The Case for a Unified Identity

Our Vision for a Unified Identity Protocol on the Tangle for Things, Organizations, and Individuals

Written By:
Jelle Femmo Millenaar
& Mathew Yarger

Content

Executive Summary

This whitepaper outlines the IOTA Foundation's vision for decentralized digital identity, to help tackle the problems of privacy and trust on the internet. We call this the Unified Identity Protocol (UIP).

Building on the W3C Community Group's proposed standards for Decentralized Identifiers (DID) and Verifiable Credentials, the IOTA Foundation's Unified Identity Protocol will enable things, organizations and individuals to identify themselves online. Under this system, users will be able to prove that their information is verified and endorsed by trusted parties and is communicated peer-to-peer without the need for observers, both increasing privacy and trust. Value and data transactions can now have an optional, identifiable source, creating trust in the provenance of transactions.

As a form of Self Sovereign Identity (SSI), the proposed solution enables explicit control over identity creation and management. The added verifiable credentials strengthen a digital identity and provide proof of physical properties in digital form. This bridges the gap between the physical and virtual worlds, solving longstanding limitations for identification on the internet. The protocol is built with "Data protection and Privacy by design" and is compliant with the privacy and data management laws around the world, such as the European General Data Protection Regulation (GDPR).

With IOTA at its core, the solution forms a neutral and trustworthy protocol for identification. There is no controlling party in the network, incentivized by profit-making, nor does the network have any form of access control. The network is public and permissionless, so anyone can participate on their own terms. IOTA's feeless transactions ensure that identity management is functionally free. Using IOTA as a base yields a number of other benefits, including quantum robustness - thereby future proofing the protocol against quantum threat - together with near real time transfers and high scalability - essential properties for establishing a global solution.

While digital identity often focuses on human self sovereign identity, this solution provides a Unified Identity. Not only people, but also organizations, devices and even objects can obtain an identity. IOTA presents a platform to unite identity under one unified protocol, with frictionless interaction between all identity types. People will be able to identify and trust other people and organizations online, reducing fraud, while devices will be able to trust other devices, drastically increasing the security of systems. In a future where everyday objects are connected, trusted human-to-machine interaction will be enabled through a trustworthy, neutral and secure Unified Identity Protocol.

Introduction

The internet forms the basis for many of our interactions in the modern world. It has created new business opportunities, better customer experiences and improved our day-to-day lives. However, it lacks essential properties of trust and privacy.

There are three levels of privacy when interacting on the internet: full privacy, verifiable identities and pseudonymity. With full privacy, neither parties, nor observers, can identify the interacting parties. With verifiable identities, parties can trust each other, because they can both provide proof about their identities. With pseudonymity, both parties recognize each other through a pseudonymous identifier. Pseudonymity is the default setting of the internet. However, data harvesting platforms, like Google and Facebook, can now link these "random" identifiers, though imprecisely, to identities in the real-world. The associated data and insights have become extremely valuable to advertising agencies, product developers, and numerous local and global businesses.

Internet users have developed a need to identify themselves online and share their experiences and personal information with each other. This trend, which began with forums, blogs and IRC chats, later developed into today's Social Media, showed a desire to be identifiable online. But this trend only served giants such as Facebook and LinkedIn further, able to gather ever more accurate profiles about their users. These profiles are so extensive that many internet services rely on them as a definitive representation of their users. However, the information put on social media is not verified. Impersonation and fraud remain threats, highlighting the persisting intrinsic lack of trust.

The need for verifiable personal information can be fulfilled by digital identity. Digital identity allows users to bridge the gap between the online and the real-world. When users provide personal information to someone online, in a "Bring Your Own Identity" (BYOI) manner, they will be able to prove that their personal information is perfectly accurate. Whereas in the current system, where companies like Google and Facebook provide an estimation of identity, there can be insufficient depth to user profiles or, in some cases, the information is altogether false.

With digital identity, the user can decide what information to share and with whom they would like to share it. This will maintain and even improve people's online privacy, while allowing many new features and new business opportunities. Businesses will be able to trust BYOI information, enhancing interactions between company and customer, but also reducing fraudulent cases and endemic security risks.

