Secure Online System - SOS

November 2023

Contents

1 Secure Online System - SOS

The Pacio “Secure Online System” (SOS) provides a universal permanent lifelong self sovereign digital Id named SID for people and businesses. SID is needed by the TEA and TARI systems but can be used for Id purposes by any app, whether business related or not.

SOS includes protection of a SID and associated data by providing for backup, recovery, blocking, and succession in the event of death or incapacity.

2 SOS Purpose

SOS will provide:

- A universal permanent self sovereign digital Id named SID for people and businesses, as required for safe participation in the digital world.

  SID will be implemented NOT as yet another Id system attempting to gain traction, but as an open source Id system making use of the many existing or still to come Id systems, with a selection of the other Ids appropriate to the SID owner being kept in a list per SID, with the other Ids ranked by type for a weighted veracity result per SID, with all data securely blockchain saved.
- Protection of a SID by providing for backup, recovery, blocking, and succession in the event of death or incapacity.

  The SID for a person or entity will be an important part of their existence. A SID is just a unique number which can be recorded on paper and kept in any conventional storage system. However, use of a SID online, including verification of a SID, will involve voice and face image information,

or other biometric data, plus the list of other Ids that the person or entity has in their SID, plus their current status, accessed or managed from a personal device with camera and microphone.

Thus to make SIDs fully functional, able to cope with loss, theft, or upgrading of the SID device, and the death of the person or entity owning the SID, safe storage and recovery and blocking methods are required.

- Optional profile associated with a SID and owner controlled release of profile data to be stored and recovered similarly to SID data.
- Optional additional device and personal or business data to be stored and recovered similarly to SID data.

SOS and SID features will be developed and launched progressively. The start of TEA and related TARI and PIPS systems will require only the first stage of SOS to be operational.

3 Universal Permanent Digital Id named SID

SOS will provide a universal permanent self sovereign digital Id named SID for people and businesses to provide safe verification of self to others, and verification of the other person/persons or entity/entities involved in an online interaction, whether financial or not.

SOS will manage SIDs and other SOS features to come via SOS accounts. SOS will run as an app on digital devices allowing biometric verification of the person owning the account using face picture and voice and/or other biometric options as available for mute people and as devices permit. No email or password will be involved.

SID will be implemented NOT as yet another Id system attempting to gain traction, but as an open source Id system which encompasses self sovereign identity (SSI) Ids and other Ids from other systems, kept in a Polygon 2.0 blockchain list per SID, with the other Ids ranked by type for a weighted veracity result per SID. The IDs supported by SOS for use in SIDs are to be called SSIDs for SOS Supported ID. The list of SOS supported ID systems will be dynamic to allow for changes over time for new IDs being added to the list, plus ranking changes.

A SID will remain fixed for life, even on moving country, changing name etc, and regardless of how many new Digital Id systems are created, as SOS will roll them into the mix also, while the SID itself stays unchanged.

SIDs will be available to all people and businesses at no charge.

SIDs will be implemented in two stages:

- Where an app accepts SIDs at or above a certain ranking for ID purposes. This will allow the start of TEA applications development as Pacio apps will accept SIDs.
- Where an app does not (yet!) accept SIDs directly, but does accept one of the SOS supported ID systems, ie one specific SSID, with SOS to handle verification as required for an app requiring that particular SSID.

4 SOS Benefits and Consequences

Permanent Lifelong ID

There are already many attempts at providing Digital Ids, and a lot more are sure to come along. A big benefit of SOS is that a SID will remain fixed for life, even on moving country, changing name etc, as SOS will accommodate any other ID system which comes along and gains traction, without a person's SID needing to change.

Near Universal Adoption by Online Users Achievable

No one system such as WordCoin "For every human" or even the system of the blockchain being used by SOS, Polygon Id, will ever get anywhere near universal adoption despite claims or hopes.

SOS will be able to do better and gain near universal adoption of SID by working with **all** available ID systems as described here.

