Signata and the Identity Guard & Anonymity Framework for the future of access control systems

Congruent Labs, March 2021

Abstract

Developers of online services spend countless hours of effort in the construction of systems to collect private information to identify users, and even more effort in maintenance of these systems to remain compliant with local and international laws and regulations. Taking payment for services only adds to this burden, as organizations must pay and rescind control to 3rd party service providers to deliver secure and fraud-resistant services for the collection and management of payment information.

In this paper we discuss the Signata service as a means to bind the next generation of identities: identities that are kept anonymous from service providers, and we present IdGAF - the Identity Guard & Anonymity Framework as a decentralized on-and-off-chain solution for the identification, authorization, and lifecycle management for modern identity. We will present the ability for users to self-assert identities onto chains via smart contracts, as well as the ability for service providers to validate and maintain known anonymous identities via off-chain solutions.

We will discuss the capabilities already in place with Signata for the management of hardware wallets and interactions with blockchains, the next phases of the product to incorporate the IdGAF as a full identity and payment platform, to introduce the new SATA token to back these systems, and how these services will provide the first proof of concept for the independent integration of other services using this framework.

Table of Contents

Introduction

The online identity management world is in a constant state of flux. Centralized identity providers (such as Google, Facebook, and Okta) are attempting to lead the charge with centralized authentication services for simplified management, and the era of the password is looking to quickly become obsolete. However, centralized identity management requires users to rescind all control of their identity and access to the service providers that manage their identities, instead of retaining the control over their individual authentication capabilities and identity assertions. These centralized providers typically fund themselves by building unprecedented tracking data on individuals, observing the use of identities *within* their services and *outside* through an ever-growing network of online tracking systems.

Signata[1] is a platform built by Congruent Labs[2] to reveal the true smartcard capabilities of Yubico[3] YubiKeys, bridge individuals' identities to their digital content, and to interact with blockchains. The core capability of Signata is currently to deliver a hardware-based wallet for cryptocurrency storage, but the technologies that underpin YubiKeys also provide the ability to authenticate, digitally sign content, and bind identities to factors of authentication.

Signata's use of well-established smartcard capabilities with YubiKeys drives a natural path to expansion of the Signata service to integrate more functionalities such as authentication and digital signatures, but also for the expansion into more integration of users identities and authentication systems *onto* blockchains instead of just interacting with them.

This document proposes to introduce a new ERC-20[4] token for Signata called SATA. This token will serve a number of purposes. In future releases of the platform the SATA tokens will be used to interact with a platform of smart contract-based decentralized identity services that Signata is currently developing - both as core internal capabilities for the product, but additionally as on-and-off-chain anonymity preserving systems that external applications can integrate and consume to build an identity ecosystem unbound by central authorities. This new platform will be known as the Identity Guard & Anonymity Framework (IdGAF).

We believe existing capabilities of identity management on blockchains is trying to realise protocols and systems that were designed against non-blockchain systems - Signata will instead deliver a platform that maintains the core tenants of blockchains, being:

- Anonymous but cryptographically trusted identification of individuals,
- Decentralized assertion of content, and
- Secured payment for services or interactions on the chain.

[1] https://signata.net
[2] https://congruentlabs.co
[3] https://yubico.com
[4] https://ethereum.org/en/developers/docs/standards/tokens/erc-20/