> *Verifiable digital identities provide the ability to prove real-world attributes online.*

The Solution

Using the standards proposed by W3C, this whitepaper will further discuss the **Unified Identity Protocol (UIP)** as an implementation of digital identity on IOTA. Using this protocol, a new digital identity can be created by anyone or anything at any time. To do so, a Decentralized Identifier (DID) is generated, that serves as a reference to a DID Document. The **DID Document** contains public keys, and other mechanisms, to enable the subject to prove their association with the DID. However a DID alone tells you little about the subject. It must be combined with Verifiable Credentials. Verifiable Credentials are statements about the creator of the DID. They can be shared and verified online in a BYOI manner, and the DID creator remains in complete control of the process. This framework can be used in processes such as:

Address validation: Customers can prove where they live for shipping and billing addresses

Age verification: Customers can prove they are 18+ for online purchases.

(Authority) Login: Customers can prove who they are and gain access to their account, without passwords. This can be useful for many websites, including eGovernment and banking.

The Three Roles of Digital identity

There are three different roles within the digital identity framework (Figure 1):

01 — HOLDER

This is usually the subject of the digital identity. They have generated their DID and cryptographic keypairs. Their personal data and private keys are under their own control.

02 — ISSUER

An issuer is a trustworthy party on a specific topic. They have their own digital identity. The Issuer provides a user with verifiable credentials, which they sign using asymmetric encryption.

03 — VERIFIER

A Holder shares their verifiable credentials with a Verifier to prove a statement about themselves. The Verifier is able to verify the credentials by performing the following verifications:

A **Data Integrity**: Are the credentials signed by the expected parties?
B **Issuer Trust**: Is the credential unaltered?
C **Signature Verification**: Do I trust this Issuer to provide these credentials?
D **Validation**: Is the credential still valid?

