DATA SHARING COALITION

Findings Unattended Home Delivery use case

Table of contents

Management Summary

Use case context	• Merchants and logistic service providers (LSPs) struggle to meet customer expectations and reach profitability in home delivery • Innovation in home delivery services by merchants and LSPs to create value for consumers • The context of this use case is a platform for (unattended) secure home delivery developed by The Chain Never Stops
Use case learnings	• Managing data access policies is essential for realising controlled and scalable data access • The three common locations for storing policies are: at the Entitled Party, at the Data Provider, and at a third party • Suitability of three locations depends on data sharing context; for unattended home delivery the third party method is used by implementing an Authorisation Register • This use case lowers the implementation effort of Authorisation Registers by developing a generic secure access hub (‘the Hub’) • The generic part of the Hub will be open sourced for re-use in other contexts after a pilot with Merchants and LSPs

Table of contents

Merchants and logistic service providers (LSPs) struggle to meet customer expectations and reach profitability in home delivery

Home delivery sector trends	Home delivery sector challenges
Off- to online shopping will continue to grow with a **YoY growth of 7.5 to 15 percent**[1]	Home delivery is expensive for merchants and logistic service providers (LSP)
Food delivery is expected to grow to **EUR 10 bln market in 2025**, 15% of the total food market[2]	Food delivery specifically is even loss making for merchants
91% of Dutch online consumers prefer their food and non-food to be **delivered at home**[3]	Merchant and LSPs can't offer the expected personalised customer experience for home delivery impacting their customer relationships
33% of households are open to unattended home delivery of groceries using **smart locked doors**[4]	No scalable solution in place for unattended home delivery

Source: [1]Parlement & Wetenschap, 2021, [2]Food Service Institute Nederland, [3]Deloitte Consumentenonderzoek 2021 [4]Customer panel large dutch food retailer

Innovation in in home delivery services of merchants and LSPs is needed to stay relevant for consumers and reach profitability

Examples of new and improved services in home delivery market

Unattended home delivery

Description: Unattended home delivery enables 'One-time-right delivery', in which customers receive the order at home while not necessarily being present themselves

Benefits:

- Customers no longer have to be at home to securely receive their purchases.
- LSPs reduce costs with route planning, delivery at early or late hours and reduced time per delivery
- For merchants, it opens new business opportunities with their customers like packaging-free fresh products and returnable packaging

Focus of this report

Example: The Chain Never Stops and retailer Hoogvliet ran a successful pilot of their solution for four months. The International Journal of Retail & Distribution Management recently published an article describing the different drivers behind the customer behaviour

Tokenised payments

Description: Tokenised payments simplify recurring payments for customers and merchants by using a token unique to that customer & retailer for use in its (web)shops

Benefits:

- Customers no longer have to fill in bank details every time they make an (online) purchase
- Merchants increase their conversation rate and eliminate the need for keeping and protecting customer's sensitive bank data

Examples: In the Netherlands, both ING and Ahold Delhaize and Picnic and Rabobank experimented with tokenised payments

Local food initiatives

Description: Local food initiatives connect producers (e.g. farmers) directly with customers to shorten the supply chain

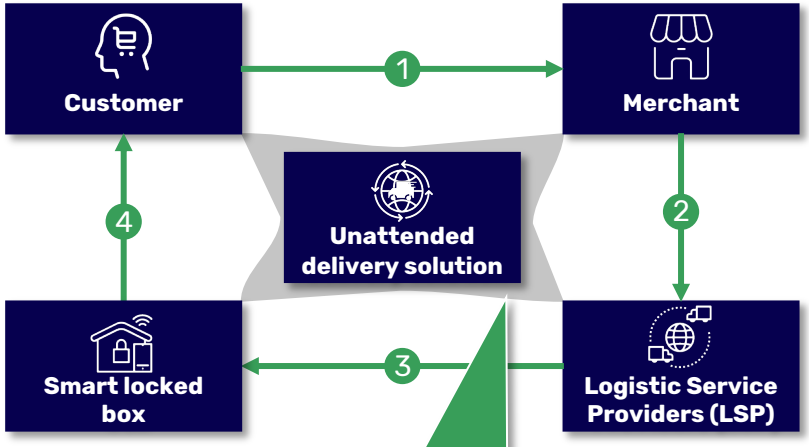
Benefits:

- Customers have easier access to local food, a trend which has accelerated during the COVID-19 pandemic
- Producers increase their margins as intermediaries are removed
- Merchants and LSPs, both new entrants and incumbents, can benefit when they adapt to these developments

Examples: Crisp, a Dutch online supermarket which focuses on fresh quality products from regional makers and growers, and Lekkerder, a platform connecting customers to farmer stores.

The context of this use case is a platform for (unattended) secure home delivery developed by The Chain Never Stops

Interaction model (simplified)



Data sharing functionalities available through the unattended delivery solution:

- The Customer can query delivery status throughout delivery
- The Customer can open the Smart locked box
- The Merchant can create a policy for orders placed
- The LSP can query Smart locked box availability for planning
- The LSP can request Smart locked box access during delivery
- The LSP can create a delivery confirmation after delivery

User journey unattended home delivery

1. The Customer makes an order online at a Merchant and selects unattended home delivery as delivery method
2. The Merchant assigns the delivery to a Logistic Service Provider
3. The Logistic Service Provider plans and executes the delivery to the box
4. Customer retrieves delivery from the box

Role	Description
Customer	An end user placing an order online at a merchant
Merchant	An organisation selling their goods online
LSP	An logistics organisation which delivers packages
Smart locked box	A (refrigerated) smart locked storage box for e.g. groceries
Unattended delivery solution	• Platform for facilitating Unattended Delivery/Collection • Solution for managing data access between all actors

Organisations involved

The Chain Never Stops

POORT8 DATA VERBINDT LOGISTIEK

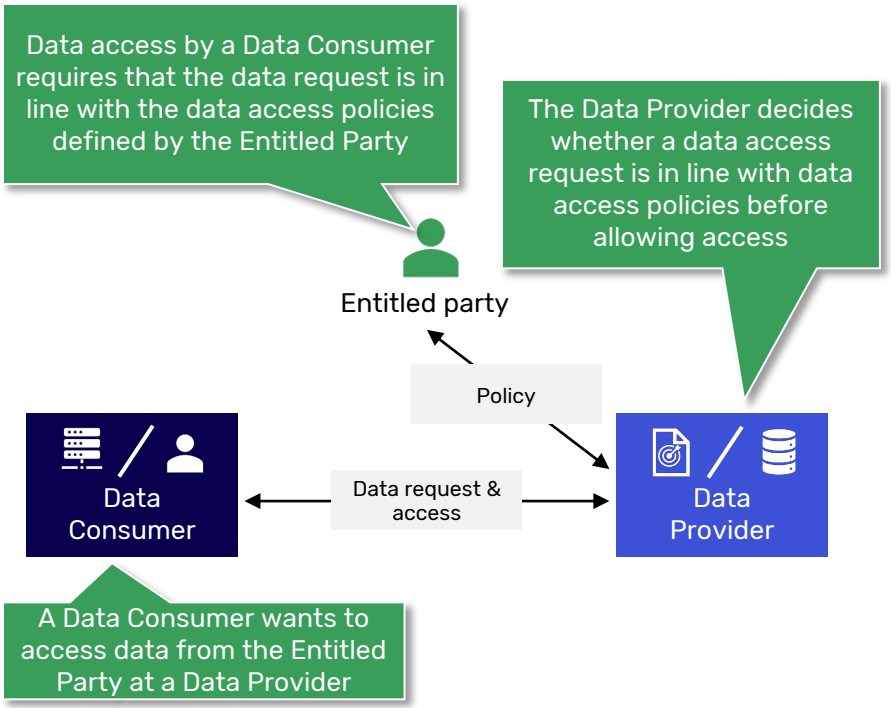
Schemes used

iSHARE

See appendix for more information on organisations and iSHARE

Table of contents

Managing data access policies is essential for realising controlled and scalable data access