No Sale of Data

No SOS/SID data can or will be sold. That is an absolute commitment made by Pacio.

Safer Financial/Business Transactions

Triple Entry Accounting (TEA) being introduced by Pacio as a safer system for recording inter- entity financial/accounting transactions to replace the fraud prone 500 year old Double Entry Accounting system, needs a permanent Id to identity the parties to a transaction. SID will provide that.

SIDs can also be used by **any** business needing a permanent Id to use for recording the parties involved in a transaction.

SID will provide a better Id for Businesses by complementing existing national systems and the Legal Entity Identifier (LEI) system by allowing for branch and department information as well as a parent Id.

This addition was prompted by TARI as branch and/or department information can be relevant to TARI, but so will this information be relevant to many other apps.

Make Any Online Activity Safer

SIDs will not be restricted to financial or business use. They can be used to help make any online activity such as messaging, gaming, whatever activity involving two or more people/entities safer. Scammers, bullies, and criminals generally count on anonymity which SID denies them.

Even spam and scam prone email could be made more secure by the use of SIDs to identify all the parties involved in the email, or if the email world fails to grasp the opportunity provided by SIDs to make email safer, then an alternative messaging system using SIDs will arise to replace email.

Encrypted Data

All SOS and SID data will be encrypted so that only the owner can view the data. (Data can be selectively revealed by a SID owner, but totally at their discretion and control.)

Consequence of Using SOS and SIDs

SOS and SID use will provide enormous benefits as described above, but there is also a consequence which may not suit some.

SIDs mean no anonymity. People and entities wishing to remain fully anonymous could not use SIDs. However, a person wishing to maintain privacy, if not total anonymity, could still make take advantage of many of the benefits of SOS/SIDs by creating a SID but not establishing a SID profile or by severely limiting what can be revealed from their profile if they do establish one.

5 SOS Supported ID Systems

The other Ids to be available for the list of Ids comprising a SID would be: Google Id, Apple Id, Microsoft Id, WhatsApp Id, LEI, WordCoin, Polygon Id, every national system that exists or comes along, i.e. **all** available ID systems, with provision for adding more as they come along.

The current research on ID Systems to be supported by SOS follows. This list will be refined as development proceeds with the included systems being ranked and ordered for inclusion.

ID Systems by Type

Centralised - is one where a single authority issues, manages, and verifies the identities of the users. The authority has full control over the data and the access to the system

data - smart cards, microchips, iris, finger prints, facial. GPS, NFC. Passports. Drivers, Birth Certificates

German Personalausweis, T-Systems, IATA Travel API, India Aadhaar, Brazilian Carteira de Identidade, Bhutan NDI app, Canada RSA ID plus, ID.me, verifiableLEI, USA Instnt MultiPass, Ukraine Diia, Spain Signicat ISTEC , Denmark MitID, UK ShareRing, British Columbia Services card, Swizz Procivis One, Jamaica NIDS, Ireland HID, Columbia SoYo,

Federated is one where multiple authorities cooperate to issue, manage, and verify the identities of the users. The authorities share some data and trust among themselves, but they also

maintain some autonomy and privacy- usename, password, 2nd factor, one time password, push notification, security key, biometerics. FOB plus SOS to allow for more corp id responsibilities.

IDverse, Apple, Google, Okta, FaceBook, LinkedIn, Persona, Yot, IDEMIA, Morpho - Trulioo, OneLogin, Ping Identity, MS Azure Active Director, JumpCloud, Oracle Identity Cloud, Auth0, ForgeRock, AWS ID, DigiCert, SecureAuth, Thales

User centered/SSI A decentralized digital identity system is one where no single authority issues, manages, or verifies the identities of the users. The users have full control over their own data and the access to the system. They can create, store, and share their identities using peer- to-peer networks, cryptography, and blockchain technology. Examples of decentralized digital identity systems are self-sovereign identity (SSI), Bitcoin addresses, and Ethereum accounts.- VC, DID, linked data proofs, smart contracts,

