BLOCKCHAIN-BASED SELF-SOVEREIGN IDENTITY IN HEALTHCARE

SYTSE OEGEMA

FATIH TURKMEN & MOHAMMED ALGHAZWI

SELF-SOVEREIGN IDENTITY

1. Existence
2. Control
3. Access
4. Transparency
5. Persistence
6. Portability
7. Interoperability
8. Consent
9. Minimalization
10. Protection

Source: Allen C. (2016) "The Path to Self-Sovereign Identity".

BLOCKCHAIN-BASED SELF-SOVEREIGN IDENTITY

1. **Existence**
2. **Control**
3. **Access**
4. **Transparency**
5. **Persistence**
6. Portability
7. Interoperability
8. **Consent**
9. Minimalization
10. Protection

Source: Quinten Stokkink and Johan Pouwelse. (2018). "Deployment of a Blockchain-Based Self-Sovereign Identity".

PROBLEM DEFINITION

Electronic Health Records

EXISTING SOLUTIONS

Covered	Not (explicitly) Covered
Basics	Partial data sharing
- user-control	Personal Annotations
- data sharing	Emergency Access
- storage	…

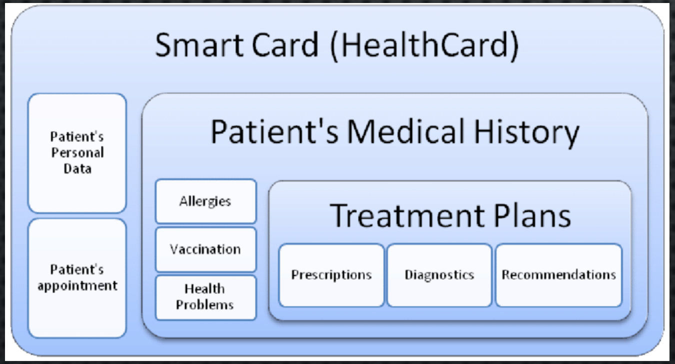
EMERGENCY ACCESS

Situations where the patient is in desperate need of medical attention

but is unable to consent to the use of its private medical data

EMERGENCY ACCESS

Offline



Smart Card (HealthCard)

Patient's Personal Data

Patient's appointment

Patient's Medical History

Allergies

Vaccination

Health Problems

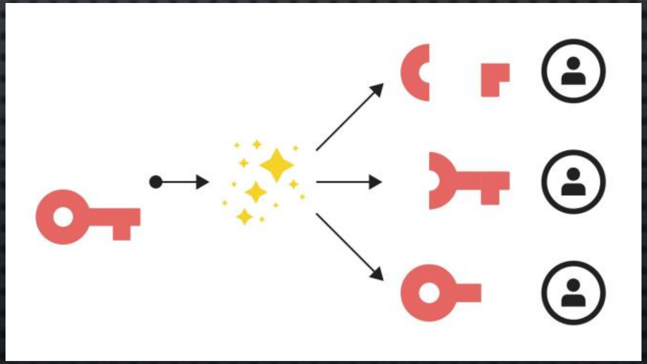
Treatment Plans

Prescriptions

Diagnostics

Recommendations

Online



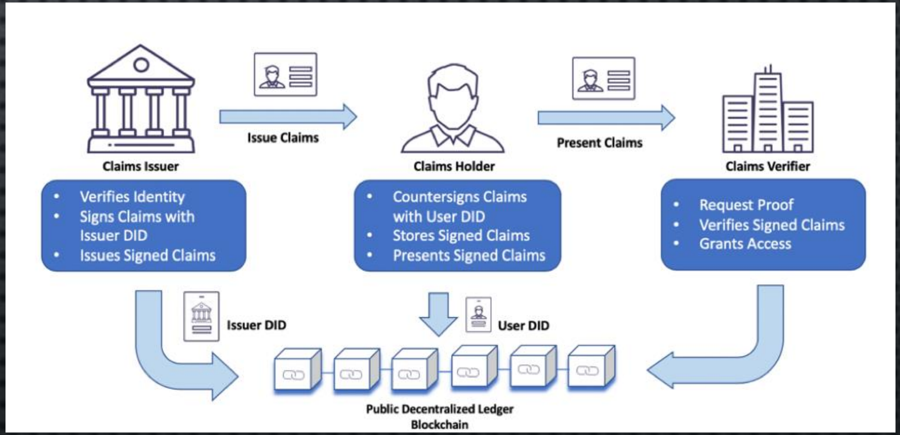
Source: Adi Shamir. (1979) "How to Share a Secret".

