Trust Your Supplier

Data Management Supplement

V1.3

Table of Contents

1. Purpose 4

1.1 ACRONYMS 4

2. Introduction 4

2.1 ORGANIZATION TYPES 4

2.1.1 Buyers 5

2.1.2 Suppliers 5

2.1.3 Verifiers and Other Third Parties 5

3. Data 5

3.1 BUYERS 5

3.1.1 Buyer Profile Fields Stored in TYS 6

3.1.2 Supplier Profile Fields Saved by Buyers 7

3.2 SUPPLIERS 7

3.2.1 Supplier Profile Fields Stored in TYS 7

3.2.2 Locations 8

3.2.3 Financials 8

3.2.4 Ownership 9

3.2.5 QUESTIONNAIRES 9

3.3 THIRD PARTIES 9

4. Data Storage (Data at Rest) 9

4.1 ON-CHAIN 10

4.1.1 Suppliers 10

4.1.2 Buyers 10

4.1.3 Third Parties / Verifiers (Ecosystem Partners) 11

4.2 OFF-CHAIN 11

4.2.1 Buyers 12

4.2.2 Suppliers 12

4.3 BACKUPS 12

4.4 REMOVABLE MEDIA 12

5. Data Security in Transit 12

6. Data Flows 14

6.1 BUYERS 14

6.2 SUPPLIERS AND THIRD PARTIES 15

7. Data Encryption 15
8. Privacy and GDPR Compliance 15
8.1 PERSONALLY IDENTIFIABLE INFORMATION (PII) 16
8.2 GDPR 16
9. Development and Testing 17
10. Data Retention 18
11. Payment Data 18

VERSION LOG

Date	Document Version	Changes	Author
11/17/20	V1.0	Initial version	Melissa Bracken
09/09/22	V1.1	AWS and China support	Ravi Sabhikhi
10/15/22	V1.2	Revisions and Updates	Melissa Hansen
10/14/23	V1.3	Revisions and Updates	Ravi Sabhikhi
09/06/24	V1.3	Revisions and Updates	Ravi Sabhikhi

1. Purpose

This document describes the types of data TYS stores and how Chainyard manages and secures that data to meet information security requirements and regulations such as GDPR. It should be used by Chainyard employees who need to become familiar with TYS data handling procedures, external partners with an interest in how their data is stored, and parties involved in penetration tests.

The ‘ 🚩 ’ symbol highlights key points to readers.

1.1 ACRONYMS

Acronym	Description
DID	Decentralized Identifier
gRPC	general-purpose Remote Procedure Call
GDPR	General Data Protection Regulation
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer
JWT	JSON Web Token
PII	Personally Identifiable Information
SPI	Serial Peripheral Interface
TLS	Transport Layer Security
TYS	Trust Your Supplier

2. Introduction

Trust Your Supplier (TYS) is a business network of buyers, verifiers, suppliers, and third-party service providers. It is deployed on IBM Cloud’s Blockchain Platform and on AWS in China. It provides a digital passport to suppliers that includes their identity credentials and supports verifiable claims using evolving W3 standards. Additionally, TYS supports third party apps in the TYS App Store, with different models that allow TYS buyers to take advantage of Ecosystem Partner data analyses and verifications.

This document addresses data management, data security and GDPR compliance in the TYS application. It is not an exhaustive manual but a description of the strategy and features of Chainyard’s data management on and off the blockchain.

The types of data saved by a member organization in TYS depend on whether the organization is a supplier, buyer or third party. The data can be further categorized by how it is stored: on the blockchain, off-chain, in the cloud with no blockchain hash, in compliance with GDPR, in a document store, or in an application cache. TYS properly secures and encrypts all data, whether in motion or at rest. Should a user or organization leave the network, there is a data retention policy in place to ensure that their data is deleted, or the access to it is permanently removed.

2.1 ORGANIZATION TYPES

Before exploring TYS data types, it is necessary to understand the categories of TYS organizations that can create data. There are three types of organizations that upload and work with data in the TYS network:

2.1.1 BUYERS

Buyers use TYS to verify, onboard, and manage new and current suppliers. Buyers are the only type of organization that can create another member organization in TYS and own a Kubernetes Cluster on the TYS blockchain network. They set up accounts for their organization's users and send invitations to suppliers to join the network. They may also send suppliers custom questionnaires, to ensure all supplier information the buyer is interested in is covered.

