6

Data Access and Transfer – Design System Principles

6.1 Objectives

The i3-MARKET Data Access & Transfer is a component that defines a secured data access and transfer mechanism allowing an encrypted path between data providers and consumers.

The data access API is the interface via which data consumers gain access to the data offered by a data provider or data space. Since this open interface enables direct interactions among stakeholders of different data spaces/marketplaces, we need not only an open interface specification that can be implemented by all but also a high level of security, as the data exchange might involve sensitive data, e.g., personal data or commercial data.

Since a data exchange shall be only authorized once all involved stakeholders, i.e., data owner, data provider, and data consumer, have signed a smart contract, the data access API must be securely linked with and controlled by the i3-MARKET Backplane. Moreover, for the monetization of data assets based on the crypto currency, the i3-MARKET Backplane must be reliably informed about the quantities of the exchanged assets. This is especially a challenging task due to the decentralized architecture (i.e., the direct, peer-to-peer access interface between data providers and consumers).

Authentication, authorization, and data transfer are the core features of the data access API. Authentication is performed by the i3-MARKET identity provider. The user is authenticated using verifiable claims. After successful authentication, an access token is issued, which contains the user role (data consumer and data provider). If a data consumer tries to access the data provider without a valid access token, it will be redirected to the i3-MARKET identity provider. A data provider validates the access token using a service provided by the Backplane. The data transfer takes place using the non-repudiation protocol. A binary data transfer service based on the non-repudiation protocol was implemented. The service offers support for concurrent data transfer and activity logging integrated with the data transparency subsystem.

The innovative elements of data access API are the following:

1. **Integration of the non-repudiable protocol for secure data transfer:** The user authentication is realized by providing the Verifiable Credentials issued by the i3-MARKET identity provider. An access token is retrieved, and the consumer is authorized for data transfer, while the dataset is split into fixed size blocks transferred one by one. The security of the transfer is enforced by an encryption mechanism implemented with symmetric keys, unique for each data block.
2. **Integration with the i3-MARKET Backplane for data transfer monitoring:** Data transfer tracking and monitoring component measures the amount of transferred data and logs this information, which is transferred to the i3-MARKET Backplane.
3. **Integration with the i3-MARKET smart contract:** The data parameters and characteristics are retrieved by querying the smart contract.

6.2 Technical Requirements

For data access API, the capabilities described below have been defined. They are structured as epics and have been documented in a Trello board as shown in Tables 6.1– 6.10.

Table 6.1 Authentication and authorization – epics.

Name	Description	Labels
Policy management	Policy is a set of rules that define how to protect the assets in order to provide trust, security, and privacy. Policy management component is in charge of enforcing the rule set provided by i3-MARKET Backplane inside of the data access system.	**Epic**
Role management	A role is a set of policies attached to an entity in order to define the access that entity has within the i3-MARKET data access system. The role management component is in charge with fetching the list of policies and verifying them against the data access system.	**Epic**

Table 6.2 Authentication and authorization – user stories.

Name	Description	Labels
Intercept access attempts	As a data provider, I want to intercept the data access API access attempts so that I can check the policy	User Story
Check attempt against rule set	As a data provider, I want to check the access attempt of data access API against policy so that I be able to grant access	User Story
Grant access to permitted assets	As a data provider, I want to grant access to assets so that the user can access the data	User Story
Get the list of policies associated with role	As a data provider, I want to access Backplane so that I obtain the list of policies associated with the user's role	User Story
Verify role access	As a data provider, I want to invoke policy management so that I will verify the role access of the user	User Story
Allow or deny access	As a data provider, I want to allow or deny access so that the data can be accessed according to policy	User Story

Table 6.3 Data transfer transparency – epics.

Name	Description	Labels
Data transfer management	Data transfer management is a component that is in charge with the control of the connection between the provider and consumer	Epic
Data transfer tracking	The data transfer tracking component measures the volume of data transferred between the producer and consumer	Epic
Data transfer monitor	The data transfer monitor component communicates with the Backplane before and after the data transfer	Epic

Table 6.4 Data transfer transparency – user stories.

