Vereign

User Story

Version 1

vereign, to • verb • /vɛre'ɪn/
(short for verified & sovereign)

to protect privacy, integrity and authenticity by self-sovereign identity and data

vereign.com

Allow us to introduce our proposal for a new service category unlike any currently in existence on the internet today.

Based on Blockchain technology, decentralized networks with democratic oversight, and self-sovereign identity (SSI), this approach enables the seamless addition of integrity, authenticity, and privacy to any kind of service.

Our service comprehensively covers hardware, software, ownership, and governance, and our solution has advanced off the drawing board to begin the trial stage in Q4 2018. In 2019, our service will be available to 3.7 billion daily users immediately following the successful trial period.

With decades of experience in technology, business, and law on their side, our co-founders worked tirelessly together for over a year with our exceptional advisory board. We know the results to be practical and achievable. Over that period of time, we assembled a world-class team to develop the proof of concept, and the results stand up to Occam's Razor[1] in that it's the most robust and simplest possible solution that provides the essential benefits required. Simple and flexible, the concept is based on a completely Open Source software stack, protects universal rights of usage and adoption, and enables an ecosystem of adoption and follow-on innovation.

[1] https://en.wikipedia.org/wiki/Occam%27s_razor

Critical Infrastructure of Your Personal Life

The term *critical infrastructure*[2] is used by governments to describe assets that are "essential for the functioning of a society and economy." Identity, data, and communication are the three cornerstones of your personal critical infrastructure and are essential to the operation of any business. Protecting integrity, authenticity, and privacy is seminal for a functioning society.

The most common identity solutions in use today are centralized platforms under single-vendor control. Much like monoculture, these centralized platforms make society brittle. There is no control over personal data, and singular corporate interests routinely trump users' interests or the economy as a whole. While they seek to protect the interests of a functioning society and economy, governments often turn to these same companies in the struggle for the protection of critical infrastructures.

Our everyday, personal critical infrastructure was designed when no one foresaw a world in which smart cities and the Internet of Things (IoT) could rapidly create a seamless integration of the digital and physical worlds. Email is our most important and successful federated communication protocol for business, used by 3.7 billion users every day. In a sense, it is the true social network.[3] Integrity, authenticity, and privacy were not part of its design, and developers have been trying to put the genie back in the bottle ever since.

This is not just the reason for the abundance of spam email, it also allowed email to become the most frequent delivery channel for malware and scam. Cyber attacks cost small and medium enterprises (SME) an average of $2,235,000 in 2017,[4] ransomware damages are predicted to hit $11.5 billion by 2019,[5] and business email compromise (BEC) has recently seen a sharp 80% increase.[6] On a personal level, many people experience this as identity theft, which is also growing[7] with a median damage amount of $429 per person, and is increasingly targeting children.[8]

Protection for Your Personal Critical Infrastructure

Blockchain, decentralization, and self-sovereign identity in particular are concepts that were developed to address the new challenges to our personal critical infrastructure. We are using these concepts to provide a solution that is intuitive, user friendly, and seamlessly integrates into existing applications. We add integrity, authenticity, and privacy to your identity, data, and communication.

As a result, you'll have an unlimited number of pseudonyms – verified identities in the form of digital passports that only contain the information you wish to share about yourself. These passports are incorporated into your emails, document applications, and workflows. Using cryptography for signatures and end-to-end encryption, every message will carry its own proof of authenticity and integrity. A social layer in the form of common interaction clues familiar from messaging applications allows you to receive confirmation that an email has reached its intended recipient. Additionally, secured through Blockchain technology, email becomes Registered Mail 2.0. The Blockchain easily proves message integrity, participants involved, and time of delivery for years to come without the need to store paper receipts.

[2] https://en.wikipedia.org/wiki/Critical_infrastructure
[3] https://www.computerworld.com/article/3267698/email/why-email-is-the-best-social-network.html
[4] https://blog.barkly.com/small-business-cybersecurity-statistics-2018
[5] https://cybersecurityventures.com/ransomware-damage-report-2017-part-2/
[6] https://www.computerweekly.com/news/252447624/Sharp-rise-in-business-email-compromise https://threatpost.com/threatlist-email-attacks-surge-targeting-execs/137385/
[7] https://www.comparitech.com/identity-theft-protection/identity-theft-statistics/
[8] https://www.javelinstrategy.com/coverage-area/2018-child-identity-fraud-study

How it works

A vereigning service consists of both a client and server. The client is a module that integrates seamlessly into existing applications via web, app, or library. It organically adds functionality to existing applications like your email client, office application, chat, and browser.

