



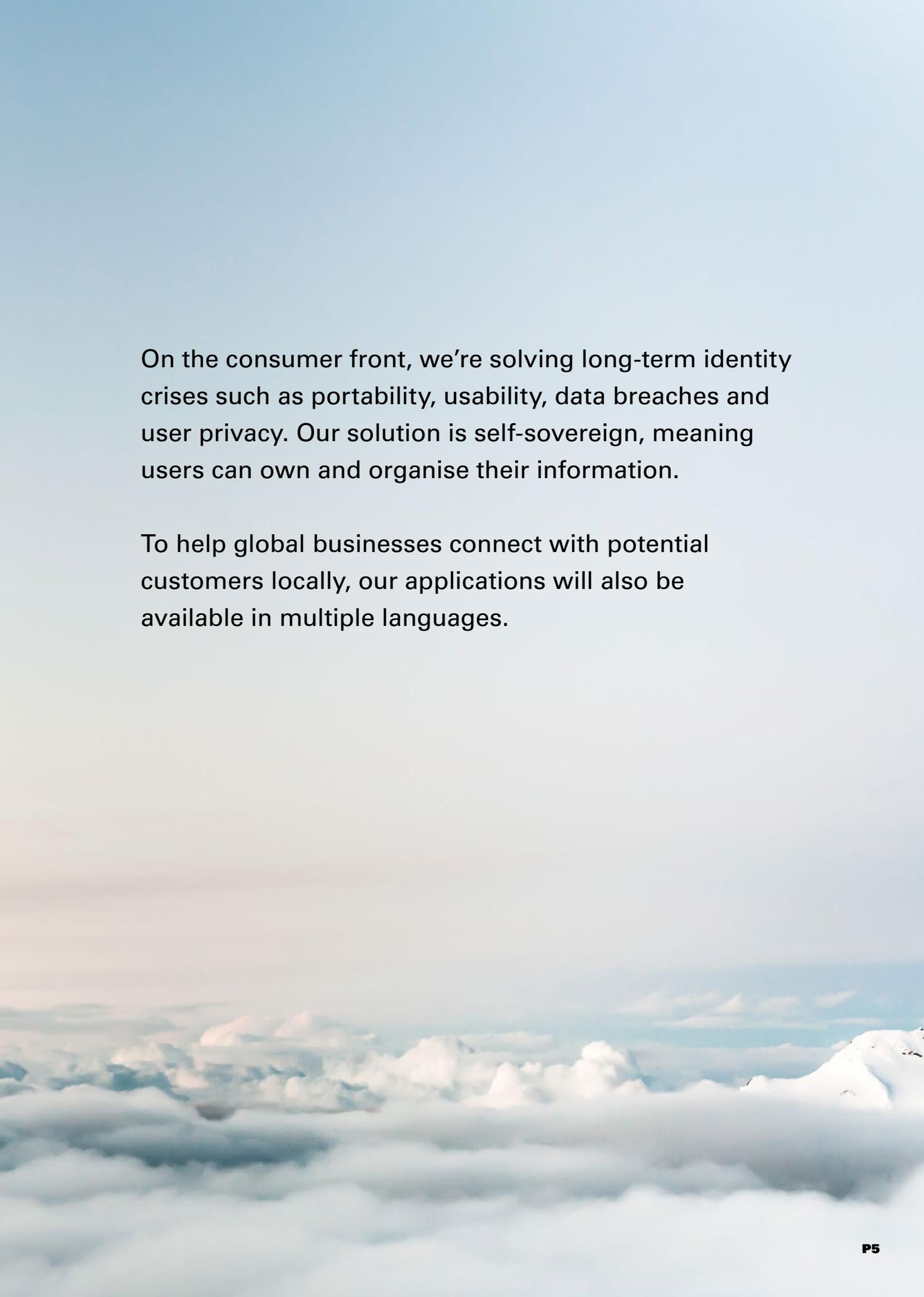
WHITE PAPER

**AS PIONEERS
IN IDENTITY, WE
CAN EQUIP YOUR
BUSINESS TO
BUILD SECURE,
BORDERLESS
RELATIONSHIPS
WITH YOUR
CUSTOMERS.**

1	Solution overview	P6
2	Features and functions	P8
3	Data plans	P9
4	Integration	P10
5	Security	P11
6	Data responsibility	P14
7	Roadmap	P16
8	Glossary	P17

Sphere Identity streamlines customer onboarding for businesses while also firmly adhering to the GDPR and other global privacy regulatory compliance. Our B2B efforts are centered on the digital commerce industry.

As a practical alternative to online forms, Sphere Identity simplifies the sign-up process and directly impacts the overall customer experience.



