GOODE INTELLIGENCE
YOUR PARTNER FOR BUSINESS RESEARCH & ANALYSIS

AN INTRODUCTION TO GADI:

the Global Architecture for Digital Identity

CONTENTS

AN INTRODUCTION TO GADI

This is a white paper from Goode Intelligence that introduces the Global Architecture for Digital Identity (GADI), the Global Trusted Platform of the DID Alliance [1]. The DID Alliance is an open industry association created to drive the development of a standardized, interoperable framework for decentralized identity services to ensure the authenticity of an established trust in digital identities.

The study has been developed with the cooperation of the DID Alliance and includes interviews with leading global stakeholders from the industry including its members. It investigates the current problems with digital identity including fragmentation, duplication, a lack of ownership and control for identity owners, and weak binding between physical and digital identity.

Firstly, it is vital to start by defining what digital identity is.

[1] https://www.didalliance.org/

WHAT IS DIGITAL IDENTITY?

Defining online Digital Identity is difficult. According to NIST, proper definition of digital identity requires the knowledge of the "context of use in order to arrive to a single definition that satisfies all". [2]

Information that makes up a digital identity can also be grouped into two high-level categories, digital attributes and digital activities. Digital attributes (inherent) include name, date of birth, social security and national ID numbers, biometric data and bank details. Digital activities (inherited or behavior) include social network interactions, financial transaction history and search queries.

[2] NIST Special Publication 800-63 Revision 3 Digital Identity Guidelines. https://pages.nist.gov/800-63-3/sp800-63-3.html

CURRENT CHALLENGES WITH DIGITAL IDENTITY

Despite significant advances with digital identity, the industry is still struggling with a variety of problems that include trust and accountability, fragmentation, duplication, a lack of ownership and control, and a lack of binding between physical and digital identity.

Organizations wanting to solve the identity problem are often left with a bewildering choice of competing identity models that can lock an organization into a solution that may be considered inappropriate in the future.

This study explores some of the major issues with digital identity in the following sections.

TRUST AND ACCOUNTABILITY

Trust and accountability are the bedrock of society. However, they are both lacking in many facets in the way identity is currently managed online. There is little identity verification when accounts are created for much of the world's major social media and messaging services.

In this era of fake news, there is declining trust in the source and a lack of accountability in who is actually publishing many news stories, especially when they are published on popular social media sites.

The accelerating speed of the internet means that a news story will break and be widely shared across social media platforms without a clear understanding on the identity of the author and the authenticity of the story.

Social media platforms, eager to increase active user numbers, have little control mechanisms in place to sufficiently verify the account owner's identity, coupled with limited regulation to enforce robust identity verification on account opening.

FRAGMENTATION & DUPLICATION

Fragmentation and duplication of digital identity creates confusion for users and complicates implementation choices for Identity Issuers and Service Providers.

Digital identity consists of thousands of data points that create a unique profile of who you are and what you are allowed, or not allowed, to do. Our digital identities are fragmented across the internet, owned by a variety of data owners including governments, financial institutions, large technology companies, credit bureaus and social network providers.

This poses a series of problems including the cost of accessing these fragmented pots of identity information by entities seeking to verify these data points and the risk of data breach with so much of our personal data stored by so many different entities.

Identity information is also overly duplicated across multiple entities creating an extremely inefficient

system that is onerous for users. Each time a digital identity is verified and created by a service provider, similar pieces of identity information are collected; name, birthdate, address and social security and national identity numbers. There is a cost for both user and service provider in this situation; a financial cost to the service provider in verifying a user's identity and friction cost for the user in having to provide identity information, sometimes difficult to remember, each time they create a new account and digital identity.

A study published in July 2020 found that at least 39 different organizations hold personal data of the average UK citizen and that almost a quarter of UK citizens are unaware of how many organizations hold their personal data. [3]

The fundamental question is why do organizations need to collect identity documentation and information that has already been collected and verified elsewhere?

LACK OF OWNERSHIP AND CONTROL OF DIGITAL IDENTITY

The majority of today's identity-related interactions are controlled by centralized authorities that demand users to disclose sensitive and commercially valuable personal information. This relationship is often heavily weighted in favor of the identity providers who are often too willing to capitalize on this information at the expense of their customer's privacy.

