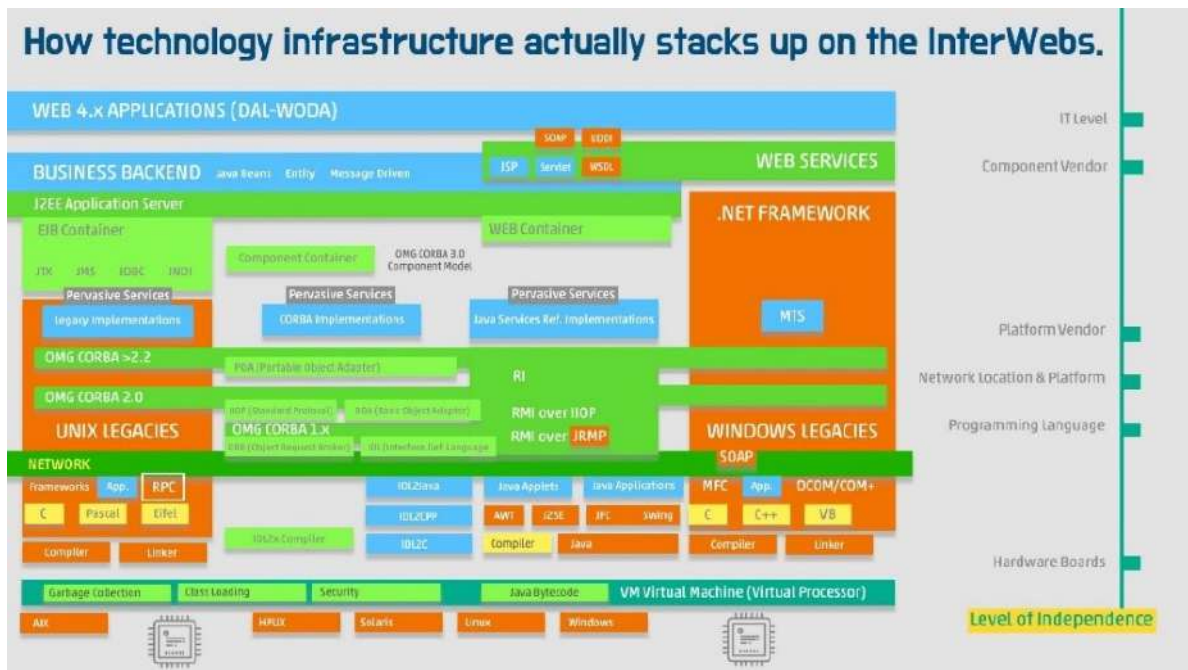
### 2. Lack of Object-Level Security

- **Web 2.0:** Security mechanisms in Web 2.0 are often implemented at higher layers, neglecting object-level security. This leaves Digital Identities susceptible to attacks targeting individual objects or instances within applications, such as injection attacks or unauthorized access to personal information.
- **Web 3.0:** Despite security measures at the transaction level in blockchain protocols, the security of Digital Identities at the object level is not guaranteed. Vulnerabilities in smart contracts or decentralized applications can compromise the integrity and confidentiality of Digital Identity data.



### 3. Complexity and Interoperability Issues

- **Web 2.0:** The proliferation of diverse protocols and standards complicates Identity Management in Web 2.0, leading to interoperability challenges. Different Identity Management systems may have varying security mechanisms, making it difficult to establish consistent and reliable Digital Identities across platforms.
- **Web 3.0:** Interoperability among decentralized protocols introduces similar complexities for Identity Management. The diverse nature of blockchain networks and decentralized applications complicates the establishment of unified Identity Management systems, increasing the risk of security breaches and Identity theft.



### 4. Privacy Concerns

- **Web 2.0:** Privacy concerns are exacerbated by the lack of object-level security in Web 2.0 Identity Management systems. Without adequate protection of personal data, Digital Identities are vulnerable to privacy violations, data breaches, and unauthorized access.
- **Web 3.0:** While Web 3.0 aims to enhance privacy through decentralized protocols, challenges remain regarding the pseudonymous nature of blockchain transactions. Ensuring the privacy of Digital Identities requires robust privacy-enhancing technologies that address the anonymity and traceability of blockchain transactions.



## To sum it up:

THE ENTIRE INTERNET

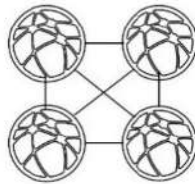


THE ENTIRE WEB



&

Do not function properly nor securely without:



**INTEROPERABLE WEB OBJECTS!**



Identity Management faces significant obstacles on both Web 2.0 and Web 3.0 due to the inherent flaws in these paradigms, including overreliance on protocols, lack of object-level security, complexity, interoperability issues, and privacy concerns. Addressing these challenges requires comprehensive solutions that improve protocol design, enhance security mechanisms, and prioritize privacy-enhancing technologies.



## The Urgent Need to Rethink Remote Onboarding: Mitigating the Escalating Threat of Deepfake Synthetic Identities

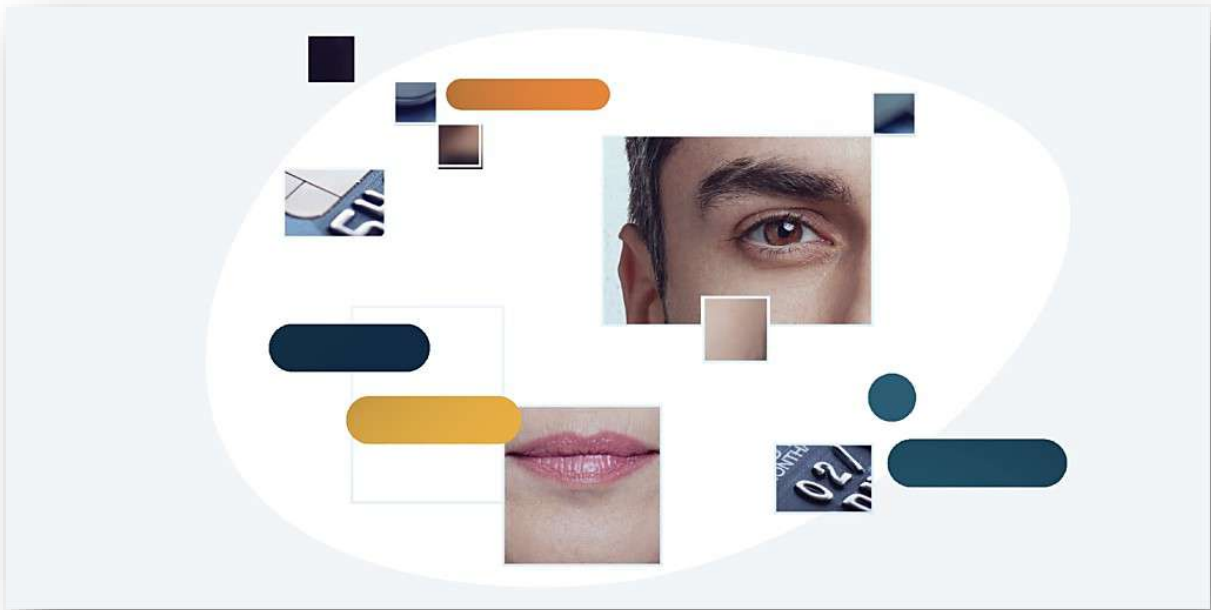


Figure 14: How Deepfakes Threaten Remote Identity Verification Systems<sup>14</sup>

Remote onboarding using "selfie" or "voice" with "liveness detection" has gained widespread adoption in Identity verification processes across industries. Despite its touted convenience, this method faces significant challenges, notably the proliferation of Deepfake Identities and the absence of robust verification mechanisms.

### Deepfake Identities:

1. Deepfake technology facilitates the creation of Synthetic Identities that closely emulate real individuals. By seamlessly blending facial features or voice recordings, Deepfake Identities can easily deceive standard verification processes.
2. This alarming trend provides a lucrative opportunity for fraudsters, including organized crime syndicates, to infiltrate institutions and engage in fraudulent activities.

### Lack of Legal Proof of Identity:

1. Remote onboarding methods such as "selfie" or "voice" with "liveness detection" fall short of providing 100% legal proof of an individual's Identity.
2. Without conclusive evidence verifying the Identity of a Single Existing Real-World Human Being, these methods leave room for exploitation.
3. The absence of Forensic measures in biometric authentication exacerbates the risk of Identity fraud.

<sup>14</sup> [How Deepfakes Threaten Remote Identity Verification Systems | iProov](#)

### **Absence of ISO 15489<sup>15</sup> Compliance:**

1. An Identity is a Record of Proof of a Single Existing Real-World Human Being.
2. Remote onboarding processes frequently overlook compliance with ISO 15489 standards, which establish fundamental principles for creating, capturing, and managing records.
3. The lack of comprehensive record-keeping and verification procedures compromises the integrity and reliability of Identity verification.
4. This regulatory gap creates vulnerabilities that fraudsters can exploit, further jeopardizing the security of the onboarding process.

### **Vulnerability to Manipulation:**

1. Remote onboarding methods are susceptible to manipulation by fraudsters, especially through the utilization of Deepfake technology.
2. Synthetic images or voice recordings can effortlessly circumvent liveness detection checks, enabling fraudsters to impersonate legitimate users undetected.
3. This manipulation undermines the trustworthiness of the onboarding process and poses substantial risks to institutions.

### **Contributing to False Identity Data:**

1. Furthermore, remote onboarding processes inadvertently contribute to the dissemination of false Identity data. Credit Bureaus often receive this erroneous data from IDV solutions, inadvertently legitimizing Deepfake Synthetic Identities.
2. As these Synthetic Identities gain credibility and obtain increasing credit ratings, they become significant threats to institutions, exacerbating the surge in attacks within the IDV fraternity.

To tackle the risks of Deepfake Synthetic Identities and remote onboarding challenges, organizations must prioritize genuine security measures and robust verification protocols. Real-World Human Beings is crucial, requiring comprehensive document verification, biometric authentication, and real-time checks. Adhering to ISO 15489 standards ensures record integrity, bolstering trust. Failure risks crimes like Identity fraud and Sybil-like attacks, threatening institutional survival. Acknowledging the impact of Deepfake Synthetic Identities and fortifying Identity Management practices with Forensic Identity Management is crucial for safeguarding operations and reputation in a digital landscape.



---

<sup>15</sup> **ISO 15489** establishes the fundamental concepts and principles for creating, capturing, and managing records. This standard applies to records in any format, structure, or technological environment, regardless of time.

## Rethinking IDV: Addressing the Root Cause

In the realm of digital Identity verification, Presentation Attack Detection (PAD) and Injection Attack Detection have been regarded as the holy grail in combating fraudulent attempts. However, the crux of the issue lies not in addressing the symptoms, but in understanding the root cause of IDV failures. *The acknowledgment that an Identity represents a Real-World Human Being precedes its digital representation.*

### Reconsidering the Approach

Contemporary Identity verification processes often rely on methods such as "selfies" and "liveness detection" to authenticate individuals. However, this approach overlooks a fundamental truth: Identity is intrinsically linked to living, breathing individuals. Believing that everything digital and algorithms alone can adequately verify Human Identity is not just a fallacy but also contributes significantly to the rise of Synthetic Identities.

#### 1. The Fallacy of Digital Verification:

The notion that digital tools and algorithms can comprehensively authenticate Human Identities is flawed. Identity encompasses a myriad of complex attributes, including physical appearance, behavioral characteristics, and personal experiences. Attempting to encapsulate this multifaceted concept within the confines of digital verification methods oversimplifies the process and neglects crucial nuances.

#### 2. The Rise of Synthetic Identities:

The overreliance on digital verification methods has fueled the proliferation of Synthetic Identities. Crafted through advanced technologies like Deepfake algorithms, these Identities mimic real individuals with alarming accuracy. Exploiting the gaps in digital verification systems, Synthetic Identities evade detection and perpetrate fraudulent activities with impunity.

#### 3. Addressing the Core Issue:

Merely detecting presentation or injection attacks within digital verification systems fails to address the core issue – the disconnect between digital representations and real-world Identities. The emphasis on superficial measures like selfies and liveness detection perpetuates this disconnect, exacerbating the problem rather than resolving it.

#### 4. The Importance of Human Context:

Identity verification must transcend the digital realm and encompass the broader context of Human existence. It's not merely about verifying a set of digital attributes but understanding the intricate interplay between individuals and their environment. Factors such as social interactions, cultural backgrounds, and personal histories are integral to authenticating Identity accurately.