Name	Description	Labels
Initialize the connection	As a data provider, I want to initialize a connection so that I will be able to start the transfer	User Story
Resume the connection	As a data provider, I want to resume the connection so that I will be able to continue the transfer	User Story
Finalize the connection	As a data provider, I want to finalize the connection so that I can conclude the transfer	User Story
Measure transferred data	As a data provider, I want to measure the transferred data so that I can report the information to the Backplane	User Story
Inform i3-MARKET Backplane	As a data provider, I want to inform the Backplane so that the system can track the volume of transferred data	User Story
Invoke linked smart contract	As a data provider, I want to invoke the smart contract so that the data can be transferred according to contractual parameters	User Story

Table 6.5 secure data transfer & anonymization – epics.

Name	Description	Labels
Data encryption	The data encryption component is responsible for the end-to-end process of encoding and decoding of data during transfer between the producer and consumer	Epic
Proxy	The proxy component can be used when the data producer identity needs to be hidden	Epic

Table 6.6 Secure data transfer and anonymization – user stories.

Name	Description	Labels
Key generation and exchange	As a data provider, I want to obtain the encryption key so that I will be able to transfer the data securely	User Story
Transfer encrypted data	As a data provider, I want to transfer encrypted data so that I will be able to enforce the transfer safety and confidentiality	User Story
Decrypt data	As a data consumer, I want to decrypt the transferred data so that I access the transferred data	User Story
Activate proxy	As a data provider, I want to activate the proxy so that I can hide my identity	User Story
Transfer data through proxy	As a data provider, I want to transfer the data through proxy so that my identity remains confidential	User Story

Table 6.7 Data management – epics.

Name	Description	Labels
Batch data transfer management	Batch data transfer management refers to one time data transfer and retrieving one chunk of data in a session	Epic
Data stream management	Data stream management component is responsible for the continuous transfer of data based on a subscription, e.g., publish/subscribe mechanism	Epic

Table 6.8 Data management – user stories.

Name	Description	Labels
Request batch data	As a data consumer, I want to request a batch of data so that I will be able to obtain the data from a provider	User Story
Transfer batch data	As a data provider, I want to transfer a batch data so that I will send the data to consumer	User Story
Subscribe to channel	As a data consumer, I want to subscribe to a channel so that I access the streaming data	User Story
Trigger data transfer	As a data provider, I want to trigger the data transfer so that the data is sent on a stream	User Story
Get data	As a data consumer, I want to get the data so that I can save data locally	User Story
Unsubscribe from channel	As a data consumer, I want to unsubscribe from a channel so that I disconnect from the stream of data	User Story

Table 6.9 Data access SDK – epics.

Name	Description	Labels
Batch data transfer management	Authentication and authorization are required for users who call the data access API from data access SDK	Epic
Data stream management	Data transfer is a component that is responsible for the management of the request data and response	Epic

Table 6.10 Data access SDK – user stories.

Name	Description	Labels
Authenticate and authorize the data consumer	As a software developer, I want to authenticate and authorize the consumer so that I will be able to obtain the data from a provider	User Story
Request data	As a software developer, I want to implement a data request so that I get access to data	User Story
Get data	As a software developer, I want to implement the get data so that I can transfer the data locally	User Story

6.3 Solution Design/Blocks

The secure Data Access & Transfer enables data providers to secure registration to access and/or exchange data in a peer-to-peer fashion once the contracts and security mechanisms for identity management have been executed and confirmed. This improves scalability and avoids the need that data providers have to share their data assets with intermediaries (e.g., a marketplace operator). In addition, anonymization can be used to hide the provider's identity.

Data Access & Transfer consists of the following main parts:

- Authentication and authorization
- Policy management
- Role management
- Secure data transfer and anonymization
- Data transfer based on the non-repudiation protocol with support for concurrent threads and logging.

Authentication and authorization:

Authentication: Verifies the identity of the user against the i3-MARKET Backplane.

Authorization: Verifies the permissions the authenticated user has in the i3-MARKET platform allowing to perform authorized actions and granting access to resources.