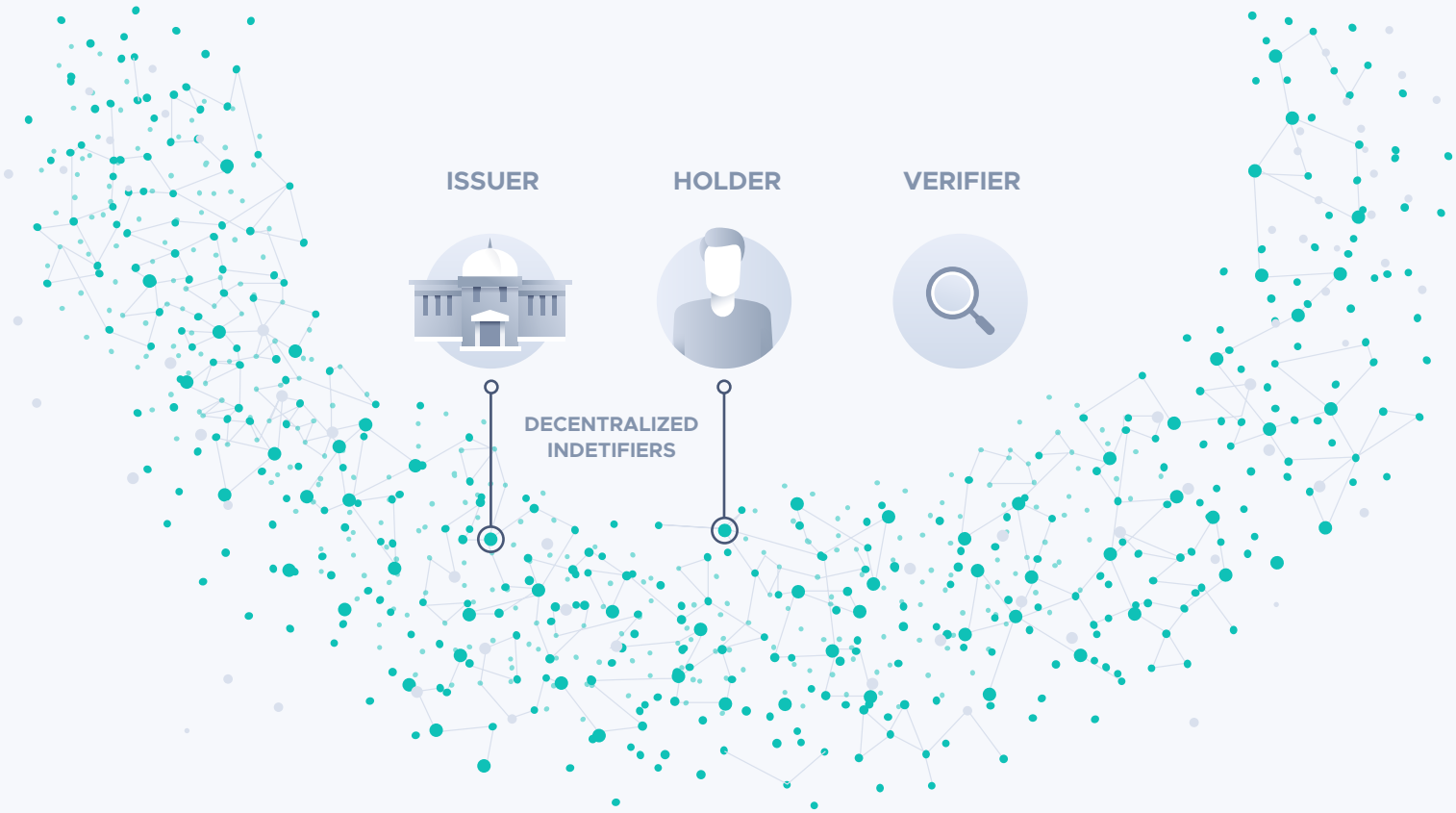

Figure 1: The Three roles of digital identity. The DID Document of Issuers (and optionally Holders) are uploaded to the Tangle, which acts as a decentralized public key registry.

Building a digital identity

The Holder can build up an online profile by collecting verifiable credentials from organizations they interact with and trust. These credentials give the Holder more autonomy over their personal data, allowing them to choose what information they share about themselves online. When a Holder seeks a new credential, the Holder first verifies themselves to the Issuer by logging into the Issuer's environment. The Holder shares their DID with the Issuer and requests the credential. The Issuer signs the credential and enclosed statements about the Holder with a cryptographic keypair registered in their own DID Document. The credential is then sent to the Holder and stored (Figure 2). The Holder now has complete autonomy over how they use this credential. Meanwhile, the Issuer can later revoke the credential, causing any future attempts by the Holder to use the credential to fail.