#### 5. The Importance of Human Context:

The limited effectiveness of face recognition biometrics in IDV systems, especially in identifying Deceased Identities, highlights its inherent shortcomings. This underscores the fact that relying solely on this type of biometric cannot reliably assist in identifying the Deceased when necessary.





*“Finally, when all else has been addressed, then the value of the face may be considered (Wilkinson and Rynn 2012). It has been shown in previous mass fatality events that facial identification is inherently flawed as a process of matching ante-mortem and postmortem information with the circumstances of the death often rendering environmental insults too detrimental to support an objective analysis. Ten percent of victims of the Asian Tsunami and fifty percent of victims of the Bali bombing of 12 October 2002 were wrongly identified by facial recognition (Lain et al. 2003).”<sup>16</sup>*

## Holistic Approach to Verification

To bridge the gap between digital representations and real-world Identities, a holistic approach to verification is essential. This entails integrating technological solutions with Human-centric principles and recognizing the limitations of algorithms in capturing the complexity of Human Identity. By acknowledging the intrinsic connection between individuals and their Identities, we can develop more robust and reliable verification processes.

## The Urgency of Action

Confronting the challenge of Identity verification demands a fundamental shift in approach. Rather than treating symptoms, we must address the root causes directly. This necessitates a paradigm shift in how we conceive and deploy Identity verification solutions.

### 1. Shifting Focus from Symptoms to Causes:

The prevailing approach to Identity verification often revolves around mitigating the symptoms of fraudulent activity. Measures such as Presentation Attack Detection (PAD) and Injection Attack Detection serve as reactive responses to fraudulent attempts. However, this reactive approach fails to address the underlying causes fueling the proliferation of Synthetic Identities and fraudulent activities.

### 2. Addressing the Core Issues:

To truly tackle the challenge of Identity verification, we must Identify and address the core issues at play. This involves nullifying both PAD and Injection Attack Detection, not as standalone measures, but as part of a broader strategy aimed at addressing the root causes of Identity fraud. These root causes may include the overreliance on digital methods, the disconnect between digital representations and real-world Identities, and the lack of robust authentication mechanisms.

### 3. The Imperative of Paradigm Shift:

To catalyze meaningful change in Identity verification, we must shift our perspective. Instead of seeing it as a static algorithmic process, we should acknowledge its dynamic nature, integrating both technology and human elements. This shift entails redefining traditional notions of Identity and authentication and adopting innovative, user-centric approaches prioritizing accuracy and security.

## Rethinking Conceptualization and Implementation

To combat Identity fraud, we must rethink verification methods beyond "selfies" and "liveness detection." Embracing holistic approaches integrating human context and real-world

---

<sup>16</sup> [Forensic Identification | Jan Bikker - Academia.edu](https://www.academia.edu/10111111/Forensic_Identification) pg. 10



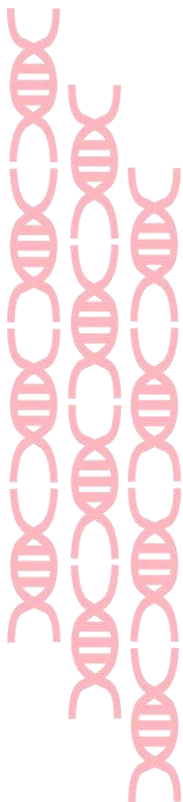
validation is crucial. By blending advanced tech with human expertise, we can create stronger verification processes resilient to emerging threats.

### **Acting Now**

The urgency of action in reimagining Identity verification cannot be overstated. With the proliferation of Synthetic Identities and the increasing sophistication of fraudulent activities, the status quo is no longer sufficient. We must act decisively and swiftly to effect meaningful change in the way we verify Identity, nullifying the root causes of Identity fraud and safeguarding the integrity of digital Identities for generations to come.

### **Conclusion**

The urgency of action in addressing the challenges of Identity verification demands a paradigm shift in approach. By shifting our focus from mitigating symptoms to addressing root causes, we can nullify both PAD and Injection Attack Detection and develop more robust and resilient verification processes. This requires rethinking conceptualization and implementation, embracing innovative approaches, and acting decisively to safeguard the integrity of digital Identities in an increasingly complex and interconnected world.



# The Emergence of Forensic Identity Management (FIM): Safeguarding Identity Integrity and Accountability<sup>17</sup>



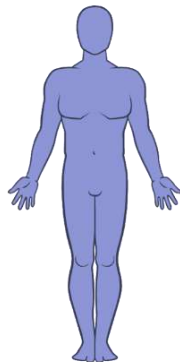
Forensic **Identity** Management

**DAL Identity International**, the first and foremost authority in **Forensic<sup>18</sup> Identity Management (FIM)**, is a pivotal domain in today's digital landscape. In an era where safeguarding identities is paramount, DAL Identity International embodies innovation and reliability. With an unwavering commitment to excellence and a relentless pursuit of cutting-edge technology, we lead a revolution in identity authentication, protection, and governance.

At the core of our ethos lies a dedication to precision and security. Through state-of-the-art forensic methodologies and advanced technological solutions, we ensure unmatched accuracy and trustworthiness in Identity Management. As pioneers in FIM, we set the standard for Identity verification solutions, pushing the boundaries of possibility in the digital Identity sphere.

Our forward-thinking approach reshapes the Identity verification landscape, empowering individuals and organizations against emerging threats in the digital era. In the realm of Identity Management of Single Existing Real-World Human Beings, FIM represents a pivotal shift toward comprehensive protection and accountability. By integrating rigorous forensic protocols, we uphold the reliability and accuracy of Identity data, ensuring integrity throughout its lifecycle.

**REAL-WORLD HUMAN BEING**



**Humans** are a living biological organism which can

- **breathe** and
- **consume** organic matter and has the ability to
- **think** and
- **act**

The term '**Identity**' refers to properties based on the

- **uniqueness** and
- **individuality** which makes a person
- **distinct** from others.

**Human beings cannot exist without an identity**

**No two humans**—not even Identical twins—are **genetically identical**

A **human being** is also born with **physical Identifiable markings**, which are only relevant to that one unique Human Body

These include:

- **Fingerprints** and
- **DNA**

*(Fingerprints and DNA is currently the only Human Attributes accepted as Forensic Evidence in a court of law)*



<sup>17</sup> [Forensic Identification | Jan Bikker - Academia.edu](#)

<sup>18</sup>- relating to, connected with, or used in courts of law, especially concerning the scientific analysis of evidence: The defense called a professional witness with credentials in forensic toxicology.

- relating, adapted, or suited to argumentation or to public discussion and debate; rhetorical:

*The Athenians were famous for their forensic eloquence in the public forum.* [FORENSIC Definition & Meaning | Dictionary.com](#)

## 1. Understanding FIM Protocol<sup>19</sup>

Forensic protocol within Identity Management involves the application of scientific methodologies to collect, analyze, and interpret Identity-related data. Rooted in principles such as the Locard Principle, FIM aims to Identify, document, and preserve digital and physical evidence associated with an individual's Identity. By leveraging forensic techniques, FIM ensures the accuracy and reliability of Identity verification processes.

## 2. The Locard Principle in FIM

Central to FIM is the Locard Principle, which asserts that every contact leaves a trace. Applied within the realm of Identity Management, this principle emphasizes the importance of capturing and preserving evidence associated with an individual's Identity. From digital footprints to physical artifacts, every interaction leaves a trace that can be analyzed forensically to establish and verify Identity with precision.



Figure 15: Locard's Exchange Principle: 'A Silent Witness'<sup>20</sup>

## 3. Maintaining Chain of Custody<sup>21</sup>

In addition to the Locard Principle, FIM places a strong emphasis on maintaining the chain of custody of Identity-related evidence. This entails documenting and tracking evidence from its collection to its final disposition securely and transparently. By ensuring the integrity of the chain of custody, FIM enhances the admissibility of Identity-related evidence in legal proceedings and regulatory compliance.

<sup>19</sup> [Evidence Collection - StatPearls - NCBI Bookshelf \(nih.gov\)](#)

<sup>20</sup> [Locard's Exchange Principle: 'A Silent Witness' | Uncovered](#)

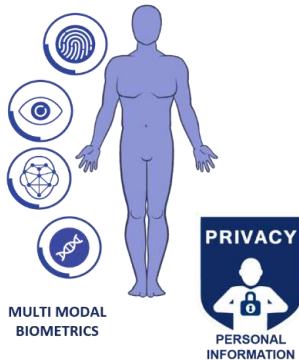
<sup>21</sup> [What Is Chain of Custody? \(thoughtco.com\)](#)





**REAL-WORLD HUMAN BEING**

CHAIN OF CUSTODY



Chain of custody (COC), in legal contexts, refers to the

- **chronological documentation** or
- **paper trail** that
- **records** the
- **sequence of custody,**
- **control,**
- **transfer,**
- **analysis,** and
- **disposition** of **physical** or **electronic evidence** which is a
- **vital factor** in determining **authenticity**

To **ensure 100%** Chain of Custody, we Register and further process the Individual into the DAL system with the following principals:

- The **Authorized DAL Operator** logs on before Registering an Individual and logs off on completion using a **Fingerprint**
- The Human Identity is linked to the Digital Identity, with all Metadata and Digital Evidence in Electronic Auditable sequence

#### 4. Protecting the Alive Human

FIM extends its protective measures to safeguard individuals while they are alive. By deploying advanced forensic techniques such as fingerprinting, DNA analysis, and biometric recognition technologies, FIM establishes and verifies Identity with unparalleled precision. This nullifies the global threat posed by Deepfake Synthetic Identities, ensuring that individuals' Identities are protected against manipulation or exploitation.

#### 5. Evolution Towards Holistic Identity Management

In the digital age, every individual possesses a Digital Twin—a digital counterpart representing their Identity in the digital realm. FIM recognizes the critical importance of safeguarding this Digital Twin and linking it with the Single Existing Real-World Human Being at forensic level accuracy. By adopting stringent forensic protocols and authentication measures, FIM ensures the integrity and security of the Digital Twin, mitigating the risks associated with Identity-related crimes.

#### 6. Honoring the Deceased Identity:

Even after an individual has passed away, their Identity remains significant and deserving of protection. FIM extends its protection to honor the Deceased Identity, preventing posthumous Identity theft and exploitation. Through meticulous forensic processes, FIM preserves the integrity of the Deceased Identity, addressing vulnerabilities that may be exploited for illicit activities such as voting fraud.

#### Conclusion:

The emergence of Forensic Identity Management (FIM) represents a critical advancement in Identity verification and management. By integrating forensic protocols and principles, FIM ensures the integrity, security, and dignity of every individual's Identity—both in life and beyond. As society navigates the complexities of the digital age, FIM serves as the cornerstone of effective Identity Management, nullifying threats posed by Deepfake Synthetic Identities and combating Identity-related crimes with unparalleled precision and accountability.