On the consumer front, we're solving long-term identity crises such as portability, usability, data breaches and user privacy. Our solution is self-sovereign, meaning users can own and organise their information.

To help global businesses connect with potential customers locally, our applications will also be available in multiple languages.

Solution overview

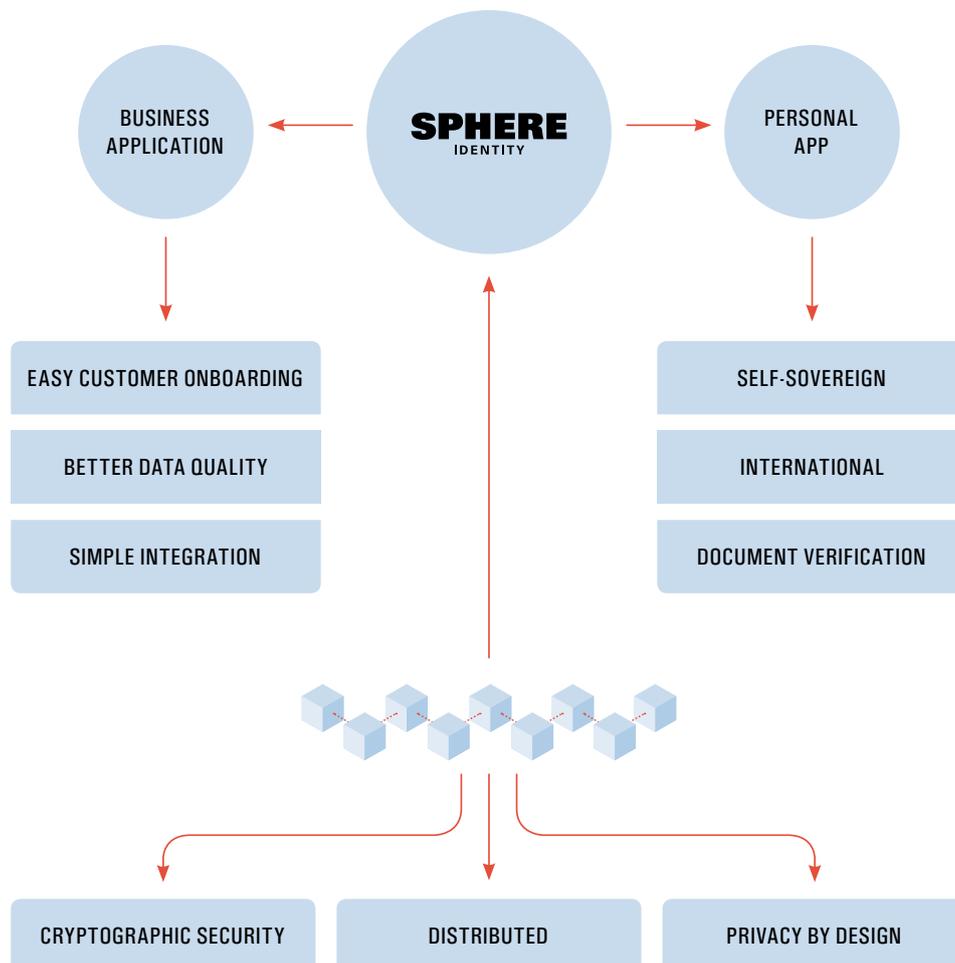
Sphere Identity's solution comprises three distinct but closely knit components:

- 1. The Business Application**
- 2. The Sphere Identity Platform**
- 3. The Personal App**

The Business Application enables businesses to onboard customers through the Sphere Identity sign-up button, on their website.

The Sphere Identity Platform serves as a seamless, secure medium for the sharing of data between businesses and their consumers. It handles consent management and ensures the integrity of the shared data across Business Application and Personal App users.

The Personal App equips individuals to organise their digital identity. Users upload and store their personal information onto the App and can share it at their discretion.



The platform provides a blockchain-based distributed service that is global, scalable and secure.

1. The Business Application

This is a web application that allows businesses to configure the data and attributes they require from customers, prior to sign-up. Customers can be onboarded through a simple QR code scan, instead of lengthy online forms. On subscribing, business users get access to the API SDK and a custom encryption library that can be seamlessly integrated with their existing systems. Along with these, they also get access to the source code that calls and generates the Sphere Identity QR code on their website. This code, once added to the website, simplifies the sign-up process as customers scan the code with their Sphere Identity Personal App.

