ANONYOME LABS

Realizing

the Business Value of Decentralized Identity

Solving the problems related to identity, authentication, and information security are at the top of today's business headlines—and this is the core purpose of decentralized identity (DI). Many whitepapers focus on DI's technical aspects, such as cryptography and zero knowledge proofs, verifiable credential formats and protocols, wallet security, and so on. Others explore the philosophy of DI, the benefits of user-centeredness, the privacy control, and why it is also called self-sovereign identity. But few whitepapers really answer the pressing bottom line question for enterprises: ***Why should we consider implementing decentralized identity for our enterprise today?***

This whitepaper sets aside the technical and philosophical discussions and instead explains the business benefits of DI. It will help an enterprise understand what makes DI important from a business perspective and explain why the enterprise should embark on an initial DI product program.

At any point in time, this is the case ...

Enterprises face many and diverse challenges that affect how they interact with their partners and customers, such as:

- Inefficient paper-based or not-so-secure electronic processes
- User privacy and identity theft risks
- Complex and expensive user management
- Challenging systems integration
- Poor user experience
- Complicated regulatory compliance
- Loss of enterprise reputation.

The list could go on.

Many of these problems derive from complex and inefficient identity management processes that are the norm across almost all enterprises.

But now,
this has happened ...

DI has ushered in a new phase in identity management. It is evolving aging centralized and federated identity management systems with an open, interoperable, and standards-based identity management ecosystem. Since DI was architected to interoperate across many disparate internet platforms and services, it is well suited to many different enterprise scenarios and can alleviate many current enterprise problems.

DI also offers an economic model that can create new revenue opportunities.

So, now we have this challenge and opportunity ...

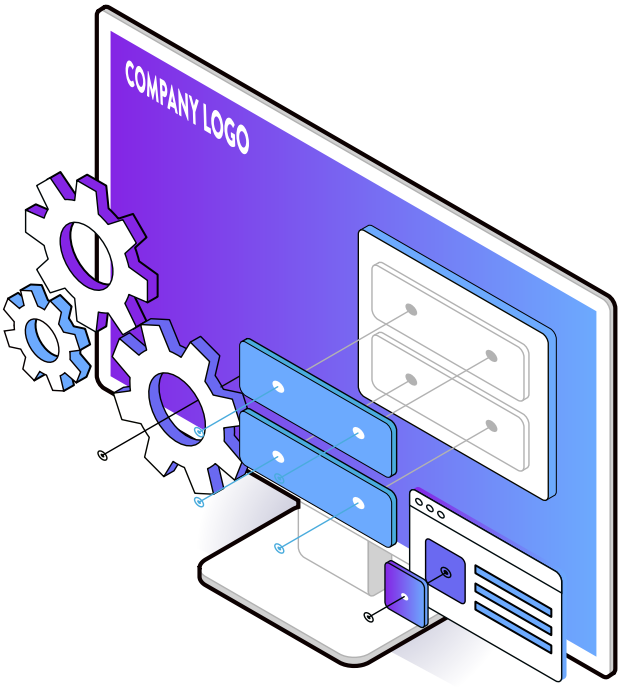
What is the business goal? What are the initial target project applications? Which project should be first? What will be the business value?

Those questions apply to any project and DI is no different. This new technology is complex, but can deliver many financial, regulatory and security benefits to the enterprise. Understandably, some organizations are hesitant to initiate test projects to explore how DI can help them realize their business goals.

In many ways, DI is at the same point as federated identity was in the first decade of the 2000s. Back then, the focus was on developing standards specifications for federation: SAML, OAuth and OpenIDConnect. Standardization is also the focus today and interoperability continues to be the key to success.

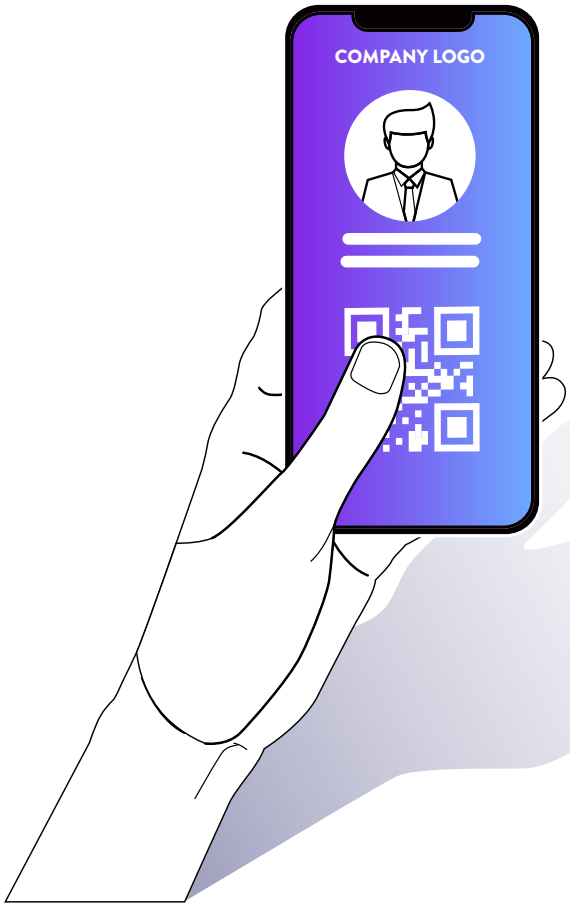
DI standards have been in development for more than five years, thanks to the World Wide Web Consortium (W3C), Decentralized Identity Foundation (DIF), Linux Foundation (Hyperledger and Trust Over IP), and more. The DI standards have matured to the point where software vendors can deliver interoperable software to the market.