## The Stringency in Forensic Identity Verification

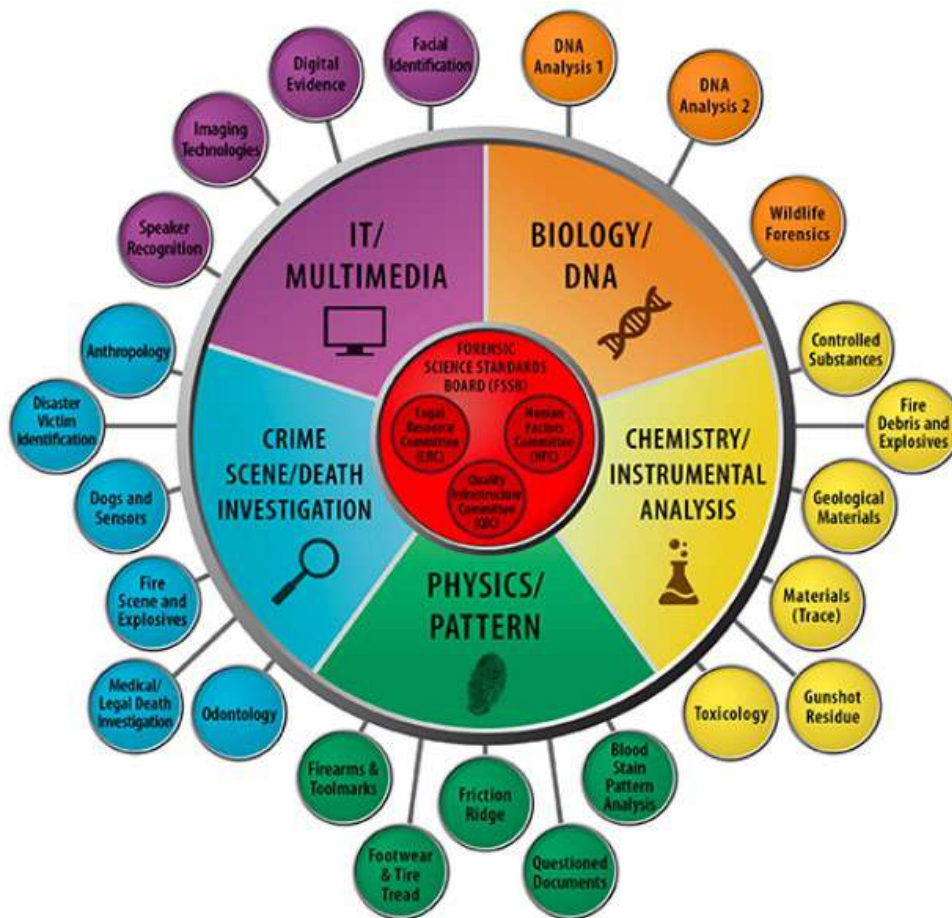


Figure 16: An Overview of Digital Forensics at NIST<sup>22</sup>

*“It is extremely important for all concerned to understand that there is unavoidable inherent error associated with forensic identification and that it is important to establish how much error can be tolerated to ensure that the correct identity has been attributed to the right individual (Lucy 2005, AFSP 2009, Aitken et al. 2010). For this reason, 2 confirmation of identity is rarely a rapid process as it requires that all avenues be explored to ensure that the degree of certainty in a match is maximised requiring that every inconsistency be scrutinised to determine whether the error associated with it, can be tolerated (Black et al. 2010). This can be extremely difficult for families and friends to understand when what they want more than anything is a swift answer and the remains of their loved ones returned to them expeditiously (Jensen 2000, PAHO 2006). But misidentification is to be avoided at all costs because it is not a single event, it exhibits multiplicity. If one person is assigned to the wrong identity then it has also been denied to the correct person who should own it and so in a misidentification there are at least two mistakes made (Mundorff et al. 2008). Therefore a forensic identification needs time to ensure that all necessary avenues are explored, that all inconsistencies can be explained and tolerated and that the inherent error is at an acceptable level for all concerned (Turney 2010).”<sup>23</sup>*

<sup>22</sup> [nist-icdf2c-sadfe-2014.pdf](#)

<sup>23</sup> [Forensic Identification | Jan Bikker - Academia.edu](#) pg. 1

Forensic Identity verification is an exacting process requiring an exceptional level of confidence in establishing one's Identity. This confidence is achieved through the meticulous deployment of various comprehensive methods. Here's a detailed exploration of the pivotal aspects involved:

### 1. Exhaustive Documentation

The process often commences with the thorough collection and scrutiny of extensive documentation about the individual under scrutiny. These documents encompass birth certificates, passports, driver's licenses, social security records, and other government-issued Identification materials. The objective is to establish a foundational understanding of the individual's purported Identity.

### 2. Utilization of Physical Evidence

In scenarios where documentation proves insufficient or contentious, forensic specialists resort to physical evidence examination. This encompasses an array of techniques such as fingerprint analysis, DNA testing, dental records, and physical measurements. Each method contributes distinctive characteristics facilitating the Identification process with a notable degree of certainty.

### 3. Expert Testimony

Forensic professionals, possessing extensive training and experience in their respective domains, often provide expert testimony during legal proceedings. They elucidate the methodologies employed in the Identity verification process, present their findings, and proffer their professional judgment regarding the likelihood of a correlation between the individual and the presented evidence.

### 4. Preservation of Chain of Custody

Ensuring the secure maintenance of the chain of custody for all evidence stands as a pivotal aspect of forensic Identity verification. This guarantees that evidence undergoes proper handling, documentation, and preservation throughout the entire process, thereby averting contamination or tampering.

### 5. Comparative Analysis

Forensic experts conduct meticulous comparative analyses to evaluate the resemblance between the evidence and reference samples (e.g., latent fingerprints vis-à-vis known fingerprints). This entails scrupulous scrutiny and comparison of patterns, characteristics, and unique features, adhering to the principles of Dactyloscopy<sup>24</sup>.

### 6. Comprehensive Documentation and Records Review

In addition to official Identification documents, forensic experts may scrutinize other records such as medical and dental records, academic transcripts, employment history, and financial documents. This aids in establishing a comprehensive profile of the individual under investigation.

---

<sup>24</sup> Forensic dactyloscopy, also known as fingerprinting, is **the use of a person's unique finger or palm prints to identify them**. It is a highly reliable form of identification, as every person's prints are unique and do not change throughout their life.



## 7. Adherence to Quality Assurance Practices

Integral to forensic Identity verification is quality assurance practices aimed at ensuring the accuracy and reliability of results. Quality controls, validation studies, and peer review constitute commonplace practices within forensic science.

## 8. Integration of Probability and Statistics

Forensic experts frequently employ statistical methodologies to quantify the likelihood of a match or ascertain the degree of certainty associated with a particular Identification. This facilitates conveying the level of confidence to pertinent authorities or courts.

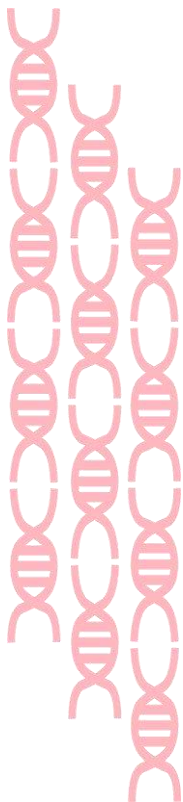
## 9. Upholding Independence and Impartiality

Forensic experts are mandated to operate with unwavering independence and impartiality, focusing solely on the objective analysis of evidence devoid of any bias.

## 10. Compliance with Legal Standards

Forensic Identity verification must adhere rigorously to stringent legal standards to ensure the admissibility of evidence in court. This encompasses compliance with rules of evidence, authentication prerequisites, and expert witness standards.

In essence, forensic Identity verification entails a highly methodical and exhaustive process encompassing a spectrum of methodologies ranging from document analysis to physical evidence examination, expert testimony, and statistical analysis. These methodologies collectively aim to establish an individual's Identity with an exceptionally high level of confidence, crucial in legal proceedings where outcomes carry significant societal implications.





## Certainty in Forensic Identity Verification (FIM)

### Levels of Certainty

**Three levels of certainty towards identification are:**

- **Consistency – profile is consistent with characteristics of a certain individual**
- **Probability- often includes circumstantial evidence, medical condition, ID card**
- **Certainty- beyond a shadow of a doubt – fingerprint match, x- ray match, dental match or DNA match**

Chapter 7 CRC Press: Forensic Science, James and Nordby, 3rd Edition 67

Figure 17:7 Forensic Science PowerPoint Chapter 07 Forensic Anthropology<sup>25</sup>

In the intricate domain of forensic Identity verification, the notion of certainty emerges as a cornerstone, wielding immense power to validate or contest an individual's proclaimed Identity. Far from a theoretical concept, certainty in Identity Management is an indispensable and irreplaceable component within the legal framework. In the subsequent discourse, we shall delve into the compelling rationale behind the pivotal role that certainty plays in the realm of Identity verification.

### Significance

Certainty in Forensic Identity Management (FIM) encompasses several critical facets:

#### 1. High Standard of Confidence:

Forensic Identity verification endeavors to establish an individual's Identity with an exceptionally high degree of confidence. This rigorous standard is imperative as legal decisions, both criminal and civil, hinge on the precision and reliability of evidence. The credibility and assurance of evidence are pivotal in determining guilt or innocence and safeguarding individual rights and freedoms.

#### 2. Upholding Justice:

At its essence, the legal system is rooted in the pursuit of justice. Certainty in Identity verification ensures accountability while protecting the innocent from unwarranted consequences. It upholds the integrity of legal proceedings by ensuring that legal rights and protections are extended to the right individuals.

<sup>25</sup> [7 Forensic Science Powerpoint Chapter 07 Forensic Anthropology | PPT \(slideshare.net\)](#)

### **3. Presumption of Innocence:**

The principle of "innocent until proven guilty" underscores the paramount importance of certainty in forensic Identity verification. A near-certain Identification forms a robust foundation for establishing guilt, while any uncertainty can cast doubt on the entire case.

### **4. Minimizing Wrongful Convictions:**

A high degree of certainty in forensic Identity verification is crucial in averting wrongful convictions, which can have irreversible consequences and undermine public confidence in the legal system.

### **5. Expert Testimony and Legal Proceedings:**

Forensic experts provide expert testimony, elucidating methodologies, presenting findings, and offering professional evaluations. Certainty in their testimony enables informed decisions by judges and juries, grounded in credible evidence.

### **6. Protecting Against Fraud:**

Certainty serves as a defense against Identity fraud, encompassing theft, financial fraud, and document forgery.

### **7. Validation and Quality Assurance:**

Forensic laboratories adhere to rigorous validation and quality assurance procedures to affirm the certainty of results, including quality controls, proficiency testing, and peer review.

### **8. Verifying Claims:**

Certainty facilitates the validation of claims, ensuring access to entitlements, benefits, and privileges only by legitimate individuals.

### **9. Avoiding Mistaken Identities:**

Certainty is indispensable in preventing errors that can lead to severe injustices, including wrongful convictions.

### **10. Public Trust and Confidence:**

Certainty influences public trust in the legal system and enhances public safety by accurately Identifying individuals with criminal histories or security risks.

### **11. Trust in the System:**

Certainty fosters trust in the robustness and precision of Identity verification processes, essential for social order.

### **12. Ethical Considerations:**

Upholding certainty in Identity verification reflects a commitment to fairness, precision, and accountability in the administration of justice.

The significance of certainty in forensic Identity verification cannot be overstated. It assures justice, preserves trust, protects against fraud, verifies claims, avoids errors, upholds legal protections, enhances public safety, and adheres to ethical principles.



## Certainty Against Deep Fakes and Synthetic Identities

In an era of technological advancement, the emergence of Deep Fakes and Synthetic Identities poses challenges to authenticity, trust, and security. Forensic Identity Management (FIM) serves as a pivotal defense against these threats:

### 1. Authentication with Unwavering Certainty:

Forensic Identity Management (FIM) specializes in authenticating individuals with a level of certainty that is difficult to replicate.

### 2. Precision in Verification:

Forensic experts ensure precision in verification, leaving no room for ambiguity in differentiating between genuine and fraudulent personas.

### 3. Counteracting Deep Fakes:

Specialized techniques analyze the authenticity of manipulated media content, such as voice and facial recognition.

### 4. Thwarting Synthetic Identities:

Forensic Identity Management (FIM) ensures the accuracy and legitimacy of Identity documents and data, preventing the establishment or exploitation of Synthetic Identities.

### 5. Strengthening Cybersecurity:

Certainty in Identity verification aids in reducing the risk of unauthorized access and cyber threats.

### 6. Legal and Ethical Implications:

Forensic Identity Management (FIM) plays a crucial role in legal proceedings and upholds ethical standards related to privacy and data protection.

### 7. Public Trust and Media Integrity:

Forensic experts restore trust in journalism and public figures by Identifying manipulated content.

### 8. Mitigating Fraud and Misinformation:

Certainty thwarts fraudulent activities and counters the spread of misinformation.

### 9. Preserving Privacy:

Forensic Identity Management (FIM) protects privacy rights and seeks legal remedies against non-consensual content.

### 10. Advancing Technological Solutions:

Forensic experts contribute to the development of technology solutions for detecting and mitigating Deepfakes and Synthetic Identities.

Forensic Identity Management (FIM) is crucial for authenticating individuals and countering digital threats. It ensures precision, upholds legal and ethical standards, restores trust, mitigates fraud, preserves privacy, and advances technology solutions. In a landscape fraught with challenges, Forensic Identity Management (FIM) stands as a guardian of security, authenticity, and trust.