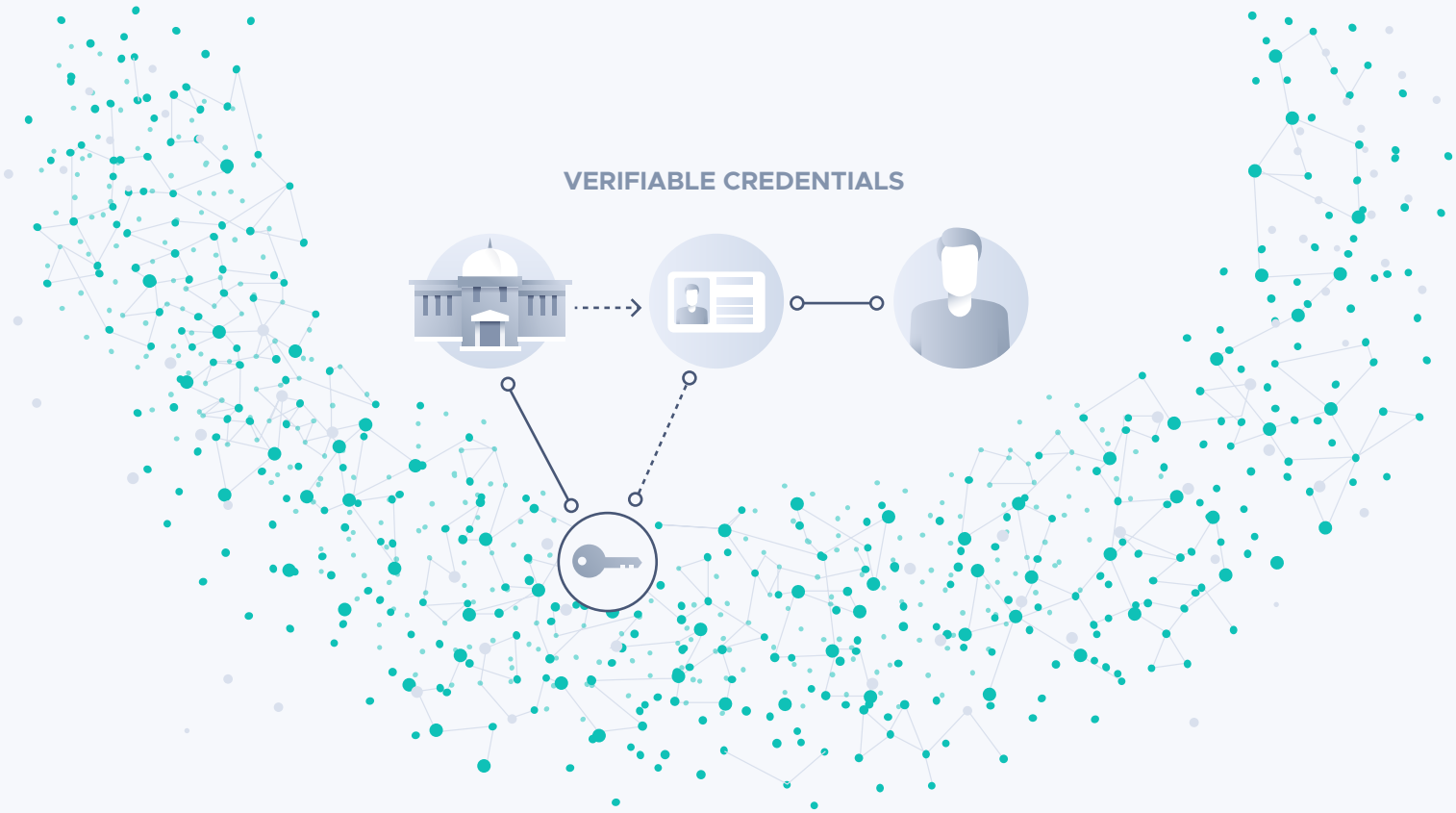

Figure 2: An Issuer provides a Verifiable Credential to a Holder. This credential is signed using a cryptographic keypair, registered in their DID Document stored on the Tangle.

Using a digital identity

When a Verifier needs to know certain information about the Holder, the Holder can choose to send the Verifier those specific attributes (Figure 3). The information can be exchanged quickly through various technologies like NFC, Bluetooth, QR, the Tangle etc. The Verifier now has a copy of the information and details of which Issuer signed the credential. The Verifier then decides if they trust the credential's Issuer and verifies their signature on the Tangle. This process guarantees that the Issuer is trusted, has signed the data, and that the data has not been altered after the signing process. In addition, not all the information needs to be revealed. Using cryptographic techniques, such as zero-knowledge proofs, users can choose to share as little information as possible. For example, instead of sharing a full copy of a driver's license, the user need only prove that they own a driver's license.

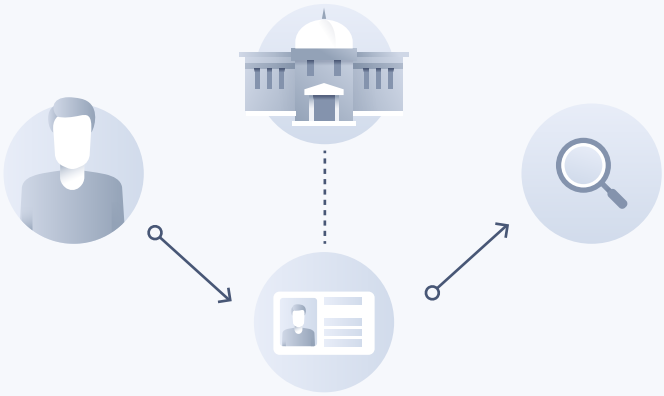

Figure 3: The user shares their information with a third party. The third party compares it to the signature on the Tangle. They verify which entity it was signed by and confirm that the data has not been altered.