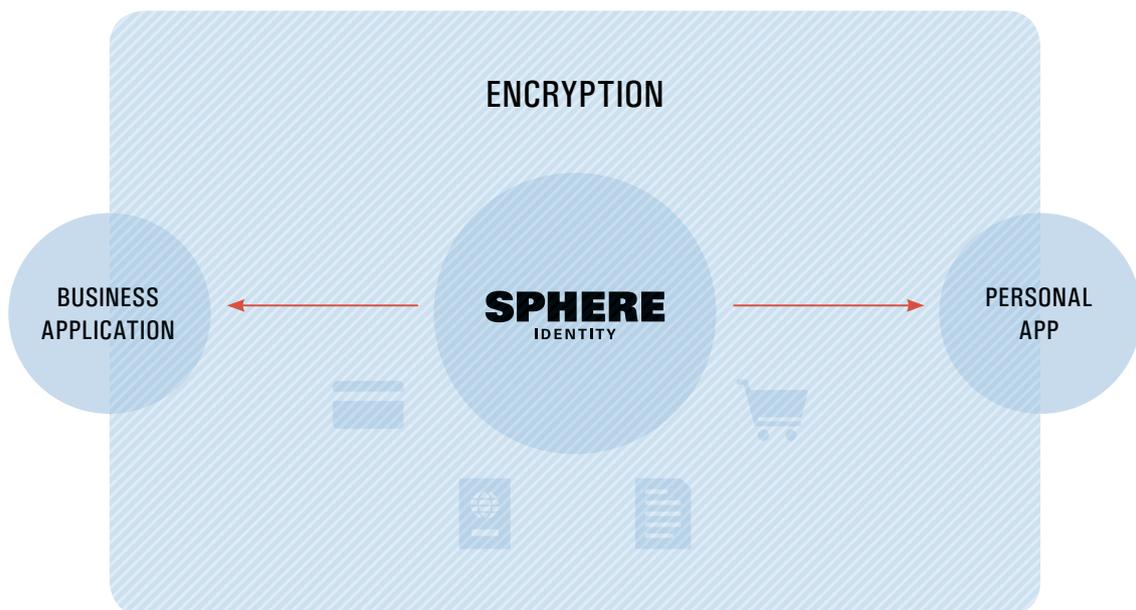
Businesses can manage their subscription(s) via a cross-platform, web-based dashboard which provides them with control and customisation. The dashboard also provides access to manage subscriptions, settings and reporting based on roles for internal security.

2. The Sphere Identity Platform

The platform provides services for Personal App and Business Application users. Its core features include consent management for data sharing between App users and businesses, tools for GDPR compliance and Usage Reporting. Microservices architecture allows for robust distributed storage, transmission and integration of consumer data.

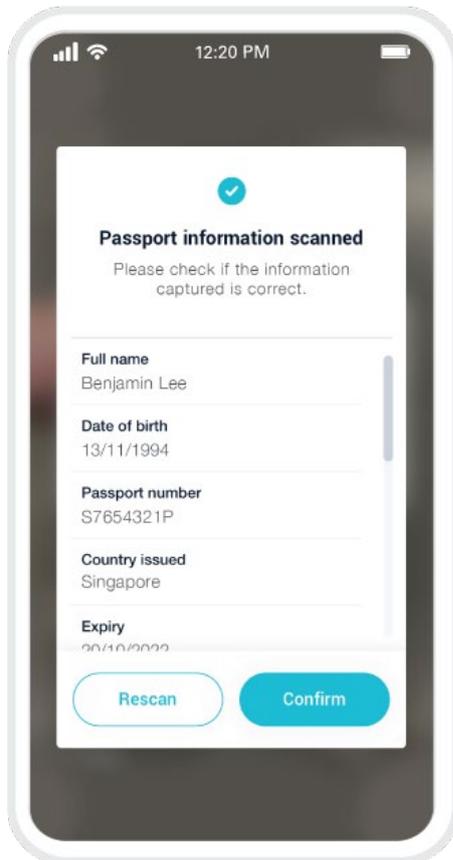
3. The Personal App

Mobile users upload their identity documents onto the Sphere Identity Personal App. These are verified by industry-leading document validation services. A Global Identity Score™ is calculated for each user, as they build their profiles. This score is determined by considering factors such as document types and their expiry dates. It helps businesses evaluate the credibility of the users who sign up on their websites through the Sphere Identity App.



Features and functions

We provide world-class verification of uploaded passports. Automated checks take place along with template matching of the image against an extensive database of documents from over 200 countries.



