Engineering Privacy for Verified Credentials: In Which We Describe Data Minimization, Selective Disclosure, and Progressive Trust

A White Paper from Rebooting the Web of Trust V

by Lionel Wolberger (Platin.io), Brent Zundel (Evernym/Sovrin), Zachary Larson (Independent), Irene Hernandez (Independent), and Katryna Dow (Meeco)

INTRODUCTION

We often share information on the World Wide Web, though some of it is private. The W3C Credentials Community Group focuses on how privacy can be enhanced when attributes are shared electronically. In the course of our work, we have identified three related but distinct privacy enhancing strategies: "data minimization," "selective disclosure," and "progressive trust." These enhancements are enabled with cryptography. The goal of this paper is to enable decision makers, particularly non-technical ones, to gain a nuanced grasp of these enhancements along with some idea of how their enablers work. We describe them below in plain English, but with some rigor. This knowledge will enable readers of this paper to be better able to know when they need privacy enhancements, to select the type of enhancement needed, to assess techniques that enable those enhancements, and to adopt the correct enhancement for the correct use case.

THREE EXAMPLES

Three examples of how people would like their privacy preserved in the process of sharing credentials help to illuminate these three techniques.

Diego attempts to use an online service and is asked to share his location in order to prove his geolocation. Diego hesitates, since the service doesn't need his location everyday, everywhere. He knows that the service may share this information with other parties without meaningful consent on his part. Thoughts pass through his mind: What location data does the service actually need? What will it read in future? Is there a way for him to share his location just this once, or to only share an approximate location?

Selena hands her driver's license to a bouncer to prove she is of drinking age. As he looks it over, she sees him inspecting her date of birth and home address. He only needs to know that she is over 21. Is there a way to disclose that she is indeed old enough without revealing her actual age, along with her home address and city of residence as well?

Proctor, negotiating with a real estate agent to purchase a home, reveals a letter from his bank stating his credit limit. He wanted to reveal its approximate amount only, but the agent insisted on verifying that the letter was authentic. Proctor feels the agent now has the upper hand in the negotiation, as the letter reveals more than just its authenticity. Could he have revealed only an approximate amount and reveal more details as the negotiations progress?

Each story features information that is verifiable: a home address, age, or credit limit. We call such information a credential,

and a detail of a credential we call an attribute. We have three strategies for enhancing the privacy of digitally shared credential attributes, and each story highlights one. Diego's story highlights the need for "data minimization," Selena's for "selective disclosure," and Proctor's for "progressive trust." Let's examine each one in detail before discussing enablers.

PRIVACY ENHANCEMENTS

We propose the following three privacy enhancements. (Sources used to curate these definitions are listed in Appendix A.)

Data Minimization

Data minimization is the act of limiting the amount of shared data strictly to the minimum necessary in order to successfully accomplish a task or goal. There are three types of minimization:

- **Content minimization** – the amount of data should be strictly the minimum necessary.
- **Temporal minimization** – the data should be stored by the receiver strictly for the minimum amount of time necessary to execute the task.
- **Scope minimization** – the data should only be used for the strict purpose of the active task.

Data minimization is enacted primarily by policy decisions made by stakeholders in the credentials ecosystem:

- Credential issuers ensure that credentials may be presented in such a way as to enable data minimization. This may require issuing multiple, related, granular sub-credentials.
- Credential inspectors establish in advance policies regarding the data they will examine:
    - what is the minimum data necessary to accomplish the task or goal?
    - what is the minimum time the data can be stored to execute the task?
    - what processes ensure that the data is applied only to the task at hand and does not, by a process of scope creep, become applied to other tasks or goals?

Data minimization policies impact selective disclosure, the next privacy enhancement.

Selective disclosure

Selective disclosure is the ability of an individual to granularly decide what information to share. Stakeholders in the credentials ecosystem enable selective disclosure capabilities in the following ways:

- Credential issuers format the credential and its attributes in such a way as to enable selective disclosure. As with the strategy of data minimization, they may issue multiple, related, granular sub-credentials. Each attribute and the overall credential may be formatted to support cryptography, a capability described in more detail below.
- Credential inspectors ensure the request is framed in such a way as to enable selective disclosure, using the cryptographic tools required.

Once data minimization policies and selective disclosure are in place, the third and last enhancement can be applied.

Progressive Trust

Progressive trust is the ability of an individual to gradually increase the amount of relevant data revealed as trust is built or value generated.