… but if we look at it like this …



The best place to start is to analyze the stated business benefits of DI and then **choose a project to apply them to**.

Creating rapid prototypes or augmenting existing solutions will help enterprises see firsthand how the DI solutions can result in tangible and immediate business value. Applying DI to their own projects will enable enterprises to determine how DI's benefits correlate with their own unique technologies and business goals.



… we can reach this destination …

Through **real-world project experiences**, enterprises can learn about DI, demonstrate its value to key stakeholders, and move from initial exploration and hands-on experience to selecting strategic efforts for wide-scale enterprise deployments.

DI can deliver immediate business value in three areas

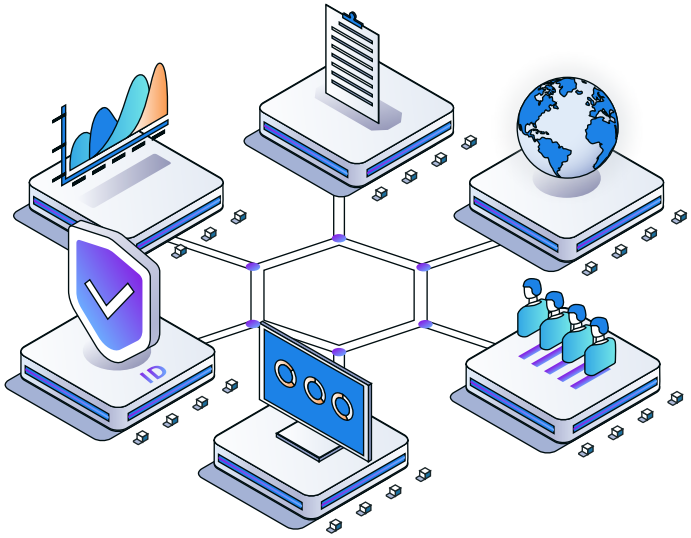
The three areas to look at are:

1. New revenue opportunities
2. Cost saving opportunities
3. Solving other common business problems.

New revenue opportunities

DI presents a wide range of opportunities for new business growth and additional revenue streams. Let's look at some:

Create financial models that use verifiable credentials



With DI, an organization can issue and verify a new type of digital credential that has broader industry applicability and significantly enhanced security and privacy protections. Verifiable credentials are cryptographically generated digital data elements that assert a variety of personal information about a user, asset or process. Using verifiable credentials, holders can prove assertions to verifiers with high-integrity cryptography. Since this can happen often without even notifying the issuer, the privacy of interactions between holders and verifiers increases. This process is generic in nature and will result in innumerable types of new revenue opportunity.

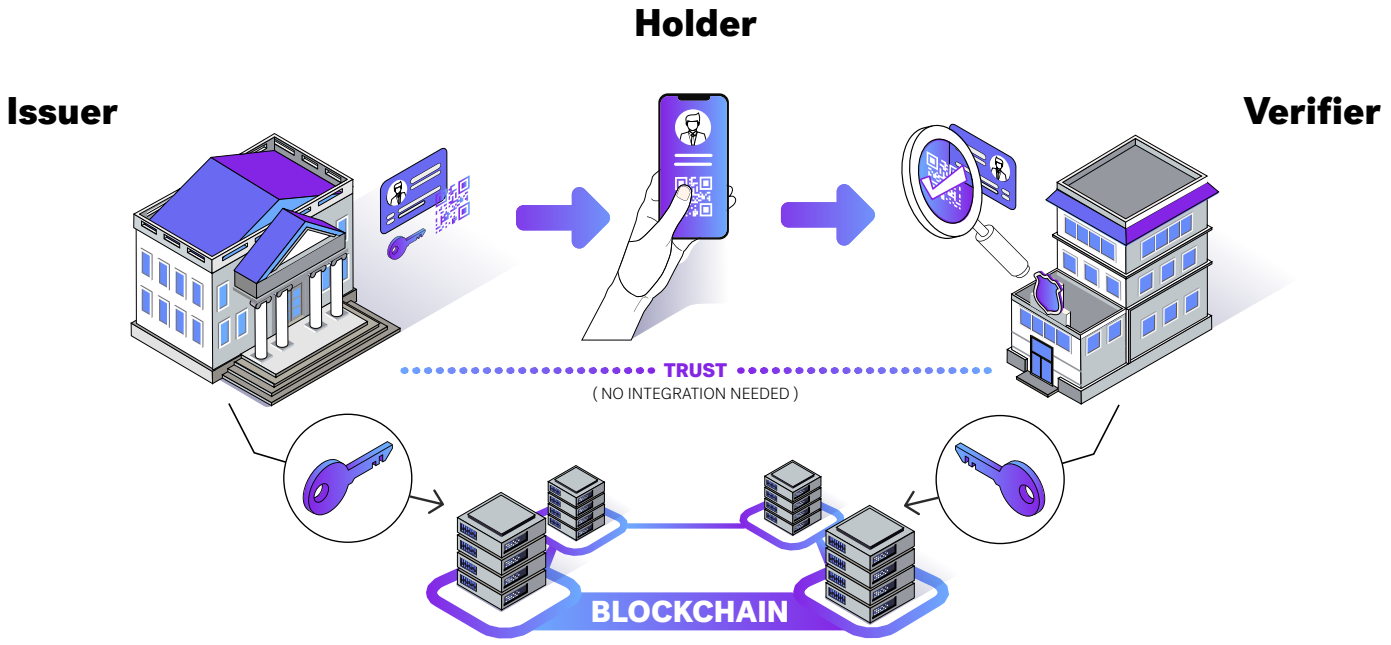


Figure 1: **Verifiable credential process**

In Figure 1, the verifiable credential process starts on the left with the issuer. An issuer is an entity (e.g., government or business) that generates and issues verifiable credentials for other users or organizations. Prior to issuing credentials, the issuer must register some information about the credential on an immutable public data store (e.g., blockchain or decentralized ledger). This information is known as a schema.

