6

Explicit Consent

6.1 Objectives

i3-MARKET's architecture has been designed to allow all the stakeholders – namely providers, consumers, data owners, and marketplace operators – to meet the strictest policies in terms of privacy and data protection, which in fact leads to meet the GDPR requirements with little effort.

Article 4 of the GDPR [26] defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her". Data controllers shall be able to demonstrate that they hold the explicit consent of the data subjects to process (Article 7) and/or trade their data. To the best of our knowledge, no technology is enforcing user consent to the point of preventing trading without it.

It is a remarkably innovative feature of the i3-MARKET project that the explicit consent of the data subjects is absolutely required for trading users' data.

6.2 Technical Requirements

The explicit consent subsystem inherits the following technical requirements from the GDPR [26]:

- Trading of sensitive data related to people/entities require their explicit consent.
- The consent can be revoked.
- If a consent is revoked, the data cannot be sold/distributed again.
- The data should be also deleted from already sold datasets.

- The enforcement of the explicit consent should not leak any sensitive data.
- The solution must support non-digitally native data subjects, which delegate consent management to an i3-MARKET provider.

6.3 Solution Design/Blocks

The explicit consent system relies on two main complementary actions: explicit consent and limited data lifetime.

Use-case 1: the data subject is an active i3-MARKET stakeholder:

The explicit consent is a legal agreement between a data provider and the subject of the data. It is out of the scope of i3-MARKET, which is just a technology. However, for every subject involved, a provider should provide an (anonymous) identifier of the consent signed by the subject using an anonymous identity only known to the provider.

As a result, a data offering in i3-MARKET that deals with sensitive data includes a list of signed consents of the data subjects. The smart contract manager (SCM) will verify the consent signatures and status when orchestrating a data sharing agreement. If a consent is not in place or revoked, the SCM prevents the exchange of the affected data.

Obviously, subject can at any time revoke a consent and therefore prevent their data to be sold again. Proving ownership of the consent requires interaction with the SCM using the subject’s anonymous identity, which requires the use of the i3M-Wallet.

Note that i3-MARKET does not analyze or check for validity of the actual consent agreements between providers and data subjects. It is the (legal) responsibility of the provider to have the consent in place when legally required. Obviously, the way the consent anonymous ID is created guarantees that the presented consent form was the one registered in i3-MARKET.

For a better understanding on how consents are managed, refer to the detailed diagrams and the SCM explicit-consent endpoints.

Use-case 2: the data subject delegates consent management to an i3-MARKET provider:

The concept of limited data lifetime refers to when a dataset is sold; the consumer accepts the legal obligation to delete it after the agreed lifetime. The lifetime of course must meet the affecting regulation. In i3-MARKET, we are using a 14-day lifetime for the wellbeing pilot.

Meeting the limited data lifetime requirement is out of the scope of i3-MARKET, which just labels datasets with the lifetime. Indeed, its implementation is the responsibility of the data providers and consumers, which should sign legal agreements stating that the dataset should be deleted after the agreed time (lifetime). Note that this does not imply that the consumer cannot access the data again after erasing it; it only means that the consumer will need to re-download them again.

When a data subject revokes consent, the GDPR not only states that her data should not be sold again but also that it should be removed from any sold dataset. Limited data lifetime is absolutely necessary to legally comply with the GDPR. Re-downloading again guarantees that data related to revoked consents “disappears” from any sold dataset.

6.3.1 Diagrams

In the following, we present four sequence diagrams representing the flows for giving consent and revoking it in two use-cases:

