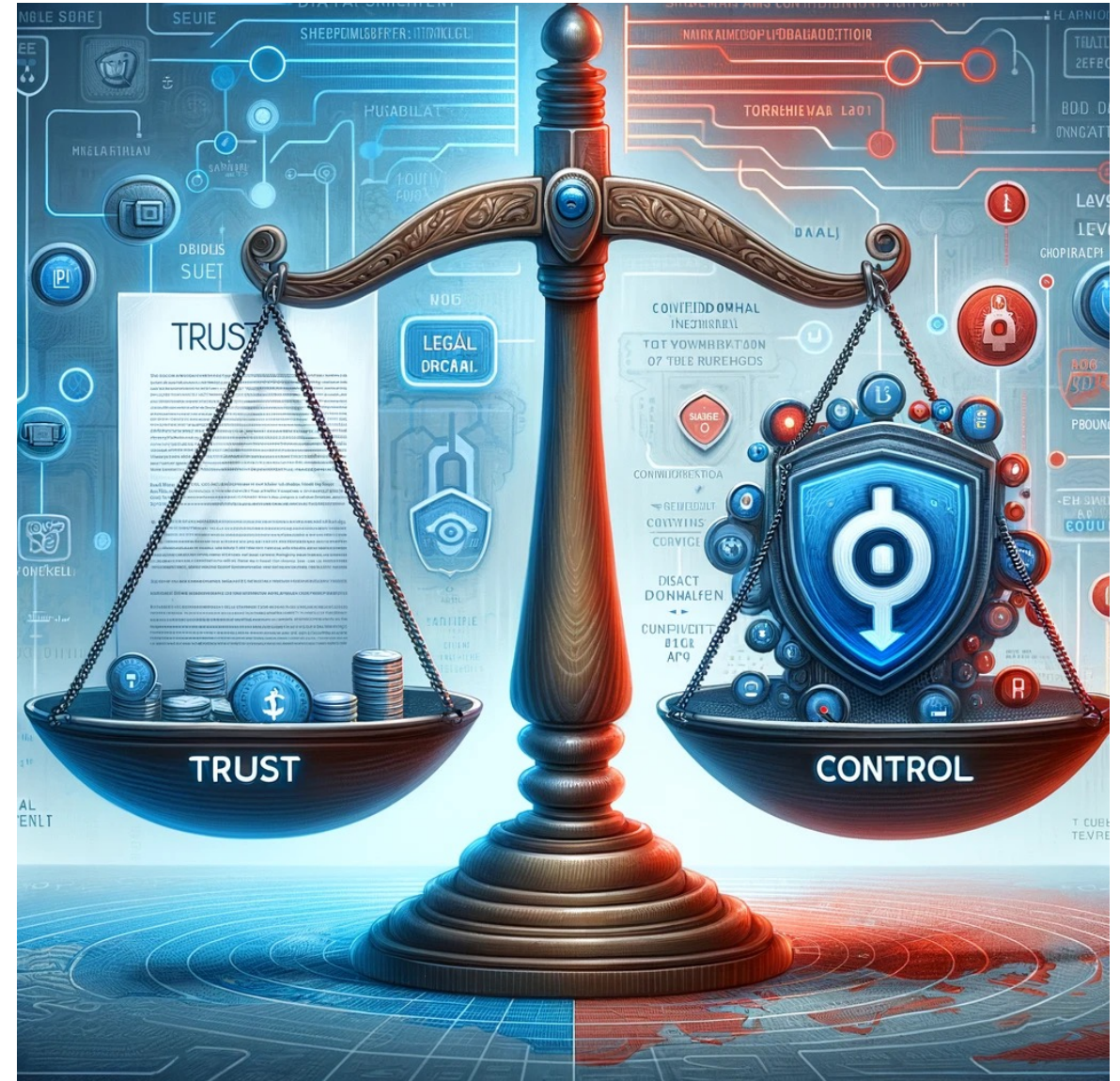


Healthy Relationships

Balancing Trust and Control when sharing confidential information





(how I feel on the inside after 10 years in the public health sector)

Steinar Noem

UDELT



Role: Consultant/advisor

Area: Digital Identity

Building a national ecosystem for sharing health information in Norway

BTW: All spelling mistakes are intentional (we invenvented the English language)

Today I will talk about

Our Journey in

making the sharing of confidential
information using `http` possible in Norway



Key take-aways from this talk (my message to you)