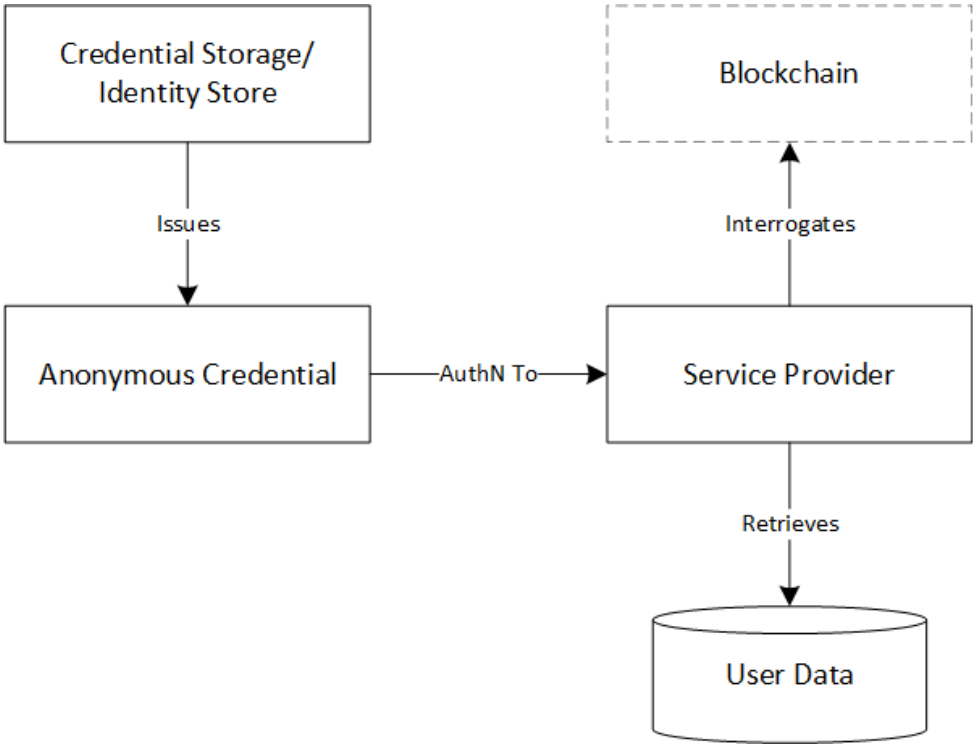

Figure 1 - Interaction Overview

Service Providers using IDGAF, including Signata as the first proof of concept, will be able to securely authenticate and authorize users with anonymous credentials by combining on-chain verification of data produced by the credential holder (assuring ownership of the credential), on-chain verification of authorizations, and off-chain verification of information held within the service itself (ensuring the credential receives appropriate authorization).

This capability will allow for service providers to authenticate users, collect payments, and provide access control to systems without knowing *any* identifiable information about the user - unless they want to collect that information themselves and the user consents to the collection of the information.

Product Description

Signata Crypto

Signata Crypto (referred to as Signata) is a service currently operating in production and available online at https://signata.net, providing the ability for registered users to:

- Add one or more YubiKeys to their account, setting up the embedded PIV[5] applet with an encryption key.
- Add or Import BTC, ETH, XRP, DASH and DOGE addresses to their account, all encrypted by their YubiKeys.
- Add secure notes to their account, also encrypted by their YubiKeys.

Signata operates as a zero-knowledge service for all secrets stored in the system. Users must configure a BIP39[6] mnemonic *recovery passphrase* to retain the ability to recover their account should they lose their YubiKeys. The encryption key that resides on their YubiKeys remains on the user's YubiKey in unexportable smartcard storage, and an encrypted version is stored within the Signata service as a backup. To ensure Signata itself does not become a target for attack, the user's mnemonic is never sent to the storage that the service operates.

For users to interact with their addresses, they simply need to connect their YubiKey, provide their PIN (similar to authorising a payment using a credit card, but only the YubiKey and user knows the PIN), and the keys are decrypted for the user to use them. Unlike common hardware wallets the keys themselves don't actually reside on the YubiKey, only the encryption key does. The encryption key is protected from unauthorized use by the user's PIN (not known by Signata), and repeated failed PIN attempts will send the YubiKey into a locked state to ensure brute-forced access cannot be attained.

