SIGNATU

DOCUMENTING CONSENT

IPEN Frankfurt 2016-09-09

Torgeir Hovden - torgeir@signatu.com

@signatucom

https://signatu.com

ABOUT ME

TORGEIR HOVDEN
Co-Founder
torgeir@signatu.com

MSc CS, MTM/MBA
NTNU, MIT Sloan, NHH

PAST
Strategic Advisor, Mozilla
CTO Telenor Digital
Principal Engineer, Microsoft
Sr. Director FAST

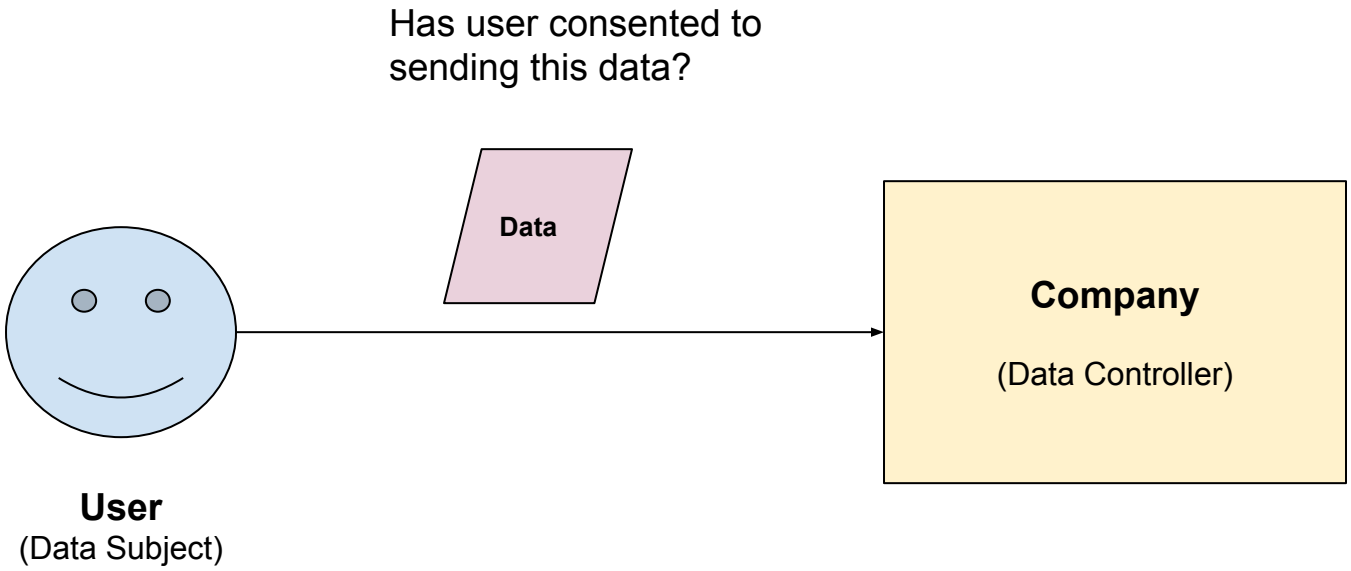
GDPR AND CONSENT

- Data Controller must be able to **demonstrate** that the data subject consents to the processing operation, according to the **GDPR Article 7.1** and the **Recital 42**.

- The exercise of the **data subject rights** or **enforcement of the privacy policy** may depend on the ability produce evidence of consent

