DAL
Diverse Authentication Library

Your Identity, Under Your Control

Introducing a new global standard for reusable identities based on real people and their owned data, not based on artificial intelligence and third-party data.

Authors

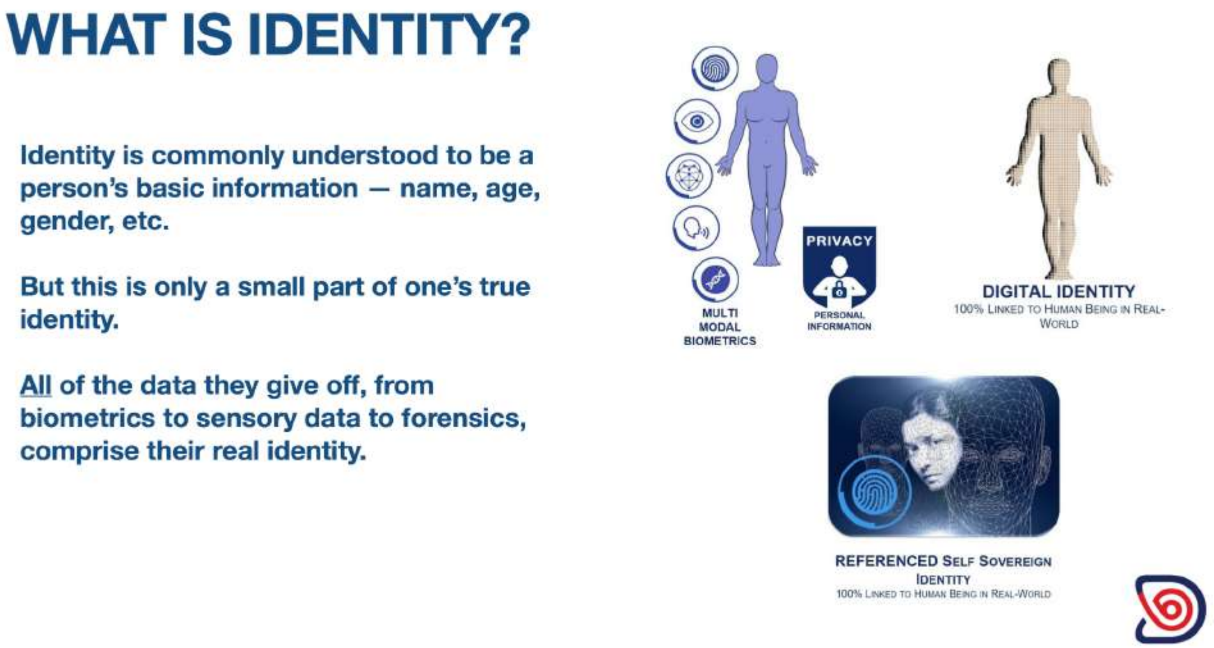
Dawid Jacobs, CEO
35-year law enforcement Forensics Expert

Gunther Sonnenfeld, CPO
27-year Systems Architect & Developer of Forensic Cryptography

Marcel Donges, CTO
30-year Enterprise Technologist & Inventor of Web 4.0

ABSTRACT

An identity is the culmination of what people believe about themselves, their origins, and their characteristics, as presented to the general public. Identities are commonly represented in government-issued IDs and are commonly understood to be a person's basic information — name, age, gender, etc. Yet this is only a small part of one's true identity, which now comprises all of the data they give off, from biometrics to sensory data to forensics. In today's world, a person's digital twin is what represents both their public and private identity, and with it comes a host of immense challenges in terms of autonomy as well as security, mostly driven by an unrealistic and somewhat illogical dependency on artificial intelligence. This whitepaper addresses DAL Identity's evolutionary system to create, preserve, and protect personal identities without this dependency, and why this solution benefits everyone involved — from companies to governments to NGOs, to private citizens.



WHAT IS IDENTITY?

Identity is commonly understood to be a person's basic information — name, age, gender, etc.

But this is only a small part of one's true identity.

All of the data they give off, from biometrics to sensory data to forensics, comprise their real identity.

MULTI MODAL BIOMETRICS
PRIVACY
PERSONAL INFORMATION
DIGITAL IDENTITY
100% LINKED TO HUMAN BEING IN REAL-WORLD
REFERENCED SELF SOVEREIGN IDENTITY
100% LINKED TO HUMAN BEING IN REAL-WORLD

Table of Contents

Introduction

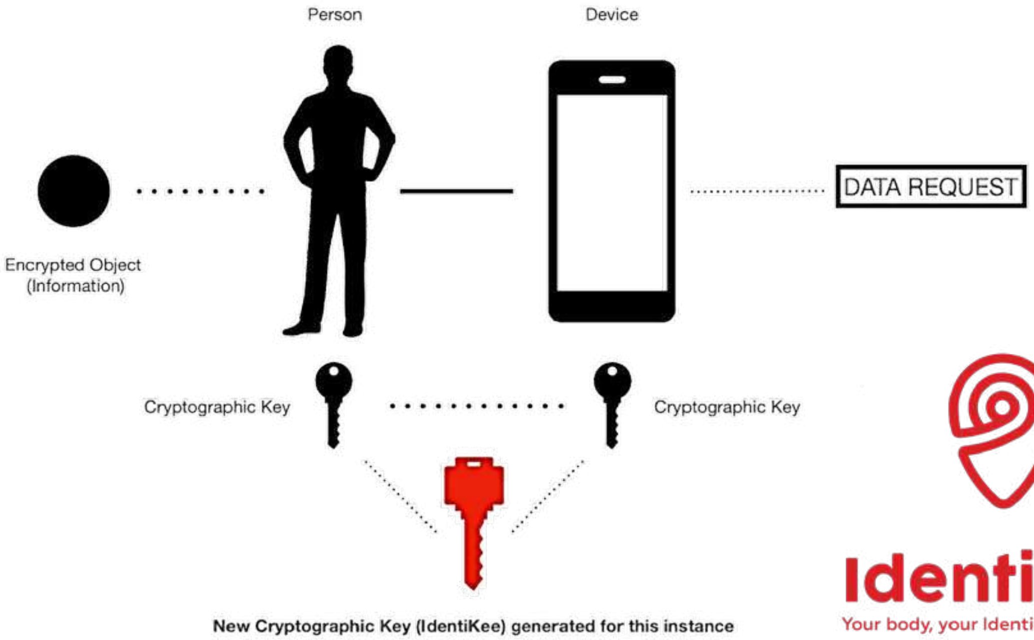
The rapid proliferation of AI has prompted a sea change in approaches to physical identity and various forms of digital identity. Nearly 70% of all identities found online are synthetics or fakes. This reality is exacerbated by poor data-capturing methods found in "selfies" and in the creation of "deep fakes". The result produces financial losses at minimum to the tune of $10.5 trillion USD per year, in which corporations, small businesses and governments alike struggle to establish or maintain economies based on the rule of law. We at DAL address an evolutionary approach to creating reusable identities based on three differentiating pillars:

+ **Succession** (establishing self-ownership such that there are no data trails or backdoors for manipulation, hacking or replication)

+ **Proof of Evidence** (establishing real proof based on real data from the real person such that their digital twin is a precise representation of all ensuing interactions)