To enable progressive trust capabilities, stakeholders in the credentials ecosystem act in the following ways: * Issuers format the credential(s) in such a way as to enable progressive trust. This may require issuing multiple, related, atomic sub-credentials. It also may require formatting the credential to support mathematical queries and cryptographic proofs. Finally, the issuer's data model may express how the various sub-credentials are related in a scenario involving progressive trust. * Inspectors ensure that requests are framed in such a way as to enable progressive trust. They structure the communication in order to to gradually escalate credential requests in order to enable a subject to progressively trust the inspector more and more, revealing the minimum data necessary to accomplish each step of the task or goal and revealing more and more as the mutual communication progresses.

CRYPTO ENABLERS

Implementing privacy enhancements depends on organizational decisions. Determination of the data needed, with an eye towards data minimization, along with a clear model of how data is used over the lifecycle of engagement, goes a long way towards enabling progressive trust. However, policies are not enough. When enhancing privacy online, some data parts must be revealed while others remain concealed. Concealment is achieved mostly by the art of cryptography, from the greek word "kryptos," meaning hidden, like in a crypt. Crypto (a short word we will use for cryptography) enables us to achieve our goal by means of three primary enablers: having a secret, having a difficult mathematical task, and having zero-knowledge enablers. The children's "Where's Waldo?" illustrated book series helps us to understand these three enablers. In these books a distinctively dressed man appears only once on each page, wearing a striped hat. Readers are asked to scour the page and locate him. We can understand the three enablers by examining Where's Waldo one step at a time.

- **A Secret**: For the new reader, Waldo's location is a secret. The illustrator knows it, and the reader doesn't. The reader is encouraged to search the page and find Waldo, but that is a difficult task. Some readers give up and ask someone who has already found Waldo to show them his location. In essence, they are asking another reader to reveal the secret. Once found, a reader could keep the information secret by circling Waldo in red and storing the book in a safe. This amounts to storing the secret for future use. Secrets are essential to crypto. They are usually called keys, and they must be managed carefully.
- **A Difficult Task**: Waldo is difficult to find on the page. The reader has to search everywhere and mistakenly identify many Waldo look-alike characters before reaching a satisfactory conclusion and finding him. Yet when he is finally discovered, or someone points Waldo out, it's easy to see where he is. That's why it's a fun task. This difference between the difficulty of conducting the task and the ease of verifying the task lies at the heart of cryptographic enablers.
- **A Zero Knowledge Enabler**: Can you prove you found Waldo without revealing the secret of his actual location on the page? There is a simple way to do so. Take a rectangular piece of white cardboard that is much larger than the book. Cut a hole exactly fitting Waldo to reveal his silhouette only, nothing else. You can now show Waldo to anyone, peeking out of the cardboard. Yet the cardboard is wide and opaque, hiding the book thoroughly, so a verifier has no idea where Waldo is on the page. The puzzle was solved and someone verified the achievement, without revealing any knowledge of how to solve the puzzle. The secret is still safe, the task still just as difficult as before.

Where's Waldo books are drawings, while crypto is built from mathematical equations, basically puzzles based on numbers. We provide the interested reader with a layman's overview in Appendix B.

THREE SOLUTIONS

We now return to our opening examples, apply the privacy preserving strategies and enablers described, and describe the improved outcomes.

The online service that **Diego** uses does an internal policy review and realizes (a) it only needs a location when a user signs up for an account, and (b) it does not need an exact address, only the county district. It changes its interface to request a Verifiable Credential for Diego's location. Diego's system creates this credential for him, which can be inspected to reveal the county district. The crypto to enable this would be similar to that described in Appendix C. With this data minimization, the online service has less risk of violating data protection rules, is less a target for hacking, and has lower overall costs, while at the same time preserving Diego's privacy.

The bar seeking to verify **Selena**'s age uses selective disclosure as built into the Verifiable Claims system. Selena will no longer share her date of birth. Instead, Selena creates a secret that we harness to craft a crypto-formatted credential. This crypto makes it easy to verify her age, but difficult to determine her exact date of birth. The bouncer's system can perform a zero-knowledge proof to determine the credential is valid and that Selena is older than twenty-one, without revealing her birthday or her secret. The bouncer sees she is over twenty-one without seeing her date of birth, residence address, or any other unnecessary information. In Appendix C we show the process step-by-step.