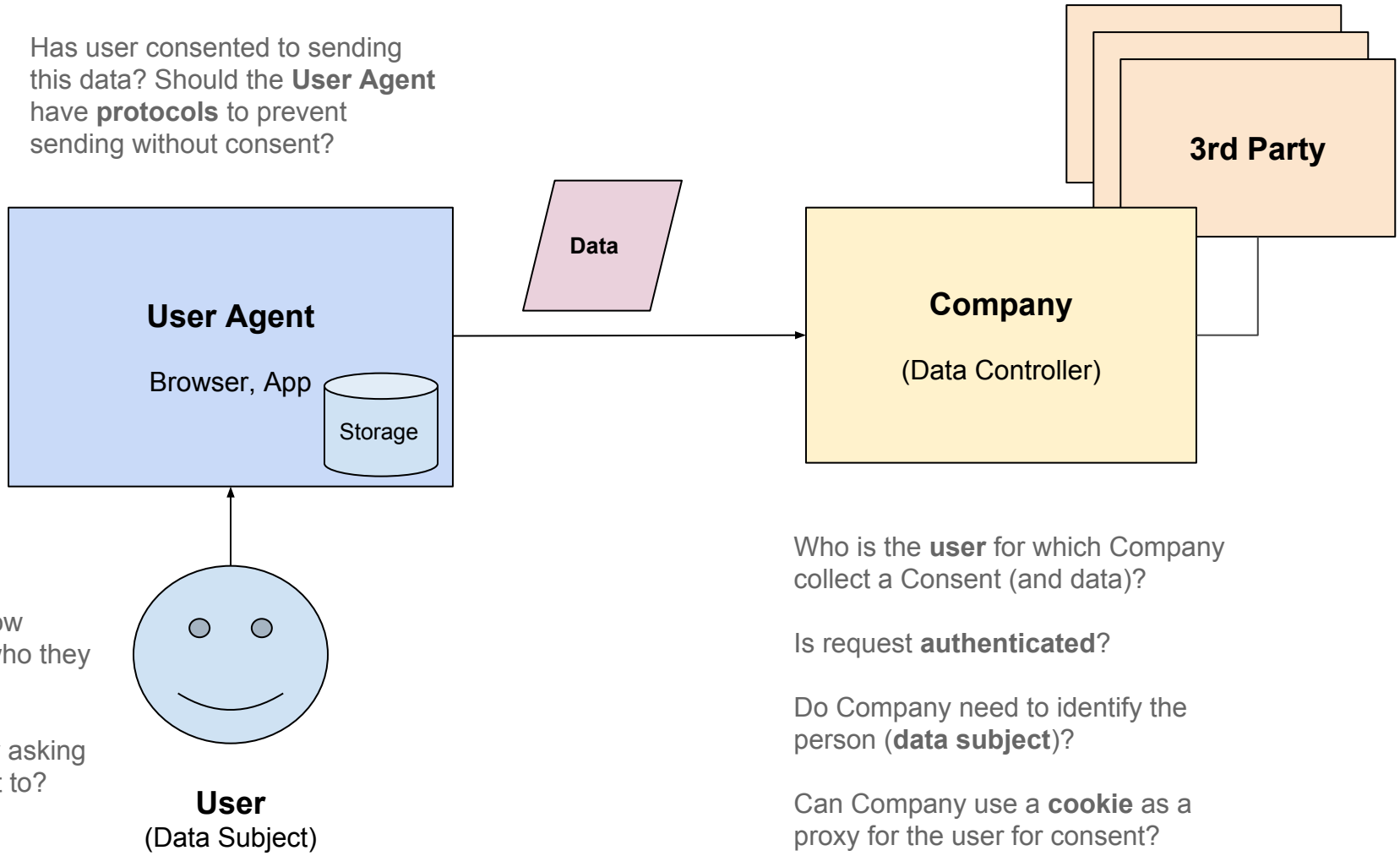
- **Documentation** of consent is needed for audit by DPA, certification bodies, authorities.

SCENARIO


Has user consented to sending this data?
Data
Company
(Data Controller)
User
(Data Subject)

SCENARIO: MORE DETAIL

Has user consented to sending this data? Should the **User Agent** have **protocols** to prevent sending without consent?



How can I know Company is who they say they are?

What are they asking me to consent to?

Who is the **user** for which Company collect a Consent (and data)?

Is request **authenticated**?

Do Company need to identify the person (**data subject**)?