Despite the advancement of data privacy legislation, once identity information is handed over to a requesting organisation, an individual loses control of it and has little control as to where that information may end up. Monetization of personal information is a common motivation for many internet companies.

This unbalanced relationship leads to a significant negative cost, to both the user and the identity provider. Identity theft, spam email, phishing attacks and fraud are all direct consequences of this broken system.

According to Verizon, in 2018, 14.4 million people in the USA were affected by identity theft. [4]

The shift towards decentralized identity (DID) and the development of 'Self-Sovereign Identity' (SSI) promises to mitigate and eliminate these issues by placing the user in control of their own identity assets (identity information and credentials).

[3] https://www.nomidio.com/
[4] https://www.verizon.com/info/digital-security/identity-theft-what-to-do/

However, SSI is not the panacea that the identity industry envisaged and introduces its own set of challenges including:

- Lack of interoperability between Decentralized Identity Platforms (DIPs) – siloed ecosystems
- DIDs are generally self-asserted without trust anchors
- Not-inclusive – limited to smart device users
- Identity Issuers and Service Providers have to pick a winner in this space – hoping that they have chosen to integrate with the one 'winning' stack
- A focus on security and privacy and not on trust and accountability
- Low acceptance rates
- Seen as revolutionary not evolutionary – excludes existing identity providers and networks
- Key recovery issues when changing smart devices
- Lack of economic imperative – new technology needs sustainable new business models to flourish

LACK OF BINDING BETWEEN PHYSICAL AND DIGITAL IDENTITY

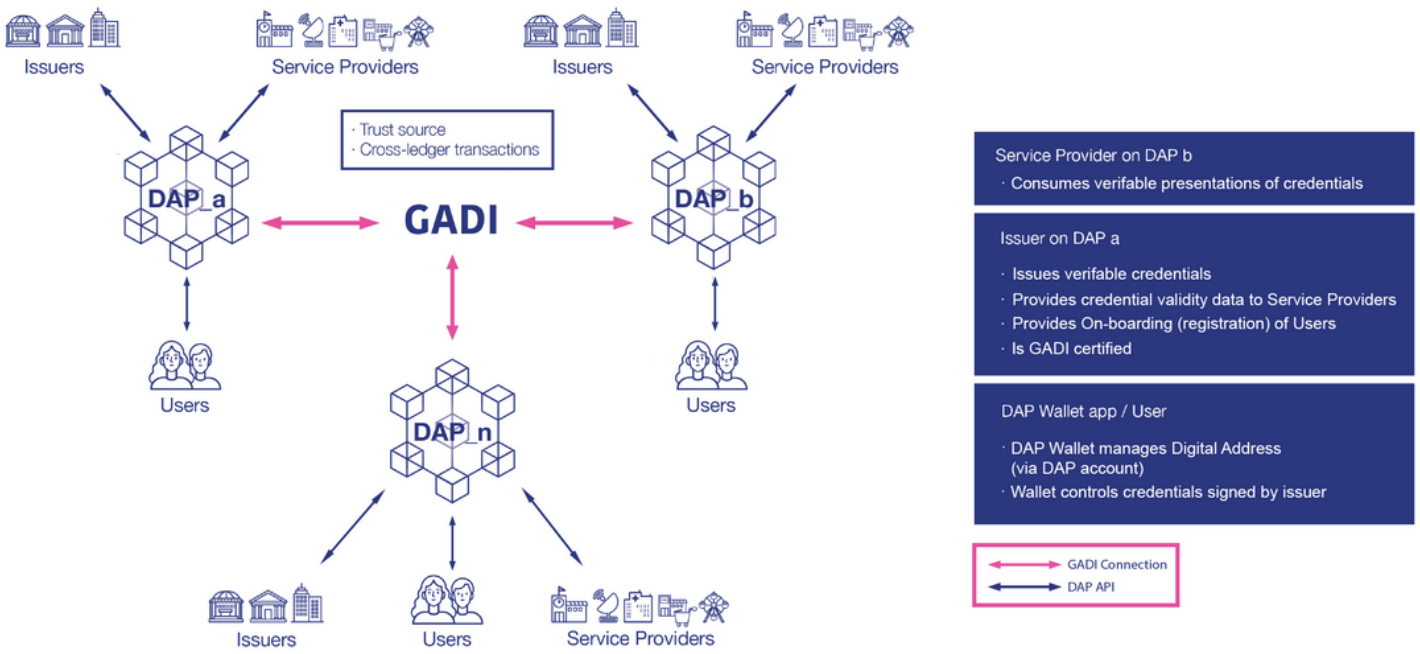
One of the greatest challenges in any digital identity system is connecting, or binding, a physical identity with a logical identity. The question of how to bind an individual to a digital representation of that individual has proven to be a challenging one.