[5] https://www.nist.gov/topics/identity-access-management/personal-identity-verification-piv
[6] https://en.bitcoin.it/wiki/BIP_0039

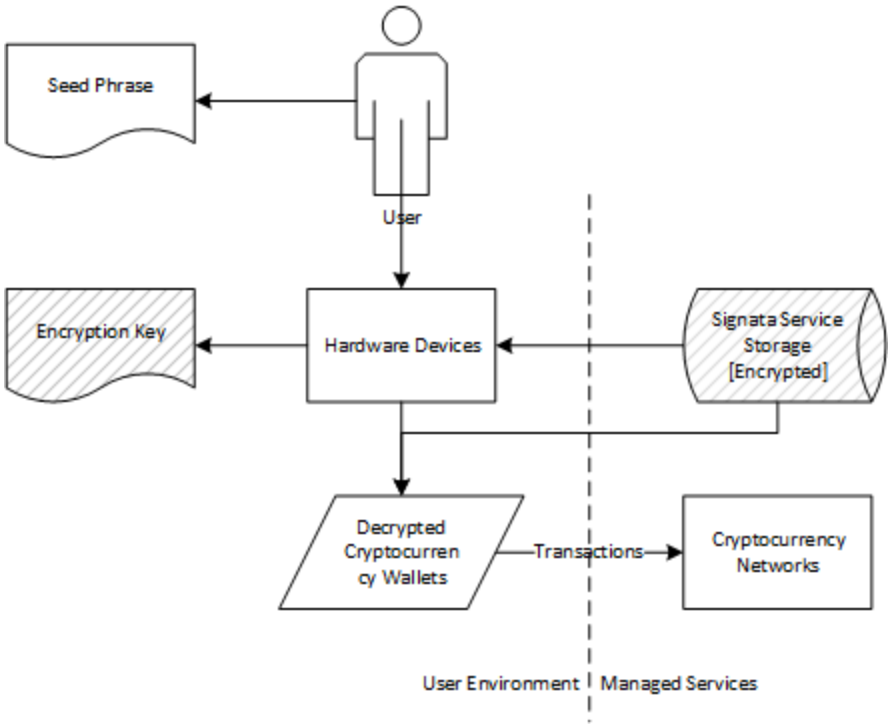

Figure 2 - Signata Crypto Overview

IdGAF (Identity Guard & Anonymity Framework)

The Identity Guard & Anonymity Framework will be delivered as a set of on-chain contracts and off-chain systems to deliver a fully-capable authentication service for applications. This framework will deliver a number of key subsystems, each bound or related to the cryptographic capabilities of blockchain addresses, records, and interactions.

As each of these systems is built and released, they will be delivered within an open identity marketplace, although the open source nature of these components will not be constrained to exclusive access via this marketplace.

Self-Asserted Identity Authorities

Each individual will establish an anchor credential within their chosen device. This anchor credential will be retained to approve the binding of addresses added or imported from other systems, providing users the capability to self-assert approval of cryptographic material for use with authentication and authorization.

Users are not restricted in the issuance of their own authority credentials, nor are they limited in the number of credentials issued by their authorities, so that users can adapt their identities to the specific contexts that they are asserting them within.

Users may, in normal operations, lose access to or have their identity authorities compromised. In the event of an identified compromise, the individual can either self-assert the cancellation of their own identity authority (assuming they still retain control over it), or replace their identity authority with a new authority (and undertake re-assertion of the new authority to connected providers).

Identity authorities ultimately introduce the largest vector of attack from external parties - compromise the authority and one can deny service or assume the identity of the stolen authority. One of the mitigations for this attack vector will be the enforcement of hardware-based key storage will be essential to the manner in which users interact with the IdGAF, much akin to how the Universal 2nd Factor (U2F[7]) provides hardware-based protection to the use of authentication credentials. Not all authentication systems can interact with hardware devices (including many mobile devices limited by physical interfaces and operating system policies), and so a credential delegation capability will also be introduced to facilitate the creation of credentials issued with constrained capabilities to ensure that users can still access systems they need without exposing credentials to undue risk within lower-assurance devices.