Once the issuer has registered the schema, it can create and issue verifiable credentials. This process begins with a holder (user) and an issuer forming a secure connection over which the issuer will transmit the verifiable credentials that will be stored in the holder's wallet.

Having a verifiable credential enables holders to prove select credential information when subject information is requested. To do this, the holder establishes a connection with a verifier who asks for proof of a data item covered by a verifiable credential. The holder will then create and submit a proof presentation. The verifier can then retrieve the issuer's information from the blockchain and use it to verify the holder's submission.

Here are some of the verifiable credential-based business models that provide distinct revenue opportunities for enterprises ready to issue or validate verifiable credentials:

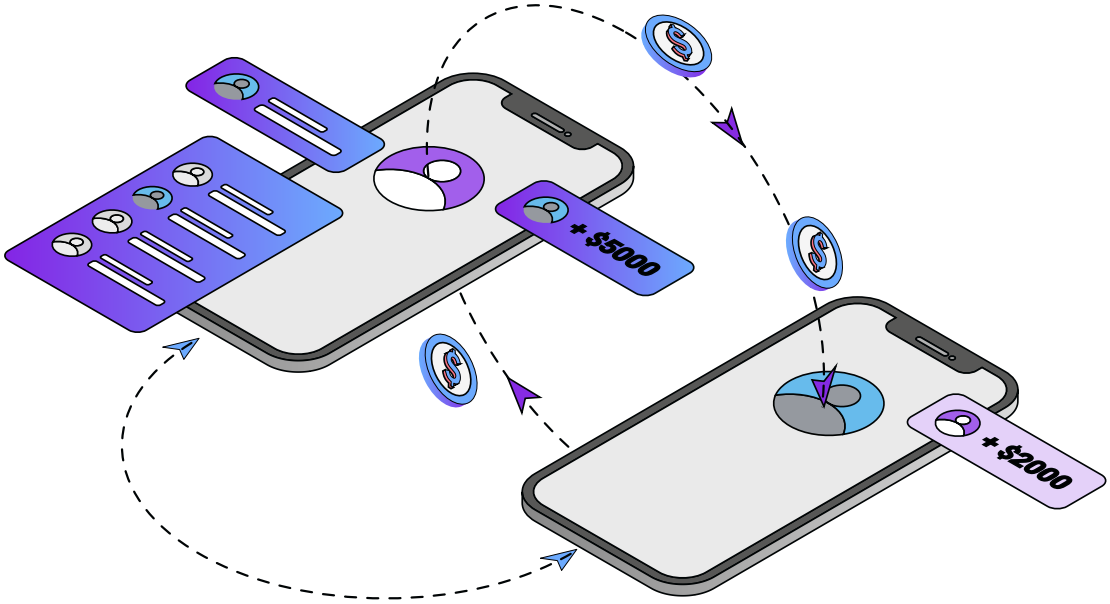
• **Holder pays issuer**: The first revenue opportunity is for the holder (user) to purchase a verifiable credential from the issuer. Examples of revenue are fees for digital passports, digital driver licenses, credit scores, digital graduation certificates or other digital asset requiring cryptographic verification. Credentials that can be used regularly and with many verifiers will have a higher value for the holder. And credentials can expire so there are opportunities for recurring revenue.

• **Verifier pays holder**: The second revenue opportunity is rewarding the individual (holder) for the data they share, whether that data has come from an issuing organisation or direct from the user. One example is businesses that give discounts to users who present an identity verification credential (e.g., loyalty card), or give a reward for providing personal information for future marketing opportunities.

• **Holder pays verifier**: Holder pays verifier for access to the DI system which gives them faster verification and therefore faster access to a resource. For example, the cost of using the 'fast gate' into a music concert is baked into the price of admission (e.g., a 'gold tier ticket'). The music goer is treated to a shorter line and faster admission.

• **Verifier pays issuer**: Another revenue opportunity is for the verifier to pay the issuer for issuing credentials. Some examples are a bank paying for a background checking company to make a check (e.g., credit score, work history, police report) during a loan application process.

• **Issuer pays verifier**: Issuer pays verifier for a verifiable credential they issue to reclaim a good or service provided by the verifier. One example is a health fund becoming an issuer to offer a rewards program dependent on the tier and duration of a member's subscription. The rewards may entitle users to goods and services that help them maintain a healthy lifestyle and may include discounts on exercise gear and subscriptions to health magazines. The issuer pays the verifier the cost of the reward so the verifiable credential will be accepted. The issuer gains greater loyalty and 'quality' subscriptions from their members as a result.



Become a trusted wallet provider

One of the key technical contributions of DI that is also a significant user-facing branding opportunity is the wallet. A DI wallet lets a user:

- Created decentralized identities
- Create and store connection information
- Receive, store and present verifiable credentials.

