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

User  (Data Subject)

Data

Has user consented to sending this data?

Company  
(Data Controller)
Has user consented to sending this data? Should the **User Agent** have **protocols** to prevent sending without consent?

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?

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

What are they asking me to consent to?
Who is the user?

Who is the data controller?

What is consented to and when?

Tamper-proof storage of consent
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.
ACME FASHION

Country code: GB. Registered in signatu 14 days ago.

**DETAILS**

- 271321
- demo+acmefashion@signatu.com
- + 45 987987
- 45 Bond Street London

- ACME Fashion is a **Data Controller**
- ACME Fashion is a **Data Processor**
- Data Protection Officer (DPO):
  Torgeir Hovden (torgeir@signatu.com)

How to properly verify the **Issuer Claim** - i.e., who is the **Data Controller** and thus legally responsible?
## Examples of User Identity Claims

<table>
<thead>
<tr>
<th>User Identity Claim</th>
<th>Type</th>
<th>Claim Authenticated</th>
<th>Identity Verified</th>
</tr>
</thead>
<tbody>
<tr>
<td>UIQT124RFGY</td>
<td>Cookie</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Torgeir Hovden</td>
<td>Name / address</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><a href="mailto:torgeir@signatu.com">torgeir@signatu.com</a></td>
<td>E-mail identity</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td><a href="mailto:torgeir@signatu.com">torgeir@signatu.com</a></td>
<td>E-mail identity</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td><a href="mailto:torgeir@gmail.com">torgeir@gmail.com</a></td>
<td>E-mail identity</td>
<td>Yes, Google Login</td>
<td>Maybe</td>
</tr>
<tr>
<td>25127112345</td>
<td>Personal ID Number</td>
<td>Yes, BankID</td>
<td>Yes</td>
</tr>
</tbody>
</table>
WHAT: SCOPE OF CONSENT

WHY WE PROCESS DATA

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

User (Data Subject)

Company (Data Controller)

Consent UI

JWT receipt

JWT receipt (optional)

Subject principal, Issuer principal, Scope (policy)

Consent DB

Data

Interaction

1

2

3

4

5

6
Signed JWT Token

> curl https://api.signatu.com/api/termsdocuments/169/ consents

[...]
**VERIFYING THE RECEIPT**

```
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiJ9.
eyJqdXJpc3RyZXRlVXNlcmNlciIsImlkIjoiNiJ9
6InRvcmdlciJXAJJXJpdHJld29tIiwic3ZjIjpjbiKxYxZXRiIw13MTY3KgUHJ
pdmFjeSBUZXJtcyJdLCJub3RyYWwiOiJodHRwczovL2FwaS5zaWduYXR1LmVsbG9vcGVydGVybXNkb2N1bWVudHMvMTY5L2h0bWw_dGVtcGxhdGU9dGVybXNkb2N1bWVudCIiLCBvbytOGljev9
7cmkiOiJodHRwczovL2FwaS5zaWduYXR1LmVsbG9vcGVydGVybXNkb2N1bWVudCIiLCBvbytOGljev9
31
```
Other JWT as Consent Receipts

"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 AS
Proudly from Oslo, Norway
Org. No: 915 331 661 Foretaksregisteret

hello@signatu.com
@signatu.com