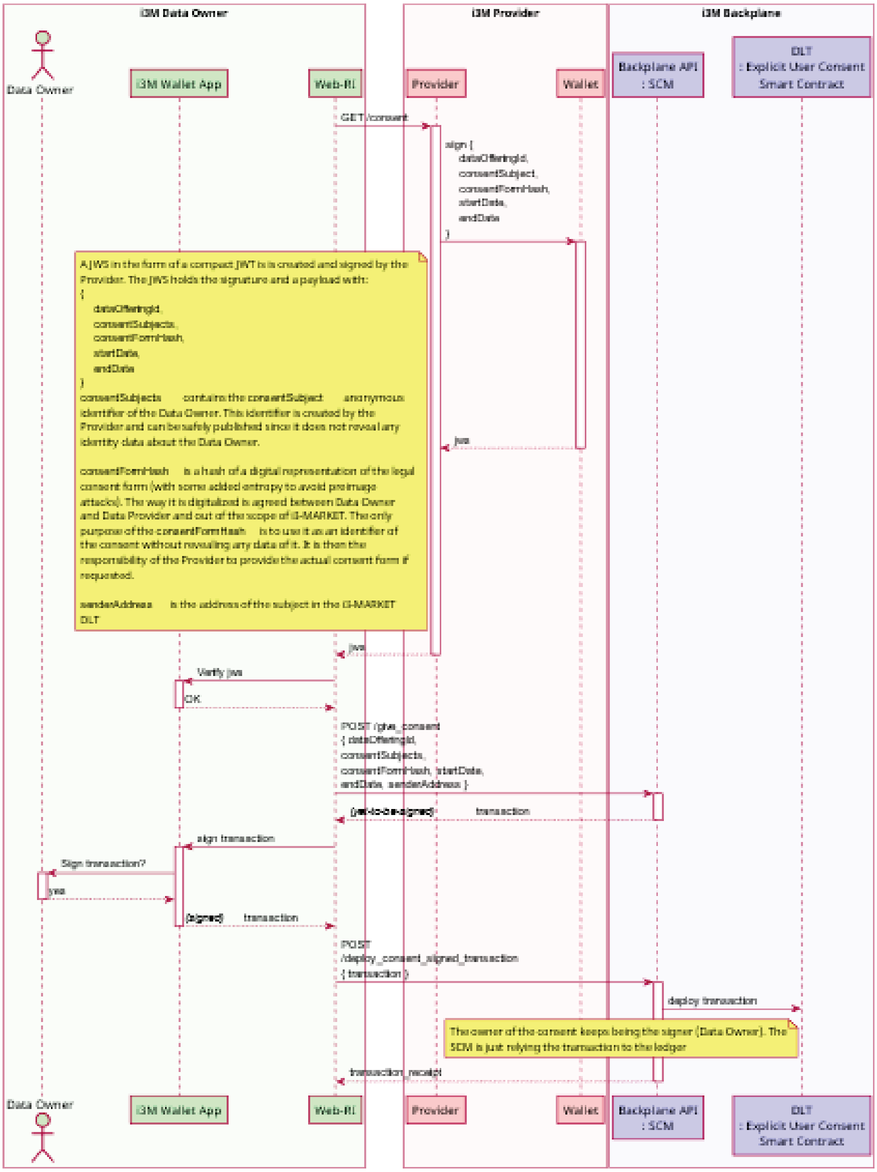
1. The data subject is an active i3-MARKET stake holder that can use her own wallet to interact with the i3-MARKET Backplane.
2. The data subject delegates consent management to the data provider, which will therefore interact with the i3-MARKET Backplane on behalf of the subject.

Use-case 2 meets the last technical requirement, introduced by the i3-MARKET wellbeing pilot, which states that data subjects may not be digitally natives or may not be interested in being an active i3-MARKET stakeholder.

The diagrams in Figures 6.1–6.4 are self-explanatory, but consider analyzing the SCM endpoints for the explicit consent for a better understanding of the flow.

Explicit consent:

- **Giving consent:**



A JWS in the form of a compact JWT is is created and signed by the Provider. The JWS holds the signature and a payload with:
{
dataOfferingId,
consentSubjects,
consentFormHash,
startDate,
endDate
}
consentSubjects contains the consentSubject anonymous identifier of the Data Owner. This identifier is created by the Provider and can be safely published since it does not reveal any identity data about the Data Owner.

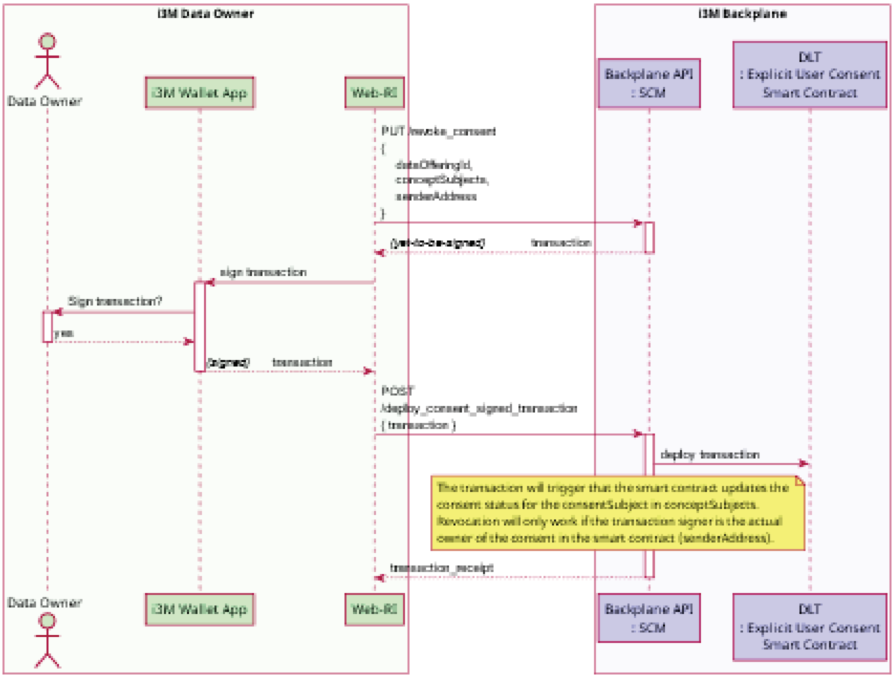
consentFormHash is a hash of a digital representation of the legal consent form (with some added entropy to avoid preimage attacks). The way it is digitalized is agreed between Data Owner and Data Provider and out of the scope of i3-MARKET. The only purpose of the consentFormHash is to use it as an identifier of the consent without revealing any data of it. It is then the responsibility of the Provider to provide the actual consent form if requested.