IMPLEMENTATION

HYPERLEDGER INDY

sovrin

identity for all



Claims Issuer
- Verifies Identity
- Signs Claims with Issuer DID
- Issues Signed Claims

Claims Holder
- Countersigns Claims with User DID
- Stores Signed Claims
- Presents Signed Claims

Claims Verifier
- Request Proof
- Verifies Signed Claims
- Grants Access

STAKEHOLDERS

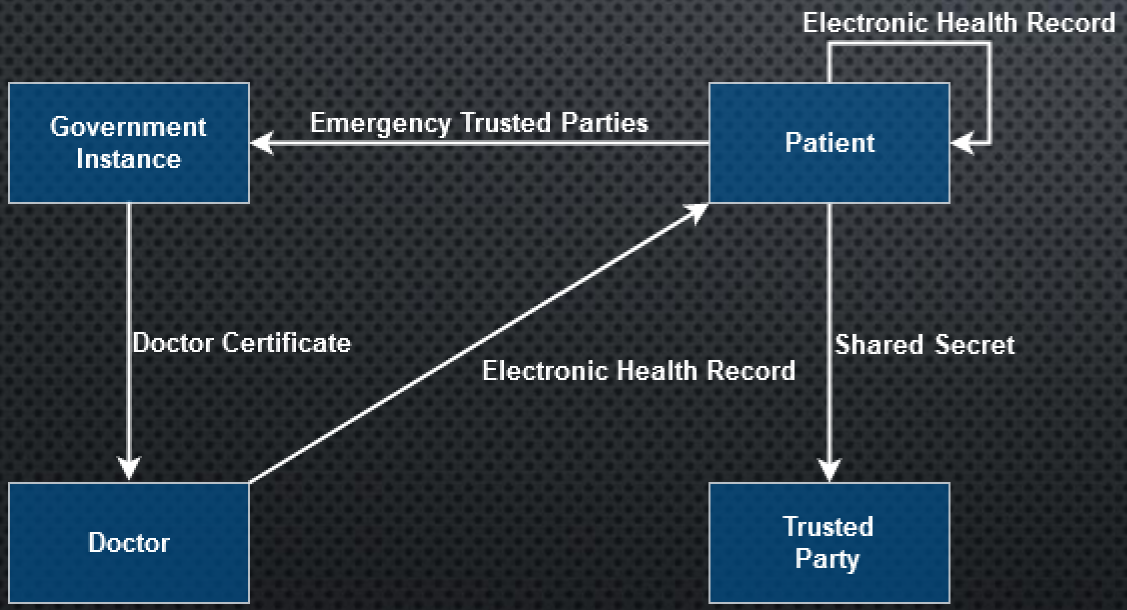
- Government Instance
- Patient
- Doctor
- Trusted Party

SCHEMAS

Created by the Government Instance

Name	Attributes			
Electronic Health Records	importance_ level	issuer	data_value	data_type
Shared Secrets	secret_owner	secret_issuer	secret	
Emergency Trusted Parties	secret_owner	secret_issuer	secret_min	secret_total
Doctor Certificate	is_emergency_doctor	name	school	