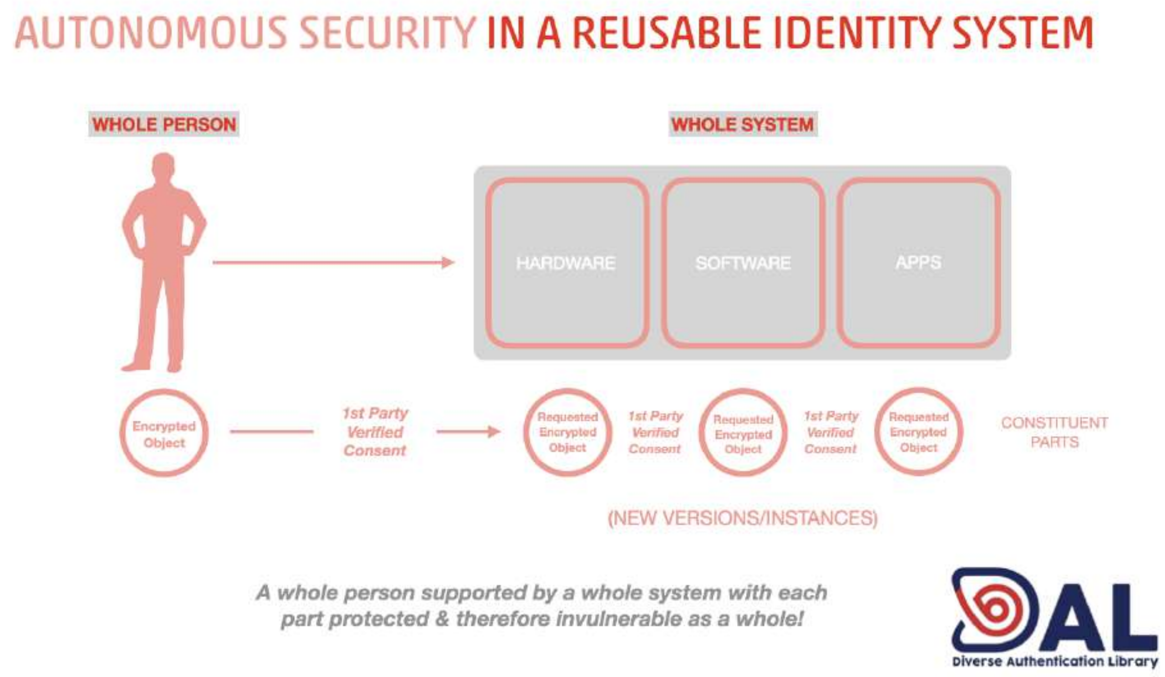
+ **Forensic Cryptography** (establishing investigative security at the moment data is generated from that real person for useful extraction)

These pillars are combined to create what is called "Trustless Trust" with autonomous security. Trustless means "without the use of trust seals" (digital watermarks or outside verification points) leaving real reputational trust as a set of real-world actions that are verified between people, peers, or counterparties.



IdentiKee™
Your body, your IdentiKee

Autonomous security means that if one part of the system is hacked or breached, *only that part will be compromised, rather than the entire system*. This is a huge step forward not just for identity management but in both web development and cybersecurity overall, on the basis that all levels and phases of data can be secured on their own, thereby providing the unprecedented capacity for a person to monetize this data on their own.

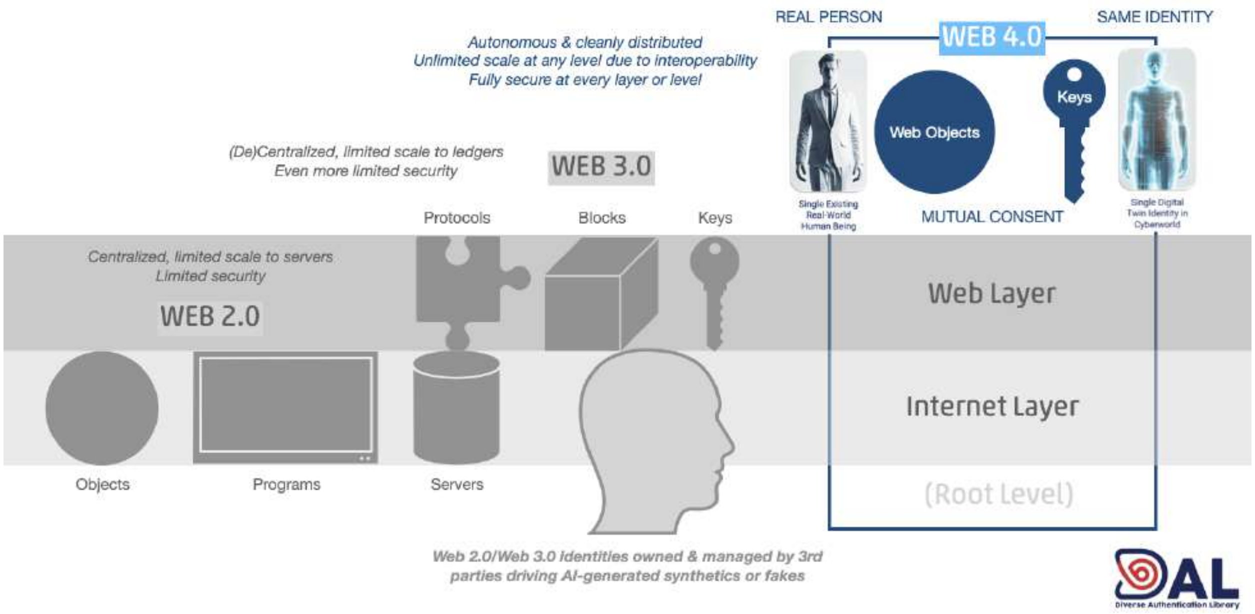

AUTONOMOUS SECURITY IN A REUSABLE IDENTITY SYSTEM
WHOLE PERSON
WHOLE SYSTEM
HARDWARE
SOFTWARE
APPS
Encrypted Object
1st Party Verified Consent
Requested Encrypted Object
1st Party Verified Consent
Requested Encrypted Object
1st Party Verified Consent
Requested Encrypted Object
CONSTITUENT PARTS
(NEW VERSIONS/INSTANCES)
DAL
Diverse Authentication Library

A whole person supported by a whole system with each part protected & therefore invulnerable as a whole!

Cryptographic identity overview

While normative cryptography relies upon pseudo-anonymous protocols for transferring data from one person or counterparty to another (as with Web 3.0), it is also the case that a person's identity cannot possibly rely on protocols alone to be authentic. In short, web protocols — *which are distinct from forensics protocols, as we will explore later* — can never represent the real, authentic data of a human being, simply because that data must be captured at the source, and then structured accordingly as it moves from one digital device or channel to another. As devices and channels expand into the greater "Internet of Things" or the "Internet of People", we can now see how the establishment of a Web 4.0 infrastructure plays a vital role in the creation of real identities based on personal information that cannot be compromised.

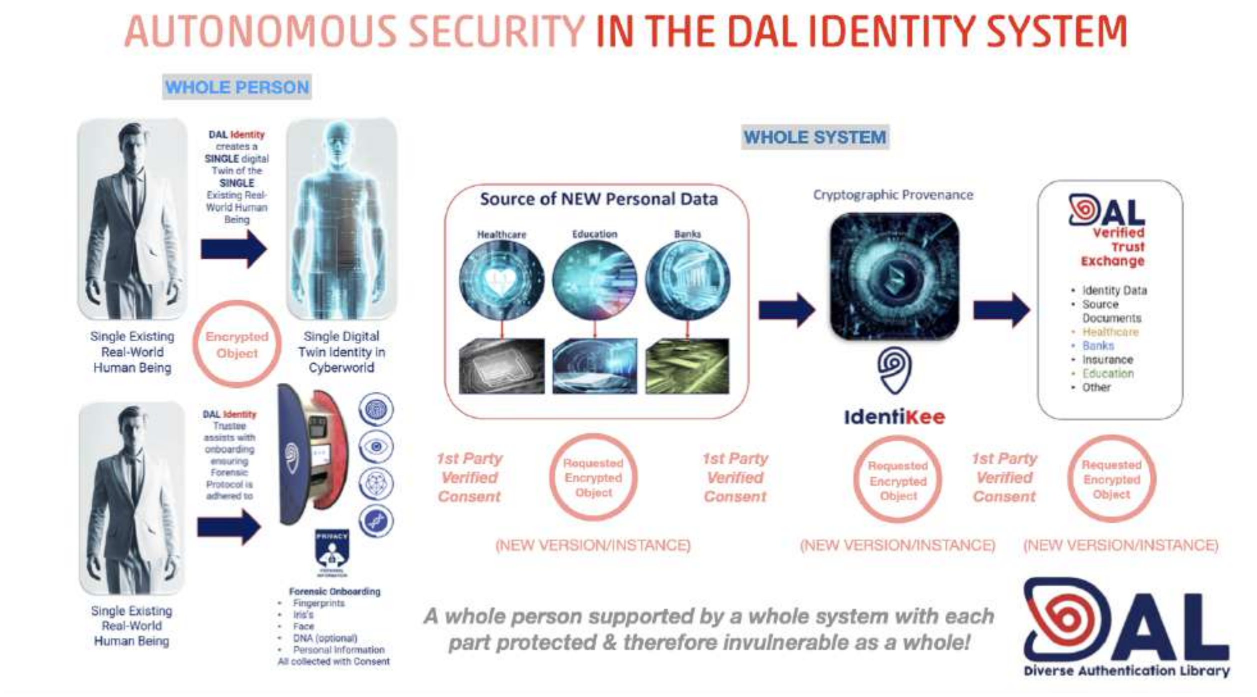
THE BASICS OF WEB 4.0 INFRASTRUCTURE & IDENTITY