## The Legal Standing in Forensic Evidence

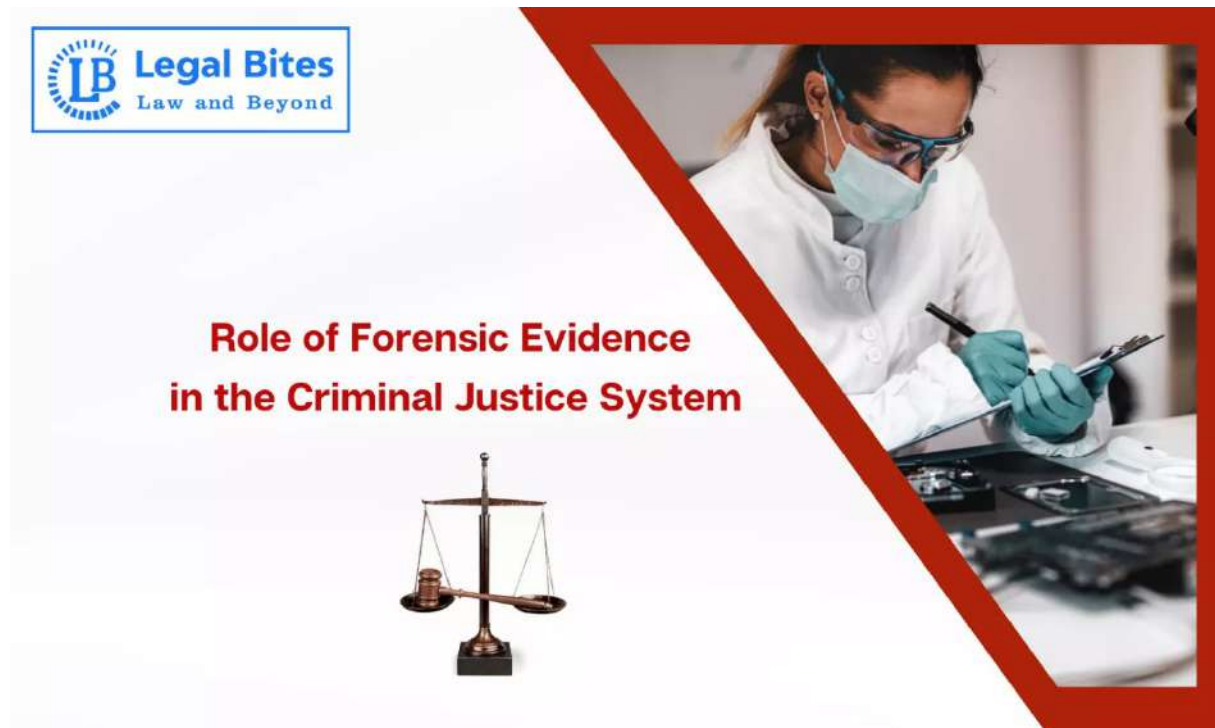


Figure 18: FORENSIC LAW Role of Forensic Evidence in the Criminal Justice System<sup>26</sup>

In the realm of forensic evidence and its admissibility in court, the concept of legal standing holds paramount importance. Forensic evidence must adhere to stringent legal standards and undergo rigorous scrutiny, including cross-examination, to ensure its reliability and credibility in legal proceedings. Here, we explore key considerations regarding the legal standing of forensic evidence:

### 1. Admissibility Criteria

Forensic evidence, like all evidence presented in court, must meet specific admissibility criteria established by legal rules and procedures. These criteria, varying by jurisdiction, generally demand that evidence be relevant, material, and obtained legally.

### 2. Chain of Custody

A crucial aspect of forensic evidence is the chain of custody, documenting the handling, storage, and transfer of evidence from collection to court presentation. A properly maintained chain of custody is vital to establish evidence authenticity and integrity.

### 3. Proper Collection and Handling

Forensic evidence must be collected, preserved, and handled following established protocols and standards to prevent contamination, alteration, or tampering, thereby ensuring reliability.

<sup>26</sup> [Role of Forensic Evidence in the Criminal Justice System \(legalbites.in\)](https://www.legalbites.in/role-of-forensic-evidence-in-the-criminal-justice-system)



#### 4. Expert Testimony

Forensic experts, such as scientists and analysts, often testify as expert witnesses, explaining methods, findings, and scientific basis. Expert testimony must meet legal standards of reliability and relevance, subject to scrutiny through "Daubert" or "Frye" hearings.

#### 5. Cross-Examination

Forensic evidence and presenting experts are subject to cross-examination by opposing counsel. This critical process allows challenges to credibility, methodology, and conclusions, ensuring evidence is rigorously tested and weaknesses exposed.

#### 6. Relevance and Materiality

Forensic evidence must be both relevant and material to the case, having a direct bearing on issues in dispute and the potential to impact the outcome. Irrelevant or immaterial evidence may be excluded from trial.

#### 7. Constitutional Considerations

Forensic evidence may raise constitutional issues, such as Fourth Amendment violations. Courts may suppress evidence obtained unlawfully, ensuring adherence to constitutional rights.

#### 8. Burden of Proof

In legal proceedings, the burden of proof rests with the party making the claim. It's their responsibility to present evidence, including forensic evidence, to support their case.

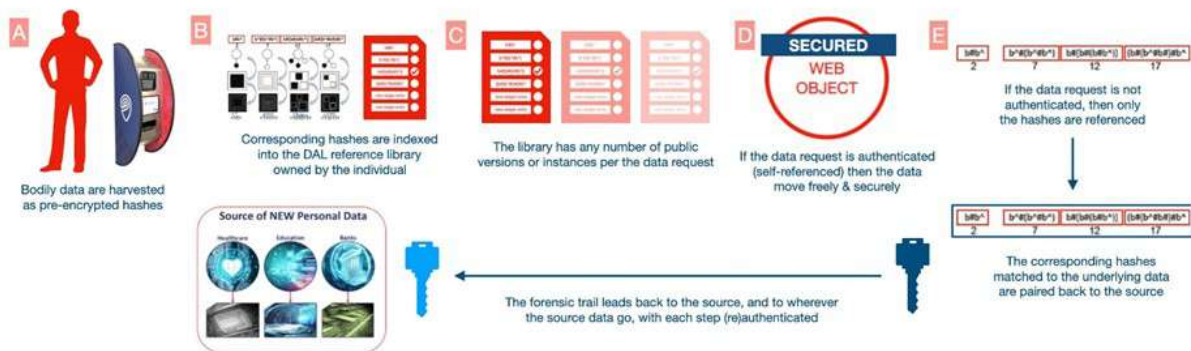
Legal standing ensures forensic evidence meets strict criteria, withstands scrutiny, and contributes to fair and just legal outcomes. Upholding legal standards safeguards the integrity of the judicial process and ensures the reliability of forensic evidence in establishing truth and delivering justice.



## Role of Forensic Cryptographic Provenance (FCP) in FIM:

Forensic Cryptographic Provenance (FCP) represents a groundbreaking approach to data security that integrates forensic techniques into cryptographic processes. Unlike conventional methods, which often focus solely on encryption and decryption, FCP redefines data security by incorporating rigorous scrutiny of data transfer, tracking its origin, transmission, and reception with precision at the object-level. This discussion explores the role of Forensic Cryptographic Provenance (FCP) in enhancing data integrity and securing Identity transactions, ultimately empowering users to navigate the digital landscape with trust and confidence.

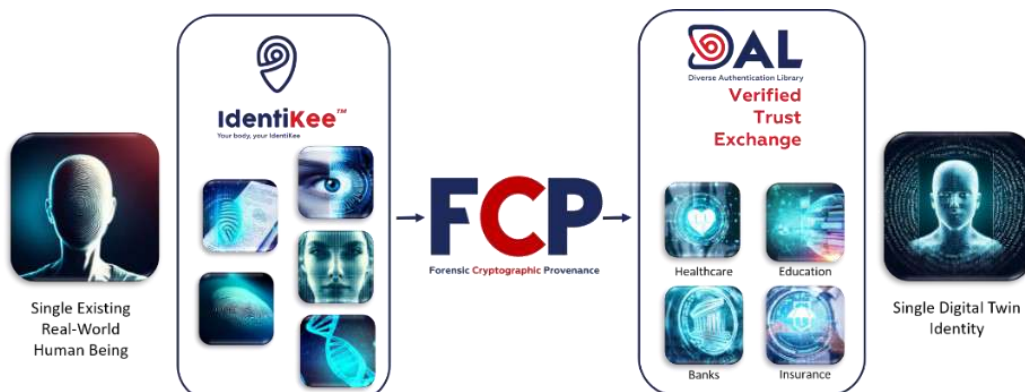
### THE FUNDAMENTALS OF DAL'S FORENSIC CRYPTOGRAPHY



**A complete, ongoing forensic audit, preserving all data integrity & the individual's identity**

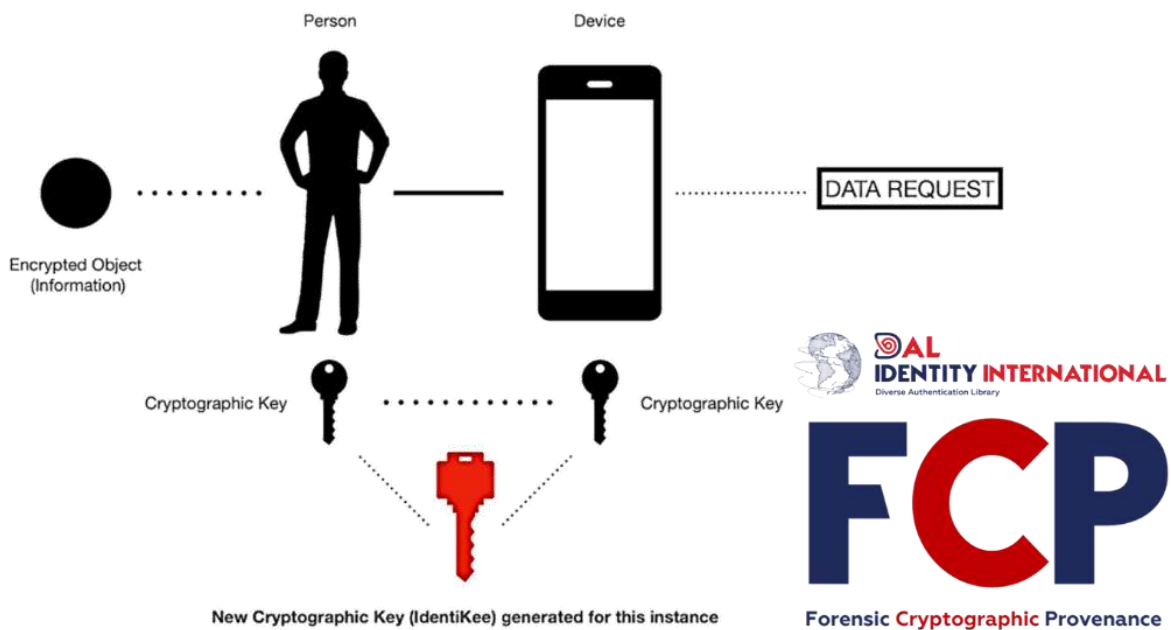
#### 1. Ensuring Data Integrity:

- a. FCP revolutionizes data integrity by providing constant forensic cryptographic provenance throughout the Identity Management process. This means that every step of data transfer is meticulously monitored and recorded, allowing for the traceability of data back to its origin.
- b. By integrating forensic principles into cryptographic processes, FCP ensures that data remains untampered and unaltered during transit, mitigating the risks associated with unauthorized modifications or data corruption.
- c. This level of scrutiny not only enhances the reliability of data but also instills confidence in the integrity of digital interactions.



## 2. Securing Identity Transactions:

- a. Identity transactions are vulnerable to tampering and unauthorized access, jeopardizing individuals and institutions. FCP employs advanced cryptographic methods to encrypt Identity data, shielding it from unauthorized access and tampering. With confidentiality ensured, FCP fortifies sensitive information against threats, instilling confidence in both individuals and organizations.
- b. Additionally, FCP tracks the provenance of Identity transactions, providing a verifiable trail of data transfer and reception. This not only enhances the security of Identity transactions but also establishes a level of trust and reliability in the Identity Management process.