Dashboard

Once you sign up, the dashboard is the gateway to all the amazing things the Vereign application can do for you. This is the place where you access your identity, passports, transactions, and the social roster of people you interact with. It is also where you can find additional information, download links to other modules and applications, and find the verified history of all your transactions along with all archived messages and documents.

Ease of use was our guiding principle. Running the dashboard application and setting up the local keys is as simple as visiting a web page or installing an app from the app store. Simplicity is also why there are no passwords by design. Instead we are using a more modern, secure, and user-friendly authentication scheme based on strong cryptography and device keys. Each device carries its unique, locally generated key with which it can securely authenticate itself to the server. Adding another device means visiting the right web page, requesting addition of the device temporarily or permanently, and scanning the QR code displayed for authentication with a device that's already authenticated.

In technical terms, the dashboard application is a "hybrid app,"[9] meaning it is a HTML5 web app that runs natively on your browser making use of local hardware. It works well on any size of device because of its responsiveness. Application data is always stored locally on the device and in the browser, and never on the server. That includes the cryptographic key pairs which are locally generated and stored. For you, this means the dashboard will run locally in your browser on your desktop, tablet, or mobile device. For tablets and mobile devices, there will also be a version of the dashboard available as an app in the app store.

Passports

Once set up, the first thing a user will typically do is add the identity data they would like to be able to use in the system. How much verification a user wants on the data is up to them. In most cases, users prefer to share only part of their information with a third party. To make this practical, we built a passport concept into the system. Passports are created by the user for certain purposes like social media activity, emails, or business transactions. Each passport contains identity information and potential verifications. At a technological level, each passport has its own random cryptographic certificate so they do not appear connected, and it will only convey the information the user wants to provide.

Passports are the basis of all interactions and data sharing within the system. When using a passport to interact with other users, that interaction adds them to your social roster which functions like a magically self-updating address book. Keeping changes in jobs, addresses, preferred emails, or mobile phone numbers updated for all your contacts is time consuming and a real nuisance, but passports make sharing such updates with all relevant parties a thing of the past. Whenever a user updates their identity data, all passports holding this data will automatically receive the update. This

[9] https://www.wired.com/insights/2013/11/responsive-html5-apps-write-once-run-anywhere-where-is-anywhere/

data is then automatically available to everyone the user regularly interacts with for as long as they choose to maintain the automatic updates with those parties.

Identification data can be verified at multiple levels. For email addresses and mobile phone numbers, the system will verify these automatically, but not all parts of an identity are so easily verified. In cases such as these, the system permits you to start with purely self-verified claims that harden over time as peer-reviewed claims or authoritative third-party verified data, all the way to a government agency verifying information like the date and place of birth. Interest in verification will be determined by their vereigned interactions with third parties and what those parties require from the users they interact with.

The passports are also used for added privacy protection in transactions with third parties. If a user does not want to share data directly, zero-knowledge proof (ZKP)[10] can be applied on top of the data within the passport. Explaining ZKP is beyond the reach of this white paper, but in essence, it allows proving certain details of the user's identity without revealing the data itself. A classic example is proving that someone is above age 18, without revealing their exact age or date of birth.

Applications

Vereigning capabilities are added to existing providers and applications via plug-ins and libraries. These give each application a unique set of keys and take care of all the complexities of key generation and management, so the user will never have to deal with them directly. Instead, the user can choose to sign in via QR code, authenticate via smart phone or other mobile device, and find their passports ready and available for interaction.

Any application used to share data with third parties, or that allows collaboration or communication, will greatly benefit from adding these capabilities. Like the web itself, this added layer of user-controlled integrity, authenticity, and privacy can improve these applications and add value to all their users. It's for this reason that we've decided to publish everything, including making the plug-ins and libraries themselves Open Source. We hope others will build upon these ideas, incorporate them, and experience how beneficial they can be in their own applications.

Registered Mail 2.0

Vereigning capabilities for email will make it natural and intuitive to have each email verified, signed, and end-to-end encrypted. By choosing the appropriate passport, the sender controls what information about themselves the recipient receives. In addition, each message will have a social interaction trail on the Blockchain. This interaction trail will prove the integrity of the content of a message and its delivery time. If the receiver also has vereigning capabilities enabled, the interaction trail can provide proof of having read the message. In combination with the secured archival options offered by our solution, email becomes the most secure, authentic, and permanent medium for everything that's important beyond what is possible in the physical world today.