CREDENTIAL FLOW



Government Instance

Emergency Trusted Parties

Patient

Electronic Health Record

Doctor Certificate

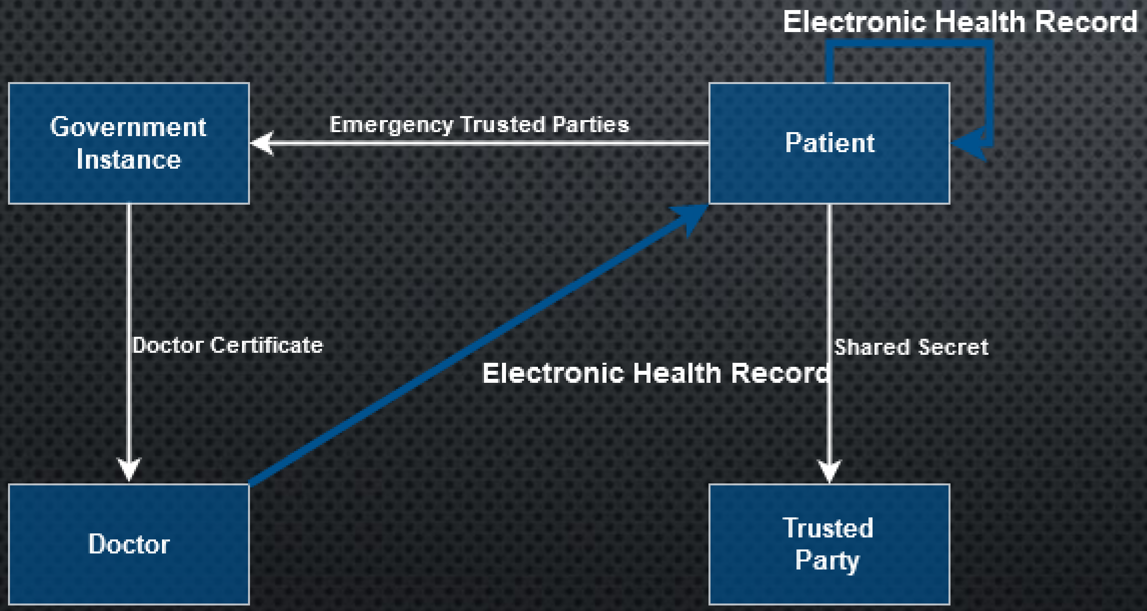
Electronic Health Record

Shared Secret

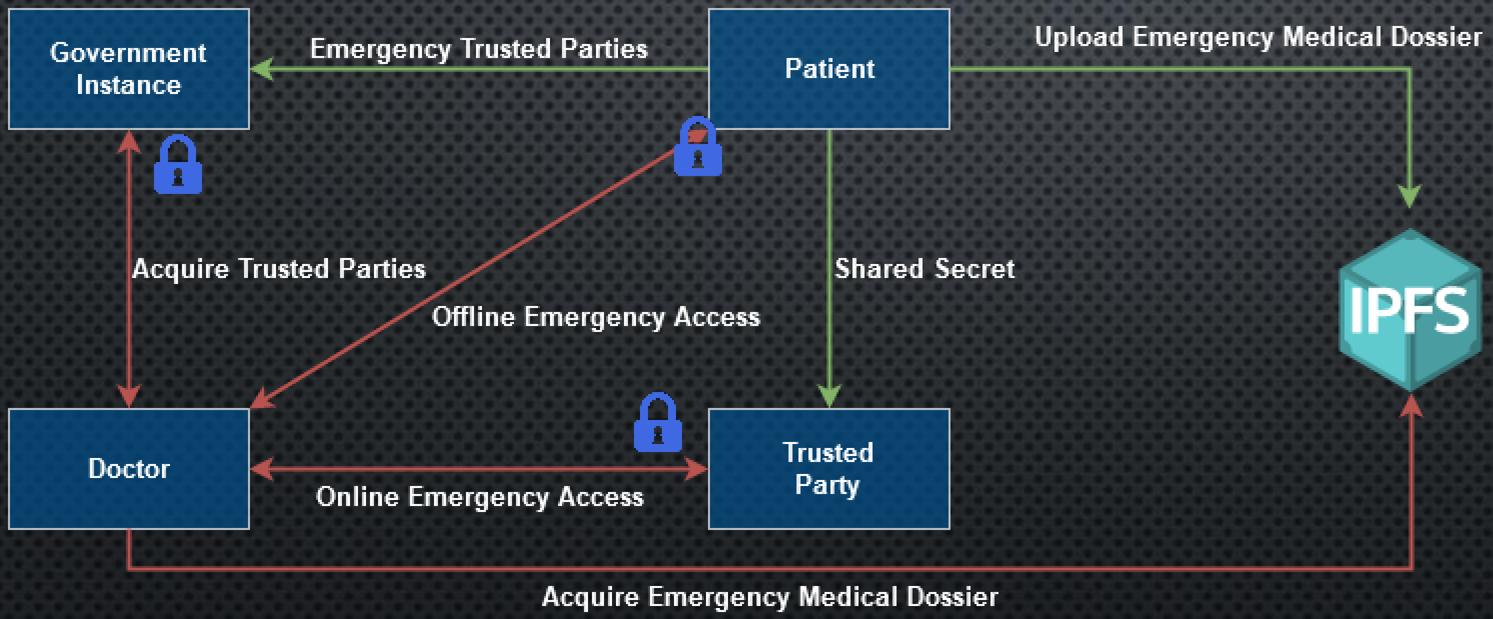
Doctor

Trusted Party

CREATION OF PERSONAL ANNOTATIONS



EMERGENCY ACCESS PROTOCOLS



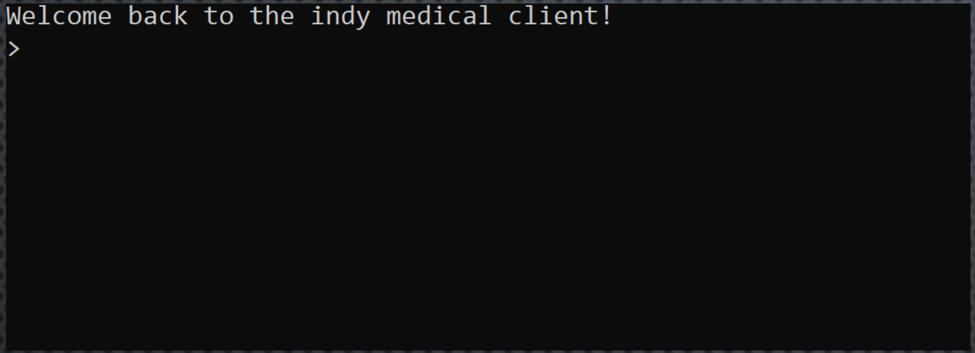
HYPERLEDGER INDY

```
"predicate1_referent": {
    "name":"is_emergency_doctor",
    "p_type":">=",
    "p_value":1,
    "restrictions": [
        {
            "cred_def_id":"NcZ4tw9KDDGnCWpG
Shk9n5:3:CL:NcZ4tw9KDDGnCWpGShk9n5:2:Doctor
-Certificate:1.0.0:TAG1“
        }
    ]
}
```

EMERGENCY DOCTOR PROOF

RESULTS

1. Existence
2. Control
3. Access
4. Transparency
5. Persistence
6. Portability
7. Interoperability
8. Consent
9. Minimalization
10. Protection



```
Welcome back to the indy medical client!
>
```

LIVE DEMO

C# CLI APPLICATION

HYPERLEDGER INDY, IPFS

Sources

- Allen C. (2016). The Path to Self-Sovereign Identity". In: Life With Alacrity.
- Quinten Stokkink and Johan Pouwelse. (2018). "Deployment of a Blockchain-Based Self-Sovereign Identity". In: 2018 IEEE International Conference on Internet of Things(iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData).
- Cataño, Néstor. (2020). "A JML-Based Strategy for Incorporating Formal Specifications into the Software Development Process Advisor".