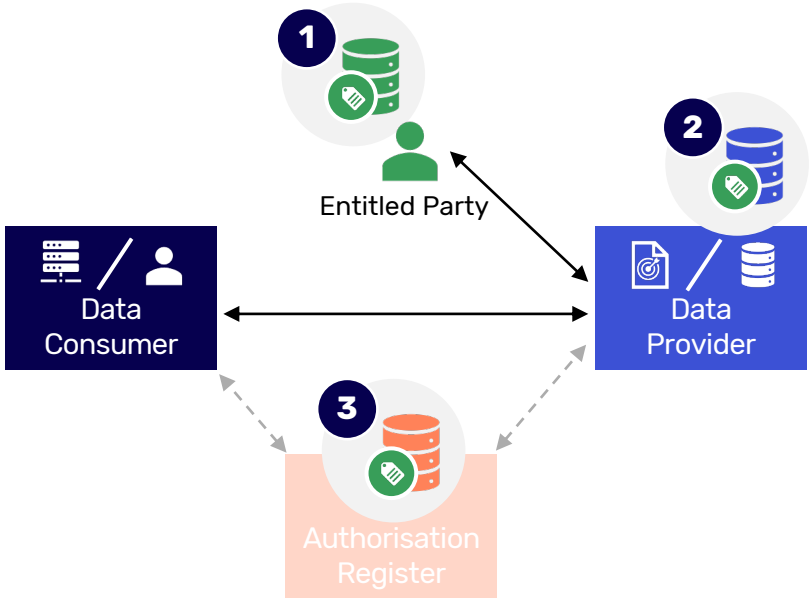
Introduction to policies for data access

- Data driven innovation requires access to data from various organisations
- Entitled Parties , having rights over the data, need a sufficiently safe and convenient way to ensure that their data is accessed according to their data access policies[1]
- Upon a data request from the Data Consumer, the Data Provider must make an authorisation decision whether the data request is in accordance with the policy. XACML[2] defines a standard for access control, including roles for making authorisation decisions
- The Data Provider needs to know the policies defined by the Entitled Party to make an authorisation decision on behalf of the Entitled Party
- The Data Provider must be able to retrieve the policies in a convenient and machine readable way to realise scalable data access

[1]'Policies' instead of 'data access policies' will be used in the rest of this document
[2]See appendix for a detailed introduction about XACML and data access

The three common locations for storing policies are: at the Entitled Party, at the Data Provider, and at a third party

Three locations for storing policies



1 Policies at the Entitled Party

The Entitled Party itself manages its policies. For every data access request, the Data Provider requests relevant policies at the Entitled Party to come to the authorisation decision.

2 Policies at the Data Provider

The Entitled Party stores (part of its) policies at the Data Provider. For every data access request the Data Provider validates the request against these pre-defined policies. The Entitled Party must be able to update its policies at the Data Provider

3 Policies at a third party (Authorisation Registry)

The Entitled Party stores policies required for authorisation decisions related to their data at a third party. For every data access request, the Data Provider queries the third party for the policies. The Entitled Party must be able to update its policies at the third party

See Appendix for detailed information regarding the types policy management

Suitability of three locations depends on data sharing context; for unattended home delivery the third party method is used

Policies at the Entitled Party

Suitable for high value data where full control over data access remains at the Entitled Party. This requires the Entitled Party to be sufficiently technologically developed to manage their own policies. Further this solution enables ad hoc authorisation decisions by the Entitled Party (i.e. consent)

Examples include: The Entitled Party manages an ERP system for policies to access data which is managed by other organisations

Policies at the data

Suitable for situations where the Data Provider can provide the necessary technology for enabling the solution and thereby taking this burden from the Entitled Party. This solution requires a technical integration between the Entitled Party and the Data Providers

Examples include: Open Banking/PSD2 , where the Data Provider (a bank) stores the data and policies of its customers (i.e. access to the account consent)