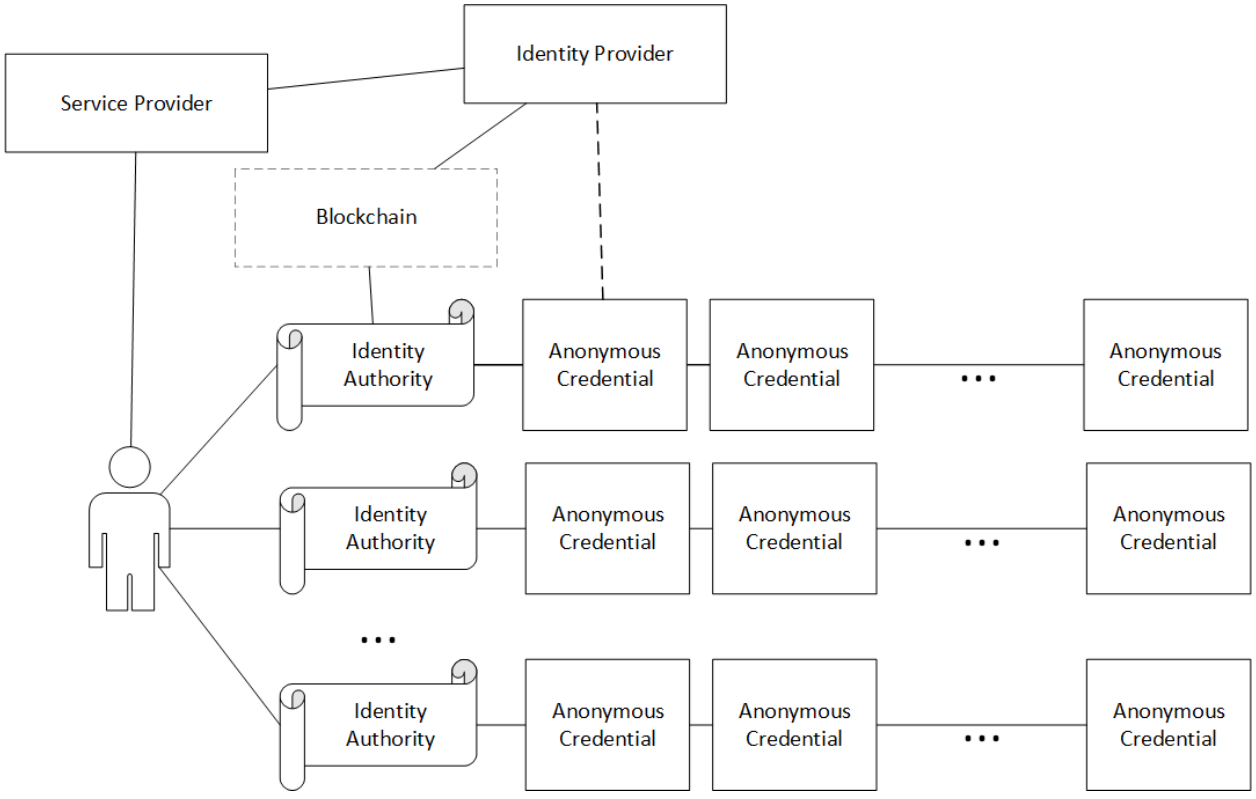

Figure 3 - Identity Authorities and their connections

[7] https://fidoalliance.org/specs/u2f-specs-master/fido-u2f-overview.html

Anonymized Identity Providers (DeREx)

In the current Identity Provider market, most providers offer the combination of some form of persistent identity collection solution, single sign-on capabilities, session management across services, and (for more advanced integrations) adaptive risk solutions for observing unexpected user behaviour.

Connected IdGAF service providers will instead deliver the core capability of persisting identities but retaining anonymity, as well as offering the ability for the capture and management of payment for services directly linked to the identity provider. With this integrated approach system developers no longer need to integrate two disparate systems to achieve the same overall outcome for their products - users can authenticate securely and pay for services within the same set of transactions, and without needing to surrender personally identifiable information to the service provider.

Service providers can additionally relieve themselves of the responsibility to capture and store identity and payment information, removing the potential exposure of identifiable information once a system has experienced a data breach or leak.

Connected providers will be presented as the Decentralized Rights Exchange (DeREx), providing a unified platform for 3rd parties to integrate and consume these services.