2.1.2 SUPPLIERS

Suppliers are companies who produce and distribute products or offer services to buyers. They may already have a relationship with a buyer organization or will establish a relationship with them after being verified in TYS. They can log into TYS after receiving an invitation from a buyer. They answer buyer questionnaires and upload detailed information to TYS that is validated by third parties, including contacts, addresses, certifications, tax documents, and financial and operational specifics.

2.1.3 VERIFIERS AND OTHER THIRD PARTIES

Verifiers, and third parties who perform supplier data analyses, integrate with TYS to access the source data, validate, or analyze it, and determine supplier ratings. These results are sent back to TYS to be displayed on the supplier's business entity page. Third parties, also referred to as 'Ecosystem Partners,' only have access to supplier data that the buyer organization using the third party's services has access to, or to the data of individual suppliers who are using their service. Most Ecosystem Partners deploy apps in the TYS 'App Store,' with 'Freemium,' transactional, and bring-your-own-license models available.

Examples of third-party companies include Dun &Bradstreet (creditworthiness), Rapid Ratings (financial health) and EcoVadis (sustainability).

3. Data

The following lists of attributes contain the fields that each organization type can store in TYS. Each organization owns their data and is responsible for its accuracy. What an organizational user can view in the application may be different from these lists, as it is dependent on their organization, assigned role, and access privileges.

3.1 BUYERS

Buyers can save both buyer and supplier-related information in the application. Buyers set up their own organizational profile data, users, and user roles defining access privileges. Buyers are also able to save UI configurations and create initial supplier profiles and custom supplier questionnaires.

The types of buyer data stored in TYS include:

- User emails, roles, and access settings
- Buyer organization profile data
- Buyer UI configurations

- Supplier questionnaires
- Rules on how the application should manage supplier answers to buyer questions
- Initial supplier profile upload

3.1.1 BUYER PROFILE FIELDS STORED IN TYS

The following buyer-specific fields are recorded on the buyer profile page during TYS onboarding and stored off-chain. They are divided into three categories of data: basic information, location, and contacts.

BASIC INFORMATION

- Business Name
- Legal Business Name
- Date Established
- Tax Country
- Description
- Business Type
- Employer Identification Number (EIN)
- Tax Registration Document
- Phone Number
- Company Email Address
- Website Address
- Number of Full-time Employees
- Number of Part-time Employees
- UNSPSC codes
- *Optional fields*:
  - Fax Number
  - D-U-N-S number
  - NAICS Codes

LOCATIONS (OPTIONAL)

- Address Type
- Country
- Address 1
- City
- State
- *Optional fields*:
  - Address 2
  - PO Box
  - PO Box Zip Code

CONTACTS (OPTIONAL)

- Name
- Job Title

- Primary Phone
- Primary Email
- Location
- *Optional fields*:
  - Secondary Phone
  - Alternative Email

3.1.2 SUPPLIER PROFILE FIELDS SAVED BY BUYERS

The only supplier information a buyer may upload to TYS are the fields needed to send the initial invitation, which can include:

- (Supplier) Business Name*
- (Supplier) Legal Name
- (Supplier) Tax Country*
- (Supplier) Business Email Address*
- (Supplier) Preferred Language
- (Supplier) Contact Information
  - First & Last Name*
  - Job Title

* Mandatory

An initial supplier profile will be created when these fields are entered.

3.2 SUPPLIERS

After accepting a buyer's invitation, a supplier can access TYS to enter their basic profile information, answer questionnaires assigned to them, and upload any relevant documents. The attributes collected and displayed on the supplier's profile page include the following:

3.2.1 SUPPLIER PROFILE FIELDS STORED IN TYS

OVERVIEW

- Business Name
- Native Business Name
- Business Description
- Legal Business Name (Full legal name of the company)
- Native Legal Name
- Date Established
- Tax Country
- Business Website
- Business Email Address
- Business Phone Number
- Business Fax Number

- Stock Exchange
- Stock Ticker Symbol
- *Tax Identification Number (EIN, SIRET Registration. ABN Tax Registration, VAT, etc.)
- Tax Registration Document
- Commercial Registration Document
- Diversity Disclosure
- Diversity Status
- Diversity Category/Subcategory
- Diversity Certifier, Certificate and Expiration
- Number of Full Time Employees
- Number of Part-time Employees
- UNSPSC Codes
- Business Type
- NAICS codes (if applicable)
- GLEIF Identifier (if applicable)
- * D-U-N-S number