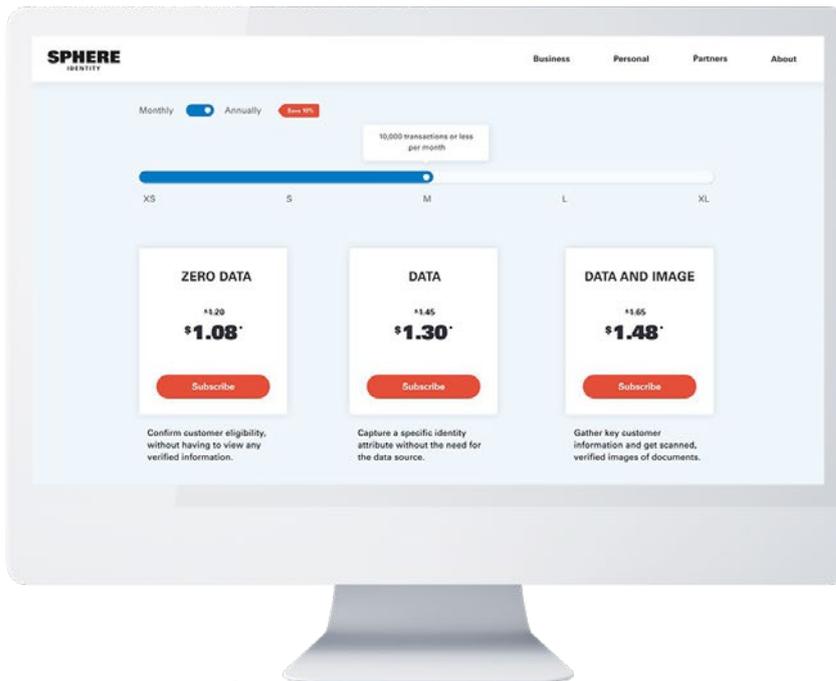
The OCR library used to extract data from scanned passport is state-of-the-art, and has over 98% accuracy in under 0.4 seconds. The OCR engine is equipped with hold-and-capture camera with continuous autofocus and image stabilisation to capture high-quality images of the documents. This enables us to provide businesses with reliable data. As OCR and digitisation are performed locally, on the user's mobile, our OCR support is also GDPR-compliant.

The distributed storage solution used by Sphere Identity is highly resilient to the risk of data failures and does not compromise the privacy or security of the data. The security mechanisms further complement the client-side encryption used. The high reliability and performance of our third-party distributed storage solution ensures that, as a business, data is always accessible.

Sphere Identity calculates the Global Identity Score™ for each App user every time they upload their documents or use the App to sign up with businesses. This score helps the businesses to identify credible users.

Data plans

A business chooses from three data plans or subscriptions, based on their requirements. Our platform supports and stores 41 document types. The process of configuring the subscription is guided through a web app interface called the Business Dashboard. These are listed on our website and our team is available to advise on the best-suited plan.



The email address used to create the account with Sphere Identity is the first factor of authentication as the dashboard has passwordless access. When configuring the subscription, the business provides information such as contact details, payment details and the recovery email address.

During subscription configuration, 12 random security words are generated. They represent the cryptographic keys used by the businesses to decrypt user data. The file containing the keys that are generated with the 12 words has to be downloaded for the process of integration. These 12 words cannot be recovered from the dashboard or by the Sphere Identity support team. For additional security, the file is protected by the password that the business user generates.

After setting up security for their account, the business can define the data and documents that their customers need to provide in order to sign up with their services.

Finally, the business can generate their API access credentials, which is then used in the integration phase. The API credentials can be regenerated from the dashboard.