The real estate agency working with **Proctor** implements a data model specifying what is required at each step of the real estate negotiation. The first step requires only proof of being an account holder in good standing at a known bank, so Proctor does not have to reveal the detailed letter at this point. As their negotiation continues, Proctor reveals more and more information as required. Some steps of the process may share Verifiable Claims encoded with crypto.

SUMMARY

The World Wide Web accelerates the sharing of credentials and other digital interactions, and many regulations have been passed and strategies proposed to protect privacy, some of which require cryptography. To align terminology, the World Wide Web Credentials Community Group has found three related but distinct privacy enhancing strategies that create a useful rubric for discussing the challenges and arriving at solutions. We share the examples of Diego, Selena, and Proctor and propose "data minimization," "selective disclosure," and "progressive trust," with accompanying crypto protocols as useful semantics for accelerating the adoption of digital interaction while protecting privacy.

Appendix A: Definition Sources

This section contains definitions we curated, based on research and oral interviews, to create the definitions of data minimization, selective disclosure and progressive trust.

DATA MINIMIZATION

Definitions of data minimization that we considered in the formation of our definition above.

- GDPR Rec.39; Art.5(1)(c) definition: "The personal data should be adequate, relevant and limited to what is necessary for the purposes for which they are processed. This requires, in particular, ensuring that the period for which the personal data are stored is limited to a strict minimum. Personal data should be processed only if the purpose of the processing could not reasonably be fulfilled by other means."
- Reducing your overall footprint of data outside of your control. Can be accomplished by using selective disclosure.
- Adequate, relevant and non-excessive.
- Reducing the amount of data you are sending in a payload to only the one ... needed. That prevents leakage of confidential information.
- Providing people with the information they need without revealing non necessary info. If I need to prove if I am old enough without revealing an actual birthdate.
- Best practices – your should deeply inspect your use case and come to a conclusion as to what is the minimum data you need to accomplish your goal. Don't be greedy. Data has proven to be toxic.
- Mathematical – finding a way to express the data that you wish as an equation related to the data you have.
- Minimizing the amount of data to achieve your goal or communicate what you need to.
- Designing systems to operate efficiently in order to maximize privacy.
- Choosing to only share the minimal amount of data about yourself or something during an interaction.
- Trying to keep the amount of info that is being disclosed as limited as possible to the requirements of the vulnerability. The minimum is what ... will lead them to move to action.
- Always happens in a context: a relationship where the two parties are considering interacting in some way. Sending only the signals that I want to send and that are needed by the other party, hem to interact with me in a particular
- The least amount of data needed for a system to function
- Collecting the least amount of date for the highest outcome.
- Also known as minimal disclosure, data minimization is the principle of using the least amount of data to accomplish a transaction. This is incumbent on all three parties in an exchange. The holder should attempt to share the minimum. The issuer needs to create attributes designed for composition and minimal use, as opposed to monolithic credentials with all the data. The verifier needs to ask only for what they need. The motivation to minimize data is that unneeded data is potentially "toxic."

SELECTIVE DISCLOSURE

Definitions of selective disclosure that we considered in the formation of our definition above.

- Ability to decide what info you give and how it can be used.
- Smart disclosure, allows [selecting] what information to give based on logic.
- Blind search. You can decide who gets to see what.
- Means by which we achieve data minimization. Form of policies. Ability to mask attributes that you do not have to

share.

- Relates to mathematical definition – the computational ability to reveal only parts of your data profile.
- Act of communicating or revealing only what you intend to, and not any peripheric data
- Having granular control over the ways in which data is shared
- Is a pattern for user interfaces allowing people to choose what to share about them during an interaction
- Method for achieving data minimization where only certain signals are being shared and there is control of who it is being shared with. That control is never perfect. The communication channel matters.
- An entity having granular control on what's revealed.
- The individual having the freedom to decide what to share, or the acquirer using data minimization approach requesting the minimum amount amount of data for the maximum impact

PROGRESSIVE TRUST

Definitions of progressive trust that we considered in the formation of our definition above. Note that we included definitions of progressive trust and progressive disclosure as well.