REAL PERSON
WEB 4.0
SAME IDENTITY
Autonomous & cleanly distributed
Unlimited scale at any level due to interoperability
Fully secure at every layer or level
Web Objects
Keys
(De)Centralized, limited scale to ledgers
Even more limited security
WEB 3.0
Single Existing Real World Human Being
MUTUAL CONSENT
Single Digital Twin Identity in Cyberworld
Protocols
Blocks
Keys
Centralized, limited scale to servers
Limited security
WEB 2.0
Web Layer
Internet Layer
Objects
Programs
Servers
(Root Level)
Web 2.0/Web 3.0 identities owned & managed by 3rd parties driving AI-generated synthetics or fakes
DAL
Diverse Authentication Library

Moving from centralized infrastructure with scale and security limited to server configurations (Web 2.0), then to (de)centralized infrastructure with scale and security limited to ledger configurations (Web 3.0), we arrive at the **Web 4.0 infrastructure** — *invented and built as an interoperating system by DAL Identity's very own CTO, Marcel Donges* — in which a single existing real world human being is represented as a single digital twin identity in the cyberworld. Web objects and cryptographic keys of that same person's real information are exchanged or transferred by way of the consent the individual grants to requesting counterparties without any 3rd party involvement.

To be clear, the only way to transfer personal data properly is to generate it as a web object at its root level (and thereafter eradicate root-level access), thereby securing the data at various points between counterparties. When we speak of identities themselves, there is no greater goal than to preserve and protect personal data such that a person's identity can be permissioned by the individual to be represented as a whole entity, or in parts that can satisfy specific requests per mutual consent. The operative word here is **consent**.

Notice that no matter what domain or industry requires personal information using whatever method it uses to do so, *every bit of information shared is consensual, including the parts through which the information is structured.* In technology terms, every requested bit of information comes in its own instance as an **encrypted object**. When this happens, if one part is corrupted for whatever reason, all the other parts remain intact, preserving the system as a whole.


AUTONOMOUS SECURITY IN THE DAL IDENTITY SYSTEM
WHOLE PERSON
DAL Identity creates a SINGLE digital Twin of the SINGLE Existing Real-World Human Being
Single Existing Real-World Human Being
Encrypted Object
Single Digital Twin Identity in Cyberworld
DAL Identity Trustee assists with onboarding ensuring Forensic Protocol is adhered to
PRIVACY
Single Existing Real-World Human Being
Forensic Onboarding
Fingerprints
Iris's
Face
DNA (optional)
Personal Information
All collected with Consent
WHOLE SYSTEM
Source of NEW Personal Data
Healthcare
Education
Banks
Cryptographic Provenance
IdentiKee
DAL Verified Trust Exchange
Identity Data
Source Documents
Healthcare
Banks
Insurance
Education
Other
1st Party Verified Consent
Requested Encrypted Object
1st Party Verified Consent
Requested Encrypted Object
1st Party Verified Consent
Requested Encrypted Object
(NEW VERSION/INSTANCE)
(NEW VERSION/INSTANCE)
(NEW VERSION/INSTANCE)
A whole person supported by a whole system with each part protected & therefore invulnerable as a whole!
DAL
Diverse Authentication Library

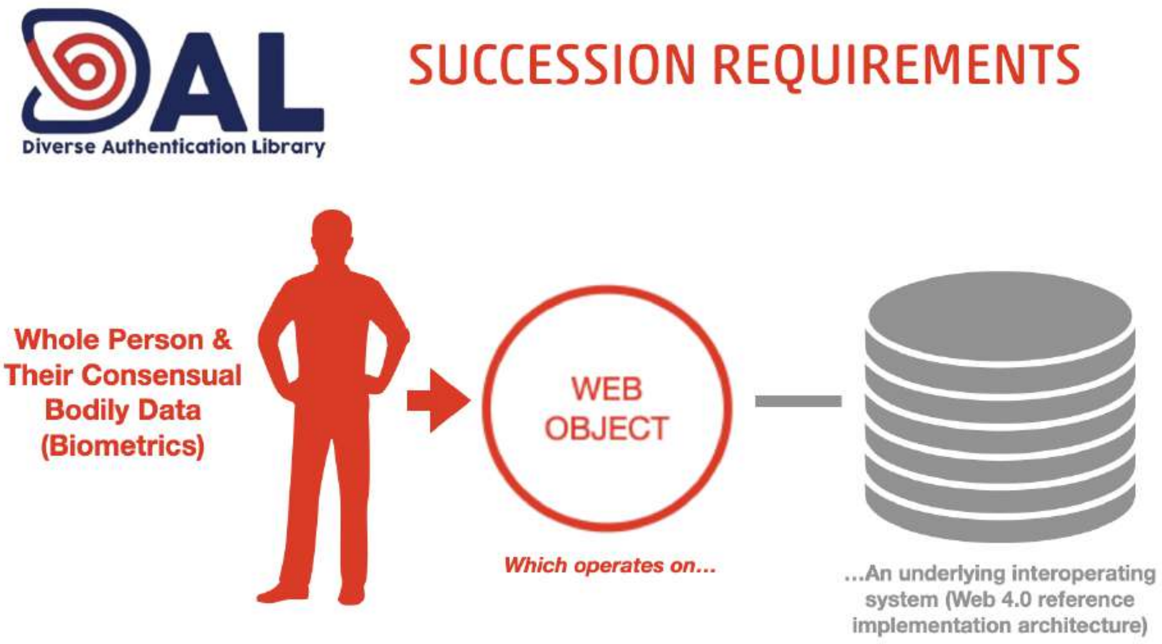
This realization flies in the face of both legacy Web 2.0 systems and Web 3.0 systems, due to the fact that neither provides control mechanisms for the individual to share data properly, nor does each protect individuals from 3rd party interference. Companies like Amazon, Google, Apple, Facebook, Oracle, Huawei and Baidu are infamous for this. The question now becomes one of first principles: *If these same companies are actually leaving more profit on the table by not doing the right thing, then what exactly will it take to get them to do the right thing?*

We submit to the reader that the answer is straightforward. A new standard for reusable identities is being introduced by way of providing thorough **forensic integrity**. This standard simply benefits everyone and at an increasingly efficient scale.

SUCCESSION

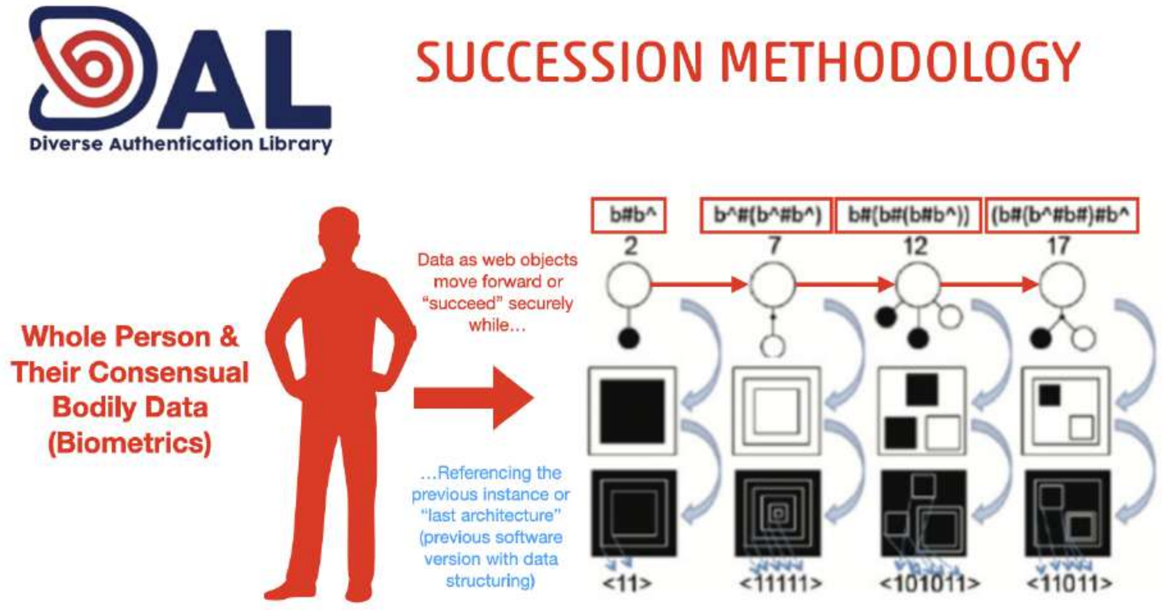
Forensic integrity has led to the applied phenomena of what we at DAL call **Succession**. Succession was borne from the same realization that legacy Web 2.0 and more recent Web 3.0 systems — *which are in reality based on very old technology approaches* — are all about third-party control. Another way to understand this is by looking at the Internet and web infrastructure; if the cables, wires, bits, bytes, protocols, and gateways for running data packets are ultimately owned by third parties (and they are), then nothing is owned by individuals, which very much includes their own identities.