* Not collected for China Suppliers

CONTACTS

- Executive Management Contact Information
  - First & Last Name, Job Title
  - Primary Phone Number, Secondary Phone Number, Email Address, Location
  - Year of Birth
- Contact Information (non-Exec)
  - First & Last Name, Job Title
  - Primary Phone Number, Secondary Phone Number, Email Address, Location

3.2.2 LOCATIONS

- Address Type:
  - Headquarters
  - Office
  - Distribution Center
  - Plant
- Address, City, Zip Code, State, and Country

3.2.3 FINANCIALS

- Currency the company operates in
- * Financial Revenue for the last 3 years
- * Financial Assets for the last 3 years
- * Financial Liabilities for the last 3 years
- * Profit for the last 3 years

*Not collected for China suppliers

3.2.4 OWNERSHIP

- Ownership Information
  - Individual Owners (and % owned)
- Ownership Information of Parent Company and Entity/Organization, if applicable
  - Individual Owners (and % owned)
- Dun & Bradstreet Report (or) any other applicable Financial Statements

3.2.5 QUESTIONNAIRES

- Generic questionnaires and responses related to Operations, Risk and Compliance topics
- Buyer-Specific questionnaires and responses related to the relationship or services with that buyer specifically.

3.3 THIRD PARTIES

Third Parties analyze, augment, or verify TYS supplier data and send their results back to the application, to enhance the supplier's profile. Instead of using the UI, these Ecosystem Partners receive supplier data through the TYS Integration Agent, using a Partner Agent to communicate with it, and send their data back to TYS over the same connection. Examples include:

- Results of various verifications of Supplier data such as financial data and security data
- Results of Supplier risk analyses such as environmental, geopolitical, health and safety
- Results of Restricted Party Screening

Third party data sent to TYS is sometimes stored for display in an app and in some cases *is not saved in the application*. Depending on the relationship with the 3rd party, when the data cannot be stored, it is sent in real time to TYS when a supplier's page is viewed by a user, and that data is temporarily stored in a cache. Where 3rd parties allow TYS to store data, a snapshot is stored on the blockchain encrypted with the buyer's keys, for license auditing purposes. This also provides a permanent record of the supplier data analyses during onboarding and the ongoing lifecycle of the buyer-supplier relationship, should they change over time.

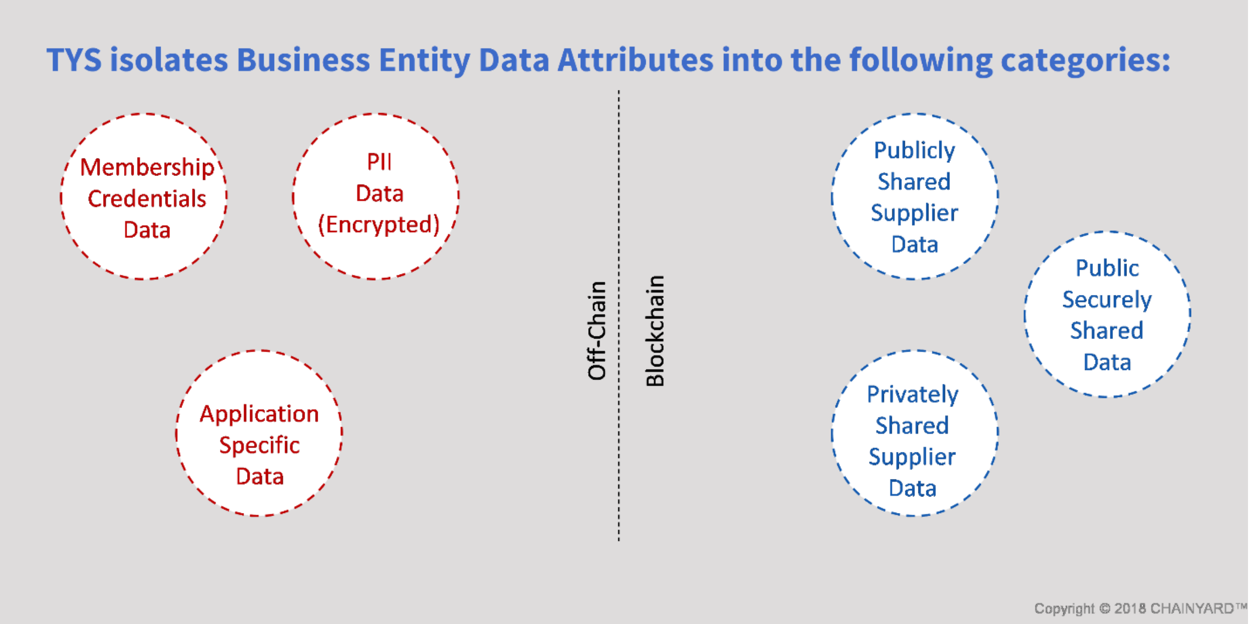
4. Data Storage (Data at Rest)

TYS data stored at rest is segmented into three categories:

1. Data stored on the ledger, referred to as on-chain,
2. Data associated with the blockchain, but stored on an external cloud database, referred to as off-chain,
3. Other data stored in off-chain application databases.