Why IOTA: Our Solution

IOTA is a scalable and feeless Distributed Ledger Technology (DLT). Similar to Blockchain technology, IOTA provides an immutable and decentralized ledger that can transact value through the IOTA token. Unlike Blockchain, IOTA uses a non-linear data structure called the Tangle which makes it feeless and vastly more scalable (Figure 1, 2). The Tangle also facilitates feeless transactions of data, such as DID registrations and credential revocations. As a single source of truth and trust in data, the Tangle can provide the trust infrastructure in a highly networked world.

Future Machine Economy

The Machine Economy Starts with Enabling Digital Trust

ECONOMY OF THINGS	IOT/enabled Business Models Permissionless Ecosystems	Impact full ecosystem and value chains new data/driven business models
REAL TIME TRANSACTIONS	Zero Fee Real Time “Machine Ready”	First real world deployment at scale of transactive M2M cases
DIGITAL TRUST	Data Integrity Cybersecurity Identity	Technical building blocks & understanding of the cross-silo data integrity challenges

IOTA is uniquely suited for the Unified Identity Protocol. The network is designed for both humans and devices, providing a platform for trusted communication between individuals, organizations and things. The IOTA Foundation’s principles of full transparency, openness and permissionless innovation provide an open and neutral environment:

01 **Permissionless & Decentralized:** Unlike a permissioned network such as Hyperledger or Corda, everyone can participate in consensus without being granted access. No party incentivized by profit-making has collective control over the network (unlike all blockchains). This makes IOTA neutral and censorship-resistant.

02 **Public:** Everyone can observe (unless using optional encryption) the transactions in the network. The network is inherently transparent.

03 **Feeless**: All data and value transactions on the network are free. Unlike other DLTs such as Bitcoin or Ethereum, registration and communication of identities can be written to the network without a requirement to purchase a cryptocurrency token.

04 **Open Source**: Everyone can view and contribute to the code.

The Tangle provides a secure and scalable layer of trust, well-suited to the UIP:

01 **High scalability:** Increasing network activity with more transactions decreases transaction settlement times, unlike in a traditional blockchain.

02 **Near Real-Time:** No block times, or lengthy validation periods. Transactions and data can be published, validated, and consumed within relatively short timespans.

03 **Low resource requirements**: Designed to allow micro and IoT devices (e.g. sensors and microprocessors) to participate, securing data at the source of aggregation.

04 **Secure data transfer**: Data is encoded to allow secure data transfer, storage and referencing. It can be organized in data streams for easy querying and access control.

05 **Quantum robustness**: IOTA's signature scheme is robust against the next generation of computing.

06 **One-Time Signatures:** IOTA addresses are used only once, reducing correlation and linkability between transactions.

Data must be immutably stored on a distributed ledger to ensure the decentralized nature of the digital identity protocol. With the network's continual uptime, credentials are always verifiable without a dependency on the servers of credential issuers. This system also increases individual privacy, because contact with the Issuer is removed from the interaction between Holder and Verifier. Issuers will not be able to track when and how often the Holder uses their credentials. The flexibility afforded of the Tangle means that the digital identity framework remains extendible in the future.

Within the digital identity framework, the Tangle is used for the following functionalities:

01 **Public Key Registry**: The Tangle enables a decentralized public key registry for Issuers using DID standards. This allows Verifiers to verify a signature without a reliance on a centralized server. The DID standard also adds service endpoints, extending the usability of Identities beyond a public key registry, to, for example, registering verifiable credential standards.

02 **Revocation**: A verifiable credential can be revoked, meaning it will no longer be able to pass verification. The revocation is immutably stored on the Tangle, making sure no Holder can attempt to use their revoked credentials.

About the IOTA Foundation

The IOTA Foundation is a non-profit foundation incorporated and registered in Germany. The IOTA Foundation's mission is to support the development and standardization of new Distributed Ledger Technologies (DLT) based on the IOTA Tangle. As of November 2019, the IOTA Foundation consists of a global team of over 120 individuals distributed in 23 countries and a growing ecosystem of leaders and partners working together to create a digital trust infrastructure.