IN Groupe, Yubico, GUnet - Hyperledger Indy, Sovrin, Jolocom, IOTA, uPort, Veres One, Civic, Selfkey, SSI IoT Elia Grou, DVCC Japan,

Some Regional or Country Notes

Europe
Signicat has launched no-code platform Signicat Mint

Kenya
Maisha Namba is a unique personal identification number assigned to every Kenyan citizen. The number is assigned to the Maisha Card as a digital identity credential

Somalia has launched a biometric identity card system.

Nigeria The National Identity Management Commission (NIMC)

Singapore Singpass app

For the first time, voters will be able to use their Singpass app

Japan
Eight firms came together to launch a digital identity (DID) and verifiable credential (VC) co- creation consortium (DVCC) to explore new use cases. The firms include banking giant MUFG, law office Anderson Mori and Tomotsune, and several Web3 firms, including Fujitsu, ITOCHU, TOPPAN Digital, and NTT Data.

Australia
Australian Payments Plus (AP+) – a consolidation of domestic payment organisations BPAY, eftpos and NPP Australia – has worked with the country's big banks on the ConnectID project.

United States
Colorado, Georgia, Maryland, and Arizona have officially added support for digital IDs in Google Wallet

Agile-Bot II has received a contract to provide secure digital identification solutions for the US Defense Information Service Agency (DISA).

Clear, a company known for its biometric identity verification tech used in airports, is partnering with Verato, a cloud-based patient matching platform, to accelerate the adoption of digital identity in healthcare to reduce friction, save time and reduce costs.

Prins AI, which uses AI to create digital identities for enterprises, brands, celebrities, and individuals

Samsung Electronics America is bringing mobile driver's licences and state IDs to Samsung Wallet. Arizona and Iowa will be the first states to offer a mobile version of its driver's licence to their residents.

Socure is provide its identity technology to fantasy sports gambling platform PrizePicks.

United Kingdom
One million people have created a OneLogin account, with 2.5 million identities issued to date. Sumsub's non-document identity verification platform

Mastek will design, build, and operate the GOV.UK One Login Technical Service Desk (TSD)

Luciditi has launched Age Proof – the first digital ID card to be accredited by the Home Office-endorsed Proof of Age Standards Scheme (PASS)

IDnow has received the accreditation on the levels medium and high for the UK's Digital Identity and Attributes Trust Framework (DIATF) IDCheck.io. Valid for two years

HM Armed Forces Veteran Cards

Austria
The Austrian government has set a date for the launch of its new national digital identity system, ID Austria – December 5.

Argentina
Launching a blockchain-based digital ID service named QuarkID. This service built on Matter Labs' zkSync Era rollup

Chile
More than 200,000 consumers have reportedly verified their World ID in Chile following the Worldcoin project launch in July.

Philippines
(PhilSys) Identification Card (PhilID)

Italy
Signicat has integrated the Italian e-identity system, SPID (Sistema Pubblico di Identità Digitale)

Czech Republic
The government is to launch the eDoklady digital ID card

Malaysia
Malaysia's National Digital Identity (IDN)

Global
The number of digital identity verification checks will surpass 70 billion in 2024, growing 16 percent

on the previous year's number of 61 billion, according to new research. This growth is being driven by businesses adopting stronger biometric verification methods to combat account takeover and card-not-present fraud, according to the report by Juniper

Research
This report forecasts that banking will see the largest volume of checks, with 37 billion in 2024, equating to 53 percent of the global identity verification market.
https://secureidentityalliance.org/

integrating Shufti Pro's solutions, Newton Global's

Veriff's identity verification offering is now available in AWS Marketplace

iProov has announced a new integration with Ping Identity, leveraging PingOne DaVinci, a no- code identity orchestration service. Liveness detection is used in biometric verification and authentication to assure that the genuine person is gaining rightful access to services.