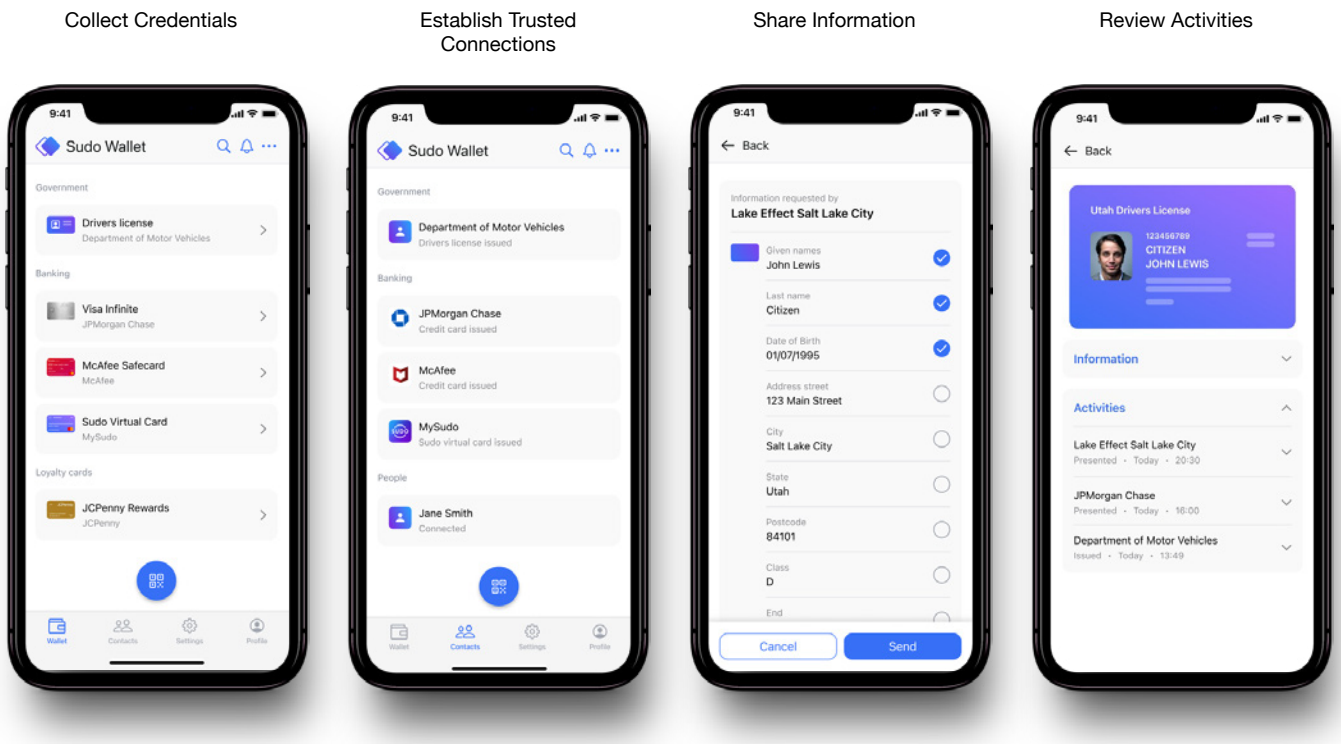


Figure 2: **Decentralized identity wallet**

Figure 2 displays some screens from Anonyome's mobile identity wallet. On the left, the user can view any verifiable credentials currently stored in the wallet. The next screen gives a list of connections the wallet has established. The third screen shows the user selecting specific personally identifiable information (PII) elements to be shared from a credential. The fourth screen shows activities related to that credential.

The opportunity for an enterprise to become a **trusted provider** of a DI-enabled wallet application is excellent because it not only enhances their own DI offerings, but it can also be used in other DI scenarios as well. The enterprise can use the wallet to give current customers greater value and to attract new customers to its offerings.

Differentiating a wallet product in the market can be done in several ways:

- Relying on existing brand trust and loyalty to market the wallet
- Offering advanced capabilities in the wallet application (e.g., a security and privacy focus)
- Integrating the wallet with an existing application that already has useful features for the user (e.g., password manager, credit scoring, private browser).

Manage relationships better

DI enhances the digital trust between an enterprise and its customers or partners.

One of the key technology offerings in DI is the ability to set up a secure and durable (or semi-permanent) connection (e.g., a DIDComm connection) between the enterprise and its partners or users (customers). The connection is not linked to an email address, mobile phone number or other identifiers that can change. Instead, it is established from decentralized identifiers (DIDs) that both the enterprise and the partner or user (with their respective wallets) hold at each endpoint of the secure connection. The connection persists until either party deletes their end of the connection by deleting the credential or keys from their wallet.

The benefit of maintaining the secure connection is that either party can easily and securely communicate with the other without having to re-establish a secure connection or require a user to login to a provider's website to read the communications. For example, representatives from an enterprise sales department can personally reach out to the user and remind them of an upcoming subscription renewal. Alternatively, users can reach out to support to ask the enterprise for help. As both parties exchange messages, they can be certain they are communicating with the right party since the connection is protected by previously established end-to-end encryption and authentication. What's more, the enterprise can use the connection to issue (or re-issue) a verifiable credential or request a verifiable credentials presentation proof.

Cost savings opportunities

Many opportunities exist to improve processes and reduce costs.

Replace inefficient processes

Many enterprise processes are highly inefficient, expensive and slow because they are paper-based, antiquated electronic processes, or a combination of the two. One example is how a user is asked to prove their identity and provide information about themself. For the initial interaction with the user, this might involve asking them to provide a set of identity information, such as a driver license, birth certificate, social security card, etc. This usually requires the user to scan those documents and submit them electronically for evaluation. This is very costly for an enterprise to manage, introduces handling liability for the enterprise, and is highly inconvenient for the user.