A Unified Identity

When discussing digital identity, the subject of discussion is usually digital identity for people. But in order to enable digital identity, we also need corporate identities to issue the credentials. The discussion usually ends there. But in the future, devices will be a big part of our day-to-day lives. Devices will be upgraded to become part of the Internet-of-Things (IoT), allowing autonomy and automation. Things will be able to make decisions and transact value and data in a public ecosystem. But they will need to be able to build trust and discern which other actors in the ecosystem are trustworthy. Identity of Things (IDoT) can enable these requirements. Similarly, objects without electronic circuitry also have a need to be identified, such as in the supply chain.

With multiple different types of actor requiring an identity protocol, it is a strong proposition to use the same underlying protocol for all of them. This Unified Identity Protocol will enable anyone or anything to create a digital identity, build an online profile of trust by collecting verifiable credentials, and share them with other actors they interact with. Interaction between people, companies, things and objects becomes seamless. And just as we can trust a person we will also be able to trust a car, or even a luxury coat. Different identities can also be linked together, creating trustworthy relationships, such as ownership of an object. IOTA already provides a protocol that enables these actors to transact value or data with one another. IOTA will now combine identity features into a single platform, creating the base protocol for the next generation of smart applications.

> *At IOTA, we are building a Unified Identity Protocol to serve as the invisible layer of trust for the internet. This protocol must be open, scalable and free, so that everyone and everything can enjoy trust as a basic digital right.*

Self Sovereign Identity for People

Information about one's life is spread across many locations. Most people have numerous unorganized important documents at home, hundreds of online accounts, and many more online footprints. Through statistical predictive analysis, computer programs can harvest unverified online information sources and create a reasonably accurate profile about our lives. These profiles are accurate enough for targeted advertising and personalized content, but lack the proof and trust for them to be used in business. This results in an antiquated customer experience where we have to submit our age and address for every purchase we make and every account we create. It also inhibits our ability to do many online tasks like requesting and extending licenses or taking out a mortgage.

Self Sovereign Identity (SSI) is about returning autonomy and privacy to the individual, while also improving our online experience. Some movements focus on data privacy, preventing companies from using our information all together, but the IOTA Foundation favours controlled information flow. With an SSI, the user can create a single online profile, containing all our personal information. They can decide who they share what information with, and the Verifier is able to verify the information to be correct, making the data trustworthy. This moves their online profile from a statistical estimation by corporate entities to an accurate and verifiable profile under their own control.

We envision a new internet without usernames, passwords, endless repeated forms, or data harvesting. Users have ultimate control and can choose to supply service providers with their personal data, who in return provide personalized experiences. Data will still flow, and perhaps even more than before, but it will always be in the interest of the individual, instead of a corporation. People will gain additional benefits in sharing their data, either in monetary value or improved customer experience. This sort of system is not possible in a non-neutral environment such as permissioned or fee-based ledgers.

Governmental mechanisms for building digital identities are currently being established throughout Europe and Asia, with demand increasing around the globe. However, they are managed by single entities, and restricted to the governments that created them. By decentralizing a framework for these standards to adapt to, we have a system for intergovernmental verification of individuals and devices. A person's digital identification will be transferable across borders like a passport. However, it will no longer require the trust of the issuing government due to the digital trust established by the open and auditable system.

> *The Unified Identity protocol builds a new internet, without usernames, passwords, endless repeated forums, or uncontrolled data harvesting.*

Legal Compliance

SSI portrays a vision of greater privacy, greater control and a more honest society. This vision is shared by many of the world's governments. The European Union's General Data Protection Regulation (GDPR) is the most well-known regulation to limit privacy invasion and corporate data ownership. The GDPR was written before Distributed Ledger Technology (DLT) became widely known. While DLT can realize many of the goals of GDPR, there is an unfortunate side effect that DLT might be incompatible or hindered by that same regulation. There is also room for interpretation with many conflicting reports on what exactly should be considered Personally Identifiable Information (PII).

The Unified Identity Protocol will ensure compatibility with global privacy and data management legislation. GDPR states that citizens have the right to provide and retract consent for the storage of PII. Since any data stored on a Distributed Ledger is immutable and cannot be removed, a DLT and digital identity solution is only GDPR compliant if it never stores PII on the ledger.