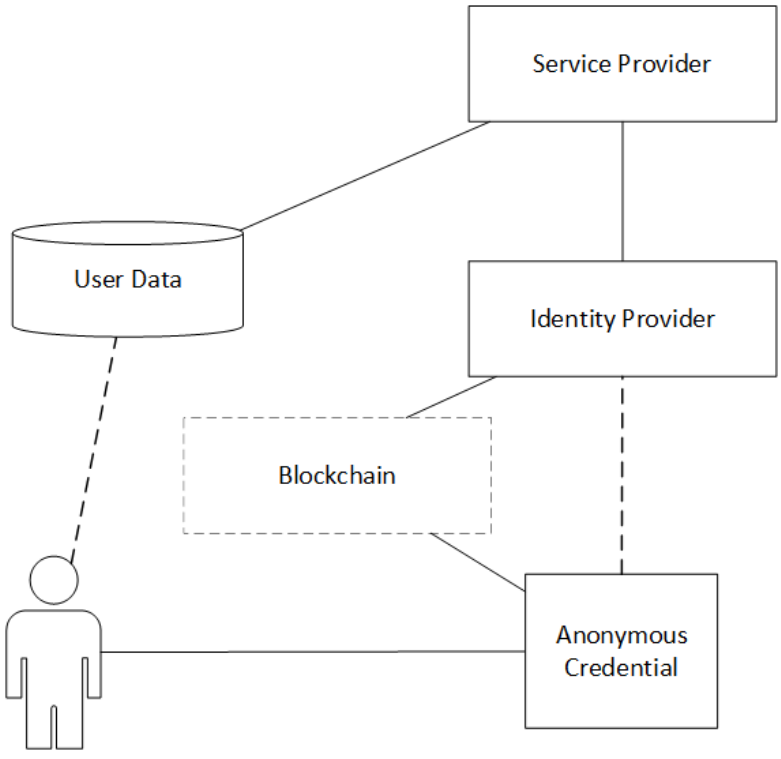

Figure 4 - Anonymized Identity Provider Overview

Decentralized X.509 (Dex509)

Public Key Infrastructure (PKI) systems have been built and naturally evolved to suit operation *on* blockchains. Considering the core capabilities of certificate authorities, the security controls imposed to protect them are designed to effectively replicate the features that blockchains now inherently offer - they store an immutable sequence of events much like the individual blocks and transactions managed on chains.

IdGAF-enabled services that interact with authentication, signing, and encryption certificates will be able to additionally push and pull certificate records into the chains. Assertions of authority/signing status of public keys will permit service providers to inherently trust assertions made by specified authorities as a transitive, but still anonymous, trust model similar to trust models within the PKI ecosystem.

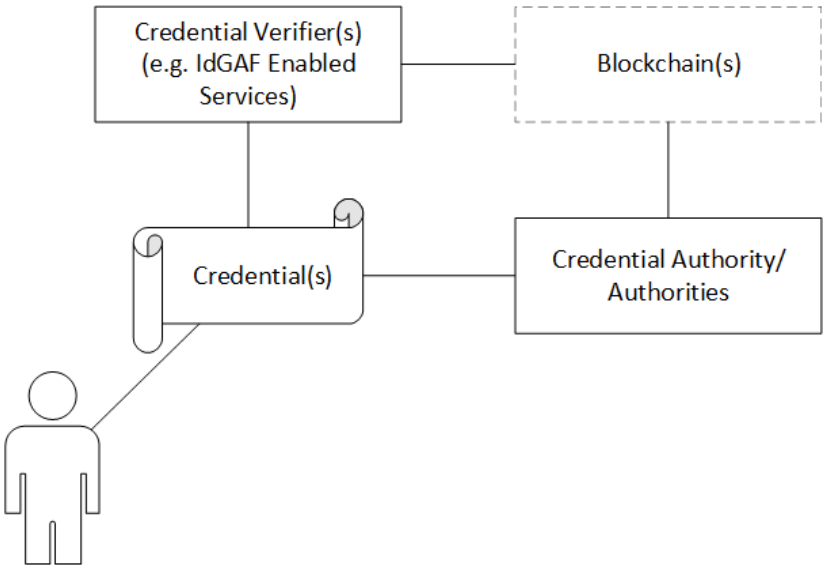

Figure 5 - Dex509 Overview

Product Roadmap

Upon release and successful uptake of the SATA Airdrop, Congruent Labs will establish 3 development streams to deliver each core product. The first development stream will be responsible for core Signata application development. The second development stream will be responsible for Dex509 application development. The third development stream will be responsible for IdGAF application development.

