Focal Use Cases for Decentralized Identifiers

Table of Contents

Directions **3**

Criteria **4**

Use Case #1: Digital Executor

Name 5
Background 5
Description 5
Sticky Wicket 5
Distinction 6

Use Case #2: Life-long, Recipient-owned Credentials **7**

Name 7
Background 7
Description 7
Sticky Wicket 7
Distinction 7

Use Case #3: Web of Trust for Personal Freedom **8**

Name 8
Background 8
Description 8
Sticky Wicket 8
Distinction 9

Use Case #4: Self-Sovereign Investor Compliance **10**

Name 10
Background 10
Description 10
Sticky Wicket 10
Distinction 10

Use Case #5: Disposable Phone Numbers **11**

Name 11
Background 11
Description 11
Sticky Wicket 11
Distinction 11

Use Case #6: Decentralized Corporate Identifiers **12**
Name 12
Background 12
Description 12
Sticky Wicket 12
Distinction 13

Use Case #7: DID Ownership Transfer **14**
Name 14
Background 14
Description 14
Sticky Wicket 15
Terms of Service 15
Distinction 15

Use Case #8: Software Release Signing **16**
Name 16
Background 16
Description 16
Sticky Wicket 16
Distinction 16

Use Case #9: Long-term, high stakes digital cooperation. Example: The United Humans funding and governance. **17**

Name **17**
Background 17
Description 17
Challenges 18
Distinction 18

Use Case #10: Single Sign On **19**
Name 19
Background 19
Description 19
Sticky Wicket 19
Distinction 19

Use Case #11: Institutional Library Users **20**
Name 20
Background 20
Description 20

Sticky Wicket 20
Distinction 20

Use Case #12: Prescriptions 21
Name 21
Background 21
Description 21
Sticky Wicket 21
Distinction 21

Use Case #16: Collective Identity 24

Use Case #17: Transaction Identification for Travel 26

Use Case #18: Digital Asset Grid 27

Use Case #19: Gun Purchase 29

Use Case #20: Code Signing 31

Use Case #21: Exchange of Business Documents 32
Name: Exchange of Business Documents 32
Background 32
Description 32
Sticky Wicket 32
Distinction 32

Use Case #NEXT 32
Name 32
Background 32
Description 32
Sticky Wicket 33
Distinction 33

Directions

Duplicate the example template #X (at the end of this document) and fill in the sections and add your name. Then, send the list an email.

Name -- A pithy name that captures the relevance of the use case

Background -- A sentence or three capturing current state of practice, the motivation, and the value it creates
Description -- A paragraph capturing the core action of the use case: what people do
Sticky Wicket -- A sentence or three capturing the awkward challenge in this particular situation
Distinction -- A brief phrase explaining what makes this use case distinct

Criteria

What makes a good use case?

A good use case is one that is:
A. **Unique** -- minimal overlap with other use cases
B. **Relevant** -- highlights the particular value of DIDs
C. **Value Creating** -- there is demonstrable value to the people at the heart of the use case
D. **Simple yet Sticky** -- simple enough to be accessible, but also captures a potentially complicated edge case.
E. **Specific** -- Uses real names and real situations to help readers empathize with the human requirements

For D, it's great when the basic functionality is straightforward and we fold in a question of "but what if..." and illustrate how DIDs handle a particular real-world problem better than existing approaches.

Use Case #1: Digital Executor

Name

Digital Executor (Joe)

Background

Today, when people die, there are no standard technologies for heirs, executors, or probate courts to properly take control of an individual's online accounts and digital assets. With a DID linked to accounts and assets, a DID owner could define a trigger for a third party to assume control over the DID Document. Ideally, this trigger would specify (a) an oracle (how to know the death/incapacity occurred), (b) a means for the new owner to assert control, and (c) appropriate checks and accountability.

Description

Kathy uses DIDs to manage her authentications to various services. As part of her estate planning, she generates a unique credential that she gives to her attorney, Gloria, with provisions specified in her will, which initially lists Mike as the digital executor. With appropriate obfuscation, that credential is specified in multiple DID documents as a probate authority, with the authorization to change the master key in case of death, which shall be recorded publicly, on chain, as a notarized invocation of the probate authority. As it happens, Kathy had a falling out with Mike and notified Gloria just two weeks before her death that her friend Miyake should now be her digital executor. Upon Kathy's death, Gloria uses the probate credential to publicly record the assertion of probate and to replace the DID's master key with a new key, controlled by Miyake, who lives in Japan (Kathy, Gloria, and Mike live in the United States). Now, any system using Kathy's DIDs for authentication can programmatically recognized Miyake's authority *and* specifically know that Kathy's credentials were modified under a assertion of probate.