- Asaph Azaria et al. (2016). MedRec: Using Blockchain for Medical Data Access and Permission Management". In: 2016 2nd International Conference on Open and Big Data (OBD).
- Qi Xia et al. (2017). BBDS: Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments". In: Information v8 n2 (20170417): 44.
- Tingting Chen and Sheng Zhong. (2012). Emergency Access Authorization for Personally Controlled Online Health Care Data". In: Journal of Medical Systems 36, 291-300 (2012).
- Adi Shamir. (1979) "How to Share a Secret". In: Communications of the ACM Volume 22 Number 11 (1979). url: https : / / cs . jhu . edu / ~sdoshi / crypto / papers /shamirturing.pdf (visited on 06/26/2020).
- Suveen Angraal, Harlan M. Krumholz, and Wade L. Schulz. (2017). "Blockchain Technology Applications in Health Care". In: Circ. Cardiovasc. Qual. Outcomes 2017, 10, e003800.

IMAGE SOURCES

- https://news.bitcoin.com/gem-health-blockchain-medical-mgmt/
- https://www.stratech.nl/phpthumbsup/sx/0/sy/0/sw/1280/sh/935/w/633/src/uploads/Logistiek-en-industrie/Nieuws/Blockchain.jpg
- https://www.innovationnewsnetwork.com/wp-content/uploads/2020/04/%C2%A9-iStock-elenabs-1-696x392.jpg
- https://www.researchgate.net/figure/Proposed-information-held-on-a-smart-card-for-medical-appointment-management_fig4_265080623
- https://miro.medium.com/max/2732/1*aF_ME8NUbOmPLTL04zQNA.jpeg
- https://www.idaptive.com/sites/default/files/inline-images/Rajesh%20Self%20Sovereign%20image1.png
- https://upload.wikimedia.org/wikipedia/commons/1/18/Ipfs-logo-1024-ice-text.png