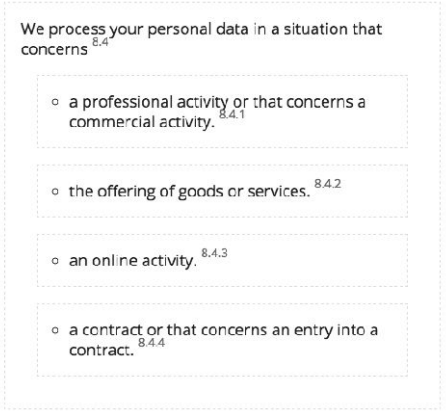
Can Company use a **cookie** as a proxy for the user for consent?

DOCUMENTING CONSENT

Who is the user?

Who is the data controller?

What is consented to and **when**?



Tamper-proof storage of consent

WHO

Who is the **user**?

The **Data Subject** whose data is being processed.

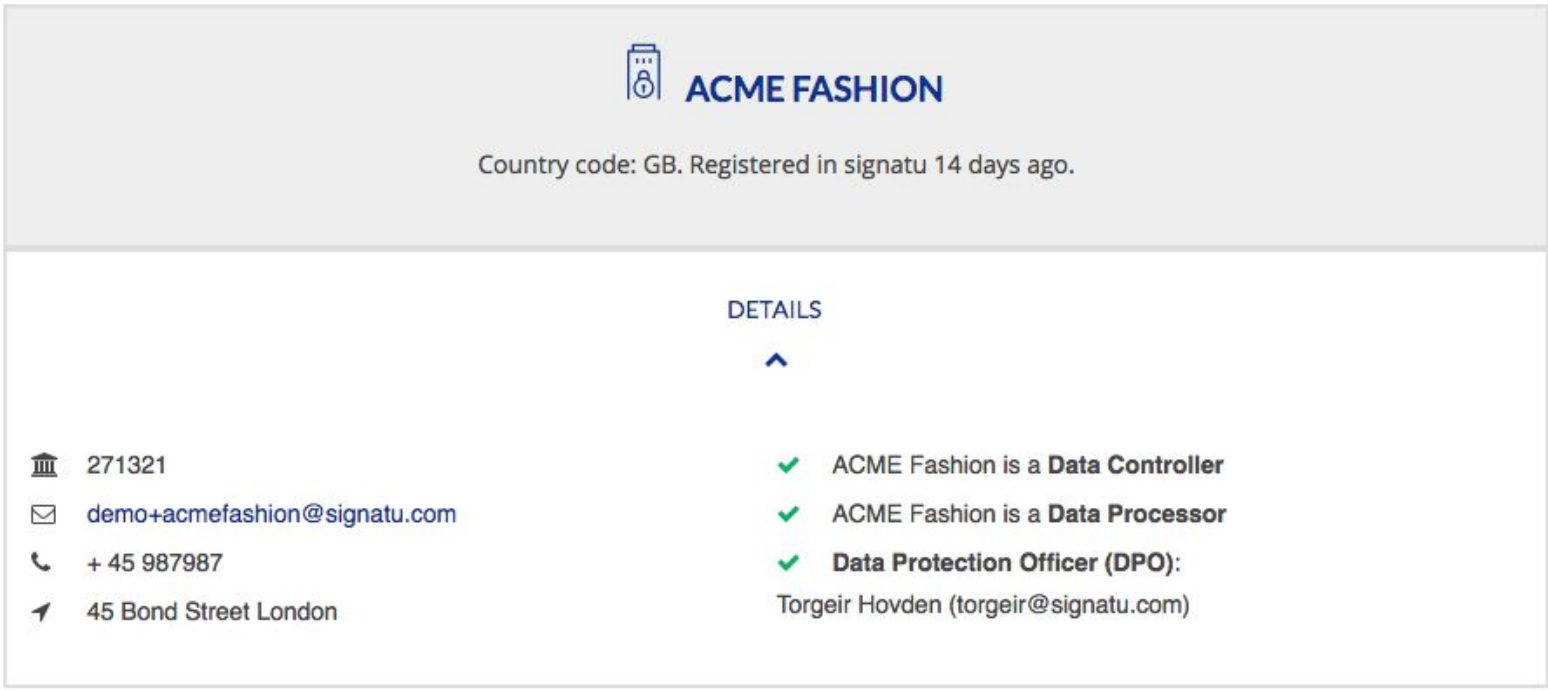
We call this the **subject principal** claim, represented by a string or URI.