- Procedure for increasing revelation of relevant data as the communication proceeds. As we continue to communicate we decide to reveal more information. It becomes more generous as trust builds.
- Being able to reveal more data as you need to given certain conditions
- Information is disclosed as needed when needed.
- You can choose to increase the amount of data you disclose over time as needed.
- Taking as little vulnerability as possible at the beginning, then gaining information and becoming willing to take on additional vulnerability by revealing more information.
- Trust is built through step by step interactions where we start making ourselves vulnerable in a very small way and we observe how this works out. Based on results we consider making ourselves further vulnerable or not. It is about increasing levels of familiarity and prediction making (I am better able to predict your behavior).
- Releasing information as needed
- Escalation of the previous steps (data minimization, selective disclosure) in line with the value increasing.
- Purpose binding is the auditable use of data, so I can audit the use of my data and determine that it was used for the purposes declared. Progressive trust is the feeling of assurance and safety that develops over time, based on a history of data used only for its bound purposes, and so based on this feeling a data holder will be ready to share more data or other data, if at some point in the relationship this other data is requested.
- Trust is required when you depend on the actions of someone who you can't control.

Appendix B: Basic Crypto Concepts

This appendix describes basic cryptographic concepts critical to the privacy preserving engineering of credential attributes. For readability, we use the short word, "crypto."

OVERVIEW

Crypto is a huge field with highly specialized jargon, too much to cover here. But non-specialists would benefit from some understanding of relevant crypto in order to make informed decisions. We begin with a brief overview of several concepts from number theory that serve as a foundation for all crypto used in this process. This is a curated list of topics progressing from the simple to the more complex. Notice how ideas are re-used and layered as you read on.

NUMBER THEORY

Number theory refers to the study of the behavior of integer numbers such as one, three, or two hundred. The following are behaviors of these numbers that make them useful for crypto:

- **Prime or not**: Some numbers are only divisible by themselves and one. These are called 'prime.'
- **One-way function**: A numerical function that takes a publicly known number, and without any secret information, computes a value. Like a one-way street, the computation goes only one direction. Given the computed value, it is hard to find the publicly known number.
- **Clock arithmetic**, aka modular arithmetic: a system of arithmetic where numbers "wrap around" upon reaching a certain value. A familiar use is in the ordinary clock, in which our day is divided into twelve-hour periods. If the time is seven o'clock now, then ten hours later it will be five o'clock, though a military man might say seventeen hundred hours. Even he will say that ten hours later it is three o'clock, and not twenty-seven hundred hour, because his clock time "wraps around" every twenty-four hours (as opposed to twelve).
- **Groups and Finite Fields**: Some subsets of all integers form a "group" that behaves in ways very useful to the performance of cryptography. In extremely simplified terms, a group is a self-sufficient set of integers, where any possible manipulation returns an answer from within the group. Finite fields are types of groups that satisfy certain demanding properties. Notice how this resembles clock arithmetic, where the same numbers are used over and over again.
- **Discrete Logarithms**: A discrete logarithm is a property for numbers in a group. Since there is no efficient method for computing discrete logarithms, they form a "difficult problem" and so are very useful in cryptography. (The logarithm `log(b)` of `a` is an exponent `x` such that `b^x` (`b` raised to the `x` exponent) = `a`.)
- **Quadratic Residues**: Quadratic refers to 'squared' numbers, a number raised to the second exponential power. Quadratic residues are a useful property of squared numbers as they behave in modular arithmetic.

PRIMARY OBJECTIVES

The curious behavior of numbers is exploited to achieve four primary crypto objectives.

- **Confidentiality**: a hidden part of a credential cannot be understood by anyone for whom it is unintended. Often called "privacy," we avoid that word here since it can mean many things in addition to confidentiality.

- **Authentication**: the identity of information shared can be validated as authentic.
- **Integrity**: the revealed part of the credential cannot be altered without such alteration being detected. Also known as validity, fidelity or verifiability.
- **Non-repudiation**: aka non-deniability, a credential's creator cannot deny at a later stage his or her involvement.

TEN CRYPTO CONCEPTS

Over the decades hundreds if not thousands of crypto protocols, processes, algorithms and protocols have been innovated to achieve these objectives, by cobbling together the above six behaviors in different ways. We present here a brief tour of the ten most significant ones in our field of verifiable credentials:

- **PKI** or "public and private keys": a system that lies at the heart of most relevant crypto since a publicly shared digital asset can be locked to, or encumbered by, a private key that is kept secret. Only the person with knoweldge of that private key can, with the right software, unlock that asset. This enables a broad range of activities such as "signature," "authentication," and "certificate validation." In general we call these activities PKI, a public key infrastructure.
- **Signature**: a signature in this context is a use of PKI. A valid signature gives a recipient "authentication", confidence that the message was created by a known sender; "non-repudiation," that the sender cannot deny having sent the message; and "integrity," that the message was not altered in transit. Signatures enable every cryptographic objective except for confidentiality. There are many types of signature schemes in use including Digital Signature Algorithm (DSA), Camenisch-Lysyanskaya (CL) signatures, and Boneh–Lynn–Shacham (BLS) signatures.
- **Key exchange**: exchange methods enable two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher. Diffie–Hellman is a common example.
- **Elliptic-curve cryptography** (ECC): an approach to PKI based on the numeric structure of elliptic curves over finite fields. ECC is useful as it requires smaller keys compared to non-ECC cryptography. There are many variants of ECC used including Edwards-curve Digital Signature Algorithm (EdDSA).
- **Hash or message digest**: one-way functions, such as SHA-256. A set of many one-way functions may be applied to a tree of data to form a Merkle Tree (or trie).
- **Zero-Knowledge** (ZK): zero knowledge is defined above loosely as a set of practices where some data is revealed while other parts are kept secret. Many ZK methods are used in cryptography incuding Fiat Shamir, Proof of knowledge of discrete logarithms, ZK Snarks, and ZK Starks.
- **Accumulators**: a form of ZK, a cryptographic accumulator is a one-way membership function that answers a query as to whether a potential candidate is a member of a set without revealing the individual members of the set. Similar to a one-way hash function, cryptographic accumulators generate a fixed-size digest representing an arbitrarily large set of values. Some further provide a fixed-size witness for any value of the set, which can be used together with the accumulated digest to verify its membership in the set.
- **Commitment**: a cryptographic commitment, which allows one to commit to a chosen value (or chosen statement) while keeping it hidden to others, with the ability to reveal the committed value later.
- **Witness**: a term that has different applications in cryptography. In this paper, a witness is a value used in a cryptographic accumulator. In Bitcoin the unlocking signature is called the "witness data."

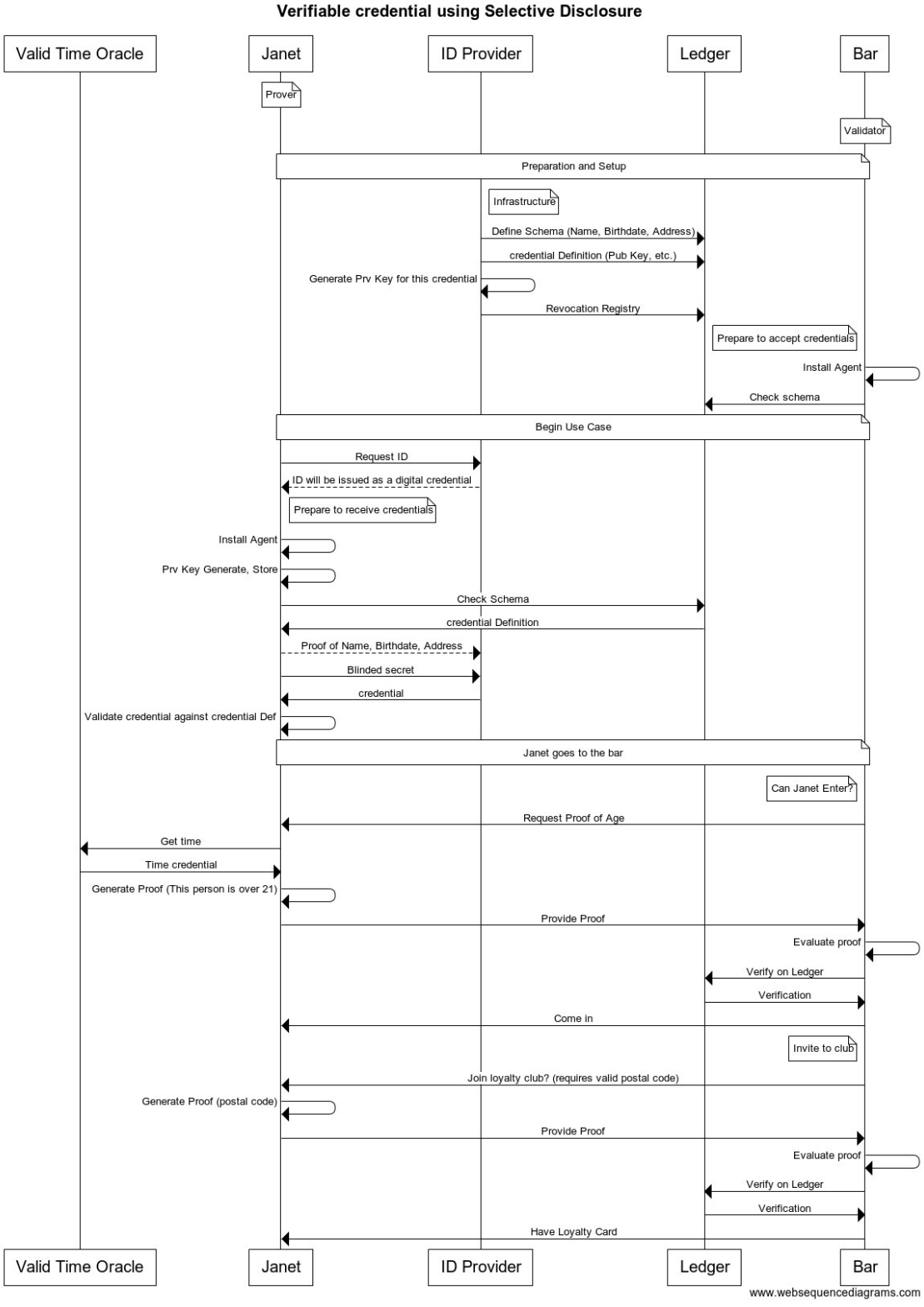
- **Quantum Computing** and Cryptography: as quantum computing is developed, it poses a threat to the difficulty of puzzles. For example, they are likely to be much faster at determining if a number is truly prime or not.