Integration

Step 1

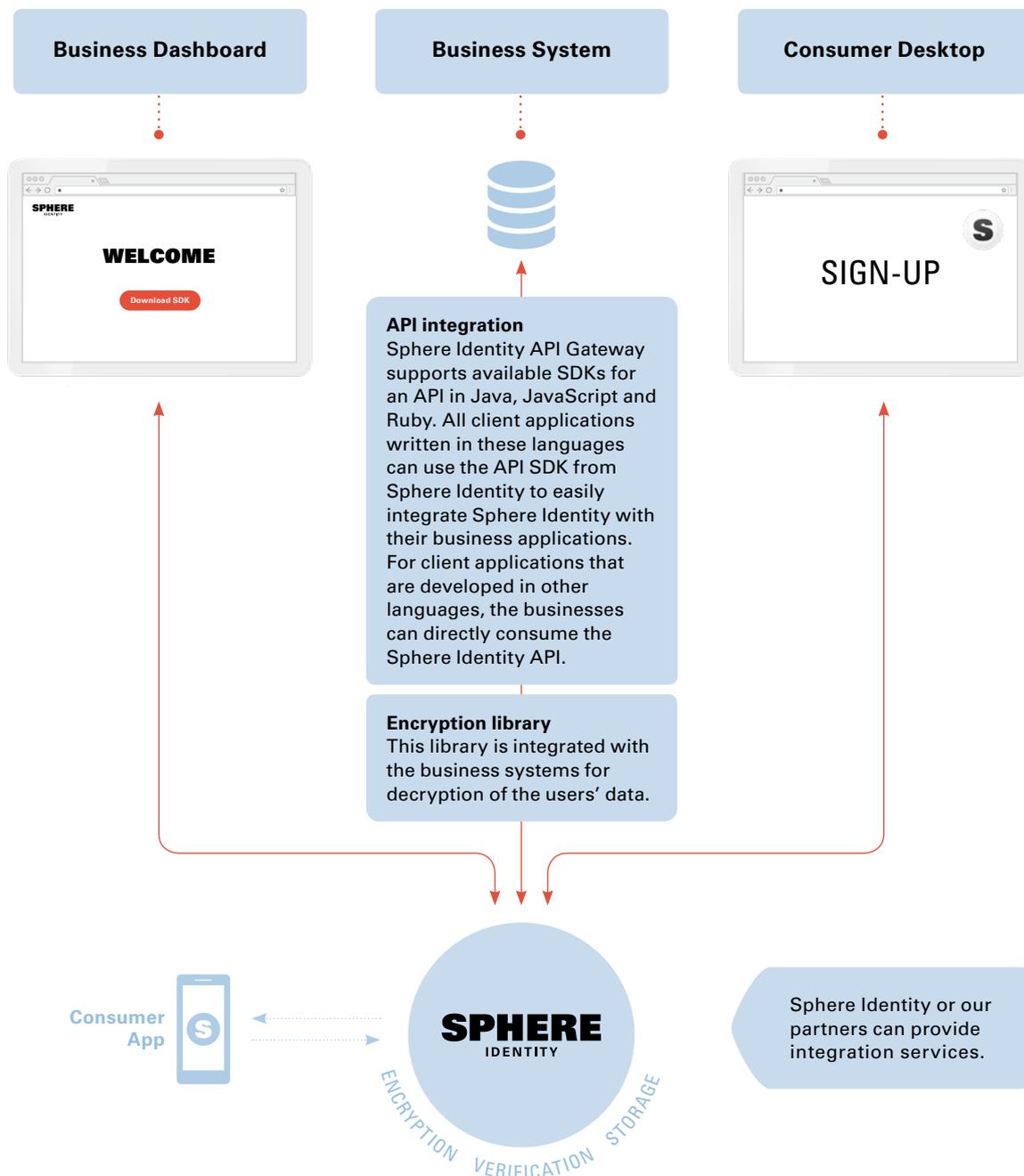
The current subscription is updated on the Sphere Identity dashboard. The SDK required for integration is now available to the business for download.

Step 2

The technical team can start integration of the business's data systems. A specification for RESTfull API is available through OpenAPI.

Step 3

Integrate the Sphere Identity button script. This JavaScript code snippet is required to generate the QR code for the consumers to sign up on the website via the Sphere Identity App.



Security

PRODUCT

Encryption

Sphere Identity uses state-of-the-art cryptography and does not have access to a user's personal data. The encryption protocol uses a combination of private/public key-pairs and a symmetric key. The encryption protocol is designed such that a users' data is available only to the businesses with whom they have shared their data.

Personal data is encrypted on the mobile device and is never stored or transmitted unencrypted. For each piece of personal information that is shared with a business, a unique key is generated, that only the recipient business can decrypt. The Elliptic-curve Diffie-Hellman protocol is used for key agreement. No two pieces of data are encrypted with the same key. Each user has two sets of keys – for signatures and for encryption. The private keys are stored in the secure enclaves in the supported mobile device platforms. A BIP39 library, which utilises user-friendly mnemonics to represent actual crypto keys is used for key management.

A user can restore access to their data via another device using the same key, that is, the 12 security words representing it.

From an implementation perspective, the libSodium cryptographic library is relied upon as a source of cryptographic primitives and is used across the entire solution for critical cryptographic operations. libSodium is a high-speed software library for network communication, encryption, decryption and signatures. It is widely regarded as a robust choice for cryptographic implementations by the crypto community and became the de facto industry standard.

Relying on the cryptographic algorithms provided by libSodium, a high-level implementation of the cryptographic functionality is generated by the Sphere Identity platform in the Rust language. This precompiled Rust library that encapsulates libSodium and provides all of the required cryptographic operations is used across the entire solution – in the Personal App, Sphere Identity Platform and the Business Application. This custom Rust encryption library used at the core of the Sphere Identity Platform provides greater control and fewer problems with interoperability. This library also provides unification of the Business Application and Personal App, allowing the Platform to offload sensitive cryptographic operations. Rust was chosen primarily because of its security, particularly in relation to memory safety and speed.