Who is the **company**?

The **Data Controller**, the entity who determines the purpose of the data processing.

We call this the **issuer principal** claim, represented by a string or URI.

WHO: COMPANY



How to properly verify the **Issuer Claim** - i.e., who is the **Data Controller** and thus legally responsible?

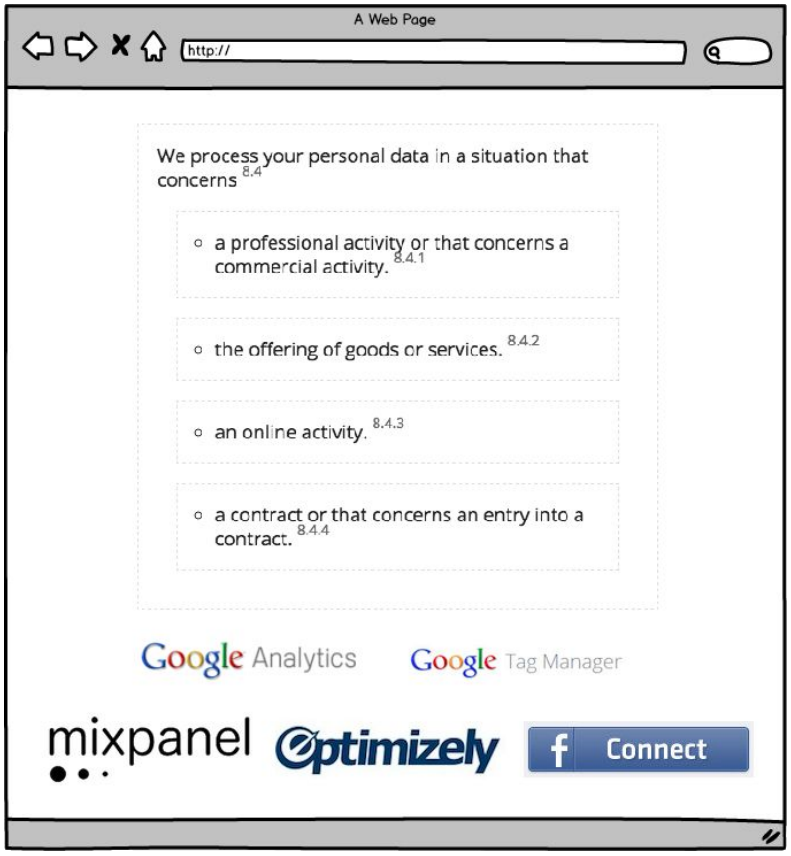
WHO: USER

Examples of User Identity Claims

User Identity Claim	Type	Claim Authenticated	Identity Verified
UIQT124RFGY	Cookie	Yes	No
Torgeir Hovden	Name / address	No	No
torgeir@signatu.com	E-mail identity	No	No
torgeir@signatu.com	E-mail identity	Yes	No
torgeir@gmail.com	E-mail identity	Yes, Google Login	Maybe
25127112345	Personal ID Number	Yes, BankID	Yes

WHAT: SCOPE OF CONSENT

granularity



Privacy Policy

WHY WE PROCESS DATA [1]

We collect e-mail in EU for the purposes of marketing. [1.1]