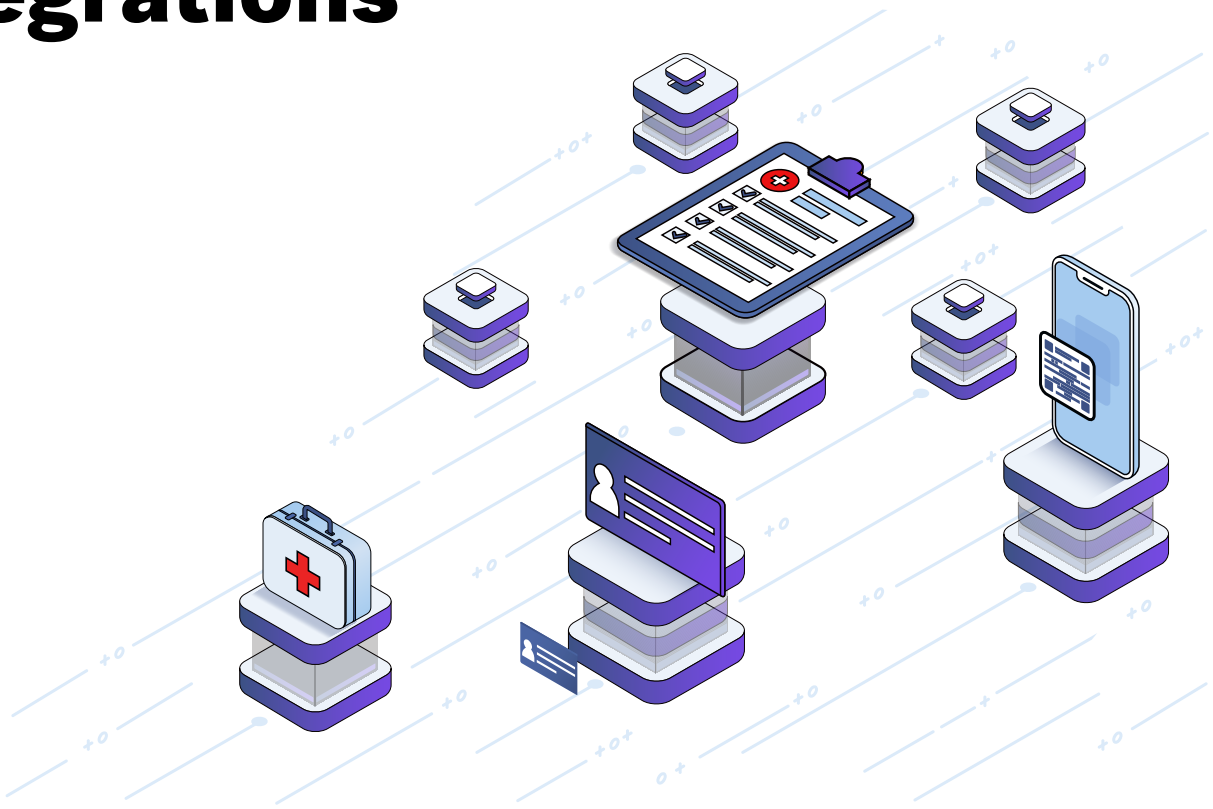
And it doesn't stop with the initial user verification. Once the user connects to the enterprise, they have to continuously prove who they are during subsequent logins. Whether it is asking a user to authenticate to a web portal, to provide additional personal information, or to authenticate themself by answering questions over the phone with customer support, these situations are complex, expensive and prone to error and abuse.

Examples of the many identity verification scenarios are:

- Applying for rental accommodation
- Applying for a loan
- Buying or renting a car
- Buying a ticket for travel
- Accessing online health care
- Accessing user support systems.

DI can streamline many of these identity processes. For example, instead of the user having to prove their identity in each of these situations using the same inefficient processes, they would use a secure verifiable credential provided by a specialized identity verification service which would ease the burden on the user and improve security protections. The credential would not only confirm the user was independently verified, but it would also contain a set of claims about the user that the user could selectively apply to many different use cases.