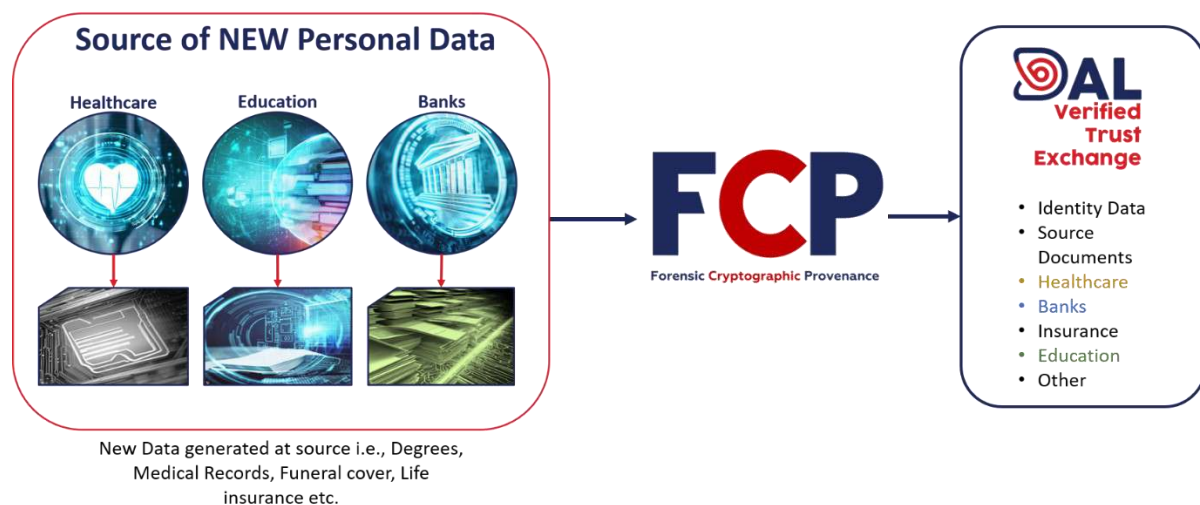


Forensic Cryptographic Provenance (FCP) is paramount in redefining data security and Identity Management. By integrating forensic techniques into cryptographic processes, FCP ensures the traceability and integrity of data transfer, while also securing Identity transactions against tampering or unauthorized access. Ultimately, FCP empowers users to navigate the digital landscape with confidence, knowing that their data and Identities are protected with unparalleled accuracy and reliability.



## The Role of Forensic Cryptographic Provenance (FCP) in Verifiable Credentials:

Forensic Cryptographic Provenance (FCP) plays a crucial role in ensuring the integrity, authenticity, and traceability of verifiable credentials within the context of DAL Identity International Forensic Identity Management (FIM). Verifiable credentials are digital representations of attested information that enable entities to prove claims about themselves or others in a secure and privacy-preserving manner. These credentials are essential for Identity Management systems like FIM, which deal with sensitive personal information and require a high level of trust and assurance.



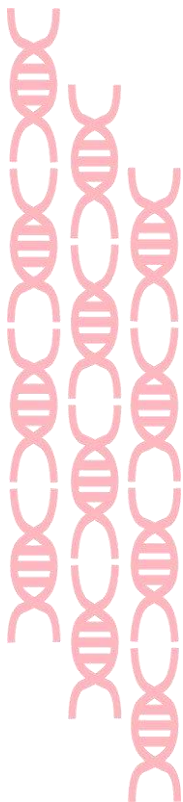
Here's how FCP contributes to the import aspect of verifiable credentials within the DAL Identity International FIM:

- 1. Ensuring Integrity:** FCP employs cryptographic techniques to ensure the integrity of verifiable credentials during import processes. By using cryptographic hash functions and digital signatures, FCP can verify that the credentials have not been tampered with or altered in any way. This ensures that the information contained within the credentials remains accurate and trustworthy.
- 2. Establishing Authenticity:** FCP helps establish the authenticity of verifiable credentials by verifying their origin and issuer. Through the use of digital signatures and public key infrastructure (PKI), FCP can verify that the credentials have been issued by a trusted authority and have not been forged or falsified. This adds a layer of trust to the import process, as entities can be confident that the credentials, they are importing are genuine and reliable.
- 3. Enabling Traceability:** FCP enables traceability by providing a detailed record of the provenance of verifiable credentials. This includes information such as the issuer, timestamp, and any subsequent modifications or transfers of the credentials. By maintaining a comprehensive audit trail, FCP enables forensic investigators to trace the history of credentials and Identify any potential discrepancies or anomalies.



- 4. Supporting Compliance:** FCP helps ensure compliance with regulatory requirements and industry standards governing the import and use of verifiable credentials. By providing robust cryptographic mechanisms for ensuring integrity and authenticity, FCP helps organizations meet stringent security and privacy requirements, such as those outlined in regulations like GDPR (General Data Protection Regulation) and/or standards like ISO 27001.
- 5. Enhancing Trust and Confidence:** Overall, FCP enhances trust and confidence in the import aspect of verifiable credentials within the DAL Identity International FIM. By providing assurances regarding the integrity, authenticity, and traceability of credentials, FCP enables entities to rely on these credentials for critical Identity Management tasks with confidence.

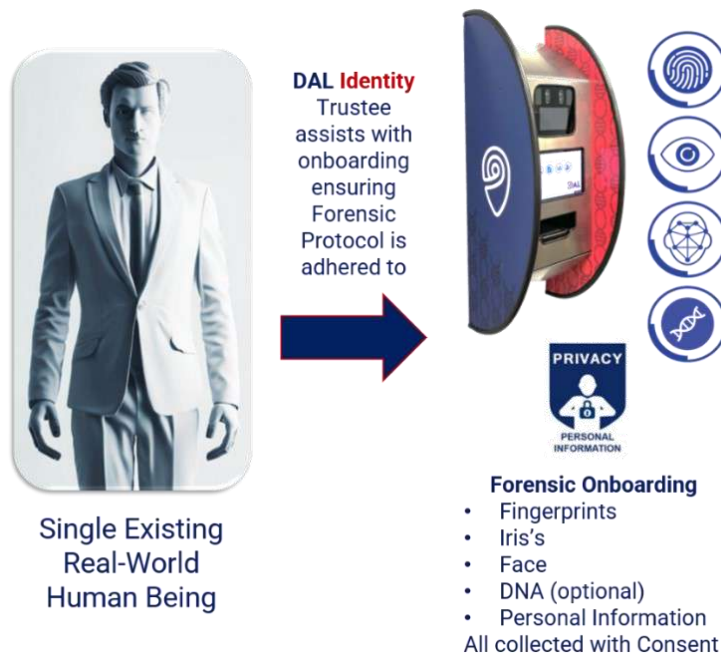
Forensic Cryptographic Provenance (FCP) plays a vital role in ensuring the integrity, authenticity, and traceability of verifiable credentials within the context of DAL Identity International Forensic Identity Management (FIM). By employing cryptographic techniques, FCP enhances trust and confidence in the import process, enabling organizations to rely on these credentials for secure and privacy-preserving Identity Management.



## DAL Identity International's Unique Forensic Approach:

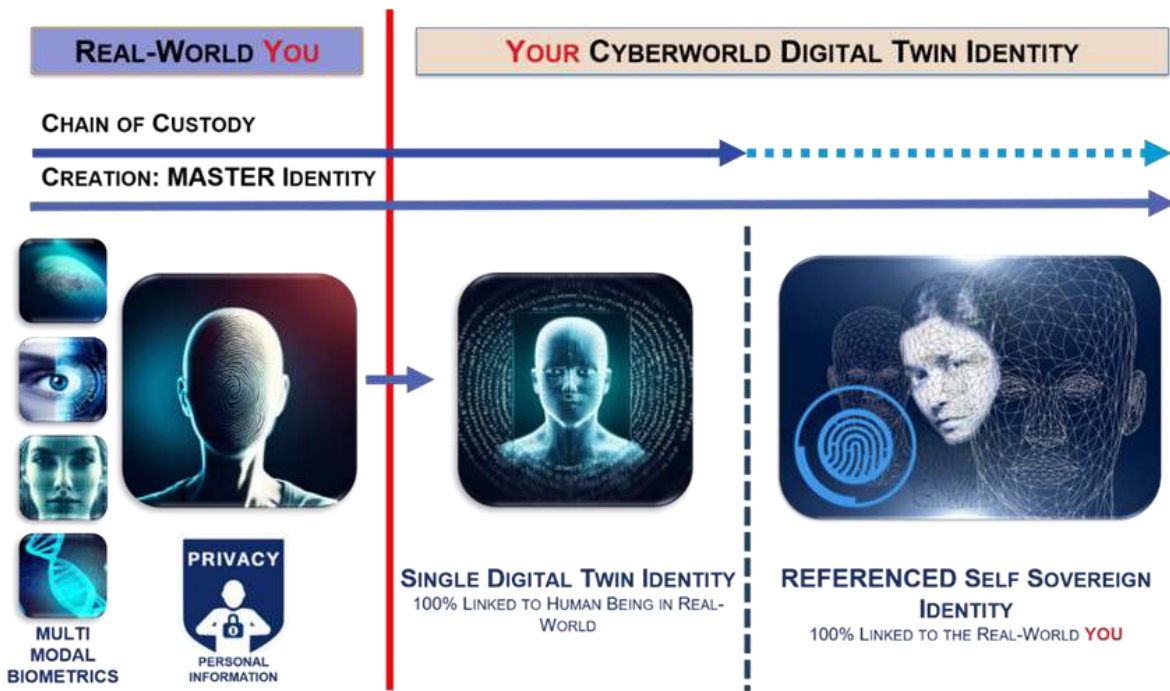
### 1. Comprehensive Forensic Identity Management (FIM) Solution:

- a. DAL Identity International distinguishes itself by offering a comprehensive Forensic Identity Management (FIM) solution that surpasses traditional Identity verification methods. Unlike conventional Identity verification (IDV) approaches that often rely on single-factor authentication or basic biometric data, DAL Identity International's FIM integrates advanced forensic techniques with state-of-the-art technology and multi-modal biometrics. This holistic approach covers all aspects of Identity Management, including the Alive Human, their Single Digital Twin, and even their Deceased Identity when they have passed, ensuring complete protection and security.



### 2. Integration of Advanced Forensic Techniques and Methodology:

- a. DAL Identity International's approach centers on the integration of cutting-edge forensic methodologies into Identity Management. Central to this strategy is the utilization of forensic protocols, with fingerprinting serving as the cornerstone biometric. Additionally, DAL incorporates DNA sequencing, iris recognition, and facial recognition technologies into its Identity Management processes.
- b. Through the utilization of advanced forensic methodologies, DAL Identity International attains unmatched levels of accuracy and reliability in Identity onboarding and verification processes. This proactive approach serves as a formidable defense against the myriad risks presented by Deepfake Synthetic Identities, ghost workers, Identity fraud, forgery, and manipulation. As a result, individuals and institutions across various sectors, including banking, financial services and insurance (BFSI), healthcare, government, and beyond, benefit from robust protection against the escalating threats posed by Deepfake Synthetic Identities on a global scale.



### 3. Cutting-Edge Technology:

- a. DAL Identity International harnesses cutting-edge technology to enhance the efficiency and effectiveness of its FIM solution. Through the use of advanced encryption algorithms, secure data transmission protocols, and real-time monitoring systems, DAL Identity International ensures the integrity and security of Identity data throughout its lifecycle. The integration of Forensic Cryptographic Provenance (FCP) enables traceability and verifiability of data transfer, providing individuals and organizations with confidence in the authenticity of their digital interactions.

### 4. Emphasis on Accuracy and Integrity:

- a. DAL Identity International prioritizes the accuracy and integrity of Identity onboarding and verification processes, emphasizing the importance of authenticating Real-World Identities. Through the implementation of stringent authentication protocols and validation mechanisms, DAL Identity International guarantees that only genuine Identities are onboarded, verified, and authenticated within its system. This proactive approach not only eliminates the threat of Deepfake Synthetic Identities but also acts as a deterrent against Identity theft and fraud. Furthermore, it fosters trust and confidence in digital interactions across diverse sectors and industries.

### 5. Commitment to Security and Privacy:

- a. Above all, DAL Identity International is committed to upholding the highest standards of security and privacy in its FIM solution. By implementing stringent security measures, data encryption protocols, and compliance frameworks such as GDPR, and ISO standards DAL Identity International prioritizes protecting individuals' sensitive information. This commitment to security and privacy instills trust and confidence in DAL Identity International's FIM solution, making it the preferred choice for individuals and organizations seeking robust Identity Management solutions.



## Conclusion:

DAL Identity International revolutionizes Forensic Identity Management (FIM) by blending advanced forensic techniques and cutting-edge technology. With a focus on accuracy and reliability, DAL employs fingerprinting, DNA sequencing, iris, and facial recognition to nullify Deepfake Synthetic Identities and Identity fraud worldwide.

DAL ensures data integrity and security through encryption, secure transmission, and real-time monitoring. Their Forensic Cryptographic Provenance (FCP) bolsters traceability and trust in digital interactions.