Identity verification or proofing is one method in which a combination of trusted, normally government-issued, documents (passports, driving licenses and national ID cards), biometric data, nominally face, and other identity information can be linked to verifiable digital identity credentials to form effective binding between physical and digital identity.

A major problem with the current approach is that there is no one source for a verified digital identity, a unique digital address that acts a trust anchor. Users have to repeat similar processes each time they are required to prove their identities. This is inefficient, adds friction for users and is costly for service providers.

INTRODUCING GADI
A VISION OF TRUST

GADI enables DAP interoperability



The Global Architecture for Digital Identity (GADI) is the Global Trusted Platform of the DID Alliance [1]. The DID Alliance is an open industry association created to drive the development of a standardized, interoperable framework for decentralized identity services to ensure the authenticity of an established trust in digital identities.

There is a great deal of excellent work and standardization efforts being carried out in shaping next generation DID systems with significant investment in solving the digital identity problem that forms the foundation of what the DID Alliance and GADI is setting out to achieve.

The mission of the DID Alliance is to establish a new trustable identity framework by providing a unique digital address to everyone which empowers them to control their distributed personal identity data to reinforce trust and accountability in the real or digital world.

The DID Alliance seeks to fulfil the promise of DID systems by helping to solve some of the most important practical problems attached to their operation and adoption by enabling a business interoperability layer as well as a technological one.

At the heart of GADI is the Digital Address; the Digital Address is a special GADI identifier issued to an individual by a certified Digital Address Issuer after Know Your Customer (KYC) processes have been followed.

Trust, **Accountability**, **Inclusiveness** and **User Ownership** are at the heart of GADI.

This section introduces the vision of GADI, outlining its main components and major benefits.

[1] https://www.didalliance.org/

GADI – VISION AND BENEFITS

Introduction
Ramesh Kesanupalli, Founder of FIDO Alliance and Co-Founder of DID Alliance has been instrumental in creating the vision of GADI working together with Soonhyung Lee of Raonsecure and Abbie Barbir of CVS / Aetna along with other key industry players. Their vision for GADI is to achieve true interoperability among DID systems by deploying requisite technologies and processes that are outside the scope of existing interoperability efforts such as W3C, DIF, and Hyperledger Aries.

GADI enables cross-ledger authentication, empowering identity platforms to cooperate to provide global coverage. It enables service providers to trust any Verifiable Credential (VC) from any identity platform and a mechanism in which to settle transaction costs via a process called GADI Token Exchange.

Benefits of GADI include:

- Solves the problem of a universal portable digital identity with every person having their own unique Digital Address
- Provides a mechanism for interoperability across DID platforms
  - GADI eliminates the need to implement a separate set of cross-ledger features for every system that it interacts with. With GADI, each DID system only needs to integrate the GADI SDK enabling them to connect to with every GADI member entity
- Identity issuers, including government ID issuers, retain identity information with GADI supporting monetization of verification process - with the associated personal identity data (PID) remaining safely with the original identity Issuer, organizations within countries with strict data export controls are still able to participate, since no PID crosses borders
- Solves the re-enrolment problem for credential recovery - Smartphone replacement
- Privacy through Zero-knowledge proof (ZKP) – no need to share private information
- Inclusiveness – A user's Digital Address can be stored on a number of media

Zero-knowledge proof (ZKP) definition: A zero-knowledge proof (**ZKP**) is a cryptographic method which allows one person (the prover) to prove to another person (the verifier) that they have the possession of some information without revealing the information to the verifier. An example of this is date of birth; ID documents, e.g. ID cards and driving licenses, are often used as a means of proving age. However, they also have other private identity information about the owner. This information is very valuable to identity thieves. ZKP can be used to create a digital copy of the ID document that allows an entity to verify a person's age (is the person over 21?) without actually having to provide the exact date of birth.