For the highest levels of privacy and security, the system is designed to generate one-time keys that are only ever used once. As the system grows, this will enable high-security scenarios for email that no other solution can offer. Among other benefits, it will make it possible to add perfect forward secrecy (PFS)[11] to email in a way that is fully compatible with existing email protocol. It will also guarantee a message recipient that sensitive information, such as medical data, can finally be exchanged conveniently by email.

[10] https://hackernoon.com/eli5-zero-knowledge-proof-78a276db9eff
[11] https://en.wikipedia.org/wiki/Forward_secrecy

Choosing email as the first service to improve was not random. Adding vereigning capabilities to email will immediately benefit up to 3.7 billion users who send and receive over 280 billion messages each day. Email is the most important professional communication channel, the largest social network, and the most successful federated communication protocol. Within email, Gmail is the largest email provider with 1.4 billion active accounts. In the Open Source world and across many local hosting services, especially those that are privacy-minded, Roundcube is the most common solution. To provide the maximum benefit to the largest number of users, we decided to start with plug-ins for Gmail and Roundcube.

Other services, starting with Office365, will be subsequently added. However, even without the integration of plug-ins or libraries, everyone can make use of the solution right away by adding services for Simple Mail Transport Protocol (SMTP)[12] and blind carbon copy (Bcc). The server will then offer the message for review and approval on a registered client device before providing an authentically protected copy of the message to all recipients. Utilized this way, both identity and authenticity are immediately available to everyone, anywhere.

Documents

Documents are often tightly integrated with and coordinated via email. Most often they capture a consensus or agreed upon version of a contract, technical document, presentation, or other structured forms of knowledge. Adding vereigning capabilities to documents allows users to sign off on specific versions of documents, implement legally recognized workflows hardened by Blockchain, and make the resulting documents available internally or publicly. While the idea of securing documents using the Blockchain has been discussed before, no system has been able to do so in a user-friendly and comprehensive manner. In particular, most systems neglect signatures and they become worthless once the corresponding document is lost. This is why a secure, tamper-proof, encrypted archival process must always be part of any solution.

Consistently with the approach for email, passports are used for selecting the right component of a user's identity and key. Each document is signed with a one-time key, archived, and then has its transaction records secured on the Blockchain. Like email, documents often form an interaction with other users in the system and establish a common document record over different revisions and multiple signatures. Vereigning will establish document provenance in an easy, accessible, and user-friendly way.

LibreOffice is the most popular Open Source office application, available both on the desktop and the web, and is used by over 200 million users. The ability to vereign documents is being added to LibreOffice by Collabora, a Vereign technology partner. Users of LibreOffice will simply be able to sign-in, scan the presented QR code with a mobile phone, and find their passports for selection to sign and archive versions of a document as required. We are targeting integration with Microsoft Office/Office 365 next. Until that integration is complete, uploading a document to the server will allow verification of authenticity, integrity, and identity in a secure and convenient way.

[12] https://en.wikipedia.org/wiki/Simple_Mail_Transfer_Protocol

Keeping Data Safe

User data includes personal identity information and the most important emails, documents, and official papers. There is no self-sovereignty unless there is a secure, redundant, reliable archive of that data, which is no trivial challenge. Losing access to all data is a major threat, and so is giving control over that data to a third party that may not always act in the best interests of the user. Reconciling the two has proven impossible until today. Vereign has solved both of these challenges in a groundbreaking way that gives users more control and security than they ever thought possible.

Our system design accommodates for the possibility of catastrophic events, such as all devices being lost, stolen, or destroyed. Users can appoint trustees who are empowered to restore access to their account. These trustees can be friends, family members, or professional trustees such as banks, lawyers, or notaries. The trustee cannot directly access the data or act on behalf of the user, though, and all device registrations and removals are captured in a permanent, Blockchain-based audit log. In addition, not only is the entire storage encrypted for the individual devices, but also for the restoration key secured in a hardware security module (HSM).[13] Even if all physical devices are simply destroyed, this approach allows full restoration of access without any data loss.