Authenticating Real-World Human Being Identities is paramount for DAL, achieved through stringent protocols and validation mechanisms to counter Identity theft and fraud.

Committed to security and privacy, DAL adheres to GDPR, ISO standards, and rigorous security measures, making it the premier choice for robust Identity Management solutions.

*"Identity theft, criminal investigations of the dead or missing, mass disasters both by natural causes and by criminal intent – with this as our day-to-day reality, the establishment, and verification of human Identity has never been more important or more prominent in our society. Maintaining and protecting the integrity of our Identity has reached levels of unprecedented importance and has led to international legislation to protect our human rights."*

**(Forensic Human Identification: An Introduction, 1st Edition - Tim Thompson, Sue Black)**





## Onboarding Protocol via DAL Identity International Forensic Identity Management (FIM) System

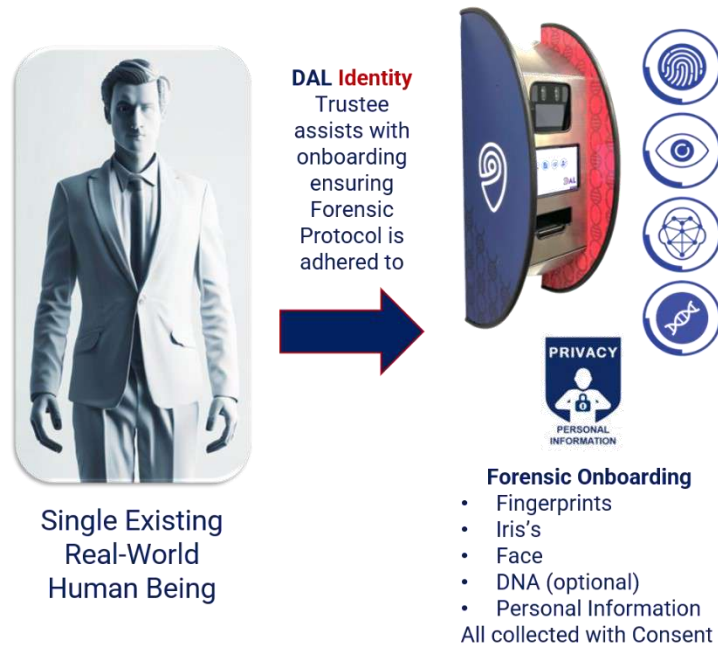


Figure 19: Forensic Human onboarding

In the realm of Forensic Identity Management (FIM), the onboarding phase stands out as the most critical aspect of Identity Management. Within the framework of the DAL Identity International Forensic Identity Management (FIM) System, this phase is meticulously executed, setting a gold standard for individual Identity acquisition protocols. Recognizing its paramount importance, the onboarding process not only establishes the cornerstone for accurate Identification but also safeguards the integrity and reliability of forensic data throughout its lifecycle. Emphasizing the significance of this phase, the following section delineates the critical aspects of the FIM protocol within the DAL Identity International framework, highlighting the integration of the Locard Principle and Chain of Custody, alongside the incorporation of biometric authentication and Forensic Cryptography Provenance.

### 1. Adherence to the Locard Principle:

The DAL Identity International system, rooted in the principles laid down by Dr. Edmond Locard, operates under the premise that "every contact leaves a trace." In the context of FIM, this principle underscores the importance of meticulous documentation and preservation of evidence of the Single Existing Real-World Human Being during the onboarding process. Each interaction, from the initial capture of biometric data to its integration into the forensic database, is conducted with utmost care to prevent contamination or alteration of evidence. Fingerprints as core to the DAL Identity International FIM ensure that evidence of the Single Existing Real-World Human Being is collected at a specific time and space by a specific person on a specific fingerprint scanner capable of maintaining the Locard Principle. This process Nullifies the threat of Deepfake Synthetic Identities at the starting point of the Identity Management solution, unlike any other IDV system.

## 2. Chain of Custody:

Maintaining a stringent Chain of Custody within the DAL Identity International system is imperative for preserving the evidentiary value of forensic data. At every stage of the onboarding process, from collection to analysis, the custody of data is documented and traceable. This ensures accountability and transparency, mitigating the risk of tampering or unauthorized access and any attack on the system.

## 3. Onboarding Procedure:

### a. Accredited Onboarding Representatives:

Onboarding onto the DAL Identity International FIM system is exclusively conducted by individuals who have undergone rigorous training and accreditation. These representatives serve as guardians of the system's integrity, possessing the knowledge and skills necessary to execute the onboarding process accurately.

### b. Informed Consent:

Before onboarding, explicit consent must be obtained from the individual undergoing the process. Consent forms are signed, with the individual's fingerprint serving as irrefutable proof of their acknowledgment and authorization.

### c. Multi-Biometric Capture:

Forensic biometric data, including forensic valued fingerprints and other secondary biometrics including iris scans, and facial images, is captured simultaneously during the onboarding session within the DAL Identity International system. This comprehensive approach enhances the accuracy and reliability of Identity verification on all the biometrics onboarded.

### d. DNA Collection Protocol:

In cases where DNA is collected, adherence to strict Chain of Custody protocols is paramount within the DAL Identity International system. The link between the individual's Identity and the genetic sample is meticulously documented and maintained throughout the entire process.

## 4. Forensic Cryptography Provenance:

To uphold the integrity of forensic data during transmission, Forensic Cryptography Provenance is a cornerstone within the DAL Identity International framework. This cryptographic technique ensures that data sent from the capturing unit to the forensic database is securely encrypted and accompanied by verifiable metadata, assuring that all forensic protocols have been meticulously followed.

Within the DAL Identity International Forensic Identity Management (FIM) System, the accurate protocol for individual Identity acquisition necessitates strict adherence to the Locard Principle, Chain of Custody, informed consent, multi-biometric capture, utilization of state-of-the-art capturing and scanning devices, and implementation of rigorous cryptographic measures. Integration of these pivotal components into the onboarding process reinforces the integrity and dependability of forensic data within the DAL Identity International system. Consequently, this approach enhances the effectiveness of proving an Identity, verification on various platforms of an Identity – either present or not present and forensic investigations, ultimately ensuring the delivery of justice.



## Compliance and Ethical Standards in Identity Management

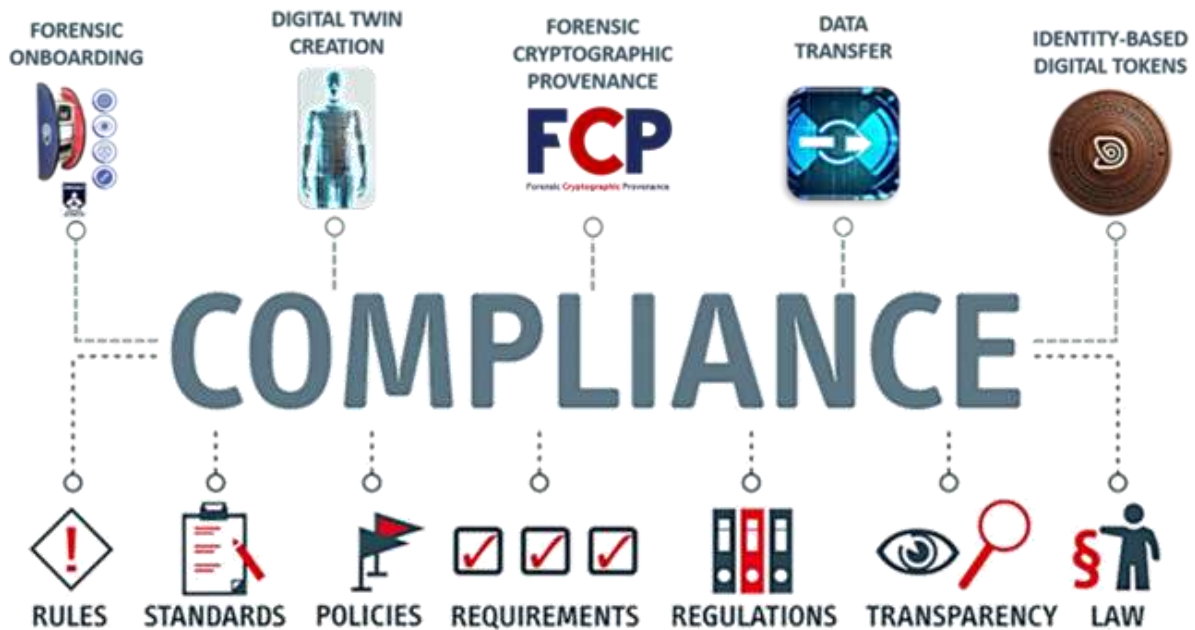


Figure 20: DAL Identity International complies to all legal and other relevant compliance

DAL Identity International recognizes that every single existing real-world Human being's Identity is a fundamental record of their existence. This acknowledgment serves as the cornerstone of our approach to Identity Management, underpinned by a commitment to ethical principles and compliance with global standards. In this section, we delve into the comprehensive compliance framework adopted by DAL Identity International, ensuring alignment with ISO 15489 and adherence to privacy standards such as GDPR and POPIA, as well as exceeding NIST compliance requirements.

### 1. Acknowledgment of Human Identity as a Fundamental Record

At DAL Identity International, we understand that each person's Identity is more than just data—it's a profound reflection of their existence. This belief drives our commitment to ethical Identity Management practices, prioritizing the integrity and dignity of every individual.

We don't see Identity as mere information; it's a vital record shaping a person's essence, be it a fingerprint, DNA sequence, or iris pattern. Our focus isn't just on authentication but on recognizing the inherent value of each Identity aspect.

Our dedication transcends technology—we align our practices with fairness, respect, and ethical conduct. By safeguarding personal identities, we uphold everyone's rights and dignity.

In today's digitally dominant world, preserving Identity sanctity is crucial. By adhering to ethics and promoting responsible practices, we enhance security and foster a more equitable society. At DAL Identity International, we're not just managing identities; we're safeguarding people's essence.

## 2. Alignment with ISO 15489

ISO 15489 outlines principles and guidelines for records management, emphasizing the importance of authenticity, reliability, integrity, and usability of records. DAL Identity International is 100% aligned with ISO 15489, incorporating its principles into our Identity Management processes to ensure the effective management and preservation of Identity records.

## 3. Compliance with Privacy Standards

### a. GDPR (General Data Protection Regulation)

DAL Identity International operates in compliance with GDPR, which sets stringent standards for the protection of personal data and the rights of individuals. Our Identity Management practices prioritize data privacy and security, ensuring transparent data processing and providing individuals with control over their personal information.

### b. POPIA (Protection of Personal Information Act)

In regions governed by POPIA, such as South Africa, DAL Identity International complies with the provisions outlined in this legislation. We uphold the rights of individuals regarding the collection, processing, and storage of their personal information, implementing measures to safeguard data integrity and confidentiality.

## 4. Comprehensive Compliance Framework

DAL Identity International's compliance framework extends beyond regulatory requirements to encompass ethical standards and best practices in Identity Management. Our commitment to compliance is demonstrated through:

### a. Transparency and Accountability

We maintain transparency in our Identity Management processes, providing clear information about data collection, usage, and storage practices. Additionally, we uphold accountability by implementing mechanisms for oversight and review of our compliance efforts.

### b. Data Security Measures

DAL Identity International employs robust data security measures to protect Identity records from unauthorized access, alteration, or misuse. Our infrastructure undergoes regular security audits and assessments to identify and address potential vulnerabilities proactively.

### c. Continuous Improvement

We continuously evaluate and enhance our Identity Management practices to adapt to evolving regulatory requirements and emerging privacy concerns. This proactive approach ensures that our systems remain resilient and responsive to the dynamic nature of the Identity Management landscape.

## 5. Exceeding NIST Compliance

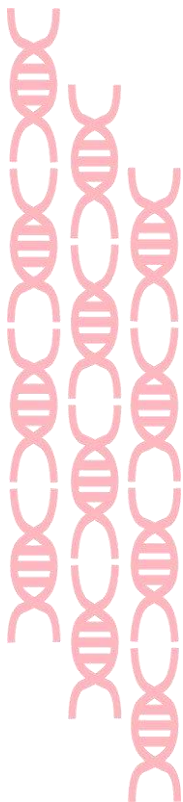
While compliance with NIST (National Institute of Standards and Technology) standards is essential, DAL Identity International goes beyond mere compliance to ensure the highest levels of security and reliability in Identity Management. By integrating industry-leading





practices and leveraging cutting-edge technologies, we exceed NIST and other compliance requirements, setting a new standard for secure and ethical Identity Management.