TYS classifies data so that it is appropriately stored by the application on or off-chain, based on the security level the data requires and whether it may need to be deleted from TYS in the future.

The types of data stored on-chain and off-chain are depicted below, with more detailed descriptions following:


TYS isolates Business Entity Data Attributes into the following categories:
Membership Credentials Data
PII Data (Encrypted)
Application Specific Data
Off-Chain
Blockchain
Publicly Shared Supplier Data
Public Securely Shared Data
Privately Shared Supplier Data
Copyright © 2018 CHAINYARD™

4.1 ON-CHAIN

Data recorded on the blockchain ledger is immutable and buried inside blocks. Tampering with these records risks invalidating the ledger, as the block hashes get out of sync. Storage is highly available, allowing for continuous operation, because the blockchain ledger is identical on all the network's nodes and the nodes are spread across more than one region.

The ledger is not a database but a system of record that is the authoritative data source for TYS. All peers on the network store a copy of the ledger locally on their file system. The only data the ledger stores is:

- Supplier records (encrypted and the keys stored off chain)
- Blockchain Transaction History
- Future feature: DID Document Record (not encrypted)
- Future feature: Verifiable Credential Records (not encrypted)

There is a separate World State database that stores the current values of everything contained within the ledger.

4.1.1 SUPPLIERS

Suppliers *are the only member type whose profile data is stored directly on the blockchain*. The created supplier object contains all profile attributes (including questionnaires) except any PII information or documents, which are stored off-chain but hashed. The Supplier data on the blockchain is encrypted, with buyers needing the proper keys to decrypt and read the data.

4.1.2 BUYERS

Buyers may enter initial supplier profiles before they invite the supplier to join TYS. These fields are a part of the overall supplier profile and are stored on the blockchain.

4.1.3 THIRD PARTIES / VERIFIERS (ECOSYSTEM PARTNERS)

Third party data sent to TYS is sometimes stored for display in an app and in some cases is not saved in the application. Depending on the relationship with the 3rd party, when the data cannot be stored, it is sent in real-time to TYS as a supplier's page is viewed by a user, and that data is temporarily stored in a cache. Where 3rd parties allow TYS to store data, a snapshot is stored on the blockchain, encrypted with the buyer's keys for license auditing purposes. This also provides a permanent record of the supplier data analyses during onboarding and the ongoing lifecycle of the buyer-supplier relationship, should it change over time.

4.2 OFF-CHAIN

Off-chain storage includes personally identifiable information (PII) that should be saved in compliance with GDPR, application-specific data such as configurations, application cache data, and supplier documents. On-chain supplier data is also stored unencrypted in an off-chain database only accessible by Chainyard.

Data that is transient and does not require immutability other than digital hashes for audit reporting, such as PII data, is stored off-chain with digital hashes on-chain. Any application-specific data related to the proper functioning of business workflows is stored in an external database on the cloud and does *not* record hashes on the blockchain.

- Supplier and Buyer PII (encrypted)
- Supplier Information (unencrypted)
- Buyer profile data
- Buyer questionnaires, supplier answers (unencrypted)
- Application configurations
- Application logs
- Public and private keys
- User IDs and Emails and their relationship to a TYS organization

Off-chain data is stored in the MongoDB and Redis databases on the cloud, which have replicas distributed across multiple zones and regions:

Mongo DB

- The data written to MongoDB goes into one of two distinct databases: 'K' or 'D.' These exist to keep keys separate from data.
  - 'K' stores the public and private keys which orgs use to encrypt their data.
  - 'D' is used as an application cache to store all other data, including supplier profiles, master data, buyer data, buyer configurations, logs, questionnaires, PII, and data associated with other user types.

Redis DB

This is an in-memory key value database for temporary data store. It communicates with the UI via an API and gives fast access to:

- User IDs/emails
- Mapping of users → ORGs

- Temporary URLs and 6-digit pins generated for new users.