senderAddress is the address of the subject in the i3-MARKET DLT

The owner of the consent keeps being the signer (Data Owner). The SCM is just relying the transaction to the ledger

Figure 6.1 Use-case 1: giving explicit consent.

- **Revoking consent:**

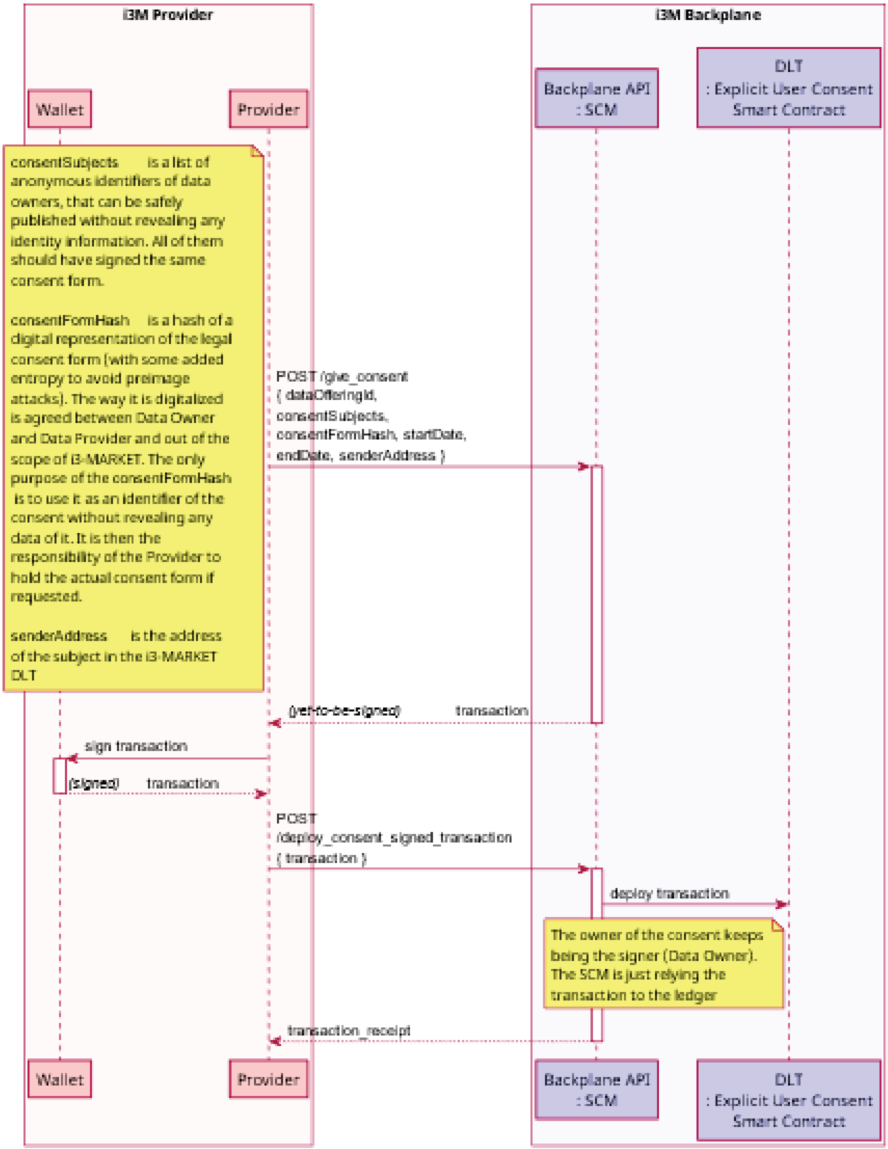


The transaction will trigger that the smart contract updates the consent status for the consentSubject in conceptSubjects. Revocation will only work if the transaction signer is the actual owner of the consent in the smart contract (senderAddress).

Figure 6.2 Use-case 1: revoking consent.