The Sphere Identity Platform uses its own layer of encryption to ensure that no sensitive data is exposed in transit or during storage. This is on top of the end-to-end encryption of personal data.

A minimised attack surface

Sphere Identity has a small attack surface which is well monitored for the earliest signs of threat. All our product design decisions are evaluated in terms of the security and

privacy risks they may introduce. As security and privacy are central to Sphere Identity's policies, no compromises are made at any point of design and implementation.

Passwordless, Multi-factor Authentication (MFA)

Sphere Identity does not use passwords in the user interfaces. Mobile users use their cryptographic keys with a challenge-response type of algorithm. Mobile device provided second factor, biometrics or PIN, is used in this case. Business users use MFA on top of email-verified passwordless authentication. The second factor will be based on WebAuthn in the future; currently, SMS codes are used. It should be noted, that in the Sphere Identity system, SMS-based second factor is never used for restoring access to accounts, where it becomes the weakest link. It is only used as a second factor during the authentication process, as an addition to the email-based verification.

Distributed, resilient storage of encrypted personal data

Sphere Identity stores data distributed and encrypted, so users have ownership of their identity information. Due to the design of blockchain-based distributed storage solutions, we are highly resilient to system failures and can recover quickly from severe service disruptions, without suffering data loss.

Public key cryptography provides strong authentication and the means for access control; for the same reason, we cannot restore access to business or end users. We cannot therefore recover documents that Personal App users have deleted. There is also no means of recovering customer data if the business keys are lost, as we do not have access or backups of private keys. Businesses have complete ownership and responsibility of the data their users have shared with them.

PRODUCT DEVELOPMENT AND COMPANY PROCESSES

Security and Privacy-by-Design

Security and privacy are fundamental to Sphere Identity. These values are embedded into the product development process, starting from the definition of business requirements to solution architecture and design, code and configuration. Rather than having them as features or add-ons, our solution is designed with security and privacy at the core.

Layered approach to implementation of security controls

Relying on single points of failure makes it easy for security compromises. For instance, the encryption keys that businesses have to decrypt user data could get stolen, which might otherwise compromise the user data being transmitted to the business systems. To avoid such situations, Sphere Identity has additional layers of security controls in place to protect user data.

Additional API access credentials are required by the business systems to get access to encrypted data. Even in case of a leak of access credentials, the bulk load of user data that has already been delivered to the business and the potential window of exposure would be limited only to new data. However, if the data leaks, it will still be protected by the encryption protocol which will still protect user privacy.

Secure solutions for secure products

Sphere Identity's products have security integrated into them from the ground up, enabling it on all levels. Our developers incorporate these secure practices early on to make it possible to mitigate inevitable implementation errors and deliver secure solutions for customers.

Automation where possible

Sphere Identity uses a fully automated Continuous Integration/Continuous Deployment pipeline. It ensures that a newly released product feature follows the highest quality standards – that is, it has been tested, undergone security health-checks and the code has been peer reviewed. Furthermore, the process is repeatable and would safely produce the same results every time, protecting the integrity of how our production services are configured. This is also followed in the automation of the security alerts built on top of a reliable, centralised security logging and monitoring solution.

Secure coding and implementation practices

At Sphere Identity, fixing design issues and championing a security mindset throughout the entire team does not end at the design phase. Secure code development and implementation practices are followed throughout the software development lifecycle.

Security testing and auditing, a regular feature

At Sphere Identity, advisory is crucial, but assurance is as important when it comes to actual security. Regular audits by independent third-party auditors are scheduled to ensure that the product delivered is up to the highest security standards. We have closely reviewed the results of the audits so far and have put remediation in place where needed. It also serves as input to fine-tune the secure development lifecycle and makes sure that we continue to incorporate lessons learned back into our day-to-day practices. Apart from regular independent security testing, the CD/CI pipeline has integrated security checks that not only cover basic static analysis of the code but include automated security testing as well. This ensures that none of our code is deployed without a thorough security assessment.

Security monitoring

Logging and monitoring of all necessary events are carried out for secure operation. An alerting system is set up to make sure that critical security controls always operate as expected. It is regularly tested and tuned to ensure ongoing effectiveness. DDoS protection is utilised to prevent hindering/blocking of legitimate system access, and hence, prevents users from losing control of their data at any time. Levels of service are also constantly monitored to support the same.