4.2.1 BUYERS

All buyer data, including user credentials, is stored off-chain in IBM Cloud databases. Login passwords are hashed and stored there along with buyer profile data, buyer PII information, buyer questionnaires for sellers, and buyer-specific application configurations. Public and private keys, user IDs, emails, and their relationship to an organization are also off-chain.

4.2.2 SUPPLIERS

Supplier-related PII and SPI information, such as contact names and addresses, are encrypted with the owner's public key, and stored off-chain in MongoDB database on the cloud. Being off-chain allows this data to be compliant with GDPR regulations such as 'Right to Forget,' giving data owners the ability to delete it. Like buyers, supplier user IDs, email addresses, and links to orgs are saved in Redis, and public and private keys are in MongoDB.

Documents the supplier uploads to TYS are stored in a document store in IBM Cloud.

4.3 BACKUPS

Backup and recovery of the ledger is native to the blockchain since an identical copy of the ledger is held on multiple nodes. Any node that fails will automatically synchronize with other nodes upon recovery. Blockchain data is also immutable, so on-chain data processed by TYS is never lost.

Off-chain data, which includes PII data, is replicated in multiple instances of each off-chain database. Off-chain data is backed up by IBM every 24 hours and the backups retained for 30 days in IBM Cloud Object Storage. For Chinese suppliers, we have two Mongo DB instances. The off-chain database is backed up to AWS every 24 hours and backups retained for a minimum of 30 days in AWS S3. TYS evaluates these backup mechanisms once annually. These backups are periodically restored as clone of the original to check their integrity of the backup and restore mechanism

4.4 REMOVABLE MEDIA

Chainyard employees never store TYS buyer and supplier data on removable media storage devices such as external hard drives, memory cards, and USB flash drives. This is also the case for sensitive information such as TYS source code or HR data.

5. Data Security in Transit

For data in transit, TYS uses appropriate communication protocols to encrypt and provide security throughout the network. HTTPS, gRPC, and TLS secure the APIs that transport data between the IBM Cloud (the HTTPS application server, the Node.js client, MongoDB, Redis), the IBM Blockchain Platform within its own enclave in the cloud, and places external to the cloud (the UI and Partner Agents).

The following secure communications are used when data is moving between these points:

- gRPC is used between Nodejs and IBM Blockchain Platform
- TLS is used between TYS Client (Node.js) and MongoDB

- TLS is used between TYS Client (Node.js) and Redis
- TLS is used between TYS Client (Node.js) and TYS Integration Services/Agent
- HTTPS is used between TYS Client (Node.js) and TYS Events Stream
- HTTPS is used between TYS Client (Node.js) and Fabric CA
- HTTPS is used between TYS Client (Node.js) and UI
- HTTPS is used between TYS Integration Services/Agent and TYS Partner Agent

AWS information (China only)

The following secure communications are used when data is moving between these points:

- Proxy Service using HTTPS is used between Nodejs in AWS China and IBM Blockchain Platform in Global
- TLS is used between TYS Client (Node.js) in AWS China and MongoDB in Global
- TLS is used between TYS Client (Node.js) in AWS China and Redis in Global
- HTTPS is used between TYS Client (Node.js) in AWS China and TYS Events Stream in Global
- HTTPS is used between TYS Client (Node.js) in AWS China and Fabric CA in global
- HTTPS is used between TYS Client (Node.js) in AWS China and UI in AWS China
- Direct Connection is used between TYS Client (Node.js) in AWS China region and Local MongoDB instance deployed in Private network in AWS Cloud in China region

