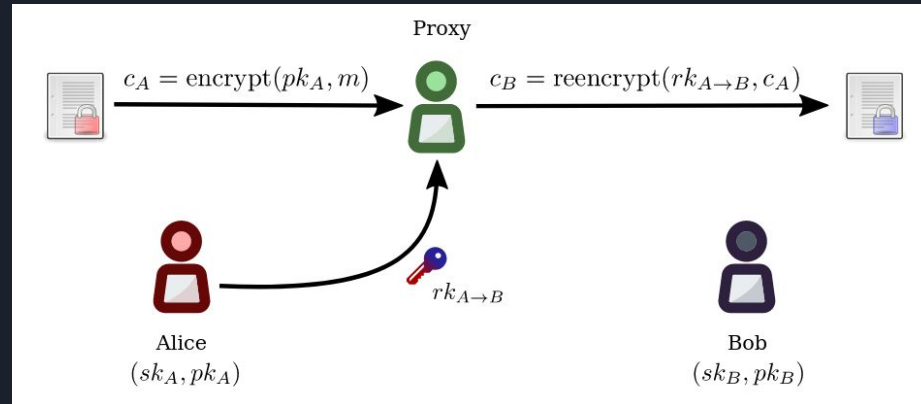# dGDP

*decentralized General Data Protection ecosystem mocked with Health Data using **NuCypher** proxy re-encryption principles*

Shane Jarvie
Abiy Seifu
Teddy Knox
Daniel Hwang

NuCypher

The NuCypher Key Management System leverages the power of proxy re-encryption to bring private data to public blockchains with a safely permissioned ecosystem.

Proxy Re-Encryption is a type of public-key encryption that allows a <u>proxy entity</u> to transform ciphertexts from one public key to another, *without learning anything about the underlying message*.

Proxy

$c_A = \text{encrypt}(pk_A, m)$ $c_B = \text{reencrypt}(rk_{A \to B}, c_A)$

$rk_{A \to B}$

Alice
(sk_A, pk_A)

Bob
(sk_B, pk_B)

Data Protections

Data privacy is not highly legislated or regulated in the United States, however the coming General Data Protection Regulations (GDPR) in the EU aim to strengthen data protection.

GDPR aims to give control of personal data back to citizens. The "Right of Erasure" illustrated by such regulation can be supported by the model we present applying **NuCypher's** implementation to a data grant/access scenario.
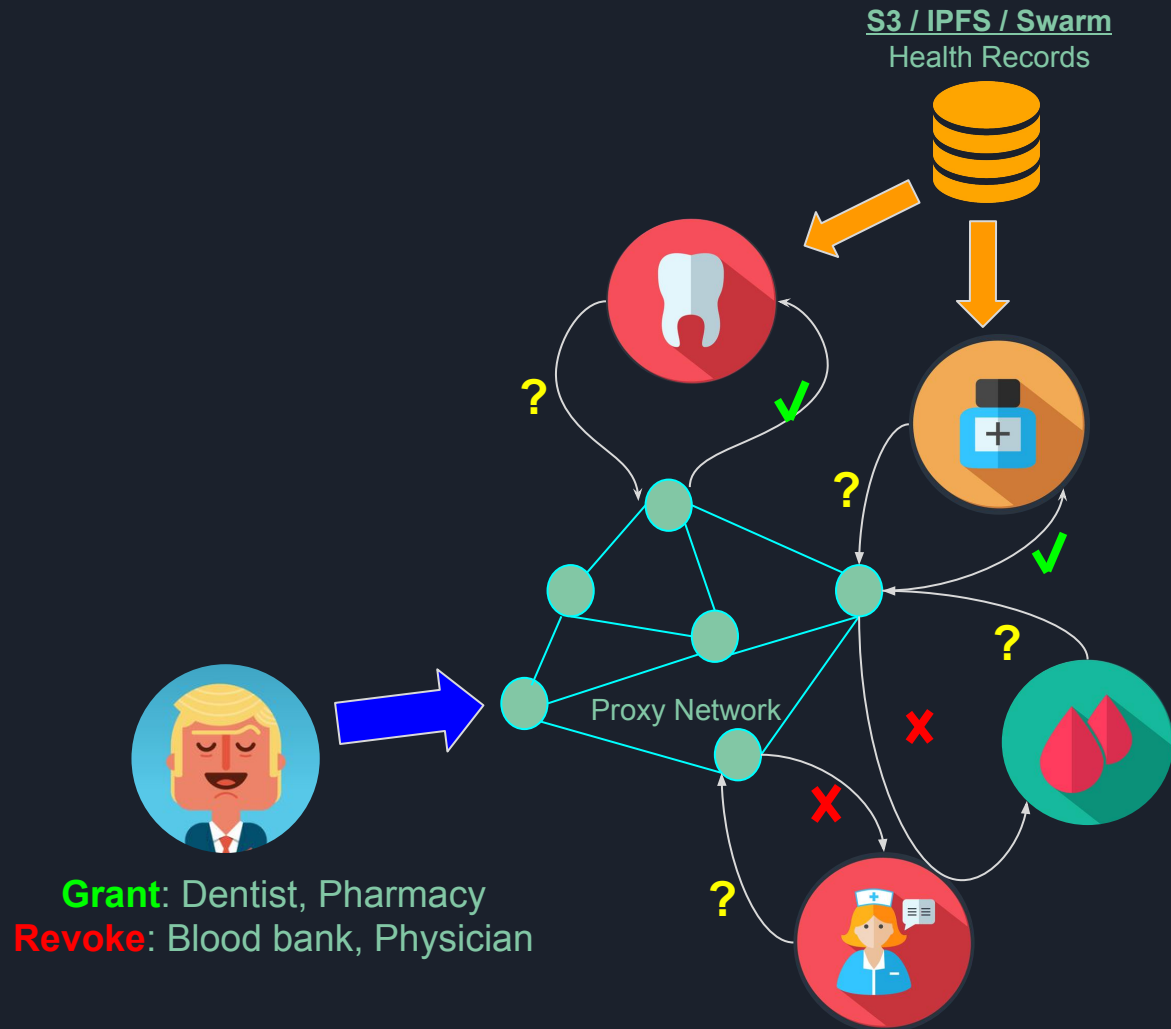
We envision an environment leveraging **NuCypher's** novel encryption and data permissions to give control of health data to patients involved with a network of health institutions.

Model

S3 / IPFS / Swarm
Health Records

Grant/Revoke Access to Specific Health Institutions

A patient can grant and revoke access permanently or temporarily to an arbitrary number of health institutions with access to data in the network. A robust token incentivization method will secure the proxy network to maintain permissions

Proxy Network

Grant: Dentist, Pharmacy
Revoke: Blood bank, Physician

Demo