The authentication and authorization subsystem has the following subcomponents:

Policy management:

Policy is a set of rules that defines how to protect the assets to provide trust, security, and privacy. The policy management component oversees enforcing the rule set provided by i3-MARKET Backplane within the data access system. The responsibilities of the policy management module are:

- Intercept access attempts
- Check attempt against rule set
- Grant access to permitted assets

Role management:

A role is a set of policies attached to an entity in order to define the access that entity has within the i3-MARKET data access system. The role management component is in charge of fetching the list of policies and verifying them against the data access system. The responsibilities of the role management module are:

- Get the list of policies associated with role from Backplane
- verify role access by invoking policy management
- Allow or deny functionalities

Secure data transfer and anonymization:

Secure data transfer and anonymization subsystem has the following components:

Data encryption:

The responsibilities of the data encryption module are:

- Key generation and exchange
- Transfer data in an encrypted way between endpoints
- Decrypt data on the consumer side

Proxy:

The proxy needs to be used when the identity of the data provider needs to be hidden. This feature is optional; therefore, there is no need to implement it if there is no specific requirement referring to the anonymity of the data provider. The responsibilities of the proxy module are:

- Activate the proxy
- Configure the parameters to hide the identity
- Data transfer goes through the proxy

Data transfer transparency:

Data transfer transparency subsystem has the following components:

Data transfer management:

This component is responsible for the management of the connection between provider and consumer and implements the following functionalities:

- Initialize the connection
- Resume the connection
- Finalize the connection

Data transfer tracking:

This component implements the following operation:
- Measure the amount of transferred data.

Data transfer monitor:

The information about how much data was transferred, when the data transfer was initiated and when it was completed, is monitored and the following operations are triggered:

- Inform the i3-MARKET Backplane that the data transfer was performed and report how much data was transferred
- Invoke the linked smart contract

Data management:

Two methods for data transfer are supported by data access API, which are supported by the following modules:

VDI:

One-time data transfer for one chunk of data in a session with the following methods:

- Request data
- Transfer data

Data stream management:

Continuous transfer of data based on a subscription, e.g., publish/subscribe mechanism:

- Subscribe to an offering
- Trigger data transfer – on the producer side
- Get data – on the consumer side
- Unsubscribe

6.4 Diagrams

The process view perspective is presented in the sequence diagrams in Figures 6.1, 6.2, 6.3, and 6.4.

The sequence diagrams of the subsystems listed below are detailed here:

- Authentication and authorization
- Data transfer transparency
- Data management
- Secure data transfer and anonymization

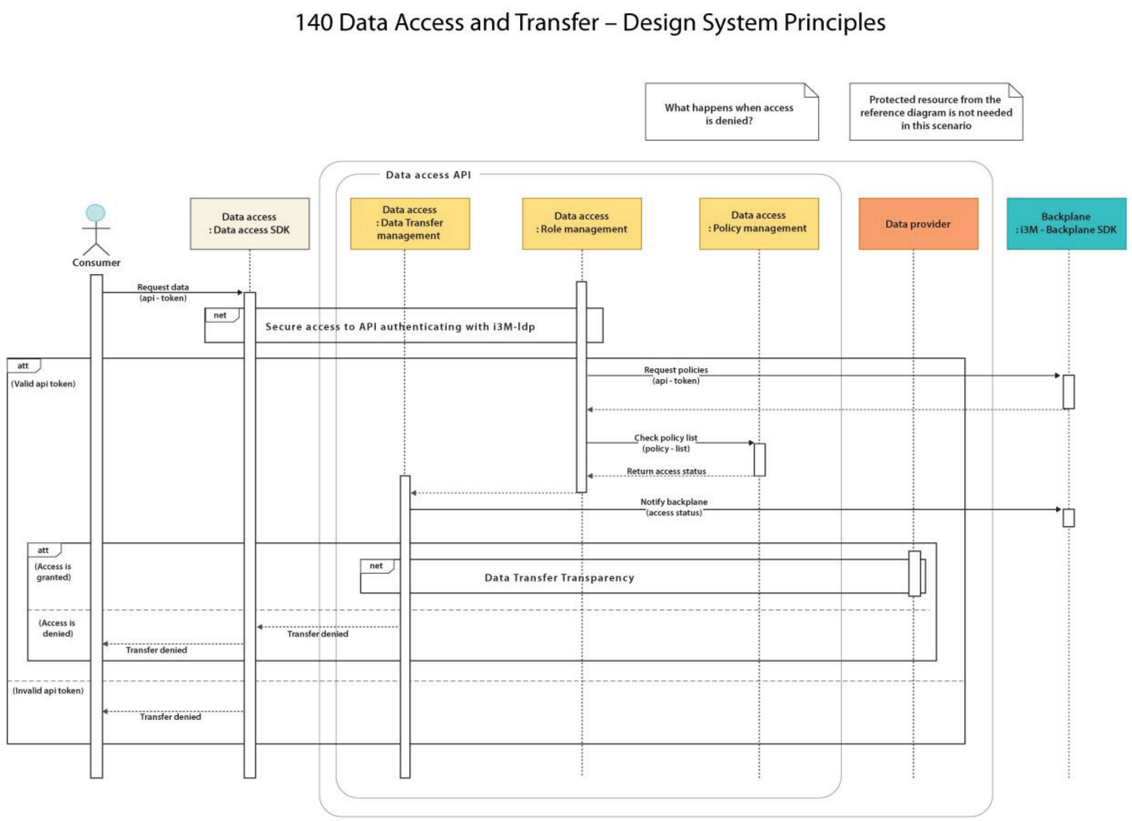
140 Data Access and Transfer – Design System Principles
What happens when access is denied?
Protected resource from the reference diagram is not needed in this scenario
Data access API
Consumer
Data access : Data access SDK
Data access : Data Transfer management
Data access : Role management
Data access : Policy management
Data provider
Backplane : i3M - Backplane SDK
Request data (api - token)
net
Secure access to API authenticating with i3M-Idp
att
(Valid api token)
Request policies (api - token)
Check policy list (policy - list)
Return access status
Notify backplane (access status)
att
(Access is granted)
net
Data Transfer Transparency
(Access is denied)
Transfer denied
Transfer denied
(Invalid api token)
Transfer denied