DAL Identity International is committed to upholding the integrity of every individual's Identity while adhering to global standards and regulations. Through alignment with ISO 15489, compliance with privacy standards such as GDPR and POPIA, and a comprehensive compliance framework that exceeds NIST requirements, we ensure the ethical and responsible management of Identity records, thereby fostering trust and confidence in our Identity Management solutions.



## Advancing Forensic Identity Management (FIM) with Web 4.0: A Comprehensive Solution

Web 4.0 represents a distinct shift from standalone web applications (Web 2.0 and Web 3.0) to interoperable microservices. Web 4.0 as an actual software was invented by DAL's CTO Marcel Donges, who saw very early in his career that web objects communicating directly with each other would be the real future of the Internet/Web. This has been corroborated by the father of the web himself, Tim Berners-Lee, who said as much to Marcel when they met this year (2024) in Davos, Switzerland. In Web 4.0, web objects as data interoperate seamlessly, without web protocols or 3rd party applications getting in the way, thereby providing total security, privacy and data accuracy.

Web 4.0 presents the most promising underlying support structure for Forensic Identity Management (FIM) by addressing critical concerns surrounding security, personal data protection, interoperability, and ethical considerations, simply because real personal data comprising a real person's identity can only be captured in its raw form, and protected as web objects which also exist in their original form.

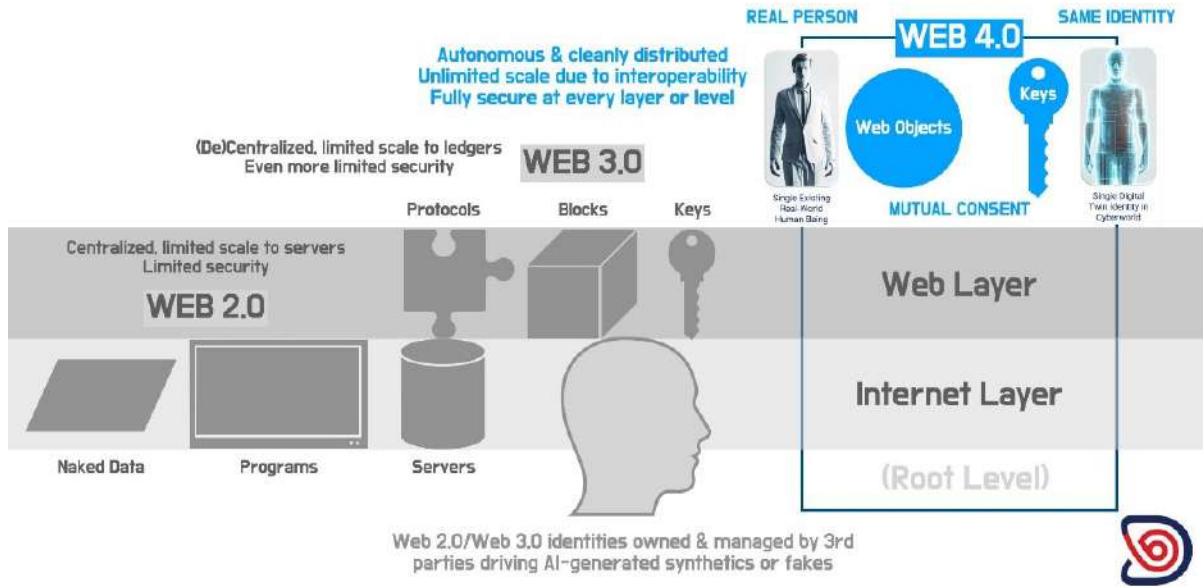


Here's more on why Web 4.0 is well-suited for this purpose:

### 1. Secure Identity Protection:

- a. Web 4.0 employs advanced encryption techniques and decentralized architectures that are kernel-structured, to ensure the secure storage and transmission of Identity-related information. By encrypting data at the object level, it greatly minimizes if not removes the risk of unauthorized access and Identity theft.

## THE BASICS OF WEB 4.0 INFRASTRUCTURE & IDENTITY



### 2. Interoperability and Consent-based Data Sharing:

- a. Web 4.0 facilitates seamless interoperability of Identity and personal data (Pii) across different platforms and microservices. Individuals retain full control over their data and can grant explicit consent for its sharing and monetization. Using the DAL Identity International Verified Trust Exchange (VTE)<sup>27</sup> super application and real Digital Locker (a wallet for storing documents and data) ensures transparency and accountability in data transactions.

**The web security solution, simplified.**

**Real Cyber twin of The Real Human Being with real, usable, Consensual Data**

**Data as Web Objects**

- Pii**
- Finger prints**
- Iris**
- Facial**
- DNA**

**INTEROPERABLE WEB OBJECTS**

**Web objects without protocols make the identity on the web totally secure!**

<sup>27</sup> The **DAL Identity International Verified Trust Exchange (VTE)** is a super App that acts as a secure Digital Wallet for all your personal data, including your Identity and proof documents. With biometric authentication, only you can access it, ensuring top-notch privacy and security. You have full control over your data, managing documents, activating new data, and controlling permissions, empowering you like never before. A groundbreaking feature is its ability to enable data monetization, letting you share your data for value. With versatile storage options for various data types, the VTE revolutionizes data ownership and control, ushering in a new era of trust and empowerment.



### 3. Enhanced Security:

- a. Web 4.0 incorporates robust security measures, including unifactored authentication (real authentication which happens in one step), biometric verification, and decentralized Identity Management protocols (not web protocols, but forensic protocols attached to web objects). These features safeguard against Identity fraud, unauthorized access, and data breaches, bolstering overall security in Forensic Identity Management (FIM).

### 4. Protection of Personal Data:

- a. With Web 4.0, personal data is encrypted at the object-level, thereby anonymized to protect individual privacy without sacrificing the integrity of an individual's real, authentic identity. In other words, a person can be fully transparent with peers through mutual consent while maintaining real privacy protection. Strict access controls and data ownership mechanisms empower users to manage their information securely while limiting exposure to potential risks associated with data misuse or exploitation. More proactively, this also opens them up to far greater data revenue-sharing possibilities with governments, institutions, corporations and independents alike.

### 5. Improved Efficiency:

- a. Leveraging Web 4.0 technologies to streamline Identity verification processes, reducing administrative overhead and enhancing operational efficiency in Forensic Identity Management (FIM) is critical to bypassing faulty digital methods, particularly automated processes tied to artificial intelligence. Automated workflows, smart contracts, and real-time data validation mechanisms expedite Identity-related transactions while ensuring accuracy and reliability.



**The functions that characterize Web 4.0**

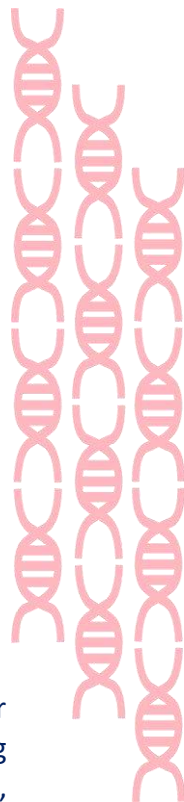
Like "Real World Things" you can grab, drag, drop, and use them in different contexts. You can grab them:

- with your hand
- your finger
- your mouse
- your VR-Controller

And move them in:

- between different Web Sites on different Web Domains.
- between different devices like Desktops, iPads, Phones, and VR/AR Glasses
- between different operating system technologies like Mac OS, android, iOS, Windows, Linux, Unix, ...
- between different vendors like Apple, Google, Samsung, Facebook/Meta, Amazon, Microsoft

Logos shown: AWS, Google, Apple, Samsung, and a stylized eye icon.



### 6. Ethical Considerations:

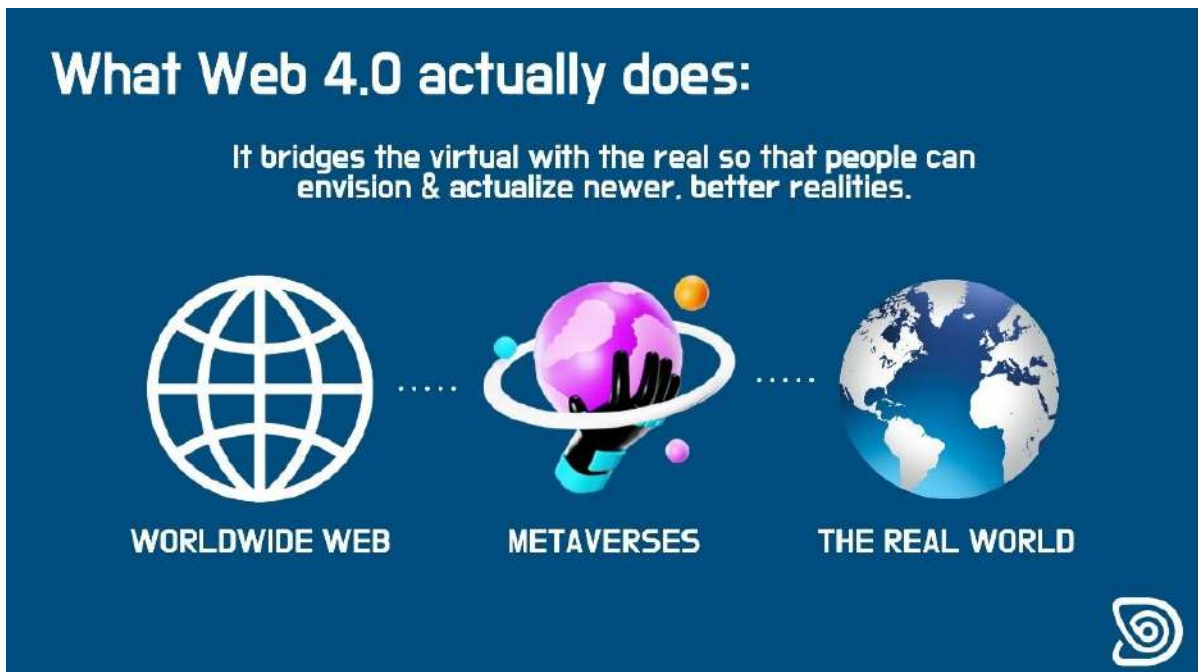
- a. The VTE on Web 4.0 promotes ethical data practices by prioritizing mutual user consent, data transparency, and full forensic accountability. By empowering individuals to make informed mutual decisions about their data-sharing preferences, it upholds principles of autonomy, fairness, and ultimate respect for privacy rights. To



be clear, mutual consent as a transaction practice or an ethical standard has not existed until now, simply because 3rd parties control the flow of commerce and social media interactions, with very few exceptions.

## 7. Global Compatibility and Compliance:

- a. The VTE on Web 4.0 adheres to international standards and regulatory frameworks, including ISO Records Management standards, GDPR, and other data protection regulations. Its inherent decentralized nature facilitates cross-border data transfers and remittances while ensuring compliance with regional privacy laws and regulatory requirements. This also opens up huge opportunities to write and execute public policies that are well-informed and which protect of all economic participants.



DAL Identity International on Web 4.0 offers a comprehensive solution for Forensic Identity Management (FIM) by addressing key challenges related to Identity security, data protection, interoperability, efficiency, ethics, and compliance. More specifically, as authentic identities proliferate a fractured digital landscape, FIM provides a unique way to safely merge web functions with virtual worlds through authenticated digital twins to produce positive real-world outcomes. Consider all the web and social media platforms (Amazon, X or Facebook) that desperately need this approach, not to mention every industry on the planet that needs to virtualize their operations in order to cut costs and generate new profit centers. DAL is already pioneering with this approach, starting with the mining, healthcare, insurance and finance industries. This harnesses the potential of emerging technologies within a decentralized and consent-driven framework, thus enabling individuals to maintain control over their Identities and personal data while fostering trust and transparency in digital interactions.