Sticky Wicket

The late date change in digital executorship from Mike to Miyake could be problematic if Kathy had directly listed Mike's credential in the DID Document. Because she instead chose to rely on her attorney, Kathy has a more flexible way to direct her wishes, while still leveraging the collective control over her authenticated logins to various services. In addition, Miyake's geographic location could make it hard for them to travel to the United States and may make it difficult to provide proof of identity traditionally used by U.S. courts. Also, because Gloria invokes the probate mechanism, Miyake need only provide a suitable credential at that time; he did not need to create and maintain a credential over a long period of time (as would be the case if Gloria weren't involved).

Distinction

Multiple DIDs with a common, blinded authority for probate assumption of control. The legal selection of the new owner is mediated through a trusted fiduciary (an attorney of record). Cross-border transfer of ownership.

The more you can flesh out the details, the better. We will consider a variety of options before we whittle down to a few canonical, focal use cases.

Use Case #2: Life-long, Recipient-owned Credentials

Name

Life-long, recipient-owned credentials (Kim)

Background

Educational Verifiable Credentials offer benefits over traditional educational credentials in that the recipient is able to store and share their credentials, and a third party may independently verify the claim (without necessarily consulting the issuer). This provides the promise of recipient-owned long-lived credentials that the recipient may use even if the issuing institution goes out of business.

Usability issues around cryptographic keys introduce a threat to achieving this goal; if the recipient loses their private key, they lose ability to prove ownership of a credential. The existing ways to re-obtain the credential include re-requesting the credential from the issuer, or TBD.

If a credential is issued to a recipient's DID, the recipient has the ability to prove ownership of a credential even if the recipient loses a private key used to show ownership of a credential referenced in a claim.

Description

Yanny uses DIDs as subjects of its Verifiable Credentials. By using DIDs, Yanny is able to prove “ownership” of a credential. Even if Yanny loses the private keys corresponding to all keys referenced in the DID document, Yanny is able to invoke the update method on the DID to once again gain control over the DID, and therefore continue to use the Verifiable Credential.

Sticky Wicket

TODO

Distinction

Emphasizes the full lifecycle of cryptographic key management; i.e. loss of control is handled in a first-class manner via DIDs, and not as an exceptional event.

Use Case #3: Web of Trust for Personal Freedom

Name

Web of Trust for Personal Freedom (Moses)

Background

In October 2017, at least 34 people have been arrested in Egypt as part of an expanding crackdown on the gay and transgender community. The crackdown was enabled by Egyptian police who used social media, gay dating apps and other websites to identify and target gay and transgender activists. If people could use pseudonymous DIDs linked to decentralized reputation generated via a web of trust, it would (a) safeguard the identities of gay and transgender people enjoying their human right to personal freedom, (b) provide a system for preventing entrapment, and (c) offer a community generated system to report abuses yet honors the human condition.

Description

As gay man in a repressive regime, Muhammed wants to find love safely so that he doesn't get arrested and tortured and persecuted. In this case, his pseudonymous DID holds a number of verifiable claims generated by a web of trust, that provide a reasonable indicator of his sexual preference. Thus, a repressive regime would face greater difficulty in generating a presentable DID to use as a honeytrap. Using a VPN, he accesses a website for gay hookups in his city, but is able to rely on reputation statistics that can keep him safe. What's more, those statistics, tied to pseudonymous DIDs so no personally identifiable information is ever revealed, live on a blockchain that is beyond the reach of that regime to modify or hack. Also, there are a number of credentials that indicate hobbies, interests, the area of employment and other details to enable relationship matchmaking. One friend is a friend of his friend, as indicated by the decentralized social graph, so that information is used to provide a more accurate reputation analysis. If he detects a likely sting operation, his concern could be broadcast to others. However, he knows if he broadcasts alerts too often, he is the boy who cried wolf and his own reputation standing would be decreased.

Sticky Wicket

The government Muhammed lives in would consider this system to be illegal. However, the Internet is essentially extranational, so our underlying framework is based on the United Nations Universal Declaration of Human Rights, which were developed in recognition of the inherent dignity and of the equal and inalienable rights of all members of the human family is the foundation of freedom, justice and peace in the world. In 2016, the UN passed a resolution that confirmed that the human right to be protected from violence and discrimination applies equally to LGBT people.

Distinction

This use case shows why self-sovereign identity can honor the human condition and even save lives.

Use Case #4: Self-Sovereign Investor Compliance

Name

Self-Sovereign Investor Compliance (Moses #2)

Background

There are certain Third World countries where successfully investing in cryptocurrencies could lead to kidnapping or even government sanctioned extortion. In these cases, the identities of early cryptocurrency developers who chose to mine Bitcoin, but who live in Third World countries, must be safeguarded. Certain global security regulations demand revealing his identity to parties that have, frankly, been hacked in the past. Those failures to preserve privacy, which are only a nuisance in America, could potentially lead to deadly consequences in the Third World. In this case, revealing his identity could lead to the kidnapping of loved ones, or even extortion by tribal leaders or corrupt governmental officials. After all Bitcoin is pre-formatted as the perfect untraceable ransom currency.