Succession establishes provenance or self-ownership by creating a mechanism that allows each person to onboard, manage and monetize their own data, by delegating each instance of data-sharing as its own last architecture. By last architecture, it is inferred that the "last or latest infrastructure" found in an operating system software for moving that personal data is captured as a snapshot, while the new version of the data awaits a request without being tied to the last version, or the last architecture. So, in this context, *the operating software "moves" with the data, and does so in that one version of the data along with the software underlying it*.


DAL
Diverse Authentication Library
SUCCESSION REQUIREMENTS
Whole Person & Their Consensual Bodily Data (Biometrics)
WEB OBJECT
Which operates on...
...An underlying interoperating system (Web 4.0 reference implementation architecture)

Think of how information is "reset" or "refreshed" in a business intelligence system, or how a database refreshes itself in a series of commands. The information changes, but the system itself doesn't. With succession, the information has its own operating system, which changes along with the information. Therefore, the information succeeds the prior set of data in that it doesn't take on any of the properties of the prior system, but it does take on new information attributes to represent the same original source, which is **the human being**.

For an identity, this is a quantum leap in authenticity and the overall quality or purity of information. Why? Because each datum is verified and organized without redundancies, inauthentic qualifiers or overlaps with other datasets. This is a process that literally cleans up datasets as they are being generated, and as they are shared between counterparties. Therefore, datasets can't be hacked or manipulated without infiltrating source data, or by infiltrating the current architecture. Both are protected at the moment they are referenced for extraction.


DAL
Diverse Authentication Library
SUCCESSION METHODOLOGY
Whole Person & Their Consensual Bodily Data (Biometrics)
Data as web objects move forward or "succeed" securely while…
…Referencing the previous instance or "last architecture" (previous software version with data structuring)
b#b^
2
b^#(b^#b^)
7
b#(b#(b#b^))
12
(b#(b^#b#)#b^
17
<11>
<11111>
<101011>
<11011>

If you don't reference the current software version carrying the data, you can't hack or manipulate the data!

In the bigger picture of an "Internet of Things" or an "Internet of People", every human being's identity evolves because they evolve as participating members of society. Yet, there are bodily characteristics that will never change, such as DNA imprints, fingerprints or iris scans. Given this reality, a human being must be given the opportunity to evolve how their identity is represented to the public, while preserving their core bodily characteristics. So, if someone wants to add an element to their identity, such as what they currently do for a living, or they want to declare a specific religious status, they should be free to do so, and they can do so by simply referencing the new information against the bodily information that does not change.

Another thing to consider is that the bodily information that does not change must be established as the person's own property so that constant changes to a person's work, life, or cultural status can take place without recourse. In a world where people are often divided due to cultural mores, their self-owned identity must be a backstop for being canceled, ridiculed, or persecuted because of their beliefs or their basic way of life.

Perhaps it is a bit clearer now as to how succession really works: An identity operates of its own accord because there is no personal liberty without it. When personal liberty is compromised, no one benefits — not the state actors trying to implement justice without consent in using personal information, nor the corporations expecting to generate revenue from consumers who have no control over their own information.

DAL
Diverse Authentication Library
SUCCESS IN PERSONAL AUTONOMY!
Whole Person & Their Consensual Bodily Data (Biometrics)
SECURED
WEB OBJECT
Freedom to express one's true self without 3rd party interference

When **mutual consent** is established in a succession of data-sharing between individuals and requesting parties, everybody wins because everybody profits or enjoys civic benefits (non-material outcomes) with exact precision.

Note that succession is not a one-time agreement between people or counterparties, in which mutual consent is granted only for that instance in perpetuity. Rather, it is a continuous consensual agreement that updates the data in every instance or in every context for a data request.

Now let's explore how Proof of Evidence is driven by a succession of data accuracy.

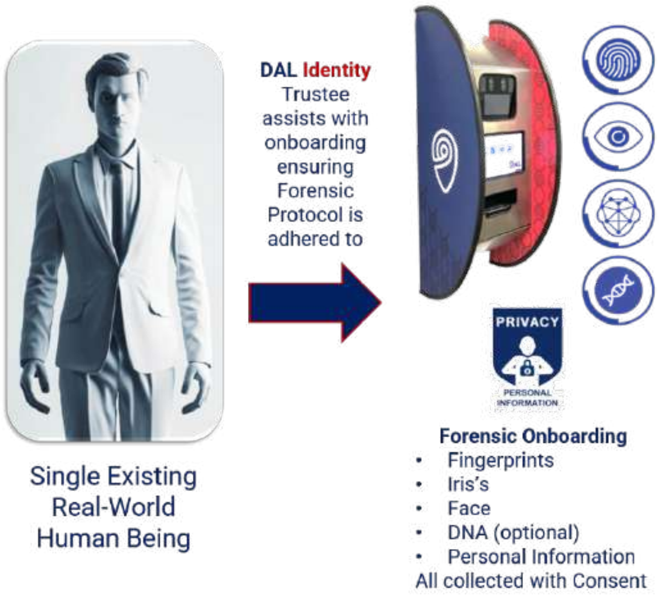
PROOF OF EVIDENCE

Proof of Evidence is the **sui agnitionis** (Latin for "self-acknowledgment") of a human being's existence in this world of corrupt government structures and organized criminal activities. When one considers how extensive a lack of proof runs across our information systems, our financial systems, and our social systems, it becomes obvious that it is harder and harder to provide evidence for a wide range of cybercrimes or identity theft. Even worse, the world is currently overrun by cartels, to which transnational crime syndicates make huge paydays running guns, drugs, and human slaves, all under the noses (or watchful eyes) of governments. We cannot stop cartel activity outright, but we can clean up these systems upon which the cartels rely for exploitation, or replace them altogether.

Let us now consider what happens when Proof of Evidence is established in the forensics process. When a real person in the real world generates bodily data, the data trail can easily match any of that person’s activities, such as when someone walks to a store, purchases an item, or shares personal information (Pii). Therefore, evidential proof is fairly easy to establish, provided that the data coming from that person’s body is accurate and authentic.

When a real person in the real world has a digital twin in the virtual world, there is either the persona that exists “as it should”, or, the human being is rendered persona non grata. As simple as this sounds, the reality of a human being whose identity can be exposed and potentially eradicated in an instant is precisely the digital world into which we’ve entered. It is also the world cartels have created for themselves, home to many innocent victims or persons non grata. Thus we find ourselves in a kind of “digital prisoner’s dilemma” in that whoever is representing a real person in the real world often has nothing to do with that person, but rather a synthetic identity that can be versioned any number of ways, all based on the person’s personal information, and not their bodily data.

Imagine multiple versions of yourself as a digital representation, in which those versions are expanded upon and used at will, without your knowledge or your consent. This is the actual reality of the digital world in which you take part on a daily basis. Not only that, this is the dynamic in which AI thrives the most, simply because its primary purpose is to simulate patterns or behaviors, not to create or engender them as “better practices”. In the DAL system, all data and therefore all intelligence is harvested, sorted, and transferred as natural intelligence. This natural intelligence is what ensures that forensic protocols are adhered to as a person onboard their personal information.



DAL Identity's onboarding process adheres rigorously to all forensic protocols and incorporates forensic biometrics as a fundamental component, collected with the full consent of the individuals asserting their identities.

The deployment of Evidential Forensic Protocols in the realm of Identity Management is a pivotal step to guarantee the integrity and authenticity of Human Digital Identity. These protocols, which demand the physical presence of the individual at the time of data capture, play a crucial role in verifying the validity of an identity and preventing fraudulent or synthetic identities.

Here are the 10 fundamentals of Evidential Forensic protocols in identity management based on a core Proof of Evidence:

1. **Foundation of Trust:** Evidential Forensic protocols are firmly grounded in the principles of trust and reliability. They prioritize capturing identity-related data, such as biometrics and personal information, in a manner that leaves no room for doubt regarding its authenticity.