Remove the need for protected API-based integrations

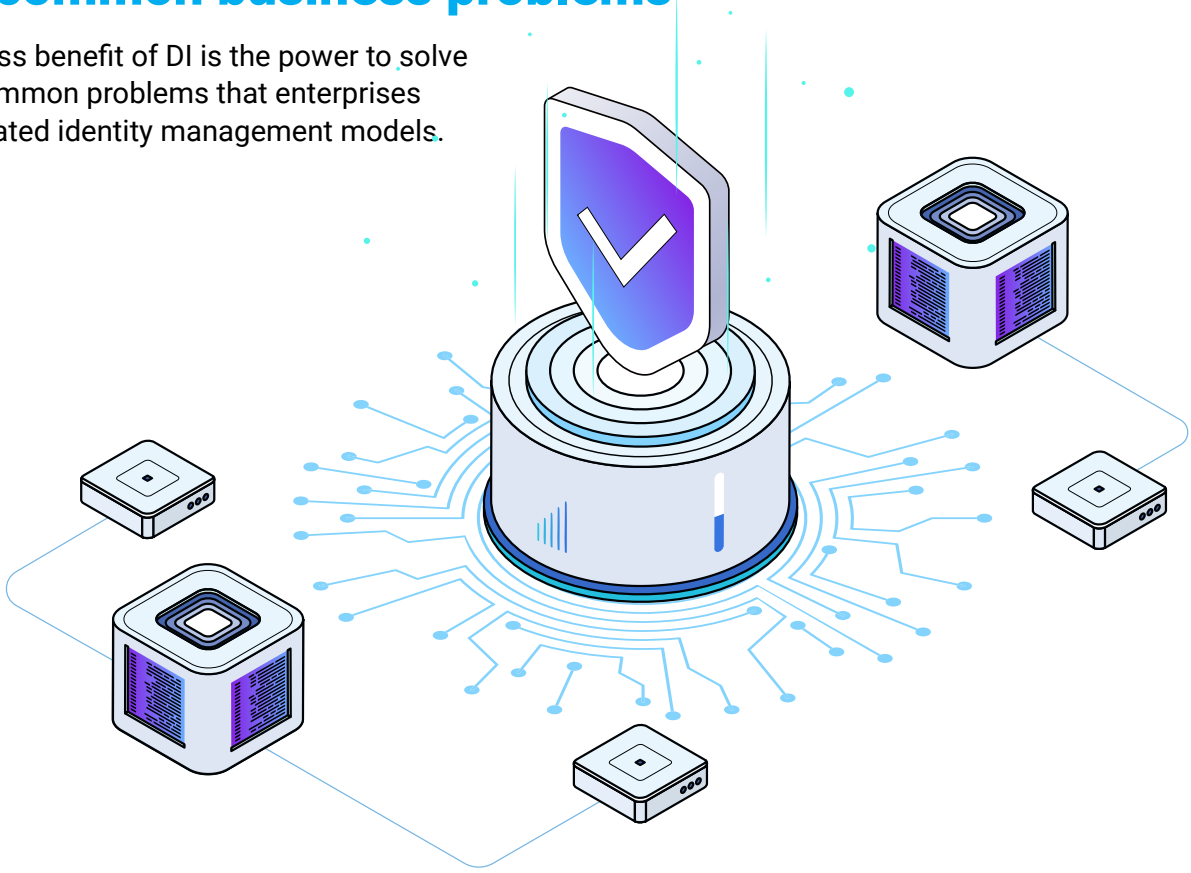


One clear advantage of using verifiable credentials is to securely transfer information. Since a verifiable credential is a cryptographically protected element that can contain various data about the user (e.g., health care record), its transfer must be done securely. Since verifiable credentials accompany the secure transfer protocols of DI, they can be sent with an encrypted messaging protocol, such as DIDComm. This contrasts with current transfer protocols that exchange data using API interfaces that are often 'protected' using an API key or a similar client-server authentication mechanism.

Using the health care example, a medical clinic may need to transfer information to a hospital. The medical clinic will need to build a customized application to transfer health record information to the hospital using a protected API interface. Conversely, if the hospital enabled a verifiable credential that allowed the patient to transfer their own information, there would be no need to maintain legacy API-style interfaces that attempt to combine several security requirements. Maintaining a protected API that withstands modern hacking attempts is costly from both a development and maintenance perspective. Using the inherent security of DI-secured communication channels and verifiable credentials (for access control), the enterprise can avoid risks and costs associated with legacy-protected APIs.

Solving common business problems

Another business benefit of DI is the power to solve some of the common problems that enterprises face from outdated identity management models.



Protect and enhance enterprise reputation

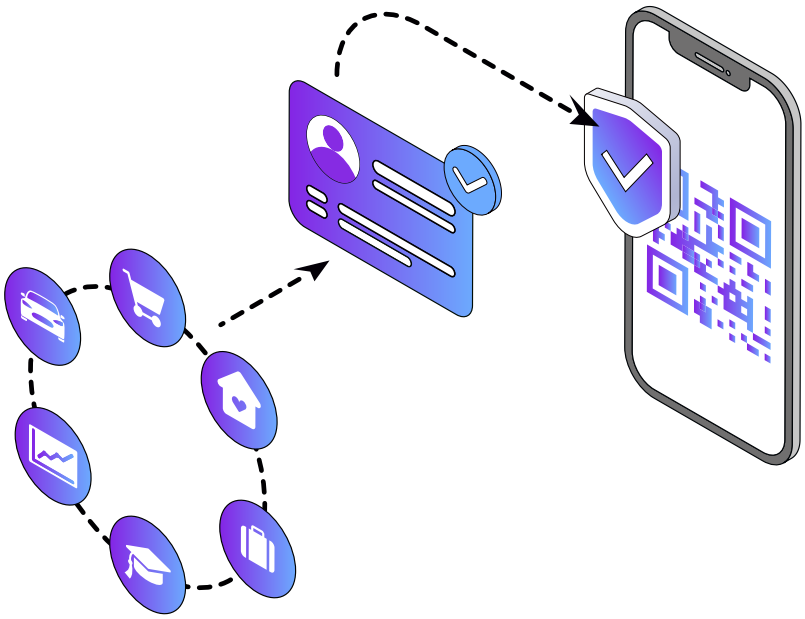
Almost weekly, headlines report data breaches in which criminals have stolen users' personal information from organizations. Most of these breaches start with a phishing attack against a user or administrator in the system, which leads to the bad actor obtaining login credentials and promotion of privilege, and then stealing the personal data.

The fundamental weakness in the system is the username/password type credential (sometimes with multi-factor authentication) that simply doesn't adequately protect user information and other valuable assets. Once the bad actor has committed the data breach, they usually promote it, which causes additional and untold reputational damage to the affected enterprise. In most cases, the reputation hit causes the organization to lose confidence, and customers to abandon the brand and find other organizations that might better manage their personal data.

DI is specifically architected to help protect against this type of attack. Instead of using weak username and passwords, a user accesses an automatic process that authenticates using public key technology and a private cryptographic key that remains safely in the user's wallet. One of the greatest benefits of DI is that users hold their cryptographic keys, connections, and verifiable credentials within their secure identity wallet.

Employing a DI-based authentication system can significantly reduce the reputational risk from data breaches, and this advantage cannot be overstated.