Description

As an early Bitcoin enthusiast and miner, Kablan wants to diversify his holdings by supporting promising ICOs so that he can reduce his concentration risk in Bitcoin, however, he needs to preserve his anonymity as a safeguard. In this case, his pseudonymous DID holds a verifiable claim that provides an attestation by a licensed and bonded EU attorney, which should fulfill the KYC/AML requirements to invest in ICOs in Europe. Thus, the government is assured he is not a terrorist or money launderer, and he is able to invest more effectively with greater personal security. This will allow him to be an effective member of the crypto community. Kablan's initial investment, if he were free to optimize via a portfolio strategy and invest in better ICOs launched in the US and EU, could theoretically eventually make him one of the top venture capitalists in his own country, who could fund multiple startups to break the cycle of terrorism and despair. Stifling crypto innovation has an impact globally.

Sticky Wicket

The attorney is required to disclose the legal nexus for the subject. Since Kablan is a resident of a country that is on a watch list, so it will make it harder for the attorney to meet KYC/AML requirements.

Distinction

By constraining the rights of certain people to invest freely and lift themselves out of poverty, AML laws are actually strengthening terrorism in an indirect way.

Use Case #5: Disposable Phone Numbers

Name

Decentralized Smartphone/Disposable Phone Numbers (Moses #3)

Background

A decentralized ID phone could use DIDs for dialing. A collection of DIDs would be equivalent to an intelligent, open, secure contact database, that could be called a DIDbook or a DIDdialer app. This social interaction reflects the needs of millennial phone users.

Description

As a single girl having some fun at a dance club, Jasmine wants a disposable controllable “phone number” that she can easily give it to guys while dancing, and decide later if she wants to date them. So the guy dancing with her shouts, over the techno, “I really want to see you again, please give me your DID!” She shouts back, “I’m Jasmine who loves to dance.” The phone number is actually a keyphrase that points to her DID, and is easily remembered. Once entered by the suitor, it associates his DID, that includes his photo so she can remember him, and just happens to include a verifiable rating for a VR game he developed, indicating that he actually has a job… unlike her ex who was a DJ and hopelessly unemployable. Also, there are a number of web of trust credentials from friends swearing he’s a great guy. One friend is a friend of her friend, as indicated by the decentralized social graph, so she can check up on him before calling back in the morning. She does, and her friend reveals, “He looks sweet, but he’s a total player.” So she burns the DID connection so he cannot reach her, and the system offers a polite “decline to connect”.

Sticky Wicket

The issue is that this only works if all phone manufacturers agree to support DIDs. This means that this functionality needs to be fully open, and human centric design must guide the evolution of DID technology toward similar use cases.

Distinction

This is the kind of use case that drives to the heart of what people really want from a mobile communications device. Human beings don’t care about RAM or radio, they care about finding love, insuring success, creating value and meaning. A killer app for smartphones is to remove the friction from finding true love.

Use Case #6: Decentralized Corporate Identifiers

Name

Decentralized Corporate Identifiers (Manu)
https://lists.w3.org/Archives/Public/public-credentials/2018May/0057.html

Background

There are many types of identifiers that corporations use today including tax identification numbers (e.g. 238-42-3893), Legal Entity Identifiers (e.g. 5493000IBP32UQZ0KL24), Data Universal Numbering System identifiers (aka. DUNS Number) (e.g. 150483782), and many more that communicate the unique identity of an organization. None of these numbers enable an organization to self-issue an identifier or to use the number to cryptographically authenticate or digitally sign agreements. A great number of business to business and business to customer transactions could be executed more quickly and with greater assurance of the validity of the transaction if a mechanism to self-issue cryptographic identifiers were created.

Description

A North American government would like to ensure that the supply chain that feeds electronic products into the country is secure. As a result, a new method of submitting digital documentation to Customs is enabled that requires that all documentation is provided as machine-readable digitally signed data. Digitally signed documentation is collected at each stage of the manufacturing, packaging, and shipping process. This documentation is then submitted to Customs upon the products entry into the country where all digital signatures are verified on the documentation. Some aspects of the signed documentation, such as firmware hashes and checksums, are then used by Customs and downstream customers to verify that the products have not been tampered with after leaving the manufacturing facility.

Decentralized Identifiers are chosen in order to ensure 1) low management overhead for the government, 2) self-management of identifiers and cryptographic key material, and 3) a competitive marketplace.

Sticky Wicket

The requirement of downstream customers to use the same documentation and digital signature mechanisms that were provided to Customs is the sticky wicket in this scenario. Governments often create ad-hoc solutions for their import solutions, which make securing the global supply chain difficult as each government has their own method of securing the supply chain and identifying corporations that downstream customers need to integrate with. If you are a global company, that means integrating with many supply chain systems (each with different

capabilities). As such, any securing of the supply chain with downstream customers must then depend on the country-specific corporate identification and PKI solution, which leads to ad-hoc solutions that drive up the cost of doing business across borders.