Specific purpose

Privacy by Design

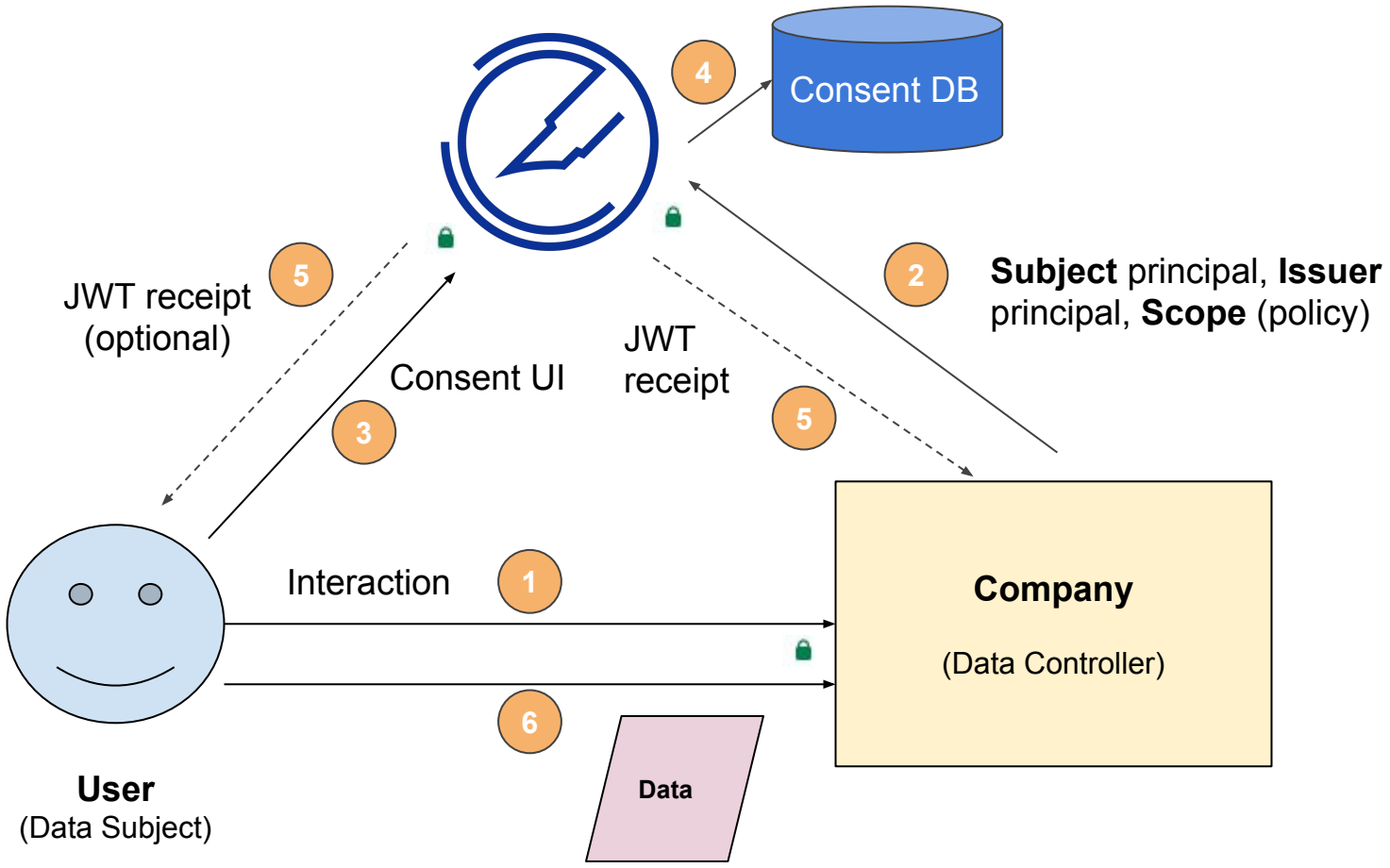
WHAT: SCOPE OF CONSENT

- Consent scope
  - Represented by URI or string
- Consent scope must be **immutable** or contain a **verifiable signature** (e.g., ETags)

REALLY? PROVE IT!