Boost user experience and convenience



DI also delivers a better user experience and greater convenience.

If we continue with the identity verification example, a user can present a verifiable credential from their wallet and both verify their identity and selectively disclose their personal information. This is much more convenient and faster than the user having to prove their identity with paper documents or login-based authentication processes.

A user being able to set up a durable connection with an enterprise offers many advantages. Typically, the user would scan a QR code with a connection invitation, then—using their wallet—set up a semi-permanent secure connection with the enterprise. Any time the user exchanges message with the enterprise, the message is automatically encrypted. The user doesn't have to log in to send or receive communications. What's more, the user can be issued credentials or present proofs via that secure connection.

Also using DI's architectural enhancements to public key-based authentication removes the need for a user to manage username/password (and second factor) for authentication. The nature of the durable verifiable credential-based connections means the user is always authenticated via their wallet's securely stored private key information. Eliminating the need for usernames and passwords is a longstanding goal—which DI realizes.

Ease regulatory compliance burden

Complying with the multitude of international regulations and evolving industry best practices is a challenge for every company. Sometimes, these regulatory requirements even conflict, asking the company to both 'know their customer' and 'minimize data collection'. DI offers a simpler approach to regulatory compliance and thus reduces risk. **Here are some examples:**

Global Data Privacy Regulations (GDPR): The European GDPR regulations have significant privacy-oriented requirements on companies with European citizens as customers. Through bi-directional national treaties, the GDPR requirements have become a de facto standard for most of the world. By using verifiable credentials and zero knowledge proofs (ZKPs), companies can avoid coming into contact with their customers' PII and dramatically reduce their risk exposure under GDPR.

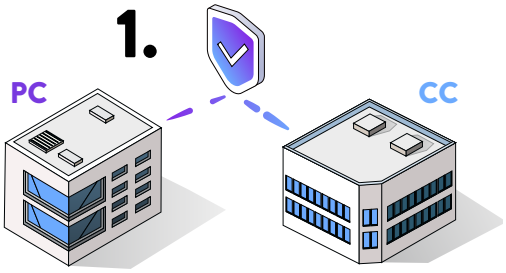
Zero trust architectures (ZTA): Zero trust architectures are now being stipulated for government and commercial deployments. The contemporary processes of authenticating a user's identity and (re-)establishing a secure communications channel continue to be a leading target of hacking attempts. In 2021, there were more than six billion such compromises, making this a leading security concern for enterprises. The damages an enterprise can experience include a diminished reputation, regulatory penalties, loss of customers, etc. The principles of DI offer a standardized approach by which to implement 'least access' policies, strong cryptographic authentication, and so on.

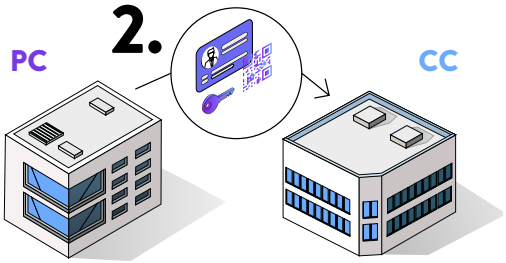
Know Your Customer (KYC)/Anti-Money Laundering (AML): Vendors and service providers are required to implement KYC/AML regulations. Under DI, a government or other trusted authority could issue verifiable credentials containing PII, such as name, address, and residency, and during the credential assertion and validation processes companies can be assured a presenter meets the necessary KYC/AML requirements.

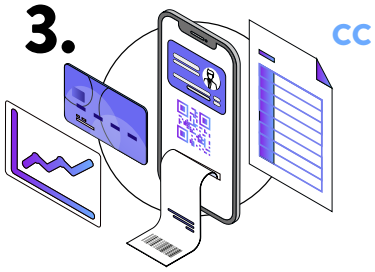
Health data and communications: Whether it's through the United States' HIPAA or Europe's GDPR, health data and communications come under significant scrutiny. Health providers often have very strict access credential requirements and highly structured websites that users must navigate in order to access medical information. DI's peer relationships and durable connections dramatically streamline access to information for authorized users while making unauthorized access cryptographically very difficult. Using DI-protected communication apps, protected medical data can be strongly encrypted and transmitted directly to authorized users who can decrypt the messages while leaving them secured from prying eyes or hackers. This is a very compelling paradigm shift that lifts the access control burdens from users and also lowers the risk for enterprises.

Start by evolving solutions with DI

A great starting project for DI is an existing system that can evolve and be improved with DI technology. Examples are replacing a paper-based system with a fully digital system or updating a digital system to a better version.







<u>Near-term integration</u>

This fits into existing system architectures by adding new functionality.

Steps:

1. Provider company (PC) creates a secure relationship with a client company (CC) by establishing a peer DID relationship.

2. PC issues a verifiable credential (VC) to CC.

3. CC uses the VC and the peer DID to both authenticate and exchange encrypted message traffic (e.g., requests, reports, purchases, payments, etc.).

4. DI protected messaging requests are facilitated through a general DI message agent instead of a complicated protected API.

Regulatory applications

This enhances existing architectures by changing the type of information that is requested and stored, thereby reducing regulatory risk and exposure.

Steps:

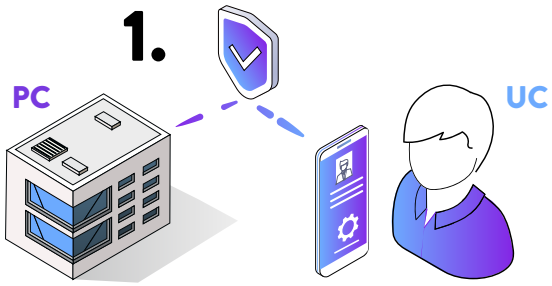
1. Provider company (PC) creates a secure relationship with a user client (UC) by establishing a peer DID relationship.