Appendix C: Drinking Age Credential Implementation

The birthday of an individual is formatted into a verifiable credential, which can be inspected to reveal the age of the credential holder without revealing their birthdate. The flow described here is based on the developing Verifiable Claims standard of the W3C Credentials Community Group. It uses cryptography developed by Jan Camenisch, as implemented by Sovrin.

This is a work in progress. Note that other types of crypto could be applied to achieve the same privacy preserving goals.

COMMUNICATION FLOW



CRYPTO DETAILS

Below are some of the detailed mathematics involved in issuing a verifiable credential as implemented by Sovrin, a non-profit organization dedicated to managing a decentralized, public network for the purposes of self-sovereign identity.

Issuer Setup

The following setup is a necessary precursor to issuing a privacy-preserving credential.

Compute

Perform the mathematical calculations required to curate the essential ingredients of the operations we are about to perform. Some of these results, like the private keys, are very sensitive and must be kept secret by the credential holder; others are to be shared.

- Random p', q', 1024-bit prime numbers, such that $p = 2p' + 1$ and $q = 2q' + 1$ are both 1024-bit prime numbers.
- $n = p \cdot q$.
- Random quadratic residue: $R \bmod n$
- Random $r_0, r_1, \ldots, r_L$ a $[2: p' \cdot q' - 1]$, where L is the number of attributes in the credential.
- $z = R_0^{r_0} \bmod n$
- $\forall i = R_i^{r_i} \bmod n, 1 \le i \le L$
- Issuer private key $SK = p' \cdot q'$
- Issuer public key $PK = \{n, R, z, \forall 1, \ldots, \forall L\}$

Proof of Correctness

As a result of the above computations, we then curate the following. This proof, along with the public keys, is the computational algorithm that will be used to validate the credential.

- Random $r'_0, r'_1, \ldots, r'_L$ a $[2: p' \cdot q' - 1]$
- $z' = R_0^{r'_0} \bmod n$
- $\forall' i = R_i^{r'_i} \bmod n, 1 \le i \le L$
- $c = H(z \| \forall 1 \| \ldots \| \forall L \| z' \| \forall'1 \| \ldots \| \forall' L)$
- $r''_0 = r'_0 + c \cdot r_0$
- $r''_i = r'_i + c \cdot r_i, 1 \le i \le L$

The Cred Def is comprised of the public key and the proof of correctness; this is published to the distributed ledger.

Issuing a Credential

With setup complete, we can now issue the credential in a privacy-preserving manner.

For Each Credential

For each credential issued, perform the following operations.

Issuer Computes

A cryptographic accumulator is constructed in order to enable zero-knowledge queries further on. It is a one-way membership function, including the claim in the membership set. The operation can then answers a query as to whether a potential candidate is a member of a set without revealing the individual members of the set.