CUSTOMER INTERACTION

While maintaining and holding ourselves to the strictest security standards largely mitigates the risk of data breach on the platform side, businesses inherently share the responsibility of safeguarding their customers' personal data. The encrypted data reaches the business system, and the business uses it after decryption. Once the data is with the systems, Sphere Identity has no further control over it. As such, it is vital that we not only deliver a secure service, but also mentor businesses on security and privacy best practices. The sales/technology info pack offered to businesses when they sign up with us, provides such guidance. Also, our engineers are always ready to help.

Data responsibility

Sphere Identity is dedicated to developing a data-responsible and conscious environment in the organisation. Our data responsibility regime is effective, fit for purpose and demonstrates a deep understanding of the privacy regulations of the geographies in which we operate.

At Sphere Identity, we:

1. Prioritise an individual's right to consent, privacy, security and the ownership of their data.
2. Implement internal and external policies that adhere to international privacy standards.

Data responsibility is a collective effort across the organisation. Our team is constantly updated about changes in policies and are equipped to maintain high standards of data responsibility.

CONTINUOUS IMPROVEMENT

Sphere Identity follows procedures that ensure continuous improvement of our compliance with data security, privacy and consent. Our four-step privacy approach to data responsibility includes Research, Planning and Architecture, Implementation and Evaluation.

Research

The Sphere Identity compliance team regularly monitors international legal and regulatory changes. All changes and updates are reviewed carefully by our Data Protection Officer. Existing company policies and privacy standards are reviewed to assess if any changes need to be implemented.

Planning and Architecture

Once a decision has been made to change internal policies, current policies are updated to conform to the new standards. At this stage, team leaders are asked to provide their opinion on the proposed changes.

Implementation

The changes to existing policies and standards are implemented and communicated to the wider Sphere Identity team.

Evaluation

Standards and policies are regularly evaluated, and internal audits are conducted under the supervision of our Data Protection Officer to monitor organisational compliance.

PRINCIPLES

Data protection

Sphere Identity strives to prevent the unauthorised use or unlawful access of data. We take precautionary measures to make sure that data quality is not compromised during storage or transfers.

We ensure that our infrastructure and algorithms follow Privacy-by-Design best practice. Operational, legal and technical measures are implemented and regularly audited to maintain a high standard of data protection.

International compliance

Sphere Identity strives to maintain a high standard of compliance. We only process Personally Identifiable Information (PII) in accordance with the General Data Protection Regulation (GDPR) and APEC Cross-Border Privacy Rules (CBPR). We focus on national and cross-border data transfer compliance. All reasonable steps are taken to ensure that the core values and principles of the organisation are upheld.

Data subjects' rights

Sphere Identity respects and prioritises the rights of the data subject while managing their data. Each data subject has:

- A** The right to be informed about their data
- B** The right to have access to their data and other specific information
- C** The right to rectification
- D** The right to erasure
- E** The right to data portability
- F** The right to revoke their consent to process data

Sphere Identity works closely with the Kantara Initiative. We have also created the Three-Party Consent Receipt which has been endorsed by Kantara as a consent receipt protocol. Through this, data subjects always remain aware of how, when and why their data is being processed.

A defined purpose for data use

Sphere Identity clearly states the purpose of all the data it acquires. We do not use the data for any other purpose other than what has been authorised.

Minimisation

Sphere Identity follows data minimisation best practices. We ensure that all data is processed only to achieve its authorised and intended purpose.

One of our subscription plans – Zero Data, is designed to model this standard. Through this plan, one party (the Prover) can prove to another party (the Verifier) that something is true, without revealing any information apart from the fact that the specified statement is true. This is particularly applicable in the context of the GDPR and other data privacy regulations.