Preventing criminals or impostors from spoofing identity verification processes by using photographs, videos, masks, or generative AI-created deepfakes or face swaps.

https://www.comptia.org/newsroom/decentralized-digital-identity-benefits-and-opportunities-examined-in-new-whitepaper-from-comptia

Polygon 2.0 blog Jarrod Watts Other ZK-EVM zkSync | Scaling the Ethos and technology of Ethereum Home – Taiko https://scroll.io/ Linea

More Classification Naming

- **Authentication platforms**: These are platforms that provide secure and convenient ways to verify the identity of users and devices across various channels and applications. They typically use methods such as passwords, biometrics, tokens, or certificates to authenticate users and devices. They may also support single sign-on (SSO), multi-factor authentication (MFA), or adaptive authentication to enhance security and user experience. Examples of authentication platforms are Okta1, Auth02, and SecureAuth.

- **Authorization platforms:** These are platforms that provide granular and dynamic control over the access rights and permissions of users and devices to various resources and services. They typically use policies, roles, or attributes to define and enforce who can access what, when, where, and how. They may also support identity federation, delegation, or consent to enable interoperability and collaboration across different domains and organizations. Examples of authorization platforms are Ping Identity3, VMware Workspace One Access4, and CyberRes NetIQ Identity Management.

- **Identity management platforms:** These are platforms that provide comprehensive and centralized management of the lifecycle and attributes of users and devices. They typically include functions such as identity provisioning, deprovisioning, synchronization, governance, and administration. They may also support identity analytics, reporting, or auditing to monitor and improve the performance and compliance of the identity system. Examples of identity management platforms are OneLogin5, BIO-key PortalGuard, and Thales Digital ID Services Platform2.

6 Other SOS/SID Details

6.1 SOS Supported Devices

Devices to support SOS and SIDs and provide verification will need to have at least a camera and microphone to use for identifying the owner using face imaging and voice checking via an AI system. All smart phones, AI Pin type devices (wearable phone alternative devices), or computers with camera and microphone will be suitable. If a SID includes in its list of Id and an Id systems requiring more biometric data such as finger prints, iris scans, heart rate sensors, or other physiological characteristics or behavioural characteristics, then that one Id of the SID list could only be established and verified on a device supporting the required data.

6.2 Blockchain To Be Used

It is proposed to store SOS and SID data using the Polygon 2.0 blockchain as being used for TEA and TARI as described in the Pacio White Paper.

Stage 5 data storage of optional additional device/system data may use an additional storage system to be decided upon at development time.

6.3 SOS Accounts

SOS works via personal and entity accounts.

Personal SOS accounts are device specific, and a person may have as many of them as they have devices. (SIDs are not device specific as they apply to the person and thus all SOS accounts a person creates have the same SID.)

Entity accounts are not device specific.

Personal Account

First SOS Account Creation

For a person's first SOS account they need to create a SOS account on one device and obtain a SID.

No data for the person needs to be entered ie no name, no email address, nada. No password is involved. Name, address etc type information comes via SSIDs added to the account, and/or the optional profile.

Creating the first SOS account requires two steps:

- the person to take face pics and record voice phrases, as required by a recognition AI that will subsequently need to recognise the person to log them back in their SOS account, with other options to be added for mute people and/or advances in device capability for other biometric ways of confirming a person's identity.
- Addition of at least one SSID to the SOS account, chosen from the list of SOS supported Ids or "Self" if the person has no other digital Id, as per the SSID addition process below.

The SID generated for the account will be displayed and can be copied. It will not be emailed anywhere.

The SOS account created will apply to the device it is created on only. There is nothing to be stored or copied for the SOS account as it is biometrically identified.

- Additional Device SOS Accounts Creation

A person may create additional SOS accounts on other devices, provided that the other device can enable the biometric identification to be performed. If not, then the SOS account on the original or first device may need to have extra biometric options added.