Figure 6.1 Authentication and authorization.

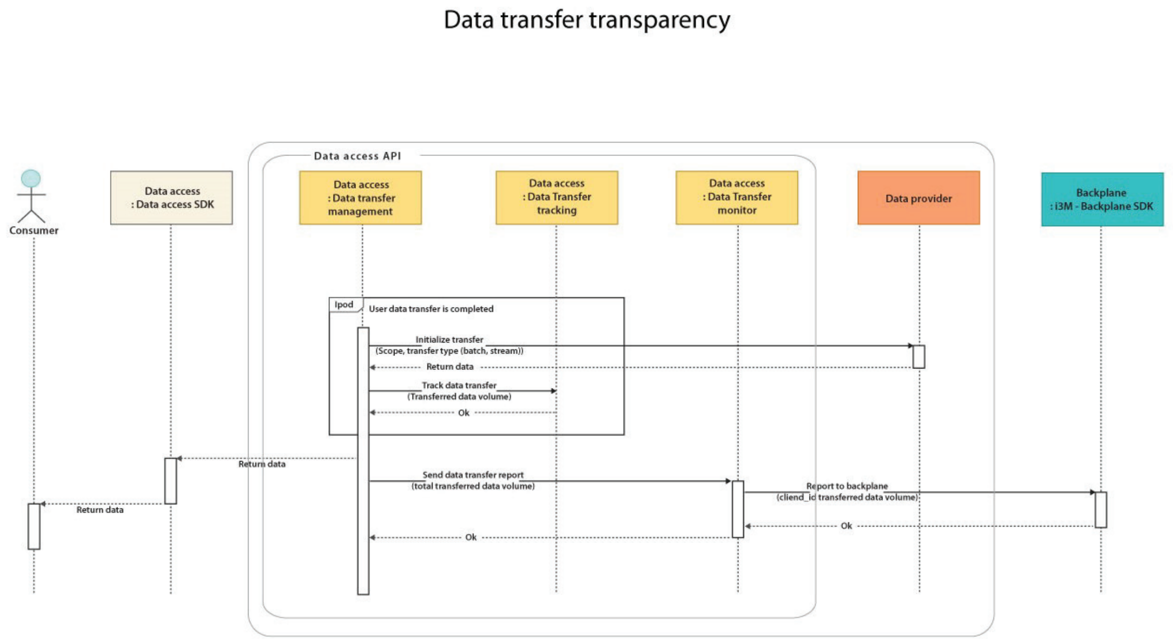

Figure 6.2 Data transfer transparency.