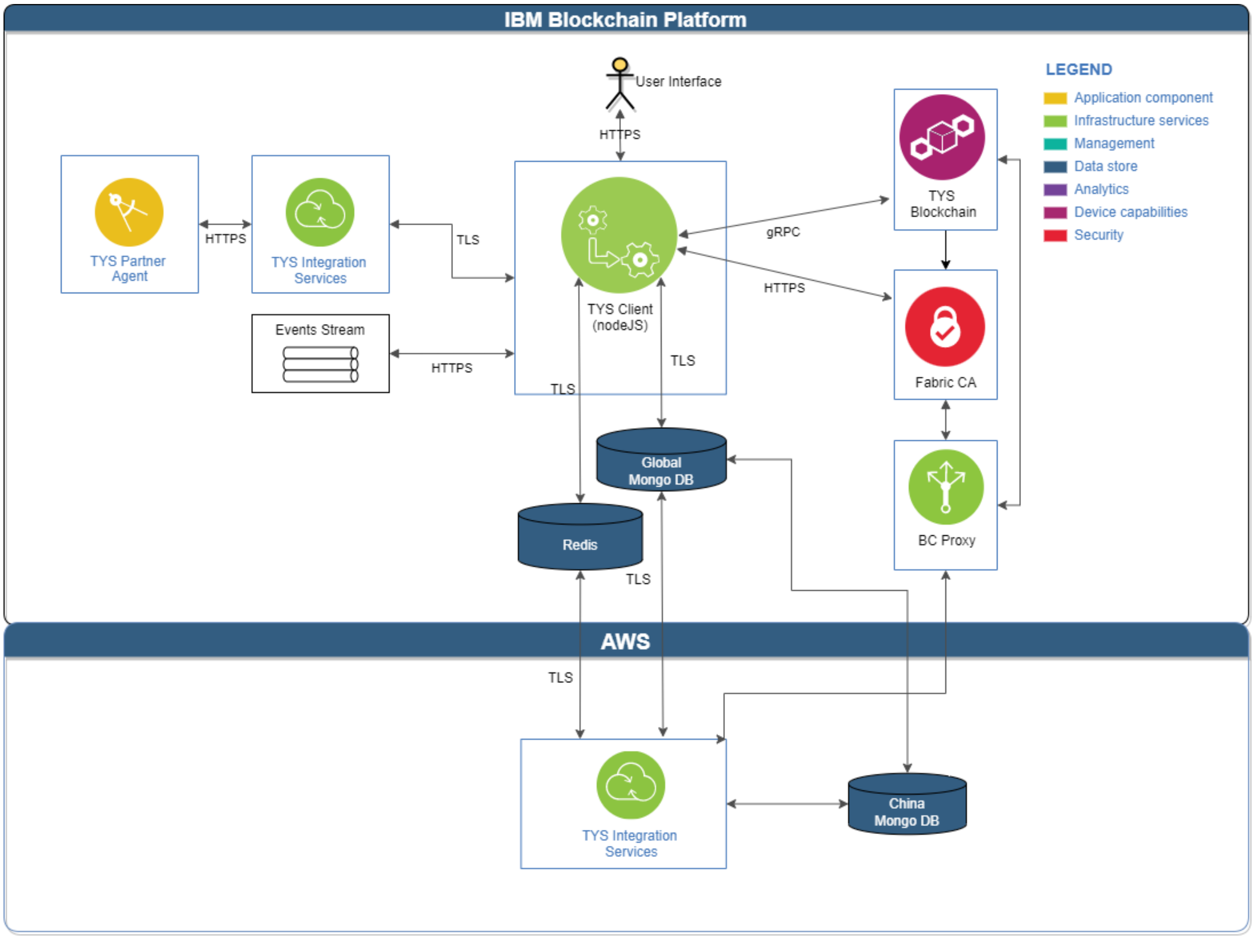


Figure 2 – Data Flow Between TYS Components

6. Data Flows

The below diagrams demonstrate how incoming data flows to the blockchain ledger and databases for different types of TYS organization. Regardless of source, all data runs through the TYS Client before getting routed to the correct place(s) and saved. Once stored, users can view the data in the UI.

The TYS Client sends messages to the Events Stream when data arrives. Events Stream will send notifications about this data out to various entities per previously set up rules. Based on configurations, the Events Stream may also send messages back to TYS Client to trigger the In-app Notifications, Email and Web Socket microservices contained within it.

Other items to note:

- MongoDB K provides the keys that encrypt the data before it is stored in MongoDB D.
- The 'UI Users' box in the diagrams lists the data that is stored in Redis about individual UI users. It is not a list of data that a user can enter to display in the application; that is included in the 'Buyer' and 'Supplier' boxes.

6.1 BUYERS

Buyers enter their own profile information, initial supplier profile information and questionnaires, and can control some configurations within the UI.

All buyer-accessible data can be viewed in the UI, though buyers have the option of communicating through TYS Integration Services to export supplier data to their enterprise application. The Buyer's Enterprise Application can receive data and messages from TYS by connecting through TYS Integration Services. It is expected that the Enterprise Application will send a request to the application to return specific data or have rules in place that automatically send relevant data to it.