In pursuit of this objective, GADI's efforts are directed to three main areas:

1. Trust sourcing
2. Cross-ledger transaction support
3. Inclusiveness

Trust Sourcing
Decentralized Identifiers (DIDs) are a type of identifier that enables a verifiable decentralized digital identity. While existing standards support decentralized identity systems to parse credentials issued by other entities, relying parties struggle to make authorization decisions. This is because relying parties are struggling to answer a number of critical questions about the issuance of these credentials including:

- What are the jurisdictional limits of the credential?
- What type of identity verification (proofing) was performed to issue the credential?
- How is the relying party indemnified?
- What are the transaction types for which the credential may be used?
- What are the exception-handling procedures in case of trust failure?

GADI will provide the trust framework to enable relying parties to answer these questions and will do so in the following way by:

- Instituting standardized credential-issuance procedures and semantics
- Certifying credential issuers according to published requirements for specific credential types
- Binding each credential type to a set of real-world contracts

This trust sourcing allows a relying party to know the precise meaning of any GADI-imprinted credential to allow them to make an accurate authorization decision.

Cross-ledger transaction support
Lack of interoperability between disparate DIDs is often cited as a weakness for these systems. One of GADI's primary goals is to enable full cross-ledger interoperability among member systems.

Existing DID standards efforts are becoming more mature in terms of

providing format and protocol-level interoperability among disparate DID systems but still come up short in terms of supporting full cross-ledger interoperability among member systems.

GADI aims to provide the vehicle for fulfilling cross-ledger interoperability by supporting a distributed ledger that acts as an exchange platform for DID-related transactions.

This also provides a mechanism in which to settle cross-ledger payments via third-party market makers, which are able to provide liquidity among token types, enabling a truly agnostic inter-ledger ecosystem.

GADI not only provides the foundation, through agreed protocols, to support cross-ledger interoperability but creates clearly defined economic models that underpin the technology.

Creating new revenue streams for government passport offices

Digital identity verification is rapidly growing as a direct result of digital transformation initiatives and has seen increasing growth due to the COVID-19 emergency. Account opening is moving online, and service providers demand a secure and safe method to verify identity. Document verification, such as a government-issued identity document, passport, driving license or national ID card, is used as a proof of identity and is an important component for identity verification. Identity documents are scanned in remotely using smartphone cameras and then authenticated to ensure they are valid and not forged. As this involves scanning printed documents there is currently little or no verification against the issuer's (government) digital infrastructure, and more importantly, no way in which the document issuer (passport office) can monetize this process. If these documents were offered as verifiable digital credentials and infrastructure was in place to support the verification of these credentials, then government departments would have a method to monetize identity and document verification. The GADI exchange ledger provides the mechanism to support this scenario and by design protects the privacy of the verified individual as they would no longer be scanning in an entire identity document.

Inclusiveness

Despite many developed regions having over 100 percent penetration rates for smartphone ownership, there is still 45 percent of the world's population that does not have them. [6] Further, The World Economic Forum (WEF) estimates that over a billion people in the world do not have a formal identity.

A significant shortcoming of existing DID systems is that they are heavily dependent on technology – owning a smartphone and accessing the internet.

Designing an inclusive system is an important aim for GADI and is a central goal of the DID Alliance.

DID Alliance has developed a solution for the inclusiveness problem by providing a set of protocols through which users can interact with a proxy system designed to interact with DID systems.

[6] https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

The solution involves a range of solutions that do not rely on smartphone ownership, where identity tokens can be biometrically bound to a user through a template-less algorithm and potentially stored on a smartcard. A user's digital address can be stored on any surface through a 2D barcode with the user's consent, using the service provider's system.

To verify identity information, service providers will be equipped with GADI-authorized token readers that will interact with the GADI trust proxy to authenticate on the user's behalf. The trust proxy then retrieves the appropriate data for the transaction and performs the authentication with the service provider's system.

THE GADI DIGITAL ADDRESS

Fundamental to GADI is the Digital Address, a special identifier issued to an individual by a certified Digital Address Issuer and unique for an individual.

The creation of a Digital Address is a vitally important step in ensuring there is both trust and accountability within the GADI ecosystem.