Limited data lifetime:

- **Giving consent:**



consentSubjects is a list of anonymous identifiers of data owners, that can be safely published without revealing any identity information. All of them should have signed the same consent form.

consentFormHash is a hash of a digital representation of the legal consent form (with some added entropy to avoid preimage attacks). The way it is digitalized is agreed between Data Owner and Data Provider and out of the scope of i3-MARKET. The only purpose of the consentFormHash is to use it as an identifier of the consent without revealing any data of it. It is then the responsibility of the Provider to hold the actual consent form if requested.

senderAddress is the address of the subject in the i3-MARKET DLT

POST /give_consent
(dataOfferingId,
consentSubjects,
consentFormHash, startDate,
endDate, senderAddress)

POST
/deploy_consent_signed_transaction
(transaction)

The owner of the consent keeps being the signer (Data Owner). The SCM is just relying the transaction to the ledger

Figure 6.3 Use-case 2: giving explicit consent.

- **Revoking consent:**

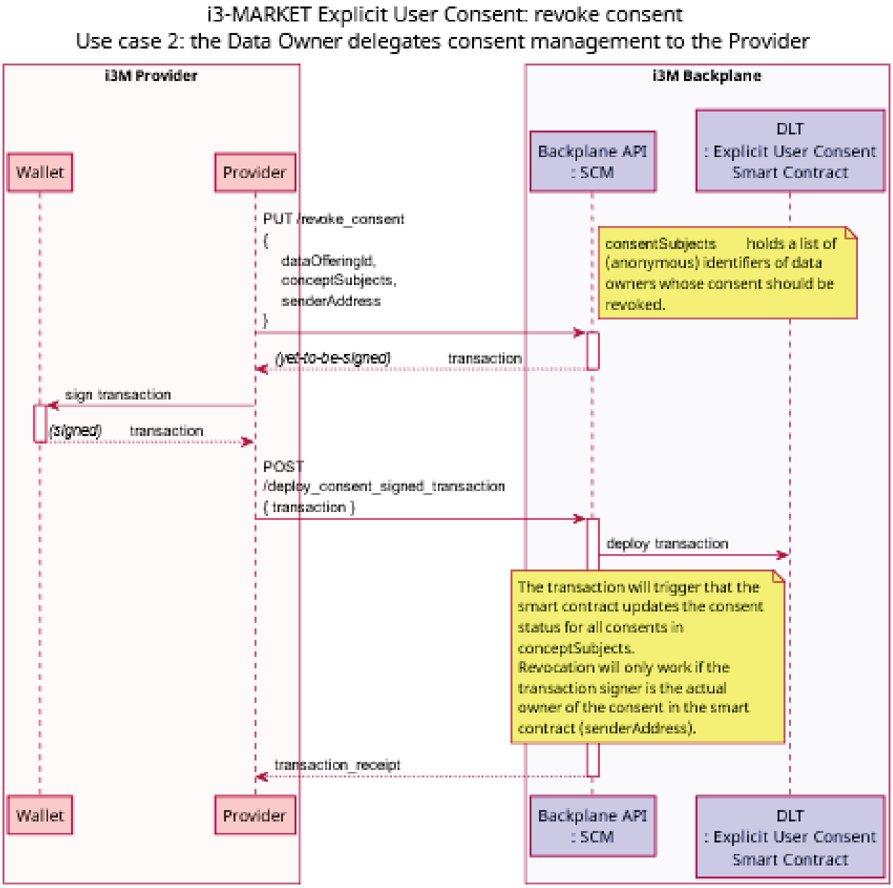

i3-MARKET Explicit User Consent: revoke consent
Use case 2: the Data Owner delegates consent management to the Provider
i3M Provider
i3M Backplane
Wallet
Provider
Backplane API
: SCM
DLT
: Explicit User Consent
Smart Contract
PUT /revoke_consent
{
dataOfferingId,
conceptSubjects,
senderAddress
}
consentSubjects holds a list of (anonymous) identifiers of data owners whose consent should be revoked.
(yet-to-be-signed) transaction
sign transaction
(signed) transaction
POST
/deploy_consent_signed_transaction
{ transaction }
deploy transaction
The transaction will trigger that the smart contract updates the consent status for all consents in conceptSubjects.
Revocation will only work if the transaction signer is the actual owner of the consent in the smart contract (senderAddress).
transaction_receipt
Wallet
Provider
Backplane API
: SCM
DLT
: Explicit User Consent
Smart Contract

Figure 6.4 Use-case 2: revoking consent.

6.4 Background Technologies

The explicit user consent subsystem has no special selected technologies since its development is actually split into other subsystems:

- Consent giving and revoking is implemented in the smart contract manager, which is described in more detail in Chapter 9.
- Consent checking before exchanging data related to a data subject is implemented between the smart contract manager and the secure data access SDK.