2. **Physical Presence:** One of the core tenets of Evidential Forensic protocols is the requirement for the physical presence of the individual during data capture. This ensures that the data collected is directly linked to a living, breathing human being rather than a digital artifact or synthetic creation.

3. **Preventing Identity Fraud:** By mandating the physical presence of the individual, Evidential Forensic protocols act as a robust deterrent against identity fraud. It becomes exceedingly difficult for malicious actors to impersonate another person or create synthetic identities when physical presence is a prerequisite.

4. **Forensic Value:** Evidential Forensic protocols imbue the collected data with forensic value. This means that the data can be used as credible evidence in a court of law to establish the identity of an individual. For example, fingerprints collected using these protocols can be utilized for forensic identification purposes.

5. **Chain of Custody:** These protocols often incorporate a provable Chain of Custody, which documents the handling and movement of data from the point of capture to its eventual use or storage. Chain of Custody ensures that the data remains unaltered and tamper-evident throughout its lifecycle, bolstering its credibility.

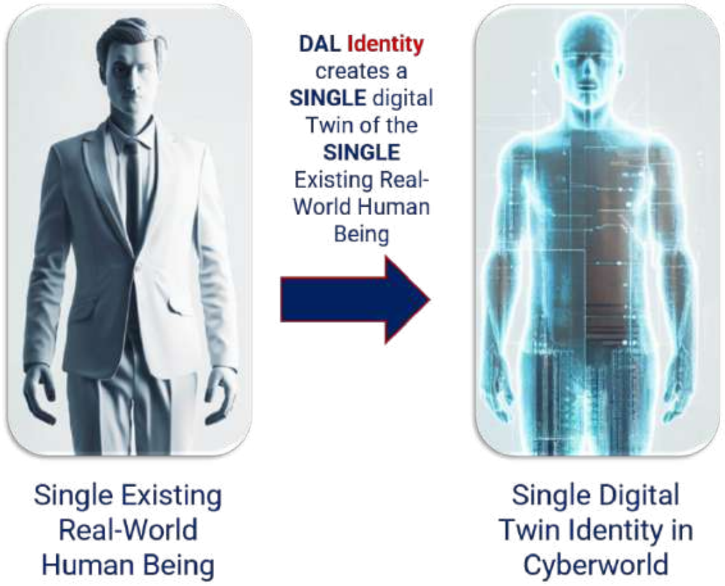
6. **Compliance and Legal Standards:** Evidential Forensic protocols align with legal standards and regulatory requirements related to identity management. This is crucial for organizations and government entities that need to ensure that their identity management practices comply with relevant laws.

7. **Consistency and Reproducibility:** The consistency and reproducibility of data collection are essential aspects of Evidential Forensic protocols. These protocols are designed to yield consistent and repeatable results, enhancing the reliability of the collected data.

8. **Protection Against Deepfakes and Synthetic Identities:** In an era where deep fakes and synthetic identities pose significant threats, Evidential Forensic Protocols provide a bulwark against such manipulations. Deep fakes typically lack the physical presence required by these protocols, making them easier to detect.

9. **Privacy and Consent:** These protocols emphasize the importance of privacy and obtaining the individual's consent for data collection. Ensuring that individuals are aware of and agree to the use of their biometric and personal information is a fundamental ethical consideration.

10. **Risk Mitigation:** Deploying Evidential Forensic Protocols is a proactive measure to mitigate risks associated with identity management. It reduces the likelihood of security breaches, identity theft, and data misuse.


DAL Identity creates a SINGLE digital Twin of the SINGLE Existing Real-World Human Being
Single Existing Real-World Human Being
Single Digital Twin Identity in Cyberworld

DAL Identity utilizes Forensic Cryptographic Provenance to establish a Singular Digital Twin Identity corresponding to a Single Existing Real-World Human Being.

Evidential Forensic protocols represent a gold standard in Identity Management. They establish a clear and unassailable link between an individual and their digital identity, bolstering trust, credibility, and the legal standing of the collected data. As the digital landscape evolves and identity management becomes increasingly critical, the adoption of such protocols is imperative to ensure the integrity of Human Digital Identity and to protect against emerging threats. Henceforth, Proof of Evidence is precisely the guideline for proper forensic investigative processes, along with a digital standard that pulls no punches.

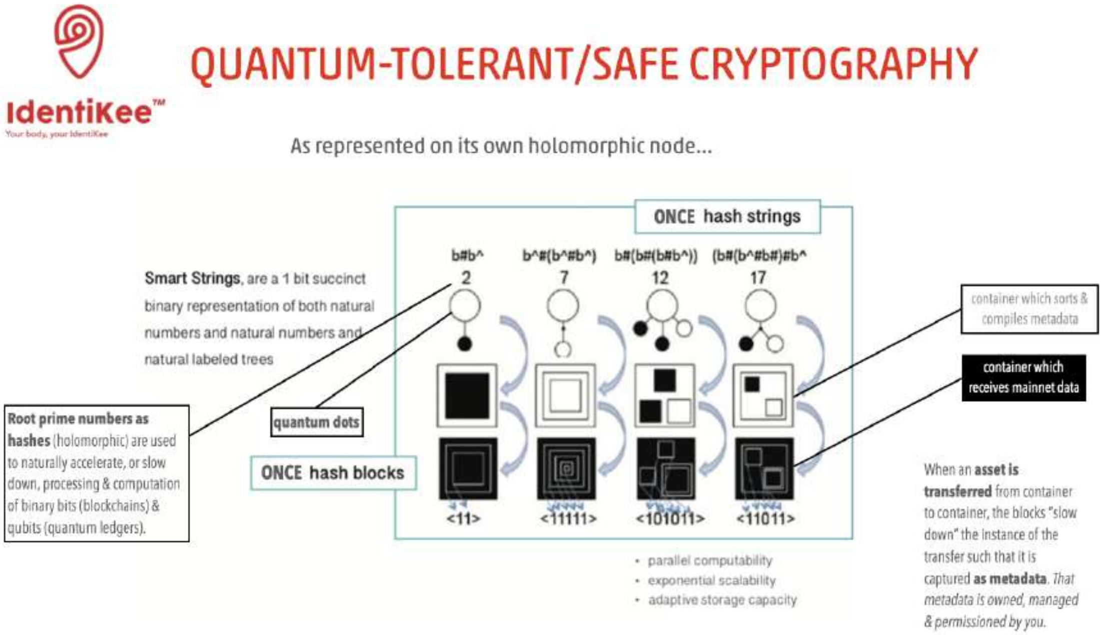
As can be seen in the application of said protocols or methodological guidelines, the evidentiary innovation resides in **total accuracy and victim/target protection**, from the moment someone shares information, to the moment an attempt is made to use that information.

Now let's explore how these critical elements are combined to make up an exciting new practice called Forensic Cryptography.

Forensic cryptography

Like Succession and Proof of Evidence, **Forensic Cryptography** is an invention of the group behind this whitepaper and is already being applied as part of DAL Identity's proprietary methodology. The critical part of forensic cryptography is precisely its implication: *It uses the combination of science, technology, and law to deliver an accurate appropriation of secure information.*

As cryptography has been commonly established to protect digital messages like Cyphertext from inside or outside attack, forensic cryptography embeds real law, advanced technology, and applied science into these same digital messages, whether they are found in bits/binaries, or in more formal syntax (script or written language, often seen as **metadata**). In terms of establishing a real identity as a real digital twin, this is also an evolutionary stair-step, simply because a human being's real identity is now no longer reduced to just numbers and algorithms. As important, when a human being interacts more and more with a variety of mixed-reality platforms, such as Metaverses, that person's activities are succinct not as a result of some mass surveillance, but because their ownership of their own data means that no outside step to encroach on their interactions is left unturned.



QUANTUM-TOLERANT/SAFE CRYPTOGRAPHY

As represented on its own holomorphic node...

Smart Strings, are a 1 bit succinct binary representation of both natural numbers and natural numbers and natural labeled trees

Root prime numbers as hashes (holomorphic) are used to naturally accelerate, or slow down, processing & computation of binary bits (blockchains) & qubits (quantum ledgers).