The flow of data input and data export for buyers is as follows:

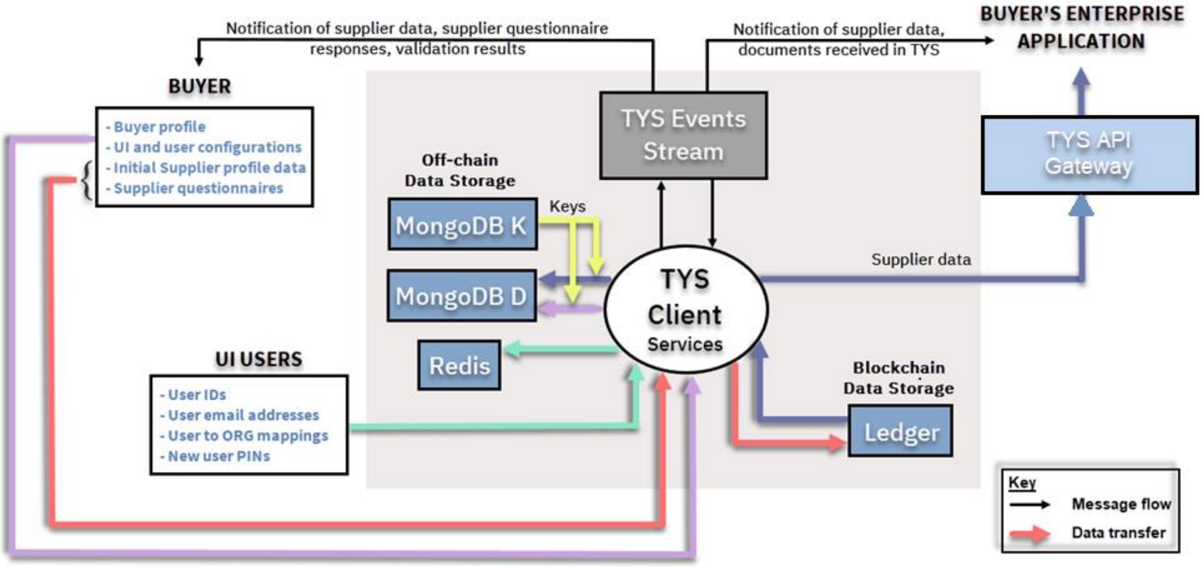


Figure 3: Buyer organization data flow

6.2 SUPPLIERS AND THIRD PARTIES

Suppliers may complete their profile information in the application’s UI. Their data is distributed to any of the third-party Ecosystem Partners whose applications are loaded on the supplier’s profile page, for these parties to validate or analyze it as needed. TYS Events Stream sends out the requests to complete or validate supplier data to the relevant parties. The third party responds with their results back to the TYS Client via TYS Integration Services (not shown):

For Chinese suppliers, the data is first written into Mango DB instance in China region AWS cloud and then to global Mango BD instance in the IBM cloud.

Figure 4: Supplier/Third Party data flows

7. Data Encryption

TYS preserves data confidentiality by encrypting data whenever possible. Data is encrypted at rest and in motion to ensure the network and databases are sufficiently hardened. All TYS organizational members and their users are issued *cryptographic credentials* for signing blockchain data and encrypting organizational-specific data such as PII. Members own public and private keys for this purpose, which are securely managed so that only the organization that owns the keys can access them.

Additional encryption measures are as follows:

- A FIPS-140-2 compliant Key Management Service
- Login passwords protected using PBKDF2 encryption and a random 16-byte salt value for each user, with a SHA-512 cryptographic hash function and hashes stored off-chain

8. Privacy and GDPR Compliance

TYS follows data privacy policies than ensure the proper handling of any data that enters the application. Chainyard keeps abreast of country-specific privacy laws and regulations and performs privacy risk assessments on the application at least annually, in context with current and proposed country-specific privacy laws worldwide. Chainyard also provides privacy education to its personnel annually.

The Chinese supplier’s information is first saved in the China region database before saving in the global region database.

All data is managed by the organization that owns it, and they alone can securely share their data with other TYS business participants.

8.1 PERSONALLY IDENTIFIABLE INFORMATION (PII)

The TYS application collects supplier PII data and stores it encrypted off-chain. Suppliers can at will share PII information with other permissioned members of the TYS network. The supplier manages the process of meeting individual buyer requests for data and the application does not allow for sharing of the data unless there is consent.

TYS currently treats the following types of information as possible PII, and shall review the list periodically:

- First and last name
- Email address
- Billing address
- Title, work department
- Manager/supervisor name
- Contact information (company, phone number, physical business address)
- Photographs
- Biographical and directory information, including linked social media profiles or posts
- Localization data

After suppliers save PII in the application, they manage the process of meeting individual requests such as for copies of PII, that PII is corrected, and that PII is deleted.

The only PII data held by Chainyard is related to buyers and is on the legal governance documents signed by both parties, held for the duration of the relationship between Chainyard and the buyer. This is kept with Chainyard's legal representative and is not on the blockchain.