When we are born, we are given our first identity credential by our parents or guardians in the form of a name. Governments register these new arrivals onto a registry list and then issue a birth certificate, a paper document that contains other identity related information, e.g. date of birth, parents' names and place of birth. This official document becomes the trust anchor that breeds other identity credentials such as a health service number, social security number, passport, driving licenses, national ID cards and marriage certificates etc. It is also the foundational identity document that is used to verify identity when we are awarded education certificates and get onboarded for employment. Each time we are issued with a new identity credential, it can be linked back to the trust anchor, the birth certificate, and our identities are strengthened by a chain of verification and custody.

The GADI Digital Address is the digital equivalent of a birth certificate. When a person is on-boarded to the GADI ecosystem, by a certified issuer, a Digital Address is created that becomes a verifiable trust anchor for all subsequent transactions. This Digital Address is created under a legal framework that governs the GADI ecosystem by certified issuers. Its creation is also bound by strict Know-Your-Customer (KYC) rules that are comparable with the issuance of government identity credentials. Each time the Digital Address is verified it matures and is strengthened through interactions with identity issuers and relying parties.

Digital Address Issuers could be financial service providers, government agencies, education providers and enterprises; organizations that are central to the trust economy.

A GADI Digital Address is created by an issuer and will be be formed by identity-related traits, including biometric data, first name, last name, date of birth, city of birth, etc.

The Digital Address will be created by applying a hashing algorithm and will be in cooperation with a participating Digital Address Provider (DAP).

Digital Address Providers (DAPs) are solution providers who are currently providing DID-related identity services. DAPs make use of a Digital Address and the GADI system to handle credential requests on behalf of either service providers or issuers (or both) that reside on other DID-based identity chains (or the equivalent). The Digital Address is like a unique signature that is registered to the GADI DLT.

The Digital Address can be delivered to smart mobile devices, to a FIDO-secured credential wallet, or, in the spirit of inclusiveness, be stored on a smartcard. In both cases, the Digital Address is strongly bound to the individual user by the combination of identity attributes and other attributes as provided by an issuer.

Once created, the Digital Address becomes the primary trust anchor with additional identities connected to it. Connectivity and interoperability are achieved by leveraging existing communications protocols including Hyperledger Aries [7] and DIDCOM by the DIF. [8]

[7] https://www.hyperledger.org/use/aries

[8] https://identity.foundation/working-groups/did-comm.html

SUMMARY

Despite significant advances with digital identity, the industry is still struggling with a variety of problems that include **trust and accountability**, **fragmentation**, **duplication**, a **lack of ownership and control**, and a **lack of binding between physical and digital identity**.

Organizations wanting to solve the identity problem are often left with a bewildering choice of competing identity models that can lock an organization into a solution that may be considered inappropriate in the future.

The Global Architecture for Digital Identity (GADI) is the Global Trusted Platform of the DID Alliance [9]. The DID Alliance is an open industry association created to drive the development of a standardized, interoperable framework for decentralized identity services to ensure the authenticity of an established trust in digital identities.

The mission of the DID Alliance is to establish a new trustable identity framework, built on the excellent work already developed, by providing a unique **digital address** to everyone which empowers them to control their distributed personal identity data to reinforce trust and accountability in the real or digital world.

The DID Alliance seeks to fulfil the promise of DID systems by helping to solve some of the most important practical problems attached to their operation and adoption by enabling a business interoperability layer as well as a technological one.

At the heart of GADI is the **Digital Address**; the Digital Address is a special GADI identifier issued to an individual by a certified Digital Address Issuer after Know Your Customer (KYC) processes have been followed.

Trust, **Accountability**, **Inclusiveness** and **User Ownership** are at the heart of GADI.

[9] https://www.didalliance.org/

About Goode Intelligence

GOODE INTELLIGENCE
YOUR PARTNER FOR BUSINESS RESEARCH & ANALYSIS

Goode Intelligence is a leading identity, authentication and biometrics research, consulting and events organisation founded in 2007, headquartered in London, UK.

For more information on this or any other research please visit www.goodeintelligence.com
Follow us on Twitter.

About DID Alliance

The DID Alliance is an open industry association created to drive the development of a standardized, interoperable framework for decentralized identity services to ensure the authenticity of an established trust in digital identities.

For more information on the DID Alliance please visit https://www.didalliance.org/