- Key claims are **issuer** principal (iss), **subject** principal (sub), and **scope** (e.g., Privacy Policy)
- Signed **JWT token** (RFC 7519) with **claims** as a Consent Receipt
- Signatu stores the consent and the receipt

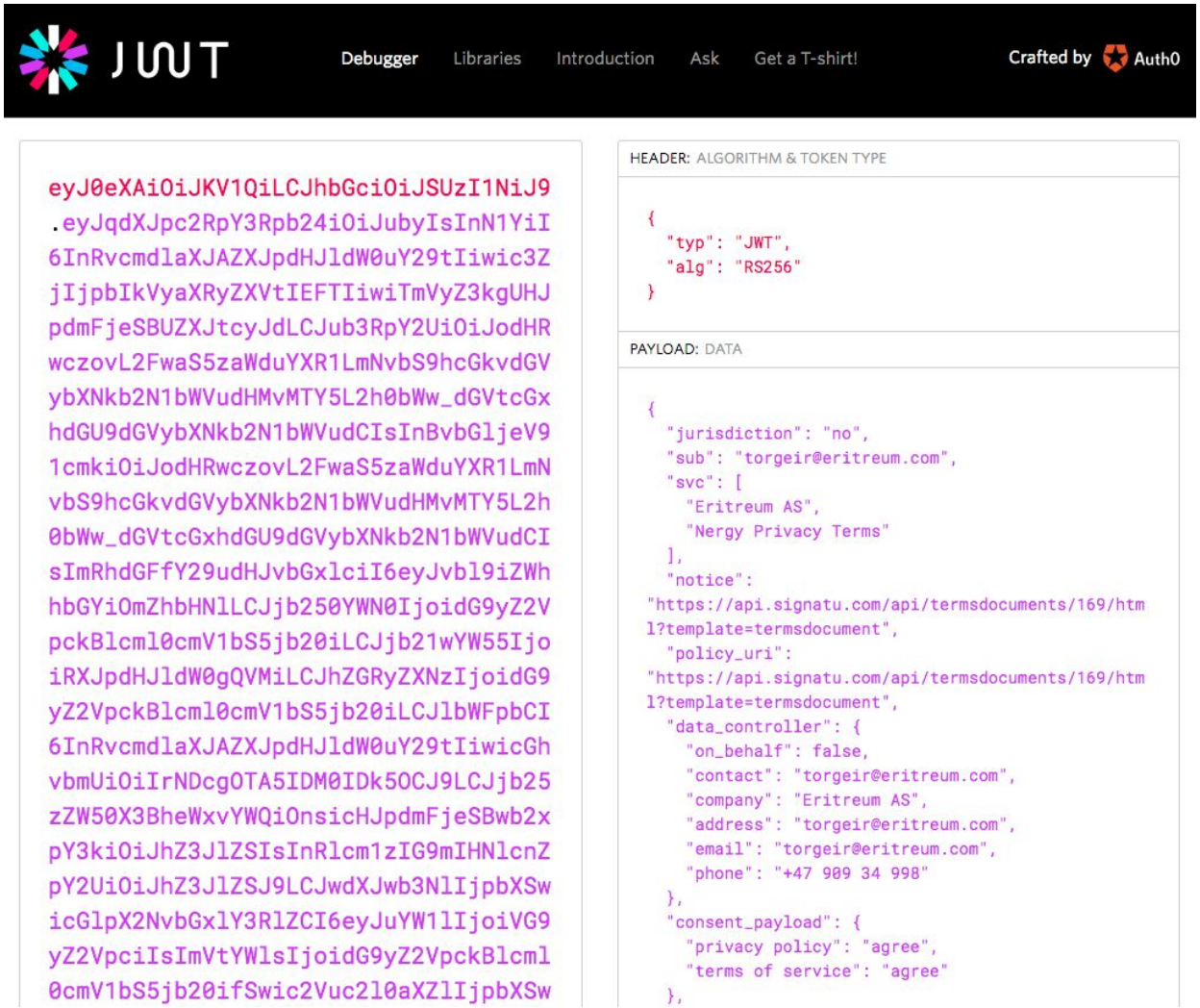
CONSENT USING SIGNATU



Signed JWT Token

```
> curl https://api.signatu.com/api/termsdocuments/169/ consents/219
[...]
"receipt":"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.eyJqdXJpc2RpY3Rpb24iOiJubyIsInN1YiI6I
nRvcmdlaXJAZXJpdHJldW0uY29tIiwic3ZjIjpbIkVyaXRyZXVtIEFTIiwiTmVyZ3kgUHJpdmFjeSBUZXJtcy
JdLCJub3RpY2UiOiJodHRwczovL2FwaS5zaWduYXR1LmNvbS9hcGkvdGVybXNkb2N1bWVudHMvMTY5L2h0bWw
_dGVtcGxhdGU9dGVybXNkb2N1bWVudCIsInBvbGljeV91cmkiOiJodHRwczovL2FwaS5zaWduYXR1LmNvbS9h
cGkvdGVybXNkb2N1bWVudHMvMTY5L2h0bWw_dGVtcGxhdGU9dGVybXNkb2N1bWVudCIsImRhdGFfY29udHJvb
GxlciI6eyJvbl9iZWhhbGYiOmZhbHNlLCJjb250YWN0IjoidG9yZ2VpckBlcml0cmV1bS5jb20iLCJjb21wYW
55IjoiRXJpdHJldW0gQVMiLCJhZGRyZXNzIjoidG9yZ2VpckBlcml0cmV1bS5jb20iLCJlbWFpbCI6InRvcmd
laXJAZXJpdHJldW0uY29tIiwicGhvbmUiOiIrNDcgOTA5IDM0IDk5OCJ9LCJjb25zZW50X3BheWxvYWQiOnsi
cHJpdmFjeSBwb2xpY3kiOiJhZ3JlZSIsInRlcm1zIG9mIHNlcnZpY2UiOiJhZ3JlZSJ9LCJwdXJwb3NlIjpbX