A supply chain identifier solution that is simple, self-administered, built on global standards, is flexible in the cryptographic mechanisms used to authenticate, and can be used by governments and downstream customers with little to no modification to the regional government or corporate systems does not exist today.

Distinction

Many Decentralized Identifier use cases focus on Self-Sovereign Identity and individuals. This use case focuses on organizations and their departments as entities that would also benefit from Decentralized Identifiers.

Use Case #7: DID Ownership Transfer

Name

DID Ownership Transfer (Stephen Curran, BC Gov)

Background

Today, the relationship between a Service User (e.g. a Person, an Organization) and a Service (a Website, Online Service, etc.) is maintained on the Service site according to the account management capabilities offered by that Service. For example, an account for an Online Service might be initially by created by a person using their name and email address. However, users creating account might be doing so on behalf of another entity such as a Company, and not for themselves, even though they used their personal information. Later if they want to transfer control of the account to that other entity or add business-specific rules for controlling that account, it's challenging. With a DID-based, peer-to-peer relationship between the User and the Service, it's easy for a User to transfer control of their account to that other entity and alter the rules for managing the account.

Description

Caroline and Hannah share a passion for Embroidery and decide to start a venture ("SS Stitches") to share their creations with the world, in the hopes that one day they can make a living from their hobby. Hannah creates Instagram and SnapChat accounts for their new endeavour. Through the social media accounts SS Stitches creations begin to gain attention. Their follower counts grow quickly, from 10s to 100s to 1000s. With that success, Caroline and Hannah are ready to take the next step and form a company to market their creations, designs and design services. They formalize their new company and agree on an initial control structure of the company (shared) and merge the assets they have built up into the company. The key assets in their new venture are the social media accounts - the access to their market.

In the old days (today), the process for changing account ownership is difficult, time-consuming and Service-specific. The holder of the userID/password has to log into each site, update the account information for each based on what account management functionality the Service provides. In many cases, Services have no concept of "organizational ownership", and just offer a userID and password for an account. As a result, Caroline and Hannah have no choice but to share the passwords to the accounts. However, a simple password change is all it takes for one of them to block access to the other.

With DIDs, the transfer process is simple and the newly formed SS Stitches, Inc, through an Enterprise DID Management Agent, can provide shared control over the accounts now, and can evolve that control as the structure of the company evolves. For each account/DID Hannah wants to transfer to the new Organization, she uses her Personal Agent (which currently controls the DID) to request a new DID Document for the DID from the SS Stitches's Enterprise Agent. The Organizational Agent creates a new key pair, puts its public key(s) and service endpoints into a DID Document that provides to Hannah's Personal Agent. The Personal Agent uses the DID key rotation capability to swap out the old DID Document with the new DID Document from the Organization. Since Hannah's Personal Agent controls private key associated with the old DID Document she can make the change. After the rotation, control of the DID is with the Organization. No muss, no fuss, and the Online Service does not even have to be involved in the change of control.

Sticky Wicket

With today's tracking and control of the account relationship solely on the side of the Service, there is no easy and consistent way for a User to transfer control of the relationship as they see fit. Further, the Organization cannot exercise it's unique internal control over the account relationship - it's limited by the account management capabilities offered by each Service. By having a DID-based, peer-to-peer relationship, with each party independently in control of their side of that relationship, such transfers are easy to self-manage, and an entity can apply business-specific rules to the governance of the relationship.

Terms of Service

A reaction from some reading this use case is that such a transfer might somehow violate the terms of service, or in some way be "cheating". A core principle of Decentralized Identifiers and Self-Sovereign Identity is that control is with the account owner to control and use, not the Service. However, the Service does have the ability to enforce terms of service. If there are requirements that the Service enforces, Verifiable Credentials can be be used to prove the account owner meets those requirements. The Service, on detection of a key rotation, must re-establish that the account owner (regardless of who that is) meets the requirements.

Distinction

Self-Sovereign Identity means that the Identity Owner is in control of their side of a relationship. They can independently transfer and manage that control according to the needs of the Identity Owner, and are not limited by the capabilities offered by the Service.

Use Case #8: Software Release Signing

Name

DID Software Release Signing (Christopher)

Background

T

Description

K

Sticky Wicket

T

Distinction

M

Use Case #9: Long-term, high stakes digital cooperation. Example: The United Humans funding and governance.

Name

Long-term, high stakes digital cooperation. Example: The United Humans funding and governance. (Bohdan)

Background

With the emergence and the adoption of blockchain, strong encryption and other technologies that enable digital sovereignty it becomes possible for people to cooperate directly in the digital space without any intermediaries between them. For now such sovereign cooperation was mostly limited to the short-lived, trade-like type of cooperation.

Persistent self-sovereign digital identities open a way for a long-term cooperation between humans, including cooperation on the large-scale, long-term projects.