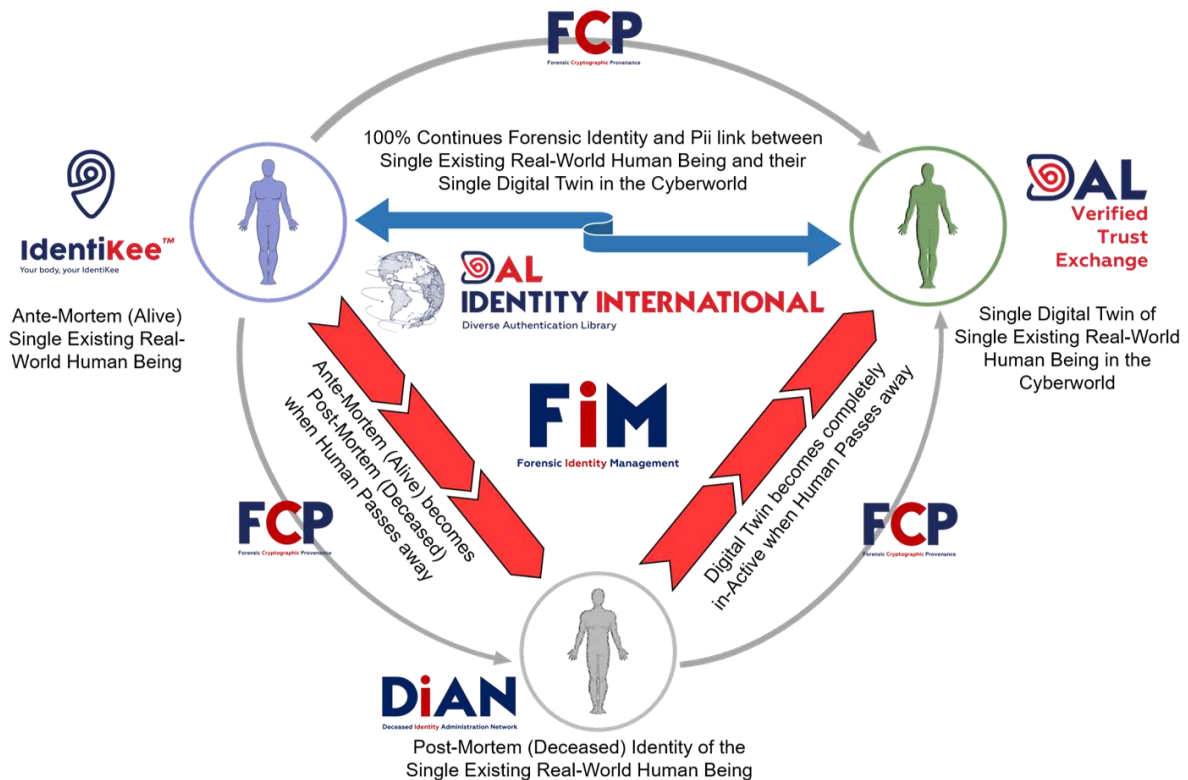
## DAL Identity International: Forensic Identity Management (FIM)

DAL Identity International is a trailblazer in the realm of Identity Management, where the Human Being takes center stage in every facet of Identity application. Our groundbreaking Forensic Identity Management (FIM) solution revolutionizes the landscape by acknowledging the Human Being as the focal point of all Identity dimensions. From the living to the deceased, DAL Identity International pioneers the deployment of full forensic protocols, methodologies, and processes, setting the standard for comprehensive Identity protection.

At the heart of our approach lies the acknowledgment of the Alive (Ante Mortem) Human Being, symbolized by the DAL IdentikEE, and the Single Digital Twin of the Single Existing Real-World Human Being on the DAL Verified Trust Exchange (VTE). Linked intricately through forensic protocols and Forensic Cryptographic Provenance (FCP), our solution ensures unparalleled accuracy, integrity, and security in Identity verification and authentication processes.

Furthermore, DAL Identity International extends its reach to the Deceased (Post-Mortem) Human Being through the DAL DiAN, providing dignified handling and meticulous record-keeping from discovery to final arrangements. This holistic approach not only safeguards against Identity fraud but also ensures compliance with regulatory standards, fostering trust and confidence in every digital interaction.













In a digital landscape fraught with threats, DAL Identity International stands as a beacon of reliability, championing the Human Being's Identity integrity at every turn.



**DAL Identity International - Forensic Identity Management (FIM)**

## Conclusion: Embracing Forensic Identity Management (FIM) in the Age of Deepfake Synthetic Identities

The surge in Deepfake Synthetic Identities presents an urgent challenge to conventional Identity verification methods. As traditional solutions struggle to keep pace with the sophistication of fraudulent activities, the imperative to fortify personal security becomes paramount. DAL Identity International's groundbreaking approach to Forensic Identity Management (FIM) emerges as the beacon of hope in this landscape of escalating threats.

Solution Comparison			Crucial Comparisons		
<b>DAL</b> Forensic Identity Management		<b>Selfie with Liveness Verification</b>	<b>DAL</b> Forensic Identity Management		<b>Selfie with Liveness Verification</b>
± 100%	 Proof of Human Being	<b>0%</b> No Forensic Evidence	0%	 AI-Generated Identity	<b>High to Very High Risk</b>
± 100%	 Identity Authentication	<b>Low to Zero</b>	± 100% Fingerprint Signature	 Consent	<b>Low Certainty</b> using Digital signature
<b>Very LOW</b> Identity is made worthless to any other person	 Risk to Individual	<b>High to Very High Risk</b>	0% Forensic Human Onboarding ensures NO Bias	 Algorithm Bias	<b>High to Very High Risk</b> 100% Dependency on Digital Algorithms
<b>Very Low Risk</b> Optimum level of KYC	 Risk to Institution	<b>High to Very High Risk</b>	± 100% Individual Onboards Once, Use it anywhere	 Interoperability	<b>Questionable</b>
<b>Allows</b>	 Deceased Identity	<b>Does not allow</b>	<b>Not Applicable to Proof an Identity</b>	 Verified Credentials	<b>Low Authenticate Certainty</b> Could be True or False
<b>Very High Trust</b>	 Trust Exchange	<b>Low to Very Low Trust</b>	<b>Very High Authenticate Certainty</b> Imported direct from Source using Forensic Cryptography	 Document & Data Accuracy	<b>Low Authenticate Certainty</b> Could be True or False

By pioneering innovative techniques and implementing robust safeguards, DAL Identity International not only addresses the current vulnerabilities but also sets the standard for future Identity Management practices. Its commitment to staying ahead of evolving threats ensures unparalleled protection for individuals navigating an increasingly digital world.

In embracing Forensic Identity Management (FIM), we recognize its indispensable role in countering Identity fraud and manipulation, especially Deepfake and AI-created Synthetic Identities. This evolution marks a crucial shift towards proactive Identification and mitigation of risks, rather than reactive responses after the damage has been done.

As we navigate this era of constant technological advancement and emerging threats, the adoption of Forensic Identity Management (FIM) is not merely an option but a necessity. DAL Identity International stands at the forefront of this evolution, offering a path towards reclaiming control over personal Identity and safeguarding against the perils of Identity fraud and manipulation, especially Deepfake and AI-created Synthetic Identities. In embracing this transformative approach, we pave the way for a more secure and resilient digital future.



## About the Authors

### Dawid Jacobs



#### Dawid Jacobs: Pioneering Human and Digital Identity Management

Dawid Jacobs is a trailblazer in the realms of Human and Digital Identity Management, originating from the vibrant landscapes of South Africa. With a distinguished background as a Fingerprint Expert and Crime Scene Forensic Investigator within the esteemed South African Police Service, Dawid's journey has been defined by his indelible mark on the landscape of identity verification and protection.

An unwavering luminary driven by passion, Dawid co-established the very first and only Forensic Identity Management (FIM) solution globally in collaboration with Gunther Sonnenfeld. This groundbreaking solution, rooted in Forensic biometrics and Cryptographic Provenance on Web 4.0, bridges the tangible reality of a living human being with its digital counterpart in cyberspace, safeguarding against synthetic identities.

Dawid's pioneering spirit extends to his pivotal role in the creation of IdentiKee, a product dedicated to Alive Human Beings (ante mortem), and the first global Deceased Identity Administration Network (DIAN), capable of processing and collecting Deceased (post mortem) Identity globally. Additionally, he founded the DAL Verified Trust Exchange (VTE), facilitating the Single Digital Twin platform linked to a Single Existing Real-World Human Being.

With over 35 years of illustrious experience, Dawid's devotion to safeguarding and validating identities remains unparalleled. To him, identity isn't merely a marker but an irrevocable testament to the existence of a singular human soul, underpinning his meticulous handling of every identity under his purview.

Drawing upon his reservoir of Evidential Forensic acumen, Dawid ingeniously crafted the DAL solution—a fusion of Fingerprint Biometrics with DNA, Iris, Dental, and Facial biometrics. This Digital Identity serves as an unequivocal representation of a living human entity, halting transactions until thorough verification is achieved while ensuring data privacy and fostering inclusivity within the DAL ecosystem.

Dawid's cerebral prowess fuels an unceasing cascade of innovative Identity Management solutions, elevating the DAL framework to unprecedented value for individuals and institutions alike. He aims to sever the conduits of financial malfeasance and criminal machinations by tethering identities solely to their rightful possessors.

In recognizing the gravity of Deceased Identities, Dawid navigates us toward a future free from Identity-related crimes by proactively deactivating Digital counterparts upon physical demise. His legacy is one of safeguarding the essence of who we are—an ode to a future fortified by unwavering identities and untold security, where institutions, governments, and individuals stand to gain immeasurably from his dedicated and innovative ethos.





## Gunther Sonnenfeld



Gunther Sonnenfeld is a globally recognized serial entrepreneur at the intersection of technology, sustainability, and cybersecurity with primary roles as a systems architect.

His foray into the challenges of digital identity and privacy protection came as a subcontractor for the likes of Google, Facebook, Amazon, Apple and Skype, where he helped develop critical data solutions involving 1<sup>st</sup> party traceability with online forensics.

Shortly thereafter, he co-developed the world's first Bitcoin point-of-sale system ([Coin of Sale](#)), expanding early cryptocurrency adoption across fourteen international markets, and also co-developed one of the first deep learning (AI) content curation platforms, [Faveeo](#). A big part of these efforts involved ways to improve personal authentication and secure information-sharing between peers.

Later on, Gunther co-invented a global patent for distributed digital rights management under the [RAIR platform](#), his 9th startup as a co-founder, transforming information security in the Web 3.0 to Web 4.0 era.

He has helped pioneer digital environmental conservation with Smart Ecologies, an invention merging IoT and sustainability in the creation of self-sufficient natural resource ecosystems using relevant real-time data for risk-mitigation and accurate economic forecasting. This breakthrough approach has been applied with groups such as Imaginea Energy, the Savory Institute, and BMR Energy (Virgin Group).

In cryptography, he invented a Web 4.0 framework called Holonomials, fortifying security against quantum computing, specifically by advancing object-level data processing with an informatics system for Small Language Modeling, an alternative to the major problems generated by artificial general intelligence. This approach was first introduced to companies such as Thomson Reuters to help improve their own search databases and query systems.

His finance expertise birthed [Currency Squared](#) with [Web 4.0](#) inventor Marcel Donges, a sustainable currency system fueled by renewable energy and measured in Joules.

Most recently, he co-invented a new forensic cryptographic standard for autonomous reusable identities with Dawid Jacobs, revolutionizing digital trust via their [DAL](#) platform solution. In doing so, he has refined and integrated his proprietary informatics/SLM process.

Gunther's accolades also include a Forrester Groundswell Award for co-developing Adobe's first small business private social network, as well as co-developing with DAL CTO Marcel Donges the first urban planning digital twin Metaverse for [NEOM](#), the world's largest (and most controversial) sustainable real estate project to date.

Over his 27-year career, Gunther has worked with global institutions such as the IMF and the World Bank, has advised governments along with multinational corporations such as Orange and Unilever on innovation initiatives, consulted major investment banks such J.P. Morgan on their early stage technology portfolios, as well as experimented with independents such as the [P2P Foundation](#) and the Institute for Collective Intelligence. He has also served as an advisor to C-PET (the Center for Policy on Emerging Technologies in Washington, DC), sitting on key nanotechnology consortiums with the UN General Assembly, UNESCO, The World



Economic Forum, the U.S. Chamber of Commerce, the NIST, as well as U.S. technology and FinTech committees for both houses of Congress.

These efforts have influenced policies that, while largely overlooked, would endeavor to protect citizen rights, as well as exposing the pitfalls of artificial intelligence, the blockchain and mass surveillance methods which plague our current Internet/web infrastructure. As such, Gunther became one of the first software architects to develop data solutions in Web 4.0 as early as 2014, before the Web 3.0 hype cycle, when he and Marcel Donges began their collaborations under the premise of “My Data, Under My Control”, which is now DAL’s moniker of “Your Identity, Under Your Control”.

These achievements underscore his hands-on dedication to innovating with digital identity at the core of real world interactions whereby real human beings can collaborate or transact in a truly safe, distributive, autonomous, and decentralized manner.