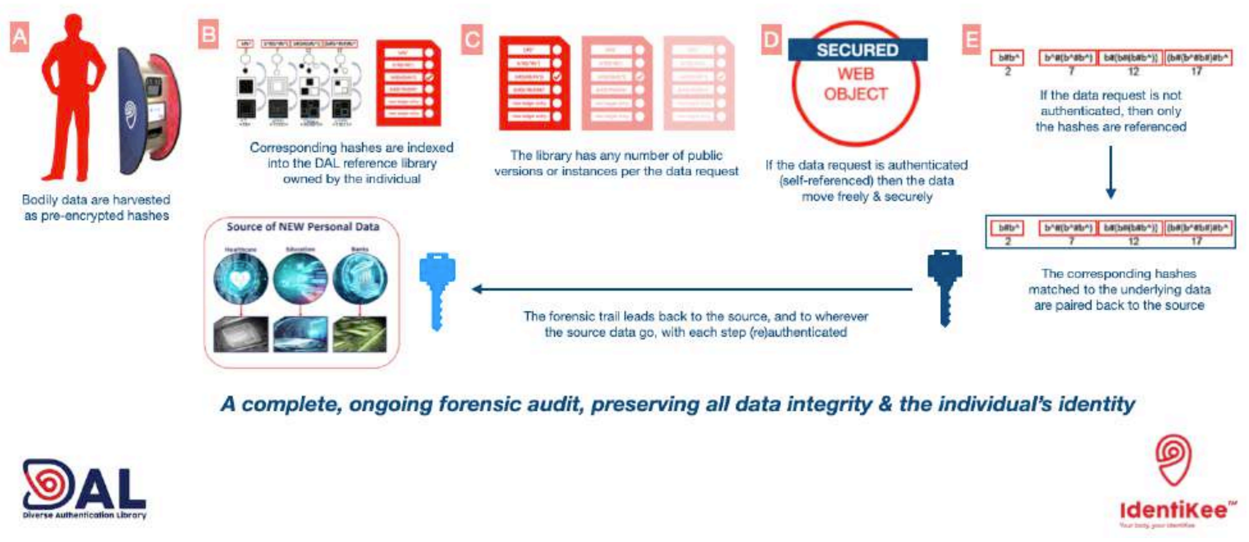
- parallel computability
- exponential scalability
- adaptive storage capacity

When an **asset is transferred** from container to container, the blocks "slow down" the instance of the transfer such that it is captured **as metadata**. *That metadata is owned, managed & permissioned by you.*

Here's how forensic cryptography actually works.

- Bodily data is harvested from the individual as **pre-encrypted hashes** or serial numbers
- Those hashes or serial numbers are **indexed into the DAL reference library**
- The library has any number of **public versions or instances per the data request**
- If the **data request is authenticated** in its current instance (a.k.a. "current state"), the data moves freely & securely
- If a data breach or hack occurs, none of the underlying data is exposed, while **only the hash(es) is/are referenced**
- The corresponding hashes which are matched to the underlying data are **"paired back" to the source without exposure**
- From there, the forensic trail leads back to the source, and to wherever the source goes, with **each step (re)authenticated**
- The result is a **complete, ongoing forensic audit** while preserving all data integrity, and the identity of the individual
- Any subsequent (inter)actions by the individual are thereby **forensically tracked & protected**

THE FUNDAMENTALS OF DAL'S FORENSIC CRYPTOGRAPHY



Bodily data are harvested as pre-encrypted hashes

Corresponding hashes are indexed into the DAL reference library owned by the individual

The library has any number of public versions or instances per the data request

If the data request is authenticated (self-referenced) then the data move freely & securely

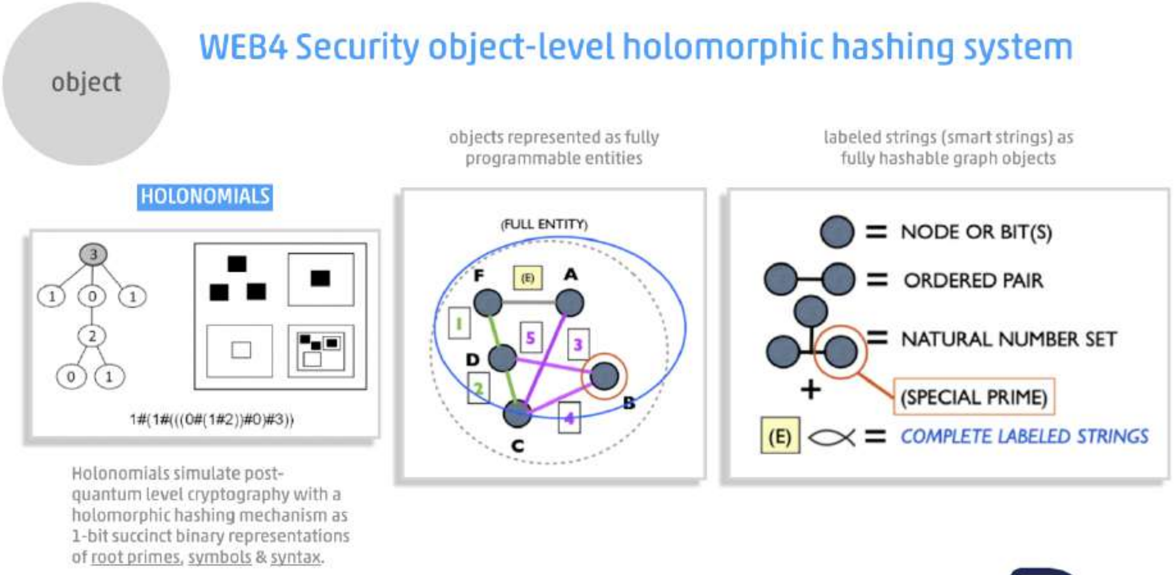
If the data request is not authenticated, then only the hashes are referenced

The corresponding hashes matched to the underlying data are paired back to the source

The forensic trail leads back to the source, and to wherever the source data go, with each step (re)authenticated

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

Given that each datum is forensically tracked and protected, it is thereby structured in a 1-bit succinct binary representation of root primes, symbols (images or other memes), and syntax. Packaged as objects that are fully programmable as data entities, these graph objects are hashed to the precise instance without any reference to the underlying personal data, only the entity or closed identity of the real person. In other words, any node that is discovered in a network can be identified as a "smart string" comprising an ordered pair, a natural number set, or a complete labeled string — and yet, no traceability to personal information can be attained.


object
WEB4 Security object-level holomorphic hashing system
HOLONOMIALS
3
1
0
1
2
0
1
1#(1#(((0#(1#2))#0)#3))
objects represented as fully programmable entities
(FULL ENTITY)
F
(E)
A
1
5
3
D
2
4
B
C
labeled strings (smart strings) as fully hashable graph objects
= NODE OR BIT(S)
= ORDERED PAIR
= NATURAL NUMBER SET
+
(SPECIAL PRIME)
(E)
= COMPLETE LABELED STRINGS

Holonomials simulate post-quantum level cryptography with a holomorphic hashing mechanism as 1-bit succinct binary representations of root primes, symbols & syntax.

When calling up evidence of any sort for any type of forensic audit, this approach changes the investigative game completely since the forensic trail is completely accurate, while none of the personal data can be attained without the consent of the individual or an established custodian approved by the individual. In cases where an individual is deceased and/or has no approved custodian, the state or governing body can make a request for evidence in which all investigative processes are forensically linked to a private or public record — the point being that **forensic integrity is established** regardless of the legal outcomes.

This is a boon for forensic pathology and cybersecurity alike because it means that massive apparatuses like surveillance servers are no longer needed to “protect” the person or citizen. Instead, law enforcement and intelligence agencies can request specific datasets from the person (otherwise known as “small data”), just as the person can share specific datasets per their civil and human rights. In other words, agencies don’t need to search for a “needle in a haystack” while individuals don’t need to worry about sharing all of their personal information for a small data request.