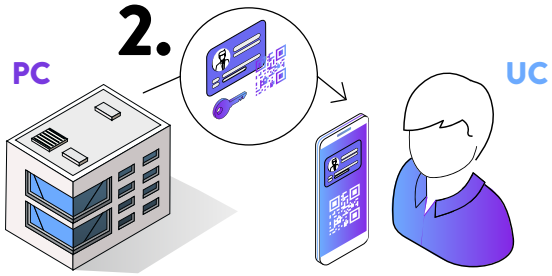
2. PC issues a VC to UC.

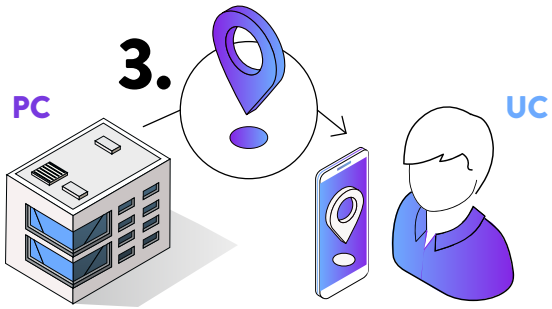
3. PC sends a request (Are you a resident of [location]?) to UC.

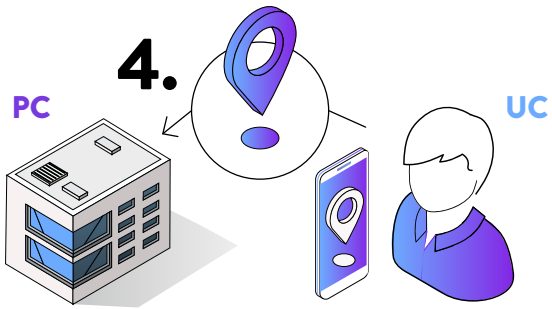
4. UC responds with a ZKP proving they are a resident of the specified location without providing their actual home address.

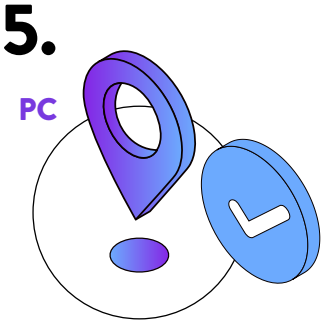
5. PC is satisfied they are working with an authorized resident without having to collect, store, or secure the UC's PII.











Revolutionary potential

Sending DI-protected (encrypted) medical communications directly to a user without requiring them to login and navigate a provider's website.

Steps:

1. Provider company (PC) creates a secure relationship with a user client (UC) by establishing a peer DID relationship.

2. PC issues a VC to UC.

3. PC can securely transmit sensitive medical data (e.g., scheduling, test results, diagnosis, prescriptions, doctor-to-patient questions and answers, etc.) over the DI-secured channels (e.g., VCs and DIDComm).

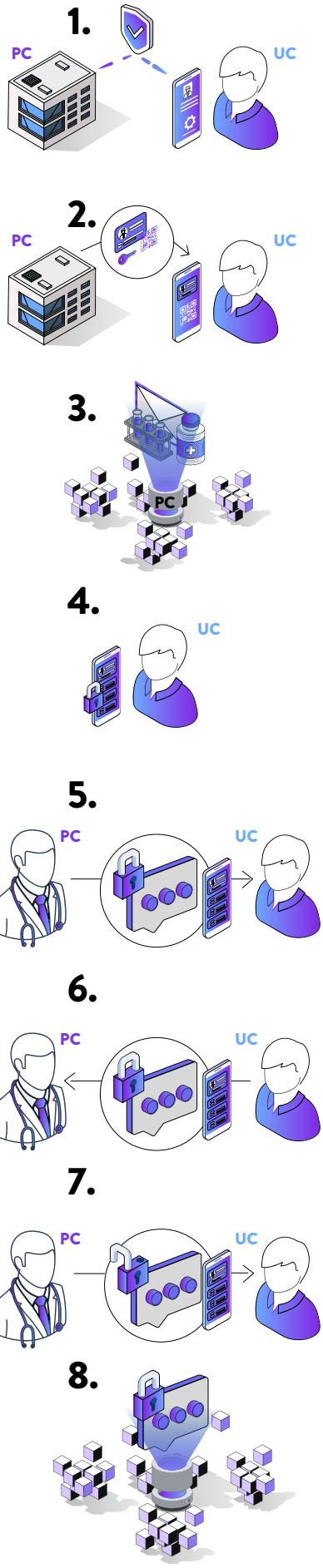
4. UC receives those encrypted messages in their DI-enabled wallet/communication app.

5. UC decrypts/reads the messages from PC (e.g., doctor).

6. UC responds to PC (e.g., doctor, provider, etc.) using DI's VCs and secure communication channel (e.g., DIDComm).

7. PC decrypts/reads/responds to UC messages.

8. PC and UC communication exchanges are protected using strong and authenticated encryption.



DI presents enormous business value

Clearly, moving forward with a DI project can make great business sense. Whether the question right now is to increase revenue, reduce costs, or solve an identity-related challenge, DI can be the answer.

References

[1] SSI Meetup, Explaining SSI to C-Suite Executives, https://www.youtube.com/watch?v=GRfnie-5z4c

[2] Self-Sovereign Identity, Manning Press, Ch 18, Explaining the value of SSI to Business, https://www.manning.com/books/self-sovereign-identity