The penultimate service to be delivered by Congruent Labs will be the convergence of all 3 development streams into a unified product and framework, facilitating the use of hardware wallets in combination with decentralized identity management and payment for products and subscriptions bound to those identities.

Q2 2021 Release

Token Release and Liquidity Distribution - The SATA token, along with this whitepaper, will be released to the Ethereum mainnet and distributed to all major exchanges (where accepted) to establish liquidity of the token.

Q4 2021 Release

Full ERC-20 contract interaction - Whilst Signata currently connects to Infura as an Ethereum provider, it is still limited to pure ETH coin transactions at this stage. The product will be extended to allow interaction with contracts on the ETH network, including the ability to trade ERC-20 tokens within ETH addresses.

Direct exchange integration - To facilitate simpler deposits and withdrawals from cryptocurrency exchanges, direct connections will be added to allow users to quickly and easily move currencies between Signata and exchanges for safer storage.

Expanded Hardware Integration - Signata’s device management service will be extracted and expanded for connectivity directly to web applications, permitting expanded interaction with hardware-stored private keys for signing transactions, and cross-platform distribution.

Identity binding - Signata currently issues encryption certificates into user's YubiKeys for the encryption of all their data. This capability will be enhanced to instead use Congruent Labs' new PKI platform for the issuance of trusted certificates for user's YubiKeys.

Dex509 & DeREx First Releases - Signata's new IronSign integration will also include the ability to bind identity information to cryptographic addresses, establishing the capability to identify, validate, and vouch for levels of assurance of wallets. Signata’s new Decentralized Identity & Access Management platform will be released for public use, with the Signata application itself serving as the first consuming service. In addition, the first release of the marketplace will be launched.

2022 Release

Marketplace Adoption - All released capabilities will be made available within the marketplace, and the onboarding of providers will be prioritised to increase product adoption.

Signata Anonymization - The new Dex509 and DIdAM capabilities will be leveraged by Signata to introduce anonymous access to the service, whilst still allowing users to retain control over their hardware wallet.

Alternative Hardware - Devices other than YubiKeys, such as generic PIV smartcards, will be integrated as a more cost effective alternative to YubiKeys for interaction with the Signata service, reducing the onboarding expense for users.

About

This whitepaper was developed by Congruent Labs Pty Ltd, an Australian software development company registered since 2017.

Disclaimer

The plans, strategies, and implementation details described in this whitepaper will likely evolve and, accordingly, may never be adopted. Congruent Labs Pty Ltd reserves the right to develop or pursue additional or alternative plans, strategies, or implementation details associated with the Signata platform.

SATA tokens are being distributed by Congruent Labs Pty Ltd pursuant to the Terms and Conditions (the "terms") of the token available at https://sata.technology/. For complete details, review the terms. SATA tokens are not securities, investments, or currency, and are not sold or marketed as such. Participation in the collection of SATA tokens involves significant technological and systemic risks. The distribution of SATA tokens is not open to individuals who reside in or are citizens of the United States or Canada. The distribution period, duration, pricing, and other provisions may change as stated in the terms. SATA tokens do not in any way represent any shareholding, participation, right, title, or interest in Congruent Labs Pty Ltd, their respective affiliates, or any other company, enterprise, or undertaking, nor will SATA entitle token holders to any promise of fees, dividends, revenue, profits, or investment returns, and are not intended to constitute securities in Australia or any relevant jurisdiction.

The SATA token distribution involves known and unknown risks, uncertainties, and other factors that may cause the actual functionality, utility, or levels of use of SATA tokens to be materially different from any projected future results, use, functionality, or utility expressed or implied by Congruent Labs Pty Ltd in the terms.