Used by this project

Policies at a third party (Authorisation Registry)

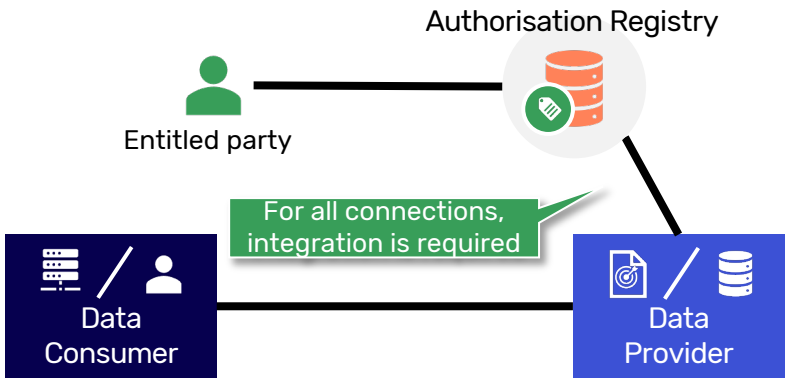
Suitable for managing policies for a range of Data Providers in a single location, and therefore applicable to situations where scaling is of importance. This solution requires a (technical) integration between the Entitled Party and an Authorisation Registry, as well as the Data Providers and a Authorisation Registry.

Examples include: Sharing freight data, Unattended home delivery (this use case), where the Entitled Party stores policies in a Authorisation Registry

See Appendix for detailed information regarding the types policy management

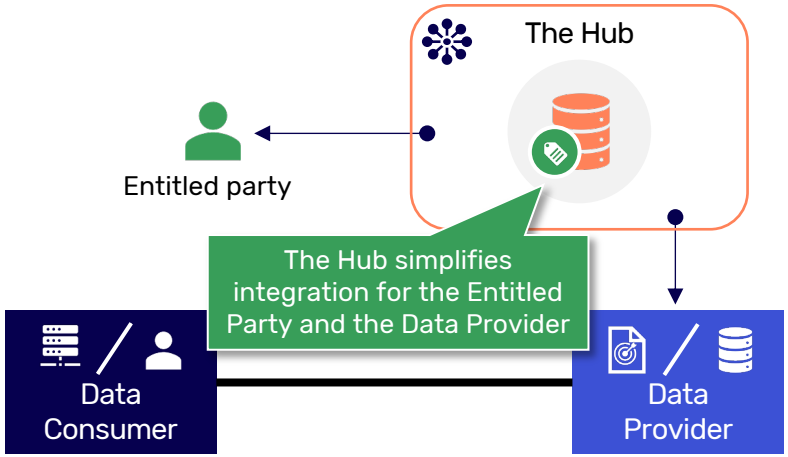
This use case lowers the implementation effort of Authorisation Registers by developing a generic secure access hub ('the Hub')

Policies at a third party



This solution requires integration of the Data Provider and the Entitled party with the Authorisation Registry. This can be a complex endeavour

Policies at a third party using the Hub

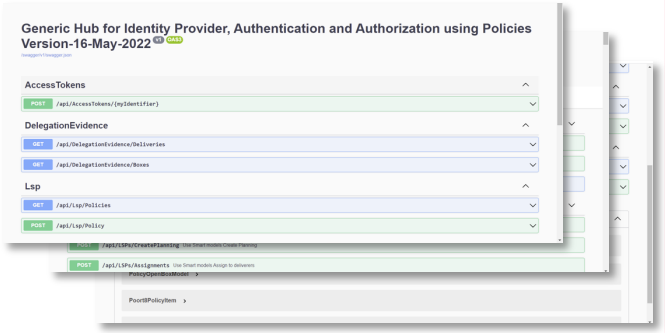


The Hub simplifies implementation effort by enabling business users to create policies in the Authorisation Register through a GUI. This removes the need for business users to involve IT departments and build the relevant functions themselves.