Description

One of the big global cooperation projects that becomes possible with the advent of the technologies that enable digital sovereignty, iis the organization of The United Humans. The United Humans is modeled on the example of The United Nations. The purpose of The UH will be to protect human rights and improve human cooperation mainly in the digital space. In practice, the main task of the UH is going to be, developing and maintaining the set of critical (most important) tools for digital cooperation (humane social networking service, identity service, digital signatures service, human based money (money directly issued to humans), wallet, etc).

In order for The United Humans to be independent it should be created, governed and funded by the digital identities that uniquely represent humans and that are *under their complete (sovereign) control*.

The funding of The United Humans organization is going to be done by taking part of “human based” money issued by The United Humans organization. “Human based” money is money issued and distributed directly to the digital identities that uniquely represent living human individuals.

In order for these digital identities to be trusted to securely control money (blockchain tokens), they need to be self-sovereign, thus the need for them to be stored in the decentralized storage (rooted in blockchain).

Also, these digital identities that uniquely represent humans, need to be self-sovereign to sign Verifiable Credentials (digital documents) to be used in high stakes cooperation processes or events, for example: voting, signing contracts, managing property rights, etc.

The specification of Decentralized Identifiers provides a standard way to create such self-sovereign identities.

Challenges

For the organization of the United Humans to be fair (human centric) and truly independent it should be governed and funded by self-sovereign identities (free from any government or market coercion), that uniquely represent living human individuals. It is not yet proven by time, that Decentralized Identifiers (Identifiers stored in blockchain) will provide true digital sovereignty to the digital identities that represent humans.

Distinction

This use case underscores the need for Decentralized Identifiers that enable self-sovereign identities, required for the long-term, high stakes cooperation between humans in the digital space.

Use Case #10: Single Sign On

Name

Single Sign On for a website (Ryan)

Background

Passwords are notoriously misused ("123456"), stolen from the supposedly-secure database on the server-side, easy to forget when sufficiently secure, and never the last word in authentication for forgotten password situations. Proving control of a DID can replace storage and retrieval of a shared secret.

Description

Use DID as single-sign-on to a website, using DID Auth (especially cases like the example between a web page and web browser with a mobile identity app) directly or via the Credential Handler API. When desirable, the relationship can add a shared secret for 2FA (except does DID Auth include any extensions that enable this subsequent ascension without starting another socket?).

Note that what is stored on the server-side is a DID, so in cases where a successful attack reads (but does not mutate) the database, all that is revealed is linkage of the DID to use the site (so probably as a consequence the user should spawn a unique DID to reveal to that site), and any 2FA secret (which should be a random number for TOTP, instead of a phone number susceptible to carrier social engineering and SS7 bugs). In other words, the user's DID Auth procedures remain valid after the hack, even for that site.

Sticky Wicket

Transfer sign-on capability from control of a password to control of the DID, as shown in DID-Auth, using appropriate devices. Optionally include 2FA, although DID Auth doesn't handle that well, yet.

Distinction

This use case describes the most common authentication action for people on the Internet.

Use Case #11: Institutional Library Users

Name

Institutional Library Users (Tzviya)

Background

A member of an authorized user community, such as a University Library, gains access to subscription resources provided by multiple publishers. When the user is within the library's physical walls, she can access the materials with her authorized credentials. When she is on her mobile phone, she can access the same materials remotely. She is required to provide her credentials as a member of the authorized community to access the materials without paying a fee for the content.

Notes: There could be a single identifier that students use to sign in to library resources, no matter which attend. The IDs are NOT about the privileges attached to their relationship with any given university, nor are they attached to the relationship between a university and a resource provider. Those privileges would be associated with such IDs, but the IDs themselves are independent.

Description

- Universities A, B, C issue a "shared resource" credential to their students
- Students with the shared resource credential have access to libraries that recognize it.
- University D would like to issue the shared resource credential to their students
- University A,B,C give University D tools to issue the shared resource credential
- University B leaves the group, and their students are no longer allowed access to the shared resources

Sticky Wicket

T

Distinction

M

Use Case #12: Prescriptions

Name

A Prescription for Alice (Adrian)

Background

Alice wants help with her urinary tract infection (UTI) and is a bit touchy about her privacy. In the old days, she would have to make an appointment in-person and get a paper prescription to take to a pharmacy. She wants to save money and have peace of mind.

Description

Because she lives in Seattle, Alice is in a state that allows Planned Parenthood to diagnose and prescribe online https://www.plannedparenthood.org/get-care/get-care-online . Alice uses the identity wallet on her iPhone to register with the online medical practice. She tells the online practice her name is Althea with password-less authentication and a verified driver's license credential to prove that she's a WA resident. The remote physician, Bob, is licensed by the WA Board of Medicine and credentialed by Planned Parenthood of WA, Inc. He's securely signed in using the identity wallet on his smartphone. Bob issues Alice a digital prescription in the form of a verifiable credential and allows Alice to download it however she pleases. Alice is a librarian and trusts her local public library to erase their logs as allowed by law. She uses one of their computers to sign-in and do all of this. She snaps a picture of the QR code that is the prescription to take to the pharmacy. Charlie, the licensed pharmacist, scans the prescription QR code and fills the prescription. Alice pays cash.