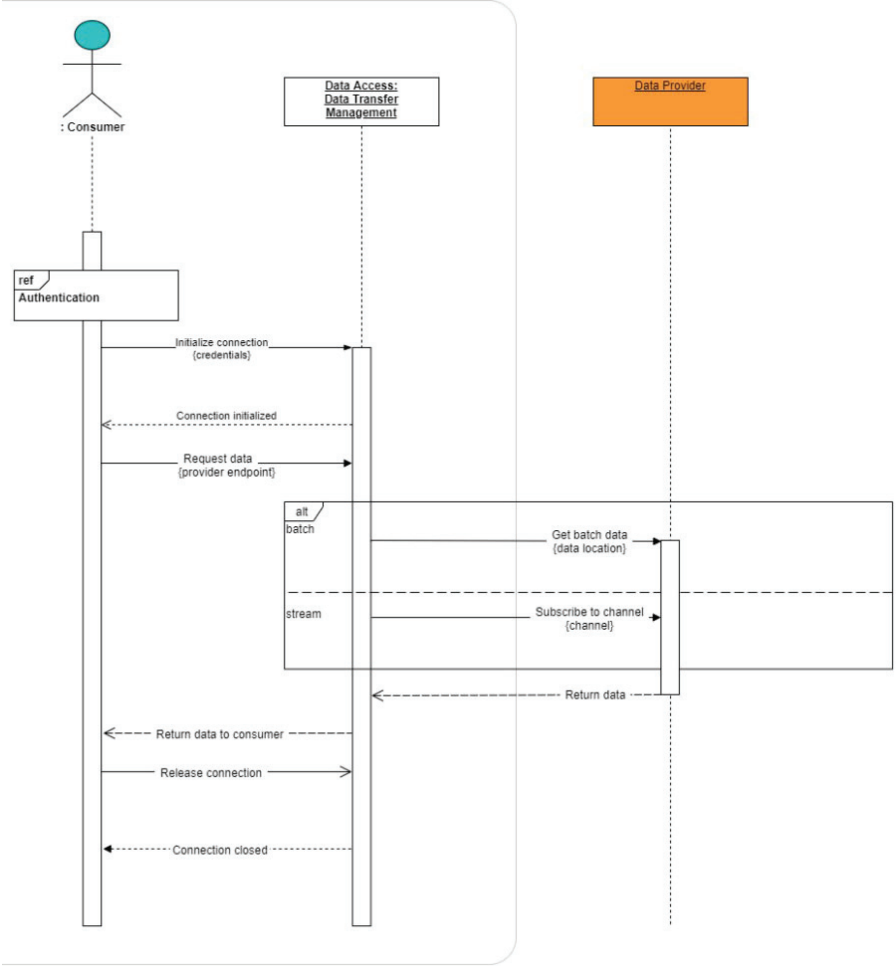

Figure 6.3 Data management.

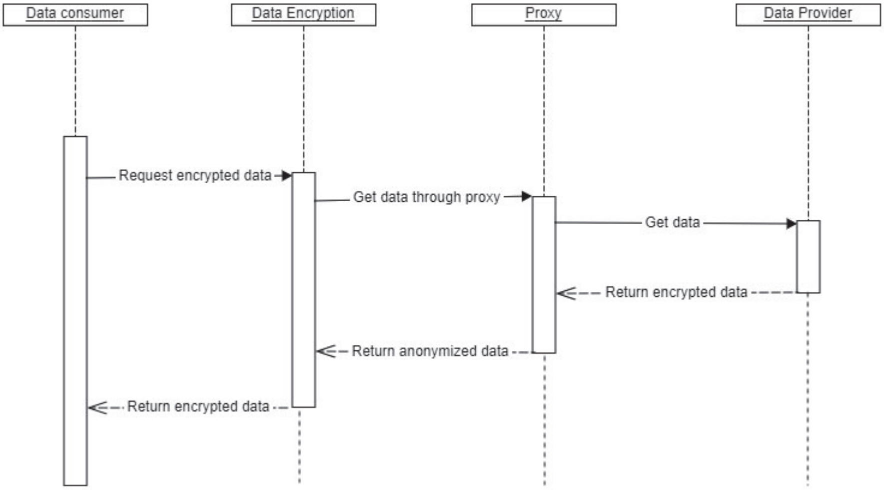

Figure 6.4 Secure.