- $\underline{N}\ \dot{T}$ = accumulator index
- $\bar{R}\ \dot{T}$ = user index
- $\underline{T}\ 2 = \eth\ S\ U_{\S}\ (\underline{N}\ \dot{T} \| \bar{R}\ \dot{T})$
- 256-bit integer representations of each of the attributes: $\underline{T}\ 3, \ldots, \underline{T}\ t$
- $\underline{t}\ 0$ = nonce

Issuer Sends 0 to Prover

This nonce is provided to the Prover for calculation of the Prover's proof of correctness.

Prover Receives 0 and Computes the Following

The prover aggregates and prepares public keys for use in validating the signatures. The prover also commits to a chosen value while keeping it temporarily hidden, making the calculation binding.

- Retrieves Issuer's public key $\underline{t}\ T\ \dot{S}$
- Retrieves Issuer's proof of correctness
- Generates:
  - $\underline{T}\ 1$ = pedersen commitment of claim link secret
  - Random $u_{\S}'$, $u_{\S}''$, $\underline{T}\ '1$
- $\underline{t}\ 1$ = nonce

Prover Verifies the Issuer's Proof of Correctness

- $\dot{s}\ \hat{}\ = \dot{s}\ \dot{S}\ R_{\underline{r}}\ ''\dot{s}\ \mod \underline{t}$
- $\dot{r}\ \hat{}\ \dot{T} = \dot{r}\ \dot{T}\dot{S}\ R_{\underline{r}}\ ''\dot{r}\ \dot{T} \mod \underline{t},\ 1 \le \dot{T} \le t$
- Verifies $\dot{S} = \eth\ S\ U_{\S}\ (\dot{s}\ \| \dot{r}\ 1 \| \ldots \| \dot{r}\ t \| \dot{s}\ \hat{}\ \| \dot{r}\ \hat{}1 \| \ldots \| \dot{r}\ \hat{}t)$

Prover Computes

- $\bar{R}\ = R_{u_{\S}}{}'\dot{r}\ 1\underline{T}\ 1 \mod \underline{t}$
- $\bar{R}\ ' = R_{u_{\S}}{}''\dot{r}\ 1\underline{T}\ '1 \mod \underline{t}$
- $\dot{S}\ ' = \eth\ S\ U_{\S}\ (\bar{R}\ \| \bar{R}\ ' \| \underline{t}\ 0)$

- $\dot{u}\hat{} = \dot{u}'' + \dot{S}'\dot{u}'$
- $\underline{T}\hat{}1 = \underline{T}'1 + \dot{S}'\underline{T}\ 1$

Prover Sends □ = { □ , □ ', □ ^, □ ^1, □ 1 } to the Issuer

Issuer Verifies Prover Setup

- Computes $\bar{R}\hat{} = \bar{R}\text{-}\dot{S}\ \dot{R}_{\dot{u}}{}^{\dot{r}\ 1\underline{T}}\ 1 \bmod \underline{t}$
- Verifies $\dot{S}' = \eth\ \ \dot{S}\ \ \dot{U}_{\dot{S}}\ \ (\bar{R}\ \|\ \bar{R}\hat{}\ \|\ \underline{t}\ \ 0\ )$ ##### Issuer Signs the Credential by Computing the Following
- $\dot{R} = \dot{s}\ \ / (\bar{R}\ \dot{R}_{\dot{u}} * \dot{r}\ \ 2\underline{T}\ \ 2\dot{r}\ \ 3\underline{T}\ \ 3 \cdots \dot{r}\ \ \dot{t}\ \underline{T}\ \ \dot{t}\ \ ) \bmod \underline{t}$
- $\dot{s}\ \ = \dot{S}\text{-}1 \bmod \dot{t}\ \ 'U'$
- $\underline{N}\ \ = \dot{R}\,\dot{s}\ \ \bmod \underline{t}$
- $\underline{N}' = \dot{R}\,\dot{u}\ \bmod \underline{t}$
- $\dot{S}'' = \eth\ \ \dot{S}\ \ \dot{U}_{\dot{S}}\ \ (\dot{R}\ \|\ \underline{N}\ \ \|\ \underline{N}'\|\ \underline{t}\ \ 1\ )$
- $\dot{U}_{\dot{S}} = (\dot{u}\ \text{-}\ \dot{S}''\dot{S}\text{-}1) \bmod \dot{t}\ \ 'U'$ ##### Issuer Sends $\dot{P} = \{\underline{N}, \dot{S}, \dot{u} *, \dot{U}_{\dot{S}}, \dot{S}'', \underline{T}\ \ 2, \ldots, \underline{T}\ \ \dot{t}\ \ \}$ to the Prover ##### Prover Receives $\dot{P}$ and Does the Following ###### Prover Computes
- $\dot{u}\ \ = \dot{u}' + \dot{u} *$
- $\dot{R}' = \dot{s}\ \ / (\dot{R}_{\dot{u}}\,\dot{r}\ \ 2\underline{T}\ \ 2\dot{r}\ \ 3\underline{T}\ \ 3 \cdots \dot{r}\ \ \dot{t}\ \underline{T}\ \ \dot{t}\ \ ) \bmod \underline{t}$
- $\dot{s}\ \ ' = \dot{S}'' + \dot{U}_{\dot{S}}\ \ \dot{S}$
- $\underline{N}\hat{} = \underline{N}\,\dot{s}\ \ '\dot{R}_{\dot{u}}\ '\dot{U}_{\dot{S}}\ \ \bmod \underline{t}$