Sticky Wicket

The challenge of this particular use-case is that only Bob and Charlie are verified identities and accountable for their interaction with Alice. Alice can be anonymous or pairwise-pseudonymous with both Bob and Charlie and everything just works. Alice, Bob, and Charlie all keep separate and legally authentic copies of the records of their interaction in case of dispute.

Distinction

The Prescription use-case is a common and high-value example of privacy engineering as we shift to convenient and cost-effective online commerce among licensed and unlicensed individuals as peers. Bob and Charlie benefit by reducing or even eliminating the influence of their respective institutions or employers and therefore make more money. They pass some savings to Alice who also gets increased peace of mind.

Use Case #16: Collective Identity

By Heather Vescent

Name: Collective Identity Use Case
DIDs for aggregate collective identity. Whereas multiple people create a collective identity that acts as more than the sum of its individuals, in a somewhat unified way.

- Infrequent ad hoc events/Santacon
- Renting/owning/sharing home together/utilities
- Informal joint venture/short-term business/emergent business “partnerships”
- The radical idea: Mutual Aid/the end of taxes: to be able to anonymously pay for other people for needs.

Notes/coments by drabiv on the w3c call - Aug 21 2018.
Very important use case for collective identity. We need a purpose for a public key. When we sign document in the name of the large document, it can be done by different people.

Background
A group of 6 people are organizing an event/conference. They are selling tickets and paying vendors. They are making arrangements with local bars and restaurants. Two of the people are handling the finances, one is handling ticketing, three are handling restaurants/catering/other bills. Another one is handling email marketing, which they must pay for. All of them want to update the team on their statuses.

This is a one off (or once a year) event. The activity is not focused on making money. Ticketing vendors and others expect a cut of the funds. The team pays a variety of vendors. They make enough in ticket sales to cover these costs, but one person always has to put themselves on the financial line - accepting funding from paypal and other payment platforms directly, taking on the tax burden, paying with their personal credit card. Not everyone in the team has the ability to take on the financial risk. They want to share the risk, enable each other to do the work, pay the people who needs to get paid. Another aspect is that each member brings their non-financial reputation to the team/event. This includes contacts, history, and their experience. This reputation is lent to the event to produce it, and both the reputation of the event grows and the reputation of the organizers grows as well. In the case that there is an issue or negative reputation situation, one of the organizers is a “fixer” to resolve any issues (financial, emotional, logistical, legal).

Description
Note: I would like to have a discussion about whether they = the collective entity, or they = the collective entity authorizing the individuals for these actions.

- They want to be able to log into jointly used accounts.

- They want to be able to manage payouts.
- They want to be able to know ticket sales data and information, without one person being the one in charge.
- They want to agree and approve payments to 3rd parties and vendors. And also each other's individual accounts. (If they could not use the group account).
- Probably more things.

Ruth is at a store buying supplies for the event. She wants to use the group bank account to pay for things. She has been authorized by others in the group to make purchases up to $$$ for the event. The receipt and other sales information is also saved to the group for auditing and tracking.

David is negotiating the venue cost, the legal paperwork, including insurance requirements, putting a deposit down. He is also working with catering option, that takes in information from ticketing information and catering options decision making by the whole team.

Raj and Jennifer are managing the finances and ticketing. Managing the number of tickets sold, the budget available, the transaction fees, other data associated with the ticket purchasers and the event. Jennifer manages the overall P&L budget and keeps a running audit of costs/payouts.

Sara and Chris are doing the marketing and outreach for the event, and like Ruth, need to purchase things with allocated budget.

Sticky Wicket
Today's systems are mainly set up for a single identity to use them, others allow teams to use them with incurred cost. There is no way for a group of people to create a collective identity with financial and log in ties. This use case is envisioned for a small group of people, but could be used for other ad-hoc, temporal business collaborations like film productions or other creative project based partnerships.

Distinctive
Instead of an individual having multiple identities, this flips that model by suggesting a collective identity composed of multiple individuals. How do the individual identities create, set rules/boundaries, revoke, track and audit these activities? How do the individual reconcile their collective identities with their individual identities? How do individual identities circulate in and out of the collective identity? There are many other questions to be asked and explored in this scenario.

Potential adjacent use cases:

- Delegated Identities: Parent, child. Guardian, pet. Adult child, adult parent. Unrelated adult, unrelated adult (non-formally bound romantic relationships, non-blood/legal family

relationships.
How is a collective identity similar/different from delegated identities?