One of the huge benefits of Blockchain is its distributed, highly redundant nature. Even if several nodes fail, the network continues to operate, and no data will be lost. And because there is never a single party controlling all the nodes, it becomes virtually impossible to falsify data undetected. Our solution follows that same approach for the server networks. In addition to local storage redundancy and protection, data integrity and availability is safeguarded by our hybrid franchise approach by applying the concepts of social franchising[14] to cloud services.

Identity Franchise Networks

Each vereigning cloud service has dozens, perhaps even hundreds, of servers often distributed over multiple data centers within the same country. These data centers and servers form a network which we refer to as an identity franchise network. Similar to a node in a Blockchain network, each identity franchise network is a node in a global, federated[15] network. Each of these networks is incorporated as a local body under governance of the users hosting their data in the network. Users therefore own and control their data in the most meaningful way, and the organization is accountable to them. The country in which the legal body for the network is being incorporated defines the applicable local law for the specific identity franchise network, and allows users to choose the governance framework for their data.

By virtue of subscribing to the service, every user gets access to the vereigning services described above. They also join the identity franchise network that hosts their own data, have access to transparency and security reporting, and may get involved in the governance of the organization. Only people directly accountable to the organization, and therefore the users, ever have access to the servers. The role of Vereign is to provide technology, competency, and the “starter kits” for such identity franchise networks that include contractual frameworks and options for financial support.

This combination allows the highest degree of trust and confidence both in redundancy and protection of data, and it also gives users effective oversight over what happens with their data by utilizing all the benefits of the cloud. It creates self-sovereignty for everyone in a sustainable, user-friendly way.

[13] https://en.wikipedia.org/wiki/Hardware_security_module
[14] https://en.wikipedia.org/wiki/Social_franchising
[15] https://en.wikipedia.org/wiki/Federation_(information_technology)

Digital Original

Federated identity network organizations will establish principles of local data storage and governance of local law wherever they are established. Unlike international cloud operators, there are no questions about foreign data access requests. They will instead be fully accountable to their users who can enforce their rights within the local legal framework. In other words, users within the European Union receive the full benefits of the EU General Data Protection Regulation (GDPR)[16] and users of the Swiss network are covered by all the benefits of Swiss privacy protection. Furthermore, legal systems and their agents, such as lawyers and notaries, are always local. Our approach adapts naturally to local laws, providing for integration with the bar and notary associations whose members would also benefit greatly from participating in the networks themselves.

Based on the existing regulatory frameworks for qualified electronic signatures, such as eIDAS[17] and ZertES[18], Vereign will work with qualified signature providers worldwide and undergo certifications itself in order to provide qualified electronic signatures to all the federated identity networks. Every signature made by the system will then be recognized as a qualified electronic signature by law, and create what can be described as a digital original. A digital original will be a digital document just as unique, enforceable, protected, and authoritative as any paper document, possibly even more so.

This digital original has the potential to be globally recognized without the need for apostilles[19], or certifications by other middlemen, and users will be able to establish networks of peer-to-peer trust and transactions.

[16] https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
[17] https://en.wikipedia.org/wiki/EIDAS
[18] https://en.wikipedia.org/wiki/ZertES
[19] https://en.wikipedia.org/wiki/Apostille_Convention

Summary

These are just some of the key aspects of a new service category for the internet to establish an incremental layer of integrity, authenticity, and privacy for identity, data, and communication through decentralized, democratic, and user-controlled networks. It will be transparent, secure, and accessible to all. The benefits of Registered Mail 2.0 alone will open new opportunities for social and business interactions and enable the creation of new markets. This layer is the missing link to self-sovereignty at scale, and provides an urgently needed answer to many of the challenges posed by the nascent token economy and the EU GDPR.

Vereign is an update to online collaboration that benefits everyone.

To our knowledge, there is nothing comparable in the marketplace right now, and we invite you to join us. Everything we do is going to follow the principles of Open Standards, Open Source, and Open Hardware. If you want to learn more about the system design, please review our white paper and join our community discussion.[20]

We would also like to invite all independent software vendors (ISV), service providers, and Open Source projects to get in touch. Let's work together to add value to what you are currently doing. Blockchain has given us the tool to have multi-participant transactions at virtually no cost. Applied as part of a vereigning service, we can rethink business models on a principle of revenue share between all participants. In particular, we hope to provide entirely new opportunities at scale for Open Source business models.

Tell us what you will want to vereign

vereign.com

[20] https://community.vereign.com