Legend — Technical integration — Graphical user interface

The generic part of the Hub will be open sourced for re-use in other contexts after a pilot with Merchants and LSPs

The Hub will be tested in unattended home delivery context



Visual of the Hub as used for unattended home delivery

- The Hub is developed by The Chain Never Stops using Poort8's AR
- Once finished, it will be deployed for the unattended home delivery setting with a Dutch Merchant and LSP

In the future, the Hub can be re-used in other contexts due to the generic design

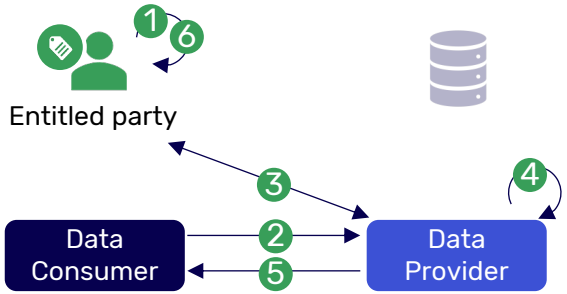
- The design of the Hub is generic, meaning that it can be used for any data sharing context where Authorisation Registers are used
- As discussed on slide 11/12, the Hub is especially relevant in contexts with many different actors involved in data sharing and where IT implementation efforts are a key burden for the organisations
- Examples of other contexts where the Hub can be reused:
  - **Car data**: Enabling backend systems of car manufactures to share data with service providers under control of the Entitled Party
  - **Energy data**: Enabling business owners to manage data access to company's energy data of various organisations

The generic part of the Hub will be open sourced once finished

Table of contents

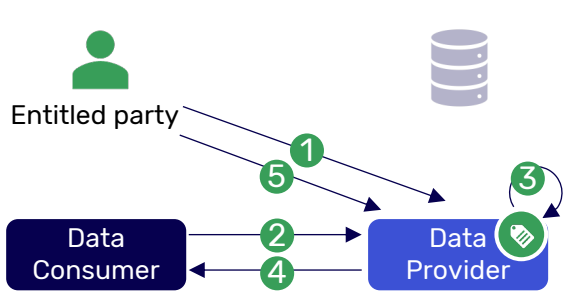
The three common locations for retrieving policies have different interaction models

Policies at the Entitled Party



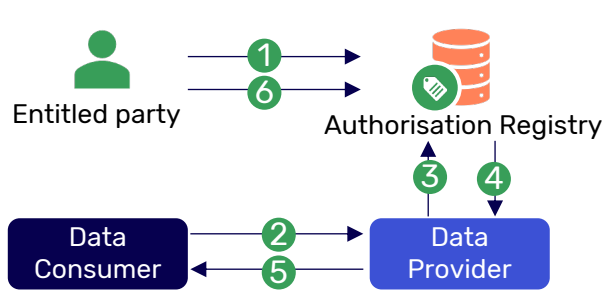
1. The EP creates and manages their own policies
2. The DC requests specific data at the DP
3. The DP retrieves relevant policies at the EP
4. The DP makes the authorisation decision using retrieved policies
5. The DP allows the DC access the data if the authorisation is granted
6. The EP periodically updates its policies

Policies at the data



1. The EP creates its policies and stores the relevant ones at the DP
2. The DC requests specific data at the DP
3. The DP makes the authorisation decision using retrieved policies
4. The DP allows the DC access the data if the authorisation is granted
5. The EP periodically updates its policies at the DP

Policies at a third party



1. The EP creates its policies and stores the relevant ones at the AR
2. The DC requests specific data at the DP
3. The DP retrieves policies at the AR
4. The DP makes the authorisation decision using retrieved policies
5. The DP allows the DC access the data if the authorisation is granted
6. The EP periodically updates its policies at the AR

- Policies

TCNS approached Poort8 and the Data Sharing Coalition for realising secure data access based on Authorisation Registers

Organisations involved

The Chain Never Stops

- The Chain Never Stops (TCNS) offers a sustainable last mile personalised (unattended) delivery solution for Merchants, Logistics Service Providers (LSP) and Customers (B2B & B2C)
- TCNS offers a combination of cloud and IoT based (B2B2C) soft infrastructure and a physical hard infrastructure of storage boxes with automated secure policy based data access
- TCNS developed the Hub and approached Poort8 because they have an AR and TCNS wishes to use a 3rd Party AR because of data sovereignty considerations