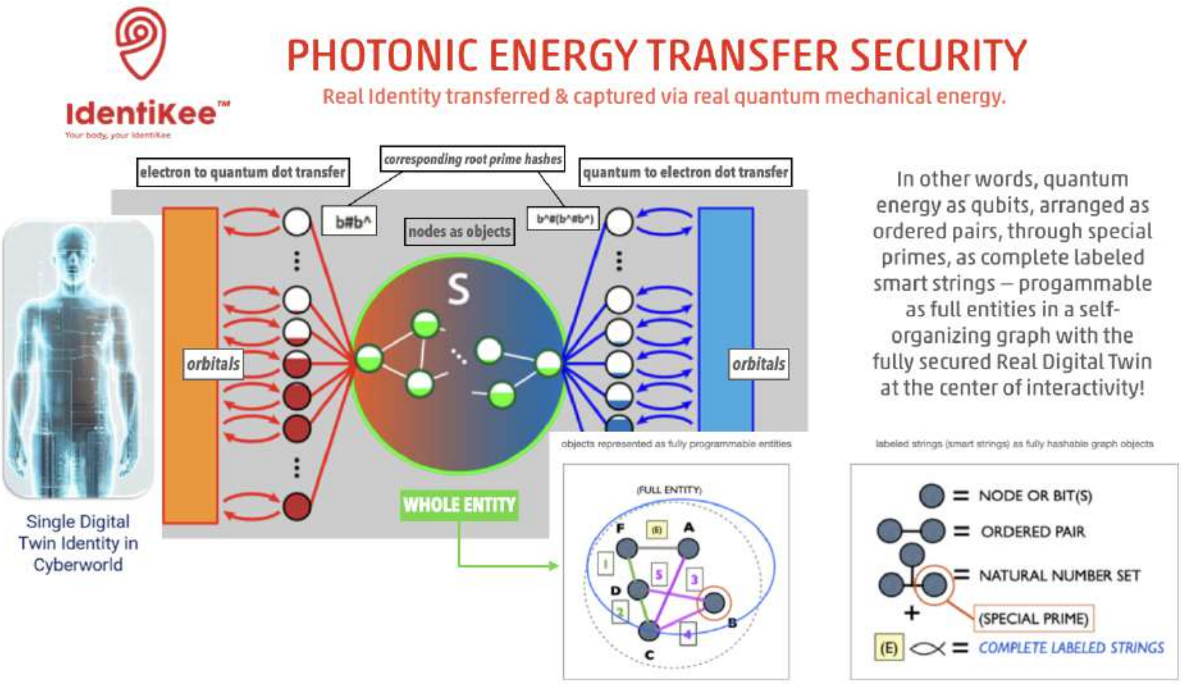
FORGING A BETTER FUTURE FOR CYBERSECURITY

As “Big Data” approaches are giving way to smaller data methods, widespread commercial uses of quantum mechanical delivery — as in the examples of high-speed payment rails and large-scale cybersystems — are only a few years away. This is precisely where AI implementations must be “kept in check”, especially when it comes to maintaining and protecting a digital cyber twin.

Remember that in order to bypass a “digital prisoner’s dilemma” in which real people are often bound informationally to fakes or synthetics of their alleged identities, it is critical that every single datum given off by a real human being must also be represented as actual real information. While this may sound obvious, it isn’t. For example, we’ve seen loopholes and workarounds with the way DNA imprints are generated. If AI is generating these means for synthetics, then we also know that **every single capture point must be authenticated as real and verifiable**.

The way we address this is by structuring the data, the information packets, the cryptography, and the delivery as one, whole entity whose constituent parts can only be parsed by the same entity.

Thus, the holomorphic mechanism (what we call “Holonomial”) is such that only in a requested single instance can a singly requested version of the data representing the same single version of a person’s identity be called up and transferred. What results from this approach is a self-organizing of networked information that is completely authentic and completely secure. Imagine now that you and your authentically represented identity are the nodes connecting your own “virtual private social network”. This would mean that everything you do online would be achieved with full privacy, no matter how much information you decide to share via your consent.



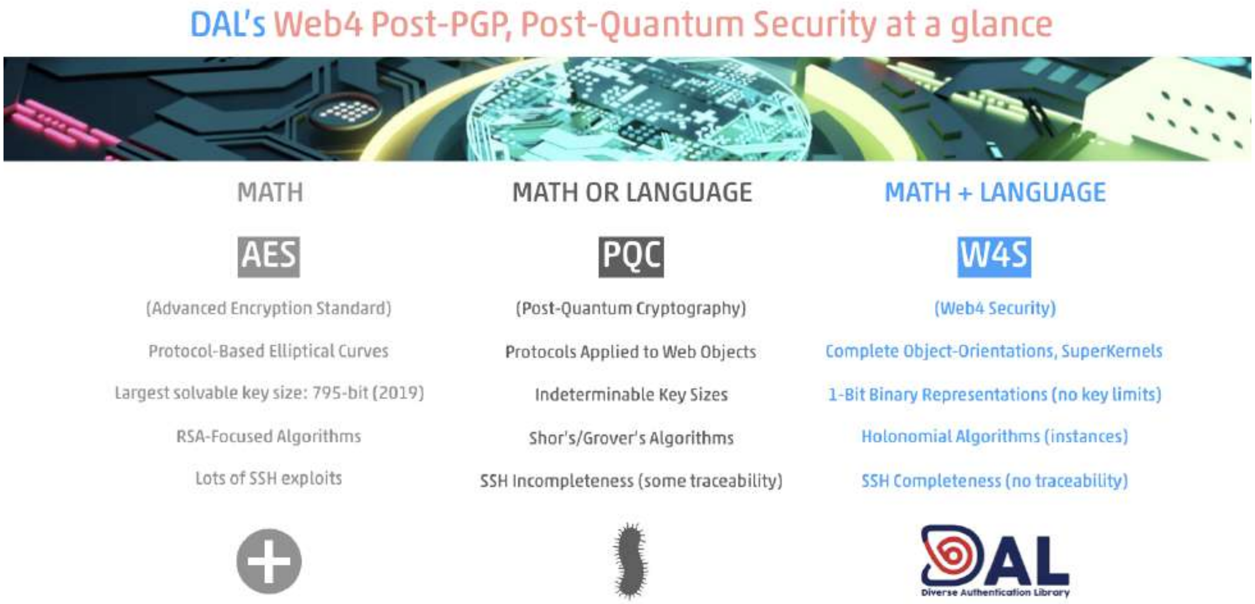
PHOTONIC ENERGY TRANSFER SECURITY

Real Identity transferred & captured via real quantum mechanical energy.

In other words, quantum energy as qubits, arranged as ordered pairs, through special primes, as complete labeled smart strings – progammable as full entities in a self-organizing graph with the fully secured Real Digital Twin at the center of interactivity!

IdentiKee™
Your body, your IdentiKee
electron to quantum dot transfer
corresponding root prime hashes
quantum to electron dot transfer
b#b^
nodes as objects
b^#(b^#b^)
S
orbitals
orbitals
WHOLE ENTITY
Single Digital Twin Identity in Cyberworld
objects represented as fully programmable entities
(FULL ENTITY)
F
(E)
A
1
5
3
D
2
4
B
C
labeled strings (smart strings) as fully hashable graph objects
= NODE OR BIT(S)
= ORDERED PAIR
= NATURAL NUMBER SET
+
(SPECIAL PRIME)
(E)
= COMPLETE LABELED STRINGS

Now let's summarize what this means in cryptographic terms, as we move from advanced encryption standards (AES), to the current standard of post-quantum cryptography (PQC), to what we at DAL have established as **Web4 Security (W4S)**. When whole data entities are established — to include identities at the core as autonomous and self-organizing — we have complete object orientations. These orientations make each datum clean and precise, with binary or numerical representations that have no key limits, algorithmic instances of those representations that are succinct, and overall completeness with Secure Shell protocols (SSH) that leave no traces leading to blunt vector attacks, network canvassing or key replications. This means we go from "Pretty Good Privacy" (PGP) to **total privacy based on mutual consent**.