According to the GDPR Art. 4 (1) Personally Identifiable Information is defined as:

> *"Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person"*

Information	GDPR-compliant use possible	Used by UIP
(Asymmetric) Encryption of PII	✗	✗
Hash of PII	✗	✗
Salted Hash of PII	(✓)	✗
DIDs	✓	✓/✗

Table 1: GDPR interpretation for the Unified Identity Protocol.

Using this interpretation of GDPR (Table 1) we believe the solution is GDPR compliant. From a security perspective, it is reasonable to consider a salted hash GDPR-compliant as long as an objective re-identification risk analysis is done, leading to a salt that is sufficiently long and random. As recently stated in a joint paper by the Spanish data protection authority (AEPD), and the European Data Protection Supervisor (EDPS), such risk assessment should consider both the hash process and any other elements that make up the hashing system, paying special attention to any information that is or may be linked to value represented by the hash. Some reports agree, while others disagree with this statement. However, we do not currently plan to place salted hashes on the Tangle for the Unified Identity protocol. DIDs for people can be stored and used off-ledger. And in the case where GDPR is interpreted more strictly, we will be able to adjust the protocol accordingly, while only sacrificing user experience or increasing architectural complexity.

The protocol will also follow the principles for limited use and collection established under frameworks like the Fair Information Practice Principles (FIPPs) from the OECD Guidelines on the Protection of Privacy.

> *The Unified Identity Protocol will explicitly align with current international and EU mandated privacy policies and guidelines.*

Organizational Identities

Many corporations are associated with greed and abuse of power. This reputation stems from the role some have chosen to take within society. Corporations are trusted with our data, but often do not act responsibly. Vulnerability, fix, patch, repeat. In software and systems we have seen this cycle repeat. Headlines on data leaks are now an ever-present feature in the news.

“Equifax Says Cyberattack May Have Affected 143 Million in the U.S.” ~ NY Times

“Marriott discloses massive data breach affecting up to 500 Million guests. ~ Washington Post

“Private messages from 81,000 hacked Facebook accounts for sale.” ~ BBC

The UIP presents an opportunity for companies to embrace a new role in the Unified Identity ecosystem. Traditional approaches do not provide cost efficient solutions to new legislation like GDPR. The UIP enables organizations to change their processes to comply with the new regulations in a cost efficient and privacy-enabling manner. Features of “Data Protection and Privacy by Design” shift responsibility over Personal Identifiable Information from organization to customer, and organizations no longer need to store that data. The relationship between customer and organization is also tightened as communication via a third party Identity provider like Google or Facebook is no longer needed.

Due to Know-Your-Customer (KYC) and Anti-Money Laundering (AML) obligations, companies can be certain who their customers are. These services also provide unique insight into the state of their customers' data. These insights can be combined and translated into verifiable credentials, providing a new "Trust Anchor" service with a potential for new business models. KYC and AML credentials would return the autonomy of personal data back to the customer. Once companies accept the KYC and AML credentials of other companies, the enrollment time for new customers is significantly reduced, as are the costs. With the personal data secured by the customer, companies can afford to store less data in their own databases, reducing risk and responsibility and fulfilling the goals of legislation such as GDPR.

> *UIP allows organizations to comply with GDPR in a cost efficient and privacy-enabling manner.*

Identity of Things

The IOTA Foundation is working to enable an "Economy of Things" where devices will be able to directly exchange services and data with one another. This opens up a myriad of ways to optimize business processes and many new business models. IOTA's feeless micropayments enable the machine-to-machine payments necessary for this model. However, we are still missing the same key ingredient: trust.

The IOTA Foundation has always taken a different approach to other DLTs on this subject. Instead of using Smart Contracts to guarantee that value is transacted based on a condition, we provide a pay-per-use model, where a service like electric vehicle charging can be broken into smaller segments, and paid individually. This ensures both parties always get exactly what they are entitled to and creates trust. However, this model does not work for every scenario. Parties often need preliminary information about each other before initiating an interaction. We observed this in our Industry Marketplace demonstrator, where machines are paid for their services - how do we ensure that a certain machine has the capability to fulfill a task?