Prover Verifies

- $\dot{S}\ \$ is prime and $2596 \leq \dot{S}\ \leq 2596 + 2119$
- $\dot{R}' = \underline{N}\ \dot{S}\ \ \bmod \underline{t}$
- $\dot{S}'' = \eth\ \ \dot{S}\ \ \dot{U}_{\dot{S}}\ \ (\dot{R}'\ \|\ \underline{N}\ \ \|\ \underline{N}\hat{}\ \|\ \underline{t}\ \ 1\ )$ ###### Prover Stores Primary Claim $(\{\underline{T}\ \ 1, \ldots, \underline{T}\ \ \dot{t}\ \ \}, \underline{N}, \dot{S}, \dot{u})$

FOR ADDITIONAL INFORMATION

The crypto used here is originally from the Identity Mixer.

The Sovrin team shares additional information and working code at the following links.

- * Verifiable Credentials Code
- * Verifiable Credentials Example Usage in Python

References

- W3C Credentials Community Group Home Page
- Data Minimization and Selective Disclosure Repo
- Camenisch, Lysyanskaya. An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation
- Pfitzmann, Hansen. 2010. A terminology for talking about privacy by data minimization: Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management
- Cooper, Tschofenig, Aboba, Peterson, Morris, Hansen, Smith, Janet. 2013. RFC6973. The draft can also be helpful, "This document focuses on introducing terms used to describe privacy properties that support data minimization."
- Hansen, Tschofenig, Smith, Cooper. 2012 Privacy Terminology and Concepts. Network Working Group Internet-Draft Expires: September 13, 2012
- Longley, Sporny. Redaction Signature Suite 2016. 26 June 2017. Draft Community Group Report "This specification describes the Redaction Signature Suite created in 2016 for the Linked Data Signatures specification. It enables a sender to redact information in a message without invalidating the digital signature."

ADDITIONAL CREDITS

Lead Author: Lionel Wolberger (Platin.io)

Authors: Brent Zundel (Evernym/Sovrin), Zachary Larson (Independent), Irene Hernandez (Independent), and Katryna Dow (Meeco)

About Rebooting the Web of Trust

This paper was produced as part of the Rebooting the Web of Trust V design workshop. On October 3rd through October 5th, 2017, over 50 tech visionaries came together in Cambridge, Massachusetts to talk about the future of decentralized trust on the internet with the goal of writing 3-5 white papers and specs. This is one of them.

Preliminary Workshop Sponsors List: BigChainDB, Blockchain Lab, Digital Contract Design, IDEO, IPFS, Protocol Labs, Toni Lane Casserly

Workshop Producer: Christopher Allen

Workshop Facilitators: Christopher Allen, with additional paper editorial & layout by Shannon Appelcline.

What's Next?

The design workshop and this paper are just starting points for Rebooting the Web of Trust. If you have any comments,

thoughts, or expansions on this paper, please post them to our GitHub issues page:

> https://github.com/WebOfTrustInfo/rebooting-the-web-of-trust-fall2017/issues

The next Rebooting the Web of Trust design workshop is scheduled for September 26th-28th, 2018 in Mississauga, Ontario. If you'd like to be involved or would like to help sponsor these events, email:

> rwot-leadership@googlegroups.com