POORT8
DATA VERBINDT LOGISTIEK

- Poort8 offers high quality data sharing software products with a focus on privacy-by-design and security-first and support with design and implementation of the required solution.
- Poort8 has developed an Authorisation Manager based on iSHARE, which can be used to control whom can access what data
- In this use case Poort8 provides the 3rd Party AR and ensures that Unattended Delivery Policies created by Shippers and LSPs can be stored in the AR

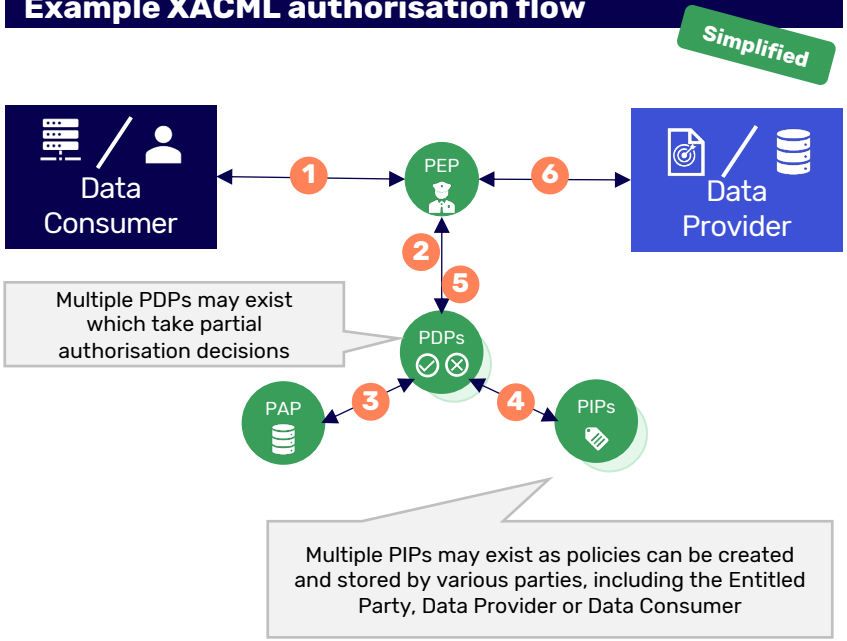
Schemes used

iSHARE

- iSHARE is a standard and legal framework for sharing business data under control of the entitled party. For this, iSHARE offers a standardised and reusable way of identifying, authenticating and authorizing entities to share data with, taking away the need for tailor-made connections.
- iSHARE allows parties to be specific about what data whom can request, and about who can do what with data once it is received – e.g., 'only use it for a month', 'do not re-share', 'not for commercial use' etc.

XACML defines a standard for how to evaluate authorisation requests according to the rules defined in policies

Example XACML authorisation flow



Source: Data Sharing Coalition Analysis based on the Data Sharing Canvas 6.3.3.

Authorisation flow steps

1. The Data Consumer requests data access which is intercepted at the Data Provider's PEP
2. The PEP performs an authorisation request at the relevant PDP
3. The PDP evaluates the request against the loaded policies from the PAP
4. If needed, the PDP retrieves policies from the PIP
5. The PDP reaches a authorisation decision based on the policies and information and returns it to the PEP
6. The PEP enforces the authorisation decision and processes the request; in the case of a permit, data access is granted.

XACML roles defined

PAP	Policy Administration Point	Point at which data access policies are created and managed
PDP	Policy Decision Point	Point which evaluates authorisation requests against data access policies before issuing access decisions
PEP	Policy Enforcement Point	Point which is responsible for protecting the data by executing access control decisions. It incepts data access requests and forwards them to the PDP
PIP	Policy Information Point	Point which provides any underlying information relevant for the authorisation (i.e. a resource, subject, environment)