- Human-Technology Collective Identities: Car/motorcycle owner (multiple owners) and the object. Solar panels that earn income for a home/property owner. Solar panel has identity to interface with the power grid. But also has identity information from property owner - is tied to their account.
- Human/AI Identity: Individuals augmented with technology are a new kind identity. Should they be addressed the same way human only identities are? Do they have other requirements/responsibilities?
- IoT Devices ownership/guardianship, vs who is habitating the space (surveillance, control)
- Underage income earners still under jurisdiction of parental control.
- Autonomous passive revenue income streams.

Use Case #17: Transaction Identification for Travel

By Heather Vescent

Name: Transaction Identification (e.g. travel use cases)

Background:
When traveling, hotels and other businesses need identification information. This is exacerbated when using new travel sites like AirBnB.

Description:
The problem: requirement to share personal information with hotels. Their data security is not secure. If one uses a stage name while traveling, you'll need to reconcile that with financial information that has a legal name. With AirBnbs and other alternative hotels, individual hosts may want a copy of the driver's license of not just the renter, but all guests (hotels often ask for this). But what are the security practices of these individuals? How can you confirm/share identity information to the satisfaction of the host/business owner and security PII of the user at the same time?

Whether the PII is collected in a computer database or on slips of paper, there may be poor security practices. It is not the business of the hotel to secure data, it is their business to provide overnight accommodations.

Thomas is a superhost in Joshua Tree and runs 3 AirBnBs. Even though AirBnB validates the guests identification before a reservation, Thomas always asks for a copy of their drivers license, which he stores as a photograph in his person cloud.

Angela is traveling for two weeks on a roadtrip. Each night is at a different motel. Each motel asks for identification information when registering for the room. Angela is concerned with the security practices of the PII collected by these motels.

Sticky Wicket:
Identity information is needed for transactions, but the people who collect and use this information have poor security practices - thus creating risk for the collected data. These systems may be low hanging fruit targets for hackers.

Distinctive:
Not sure if this is a good application of DIDs. It might be a heavy weight solution to this problem. There may be a better solution in conjunction with a specific payment mechanism (credit cards).

Potential adjacent use cases

- Where to use identity when traveling?
    - Stage names
    - Dead Name Club
- In conjunction with a travel AI/agent
- Real estate wire transfer details
    - Buying property, closing deals. Hacker has successfully phished a real estate agent, but wait quietly until a wire transfer message is sent to one of their buyers. After the legit real estate agent has sent the wire instructions, the hacker emails the buyers with *updated* wire instructions from the phished email account. The updated wire instructions go to the hacker's bank account.

Use Case #18: Digital Asset Grid

By Heather Vescent

The Past inside the Future: Return of the DAG (Digital Asset Grid)
A lot of what we discuss trying to do with DIDs reminds me of some work I did at Swift on the DAG/Digital Asset Grid project in 2011/2012. Some people working on DIDs were on that project (Drummond, Phil, Steve, Kaliya, Mary Hodder, myself and others I am sure I am forgetting) lead by the amazing Peter Vander Auwera.

#
Indulge me as I go into a little bit of history. The DAG project was the culmination of a yearish collaboration project to envision a digital safety deposit box. This was envisioned as a new platform service offered by banks to their customers to secure (and enable sharing of) digital documents.

The project was spearheaded by Innotribe, the innovation division of Swift. (Disclosure, I worked for them as both film producer and as their Americas innovation lead.) The project was funded in segments, and (I'll brag a little bit) my videos showed the future visions that helped secure internal funding to move the project forward. The video, Slices of Life, (which I created/produced) showed three use cases of the DAG.

Sadly, this project went dormant after completion. It was given to the community, but Swift funding ended (yay politics!). But I knew it was only a matter of time before someone would build something with the same idea. The only question I had was, when and who?

Enter DIDs. It was a shock and surprise to me to realize that blockchain might be able to realize that vision. Back then, in 2011/2012 we were really only looking at blockchain for cryptocurrencies (and I was totally drinking that kool-aid - as a researcher in the space. Yeah, my heart got broken by the crypto-bros. Little known fact I've never shared: I went to work for Swift with the secret intention of getting BTC transacted on their network. I was clearly too early.)

Anyway, as I'm working on the use cases for DIDs, I thought, why not revisit these use cases and see if they could be addressed with DIDs.

Here's the video, Slices of Life that shows these 3 use cases: https://vimeo.com/52354667

I haven't followed the format for each of these use cases. Instead, I'd like to see if anyone is interested in collaborating with me to further flesh these out and more directly apply them to DIDs. If you are, please contact me and we can put them into the use case structure that Joe requests. I think the video shows the Name, Background and Description clearly.