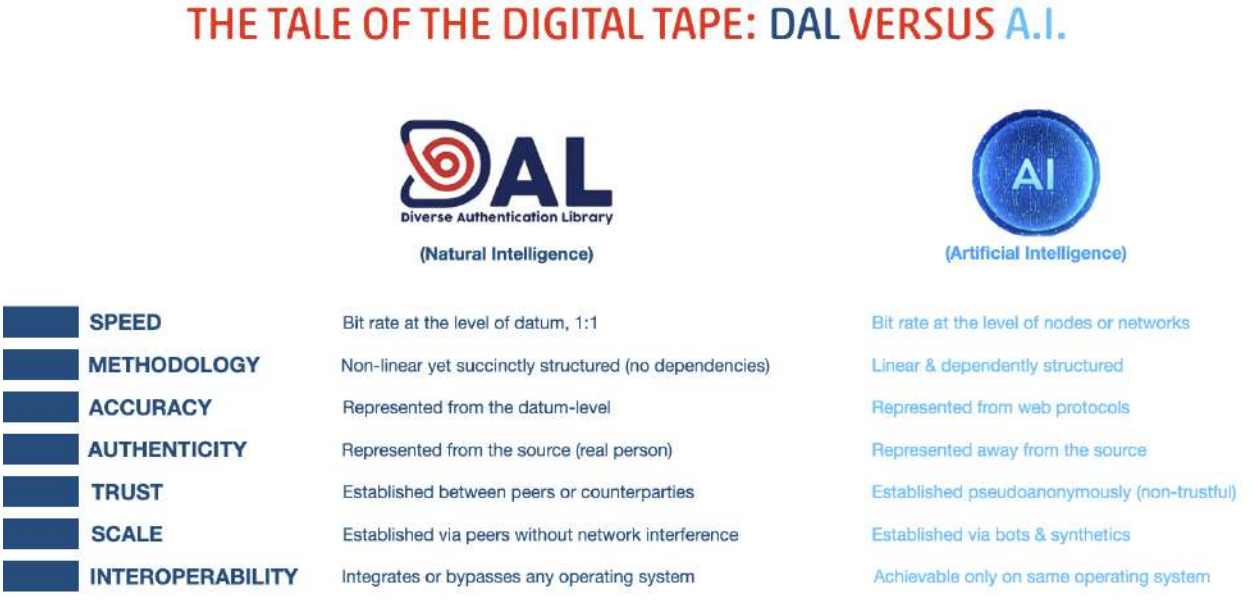


DAL's Web4 Post-PGP, Post-Quantum Security at a glance

MATH	MATH OR LANGUAGE	MATH + LANGUAGE
AES	PQC	W4S
(Advanced Encryption Standard)	(Post-Quantum Cryptography)	(Web4 Security)
Protocol-Based Elliptical Curves	Protocols Applied to Web Objects	Complete Object-Orientations, SuperKernels
Largest solvable key size: 795-bit (2019)	Indeterminable Key Sizes	1-Bit Binary Representations (no key limits)
RSA-Focused Algorithms	Shor's/Grover's Algorithms	Holonomial Algorithms (instances)
Lots of SSH exploits	SSH Incompleteness (some traceability)	SSH Completeness (no traceability)

GENERAL COMPARISONS TO CORE AI METHODS

It is important to note that W4S is a standard that we have evolved over the last 25 years, ever since object-oriented architectures and object-oriented programming began with Delphi and related approaches. One of the main patterns we saw in our early development were major inconsistencies in the way artificial intelligence was conceived by the likes of Marvin Minsky, John McCarthy, and Geoffrey Hinton. Mainly we saw that reductionist and deterministic approaches (linear methods) could never achieve full data representation. We also saw that as time went on, these same approaches made information systems like search engines or large databases more inefficient and of worse quality, not better.



THE TALE OF THE DIGITAL TAPE: DAL VERSUS A.I.

	DAL Diverse Authentication Library (Natural Intelligence)	AI (Artificial Intelligence)
SPEED	Bit rate at the level of datum, 1:1	Bit rate at the level of nodes or networks
METHODOLOGY	Non-linear yet succinctly structured (no dependencies)	Linear & dependently structured
ACCURACY	Represented from the datum-level	Represented from web protocols
AUTHENTICITY	Represented from the source (real person)	Represented away from the source
TRUST	Established between peers or counterparties	Established pseudoanonymously (non-trustful)
SCALE	Established via peers without network interference	Established via bots & synthetics
INTEROPERABILITY	Integrates or bypasses any operating system	Achievable only on same operating system

More simply put, if garbage is going into a system, only garbage can come out. When it comes to information, garbage can "look good" or "sound good" without having any semblance of truth or authenticity. Our digital realities and our media platforms corroborate this reality: We are living in **an era of untruth**.

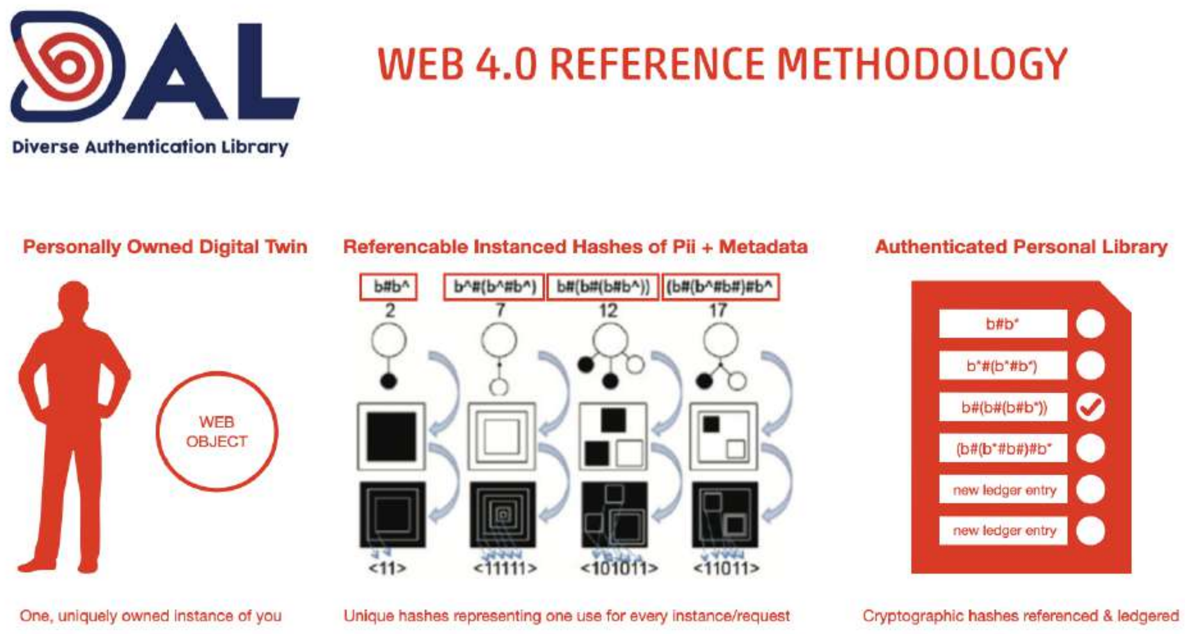
The only way out? To change our approaches to information, and build many alternative systems from the ground up. This begins and ends with a real identity based on the real interactions of a real human being, maintained and protected by that person's own reference library.

To be clear, there is nothing wrong with AI as a tool for simulating patterns and automating processes. When AI is used to facilitate naturally occurring data and naturally occurring interactions in which the core data is secured as an evidentiary natural function of a real human being, then the results can be quite positive and quite powerful. But to rely on AI as the core function of pervasive intelligence is akin to making an island of smart people the arbiters of what is intelligent and what is not. This becomes a double-fold problem in which the perception of intelligence cancels itself, even if every person on the island "agrees" to what intelligence is as a concept. In other words, there is no collective consensus on true intelligence, just as there is no collective consensus established in science, nor its methods.

The only thing *we can do* is preserve, protect and exchange what is real, what is provable, and what is applied as agreed between counterparties. The rest is up to evolution and the laws of nature.

CONCLUSION

Now we can fully understand how a **singly instanced digital twin identity** is protected and referenced in a library that keeps a precise record of the data in hashes, but not a precise record of the data itself. The only way for the underlying data to change is for the person to provide the change, provided there are no inconsistencies in the reference to their original bodily data. In other words, whatever new data that are entered must also reference and match the person's original/physical DNA, Fingerprint, and Iris data.


DAL
Diverse Authentication Library
WEB 4.0 REFERENCE METHODOLOGY
Personally Owned Digital Twin
WEB OBJECT
One, uniquely owned instance of you
Referencable Instanced Hashes of Pii + Metadata
b#b^
b^#(b^#b^)
b#(b#(b#b^))
(b#(b^#b#)#b^
2
7
12
17
<11>
<11111>
<101011>
<11011>
Unique hashes representing one use for every instance/request
Authenticated Personal Library
b#b^
b^#(b^#b^)
b#(b#(b#b^))
(b#(b^#b#)#b^
new ledger entry
new ledger entry
Cryptographic hashes referenced & ledgered

Between Succession, Proof of Evidence and Forensic Cryptography, the team at DAL is poised to make a significant mark on Identity Management now and well into the future. One of the great failure points in identity management has been the inability to regard the physical presence of the human being as vitally important to one's existence in "the matrix" of a digitized world, in addition to the fact that forensics has been rendered impotent without this establishment of a real persona. It is incumbent upon all of us to regard identity as both a truly human endeavor, and one that uses forensics to protect the human being at all stages of work and life. In a digital world that has chosen to disregard human life at the whim of a bot or a fake persona, there is no greater time to answer this clarion call.