With Identity of Things (IDoT) devices are provided with a unique global identity, able to prove many attributes including their capabilities, specifications and authenticity. People, organizations and other devices will only pay devices that can prove their ability to fulfill the required task. This basis of trust prevents fraudulent activity. In addition, by using the IOTA ledger, the progress of the task can be immutably logged. With the combination of the IOTA protocol and the Unified Identity framework, we can automate the entire interaction between all parties, without requiring predefined trust. The Industry Marketplace provides a perfect example of how this framework and level of autonomy work.

There is a growth in applications that generate Digital Twins for physical devices or objects, such as the Asset Administration Shell (AAS) developed for our Industry Marketplace. Digital twins are online profiles representing a device or object. They provide a virtual state that mirrors reality by emulating the device or object's physical state through data input sources like sensors. A digital twin is often used to monitor state and execute actions based on the information. Digital twins are only rarely shared outside the associated application and organization due to complexity in sharing and matching profiles. However, empowered with a digital identity, digital twin sharing would become possible. Once data is verifiable and trusted, digital twins can form the basis for the digital representation of physical devices and objects. This allows other identities to interact with them automatically, and provide services such as predictive maintenance.

Security is a major barrier in advancing technologies that use IoT. Whether it is the smart devices in our own homes, or at a larger scale, the critical infrastructure of organizations and cities, security must be at the core. It is central to any globally-unifying identity solution. By integrating advanced research in cryptography and digital ledgers, and combining it with a scalable access and management system, security will become a core functionality of the systems we build. By using scalable device DIDs, integrating verification and reputation schemes, and allowing for transparent tamper-proof accountability, we begin to understand how we can future-proof the security of our systems, allowing us to start trusting the process, and not the patch.

Object Identities

Not everything has the necessary circuitry to manage its own identity. Non-electronic objects are also a core part of our everyday lives. Even without connectivity, non-electronic objects can also benefit from a digital representation. The benefits become particularly salient when considering the supply chain. Objects enter an informational void as soon as they are processed in a factory and loaded into a vehicle. Any uniquely-identifying information is blended with the other units. The link between origin, quality, chain of custody and transport sensor data is lost. Often these objects are tracked via written or printed documentation, which can be lost, destroyed or mismatched. It is a waste of resources to conduct error-prone information transfer between parties, as the object makes its way through the supply chain.

Digitizing non-electronic objects allows us to build a digital information profile which remains paired to the object throughout the supply chain. The information exchange is automated as the object itself carries the information. The information is trusted through the use of verifiable credentials. In addition, objects can be linked to other information sources during transit, such as temperature or motion sensors, providing immutable proof of safe transport and quality.

Non-electronic objects will not be able to control their own identity. They need representation from an online agent. The agent not only holds the data and credentials, but also decides who has access to that information. This is a weak link within the identity protocol - someone needs to control the agent and be paid for that service. When an agent goes offline, the object's information is no longer reachable. It remains however, impossible to falsify information about the object. Using

IOTA, any data will have immutable anchor points in the Tangle, proving the data to be unaltered, and verifiable credentials will be signed by their Issuers. To restrict the control of the agent, an object may sacrifice its “privacy” by publicly registering their data and credentials directly on IOTA.

Conclusion

With a Unified Identity Protocol, IOTA extends its capabilities. It will not only serve as a platform for feeless microtransactions and immutable data anchoring, but also become the internet’s invisible layer of trust. The Unified Identity protocol is one of the first protocols that goes beyond the identity of people and organizations to include devices and even objects. It will provide a platform for trusted interactions between everyone and everything. Identities in the Unified Identity protocol will be able to freely create and manage their own identities, enhancing autonomy and privacy. Chosen information can be shared selectively, and then instantly, freely and securely verified by the receiving party. The addition of the Unified Identity Protocol demonstrates IOTA’s flexibility and is an important step to becoming the trust infrastructure of the internet.

Final Words

This document represents the IOTA Foundation’s vision for a Unified Identity Protocol. It will later be extended by a set of one pagers, case studies, technical blueprints and developer tools that show, explain and enable multiple use cases across the different IOTA’s verticals. The initial implementation of the UIP can be found on Github. This experimental implementation of UIP will be further developed and maintained for the first half of 2020. It will be the basis for an experimental digital identity application and potentially other apps and tools. Eventually, around mid 2020, the development of a Rust implementation will be started to deliver a better performing implementation which can be used on a broader set of platforms.