No SID creation is involved with an additional device SOS account as a person has just one SID, created at the time of creation of the first SOS account.

Entity Account

A person logged in to a SOS account can create an Entity SOS Account for which the profile data is not optional.

An Entity SOS account can have multiple personal accounts linked to it.

Entity accounts are not device specific – device specificity applies to the devices of the people who act on behalf of the entity.

6.4 SOS/SID Setup and Maintenance Processes

The processes involved in setting up and maintaining SOS and SIDs with development stages shown in []s are:

- Create a SOS account with SID – described in the SOS Accounts section above [S1]
- Add an SSID to a SID by choosing a SSID system from the list of supported ID systems, entering the ID, and verifying ownership of that Id by whatever method that system uses [S1]
- Create an additional personal device SOS account – described in the SOS Accounts section above [S4]
- Optionally add/edit/delete a SID profile and rules for revealing the data to others [S3]
- Delete a SSID from a SID but not to reduce the count of SSIDs to zero [S2]
- Delete a SOS account but not to reduce the count of SSIDs to zero [S3]
- Delete a unique (only) SOS which renders its SID inaccessible without a possibly manual recovery process at a fee. [S4]
- Add/edit associated SID or other data as may be decided upon to facilitate recovery of a SID after device loss, and for succession in the event of death or incapacity [S5]
- Optionally add other device data to a SOS to be protected via the SOS backup, blocking, and recovery process for a SID such as WhatsApp data, images, videos, general files. [S6]

Note that there will be no process for deleting a SID. Once created a SID lives indefinitely or for as long as the blockchain lives.

6.5 SOS Operational Processes

The processes involved in using a SOS account and an SID development stages shown in []s are:

- Log in to a SOS with biometric verification [S1]
- View a SOS account information including its SID and SSID(s) [S1]
- Confirm the SID to an app via SOS biometric verification for logging in to that app or to confirm the SID for use by an app, where the app accepts SIDs [S1]
- Confirm a SSID of a SID to an app for logging in to that app where an app does not (yet!) accept SIDs directly, but does accept one of the SOS supported ID systems, ie one specific SSID, with verification to be handled as required for an app requiring that particular SSID [S3]
- Obtain a report on SID use [S3]
- Allow an app to verify a SID for account creation KYC type purposes [S4]
- Block use of the SID eg during illness, travel, after loss of a device etc [S5]
- Recover a SID following loss or theft of a device, or its replacement/upgrading, or for transfer after death/incapacity [S5]

- Recover other optionally stored device data following loss or theft of a device, or its replacement/upgrading, or after death/incapacity [S6]

7 Fees

The proposed fees for SOS are:

- Creation of a SOS account and SID: free
- Addition of any number of extra IDs to a SID: free
- Reporting on the status of a SID and its use to the owner: free
- Blocking use of a SID after loss or theft of a device: free
- Release of SID profile data as controlled by the owner: free
- Verification of a SID to an app for logging in or use: free
- Verification of a SID user to an app for account creation KYC type purposes ie being added to the app: $1 paid by the app
- Backup storage and recovery options for SID data: 1c per device per day
- Backup storage and recovery options for additional data: price to be set according to actual costs once SOS is running but expected to be of the order of 1c per GB per day

Payment of Fees

Fees will be payable in phone credits where possible (may not be an option in all countries), and/or via a Pacio utility token to be created.

Why would anyone want and be prepared to pay for SOS extras?

- Low cost reliable backup etc that is not Google, Microsoft, Apple, Meta and similar. Some people might trust those companies, but a growing number of people do not.
- Better security thanks to blockchain and encryption ie safer
- No sale of data to anybody ever
- Unique recovery and blocking systems, potentially very valuable.

Pacio Core Ltd
Hewanorra House, Pointe Seraphine, Castries, LC04 301, Saint Lucia

Site: pacio.io
Email: pcl@pacio.io