8.2 GDPR

TYS's design includes compliance with privacy laws such as GDPR. Since blockchain ledgers are immutable, TYS records PII information in encrypted form off-chain so that the "Right to Forget," among other subject rights outlined in GDPR, can be enabled.

TYS in the controller role as an example sales and marketing activities shall maintain a record of processing activities responsibility. The data and processing activities such as processing backup and restore right to forget will follow GDPR and county specific requirements.

1. Name and contact details.
2. Follow purpose and processing guidelines.
3. Categories or personal data (Company name, name, title ….)
4. Upon request personal data could be disclosed to include recipients in third countries or international organizations.
5. Where applicable transfer of personal data to a third country or international organizations. Referred to Article 49(1).
6. Follow security measures referred to in the Artical32(1

TYS in the processor role where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:

1) The name and contact details of the processor for each controller on behalf of which the TYS as a processor is acting.

2) The categories of processing carried out on the behalf of the controller.

3) where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards.

4) Where possible, a general description of the technical and organizational security measures referred to in Article 32(1).

TYS allows the buyer to request information from the supplier, which may include PII data. The supplier must consent or obtain consent to collect and provide such data. The supplier determines whom to share the data with and provides access.

TYS complies with and implements GDPR requirements for PII data as follows:

- Suppliers provide consent before sharing any of their PII data with other organizations.
- Suppliers determine whom to share their PII data with and provide access.
- Buyers and suppliers are responsible for ensuring that their PII data is accurate and complete, and to erase or correct any that is not.
- Buyers and suppliers are responsible for managing any objections about their PII data, such as individuals exercising their right to object to processing. A TYS feature is on the roadmap that gives the 'capability to object.'
- The owner of PII data decides how long they want to retain it and when to delete it.
- The "right to forget," as required by GDPR, is implemented so that PII data owners may permanently remove PII data from TYS at any time. When enacted, all off-chain PII data is deleted from all replicas and related keys are destroyed.
- All PII and Sensitive Personal Information (SPI) information will not require immutability or historical tracking and will be stored off-chain on MongoDB. The associated hashes are encrypted and stored on the blockchain.
- Chainyard meets the 'right to data portability' by promptly providing personal data in machine readable format upon an individual's request.
- Member organizations' GDPR-assigned roles will be notified via email and application notifications should there be a breach in PII data.
- TYS follows ISO 27701 guidance on privacy information management systems and adheres to GDPR regulations for PII stored within the application.
- TYS will continue to review and improve designs to support GDPR and other evolving privacy regulations.

9. Development and Testing

Chainyard never uses actual buyer or supplier data, described in section 3 above, in TYS development activities or TYS test environments. Developers and QA personnel instead mock-up data for those purposes. Buyers are in control of the data they choose to use when testing in the UAT environment.

10. Data Retention

Data retention varies based on whether the data is stored on or off-chain. TYS data stored on the blockchain is immutable. However, the data owner can permanently block access to it by destroying the keys used to encrypt it. Otherwise, data recorded on the blockchain ledger lives indefinitely and cannot be deleted. In the future, it is possible that the ledger may be able to prune blocks based on age. Off-chain data related to those blocks will also be able to be deleted, based on timestamps.

Non-blockchain data including PII will remain within TYS, MongoDB and RedisDB until the buyer or supplier owner removes it. PII data owners decide how long to retain PII data and can delete it at any time. When data is deleted, TYS removes it from the database and all replicas and destroys the related keys.

TYS will remove the PII data of TYS employees who have separated from the company. It is the responsibility of individual organizations to delete PII data associated with an employee if that employee leaves the organization.

TYS will delete an organization's off-chain data from TYS databases and replicas within 60 days of an organization's termination of TYS membership. When a buyer leaves the TYS network, all buyer-owned information will be removed from TYS. However, data from suppliers invited to TYS by the buyer will continue to exist in TYS unless the supplier makes an explicit request that it be removed.

TYS will delete an organization's off-chain data if they are not active in TYS for a period of two years (no user logins and no data updates).

11. Payment Data

Where applicable, TYS does not store credit card information used for payments, instead transmitting it directly to Stripe, a third-party provider, through a separate interface. Stripe receives the information, processes the payment, and sends a confirmation back to TYS along the same interface. In the future, TYS may support IBM Worldwide and other payment interfaces.

TYS can also invoice customers so that they may pay via ACH, check, or wire transfer. All invoices are stored off-chain.