Fixing healthcare data exchange with decentralized FOSS

Protect your API's with a decentralized trust layer

Steven van der Vegt
Open standard to enable safe and correct exchange of healthcare data.
Goal

Create a (inter)national network of connected nodes, to enable frictionless healthcare data exchange with the patient in control.

Breaking down the silos, enabling innovation, empowering care professions and patients.
Fixing healthcare data exchange with decentralized FOSS

- What is healthcare data exchange?
- Why is it broken?
- Why fix it with decentralized FOSS?
Medical data

- Medical files
- Lab results
- Electronic health records
- Images
Exchange

- Hospitals
- Mental healthcare institutions
- General practitioner
- Home care nurse
- Patient
• Lots of small networks around a disease, financial flow, between vendors, regions etc.

• It is difficult to do it correct

• Standards are very broad but also incomplete
EHR API's

2way TLS over Internet

HomeCare
No medical data over the Nuts network, all p2p
Everything is encrypted
Data only exchanged with relevant parties
What is Nuts?

Nuts is a toolbox to secure all conditions needed for safe (medical) data exchange

1. Who is knocking (identity)
2. Where to knock (discovery / registry)
3. Is patient OK? (consent, legal basis)
4. What happened? (Logging / audits)
Decentralized Identity

- I Reveal My Attributes
- Secure offline channel from trusted issuer to verifier
- Able to sign contracts
$ curl -X POST \\http://localhost:11323/api/consent \\-H 'Content-Type: application/json' \\-d '{
  {
    "type" : "PractitionerLogin",
    "language" : "EN",
    "version" : "v1",
    "legalEntity" : "Hospital East",
    "valid_from" : "2020-02-02T14:32:00+02:00",
    "valid_to" : "2020-12-24T14:32:00+02:00"
  }
}
'}
Attributes

Sign a contract

EN:PractitionerLogin:v1 I hereby give permission to {{acting_party}} to make request to the Nuts network on behalf of {{legal_entity}}. This permission is valid from {{valid_from}} until {{valid_to}}.

With the attributes: name, date of birth, medical number.
Inloggen met IRMA

Eén moment alsjeblieft
Patient consent

- Make sure there is a legal basis for the data exchange
  - Explicit consent
  - Implicit following a treatment
- Consent consists of a triple:
  - Custodian of the data
  - Actor (entity who gets the permission)
  - Patient
- Limited to medical scope, period, etc.
$ curl -X POST \
http://localhost:11323/api/consent \
-H 'Content-Type: application/json' \
-d '{
    "subject": "urn:oid:2.16.840.1.113883.2.4.6.3:99999999", 
    "custodian": "urn:oid:2.16.840.1.113883.2.4.6.1:00000000", 
    "actor": "urn:oid:2.16.840.1.113883.2.4.6.1:00000001", 
    "performer": "urn:oid:2.16.840.1.113883.2.4.6.1:00000007", 
    "records": [{
        "consentProof": {
            "ID": "1112222-2222-3333-4444-555566667777", 
            "title": "Toestemming inzage huisarts.pdf", 
            "URL": "https://some.url/path/to/reference.pdf", 
            "contentType": "application/pdf", 
            "hash": "string"
        },
        "period": {
            "start": "2019-05-20T17:02:33+10:00", 
            "end": "2019-11-20T17:02:33+10:00"
        },
        "dataClass": [ 
            "urn:oid:1.3.6.1.4.1.54851.1:MEDICAL"
        ]
    }]
}'
Distributed by Corda

- Open source distributed trust framework
- p2p ledgers
- Uses notaries for consent
- A bit enterprisey, but it does the job
Registry

- Where to find endpoints of type "Medication" for org "Hospital"?
- What's the current public key of an org "Hospital"
- Decentralized, managed by a chain of trust
Certificate tree

- Nuts root
  - Nuts CA
    - Nuts vendor CA
    - Corda root CA
      - Corda doorman CA
      - Corda network map
    - Vendor CA
      - App cert
    - Node CA
      - Corda identity cert
      - Corda notary

Foundation, offline
Foundation, online

- Issue CA to vendors
- Issue TLS Certs, Sign identity
Data retrieval

Actor

XIS Actor

Nuts node 1

Nuts node 2

XIS Custodian

View data

<<qr_code>>

<<irma_signature>>

start_session()

<<qr_code>>

query_consent()

<<consent>>

find_endpoint()

<<endpoint>>

<<Ui>>

data request

<<data>>

Security

- two-way TLS proves the identity of the vendor.
- the IRMA signature proves the identity of the user.
- a signature with the organization key proves the identity of the organization.

check_identity()

<<ack>>

check_consent()

<<ack>>
What's in the box?

• Decentralized Identity
• Registry with chain of trust
• Local development network
• Demo UI
• Consent distribution
• Event system using nats.io
Developer Happyness

- Easy JSON Rest api
- All APIs in OpenAPI spec
- Simple documentation (in English)
- Getting started guides
- Example code
- Everything is containerized using Docker
Demo time!

- Oh boy....
Status

- We pissed some people off
- Part of an advisory board for the Ministry of Public Health
- 4 Pre-production nodes
- Won a privacy award (yeah!)
You can help!

https://github.com/nuts-foundation
https://nuts-documentation.readthedocs.io/
nuts-foundation.slack.com
Q&A