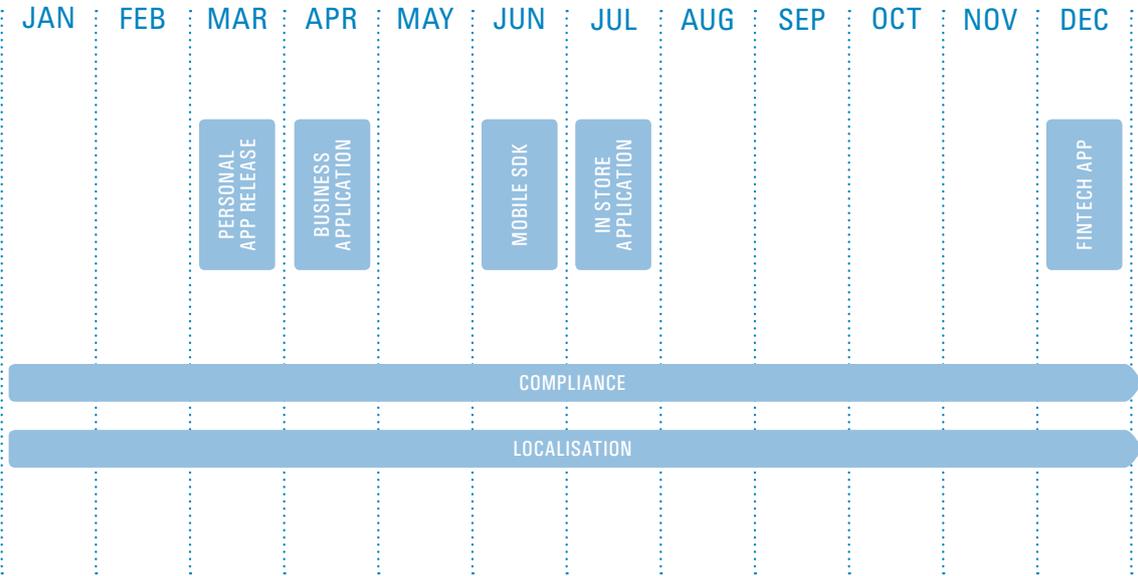
Consent

Sphere Identity equips organisations to adopt good privacy and data sharing practices through the use of Consent Receipts (ISO 29184). These receipts list the type of data being transferred and their authorised use. They also support compliance with privacy regulations such as the GDPR and APEC CBPR standards.

The consent receipts were developed by Kantara Initiative, a non-profit organisation passionate about giving control of data back to people.

Sphere Identity is a member and active participant of the Kantara Initiative. Based on ISO 29184, we have created the Three-Party Consent Receipt Model. Through this, data subjects always remain informed about how, why and when their data is being processed.

Roadmap – 2019



Glossary

An API (Application Programming Interface) is a code that allows a piece of software or hardware to communicate with another piece of software or hardware.

CBPR (Cross-Border Privacy Rules) is a regulation developed by the Asia-Pacific Economic Cooperation (APEC). It is a voluntary, accountability-based system, enforceable on certified businesses and participating governments.

Distributed Storage is an information system that holds data in separate locations, connected through a network.

Encryption is the coding of a message in such a way that it can only be read by the intended recipient. It is done through an encryption algorithm that only the sender and receiver know how to use.

The GDPR (General Data Protection Regulation) is a European Union data protection law enforced in 2018. The GDPR has provided consumers with new rights in regards to the control of their data. It emphasises a business's responsibility to obtain the explicit consent of a data subject before collecting their data for a particular purpose. It is applicable to any company that stores the data of or monitors EU citizens and residents.

The Global Identity Score™ is a value which corresponds to the verification level of a Sphere Identity Personal App user. The score is calculated every time a user uploads their documents to the App, using factors like document type and expiry date. It helps businesses identify the credibility of users.

MFA (Multi-Factor Authentication) is the verification of a user's identity by combining two or more pieces of information, recognition, or possession. For example, for Sphere Identity Business Application users, the first factor of authentication is email, and the second factor is SMS.

The use of **Microservices** is a modern approach to software building that is focussed on decoupling functionality to allow more agile and continuous development practices. By applying Microservices architecture, businesses can scale any particular part of an application without having to redevelop other parts of the solution.

PII (Personally Identifiable Information) is any data which enables the identification of an individual. This identification can be direct, with the individual being identified with just that individual piece of information, or indirect, where that piece of information is used in combination with other pieces.

Privacy-by-Design is a set of considerations that aim to protect the personal information of users at every stage of product development. At Sphere Identity, the principles of Privacy-by-Design are followed from conception to development.

A QR (Quick Response) Code is a machine-readable label that links users to businesses through the Sphere Identity platform. It is used during the consent process as users share their information with businesses.

Rust is a functional systems programming language. Its advantages include speed, memory efficiency and the ease with which software can be designed to run multiple pieces of code at the same time. It can be applied to multiple different targets, including Web Assembly.

An SDK (Software Development Kit) is a “toolbox” which software developers use when creating or integrating new functionalities. An SDK can include code libraries, instructions to perform specific functions and other documentation.

A Self-sovereign Identity solution allows users to have granular control over their data. Typically, a user will be able to store their data on their phone hardware, or in the case of Sphere Identity, on distributed storage.

A Zero Data Plan allows a business to capture data, without seeing the specific data attributes or data points. For example, a business is able to verify whether an individual is over or under a certain age without seeing that age or the individual’s date of birth. By subscribing to a Zero Data Plan, a business can minimise the amount of data they store and thereby, the responsibility which with it comes.



product@sphereidentity.com
sphereidentity.com