1. Selling a motorcycle (Developed in conjunction with Phil Windley & Steve F)
    a. Dealing with the various entities/ownership/data
    b. Potential buyer: verified credentials
    c. Potential sellers: reputation
    d. Motorcycle data: IOT
    e. Government ownership transaction
    f. Financial transaction

2. Due Diligence on a Business Deal (Developed in conjunction with Anthemis's investments and Dominic Sayers (https://twitter.com/dominicsayers)

    a. Potential business buyer: Verified credentials
    b. Developer:
    c. Legal and regulatory credentials: Making sure all the permits and etc are legit and up to date. Real estate disclosures & agreements.
    d. Transaction: Financial bids/closing

3. Baby and doctor interaction (Developed in conjunction with Fidor bank)
    a. Patient Delegation: baby
    b. Delegation: Parents
    c. Delegation: caretaker (grandma)
    d. Doctor
    e. Data about patient from doctor
    f. Data about patient from IOT device
    g. Sharing data with doctor
    h. Doctor authorizing pharmacy/medicine for patient

Use Case #19: Gun Purchase

By Heather Vescent and David Challener

Name: Gun Purchase
Or buying or selling any highly regulated product, that must check multiple federal and state databases.

Background
Buying guns is a highly charged topic in the US. There are federal regulations, state regulations, and even local municipality regulations in regards to concealed carry permits. There are limitations on the kinds of guns that can be sold per state (California vs Texas, eg. sales of AR-15 are not permitted in California, yet the gun is grandfathered for ownership.)

This use case was inspired by Motorcycle sale/purchase scenario from Heather Vescent's film made for SWIFT.

Description
California buying scenarios (following current state laws);

1. Allison wants to buy a pistol. She finds one at a local dealer. She fills out the paperwork at the shop, puts down her credit card, proves her training certification number. All this is verified while she waits 10 days before she can pick it up.
2. Jason is buying a rifle from a friend, Andy. They exchange money, but have to do the legal transfer at a registered dealer. They meet, with the gun, at a shop in Burbank. Andy must prove a bunch of information about himself, Jason has to complete a bunch of information about himself, and then the dealer will confirm all the information. They fill out the

paperwork, hand the gun over to the dealer, who holds it for 10 days before Jason can pick it up.

North Carolina buying scenarios (following current state laws);

3. Allison wants to buy a pistol. She finds one at a local dealer. She goes to the local police station and registers for a permit. Two weeks later she is called and told she can pick them up. Since she does not have a “carry permit”, she gets two documents, each of which allow buying a gun for the next 5 years. She goes to the gun dealer and presents the permit, and driver's license. The dealer then goes through a background check and checks that Allison is at least 21 years old. 10 days later she receives her gun.
4. Jason is buying a rifle from a friend, Andy. Again Jason must have gone through the process to get a permit. Jason presents the permit to Andy. Andy must know that Jason is at least 18 years old (not 21, as is required for a gun dealer) and resides in North Carolina. They exchange money, and Jason gets the gun. (No background check is necessary,)

Other transfer scenario

- Owner sells for money
- Owner transfers registration (no money) (e.g. relationship ends)
- Owner wishes to give the gun to a relative out of state
- Owner wishes to sell the gun out of state
- Owner moves to another state
- Owner dies, what to do
- Owner wishes to compete at a shooting contest in another state

Sticky Wicket

In order to buy a gun, sellers must check the status of the buyer in multiple databases. Much like the Motorcycle scenario, there are requirements for buyer, object, seller, and government registration. To make this more complex, state laws vary.

Buyer: Can this individual buy a gun?

- Identification: who is it?
- How old is the individual?
- Where does the individual reside?
- Background check
- Firearm safety certification
    - Criminal database: Check for felony convictions
    - US Military database
    - Medical/Health database: Check for psychological disorders
    - State database
    - Federal database
    - Others: e.g. “Of known good reputation”
- Funds
- Firearm Registration
    - # guns allowed ownership

    - # guns already owned

Firearm: Can this gun be sold in this jurisdiction?

- Gun must be checked to be on “sale” list
- Legit, stolen
- Cross state lines?
- Where was it registered?

Seller: Can this person sell a firearm

- Registered dealer
- Waiting period
- Online sales / private seller / gunshow

Government

- Various databases
- Gun registries

Firearm education

- Certification records

Distinction

This is a distinct use case because it requires information from many different databases. It requires customization based on local and federal laws. And it’s constantly changing.

Use Case #20: Code Signing

Name: Code Signing

One of the main uses today of non-Certificate Authority identity is for code signing.

Background

Description

Sticky Wicket

PGP is 27+ year old architecture, it has a variety of issues (see RWOT #1 topic papers), it doesn’t support revocation notification,

Distinction

(Note this could be attached to Amira)

Use Case #21: Exchange of Business Documents

Name: Exchange of Business Documents

Trusted exchange of business documents such as Purchase Orders, Invoices, Waybills, Shipping Confirmations, etc. between two parties.

Background

TODO

Description

TODO

Sticky Wicket

TODO

Distinction

TODO

Use Case #NEXT

Name

D

Background

T

Description

K

Sticky Wicket

T

Distinction

M