SwicGlpX2NvbGxlY3RlZCI6eyJuYW1lIjoiVG9yZ2VpciIsImVtYWlsIjoidG9yZ2VpckBlcml0cmV1bS5jb2
0ifSwic2Vuc2l0aXZlIjpbXSwic2hhcmluZyI6W10sImNvbnRleHQiOlsiYWN0aXZlIHByaXZhY3kgcG9saWN
5IGNvbnNlbnQiXSwiYXVkIjoiIiwic2NvcGVzIjoiIiwic2lnbmF0dV90b2tlbiI6IkJIU0ZOQyIsInNpZ25h
dHVfcHVia2V5IjoiaHR0cHM6Ly9hcGkuc2lnbmF0dS5jb20vc3RhdGljL3NpZ25hdHUtand0LnB1YiIsImlzc
yI6Imh0dHBzOi8vYXBpLnNpZ25hdHUuY29tIiwianRpIjoiQkhTRk5DIiwiaWF0IjoxNDY0NzgzNTEzfQ.VrC
F3mOOjV97MYM4WH6nKhXYYqZQ6AMmQLBWnEF31A7nlXKeqGllRJaSag1tFWJoB1ylizGaGWIMcMVTPLQDSF6I
JWubQR3ohG83ujKiIEHXe9ScZ95ekC8TOBl12KiqoAWamSVY38Jev-CLzdGUagxQpQMr4hso0prK7VxFwOsX8
xwL-2Nr_C1rKvj9K0M-zOAcB-ZRsmJDOIV5G-bPXms88-SDiIDr932TYOA_IRZk9VPABSFGJMseaX0skpp-f5
ckIBdbkG4KktL8YPfGZK5EUDPdcr147z03XLRAZrBVQ8adxfZk78KNDYEoIv0WdIoK4w1M56VPuBnyI88AYQ
```

VERIFYING THE RECEIPT



Other JWT as Consent Receipts

kantara INITIATIVE™

"The Kantara Consent Receipt Specification is for proof of consent, and uses signed JWT tokens and a common format for creating a consent record."

Currently tested by **MyData Finland** Gov project and as a **Digital Catapult** project in UK.

SIGNATU

SIGNATU AS

Proudly from Oslo, Norway

Org. No: 915 331 661 Foretaksregisteret

hello@signatu.com

@signatucom