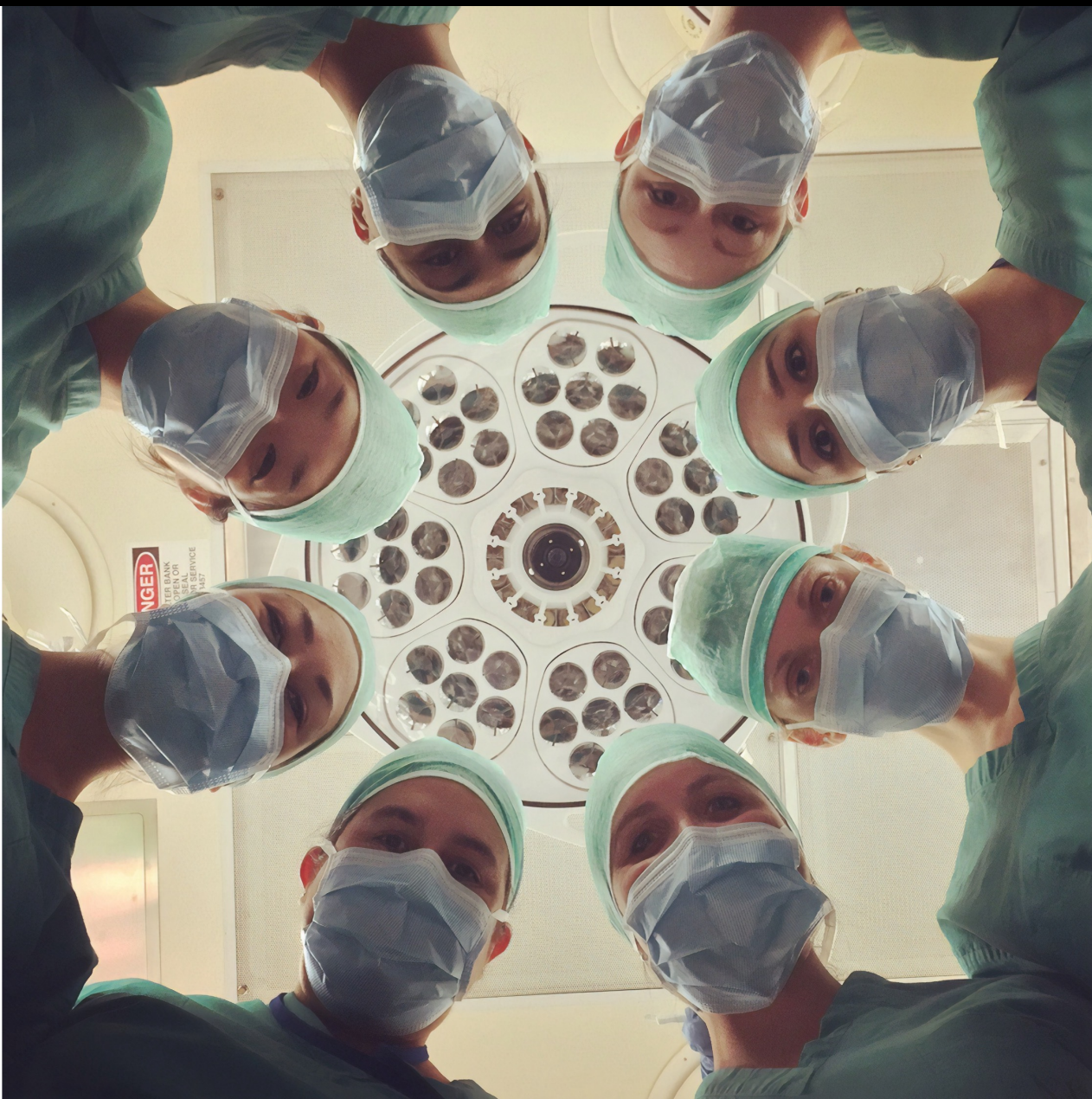
- Understand the underlying needs and requirements better – spend time on analysis before crafting solutions
- Legal requirements are shades of gray, not black/white
- We are over-complicating authorization!



The Norway

- 5,5 million inhabitants
- Geographically distributed population
- 4 health regions





A strong political motivation

- Geographical challenges (sparsely populated)
- Aging population (multi-morbidity)
- Preventing death (medication)

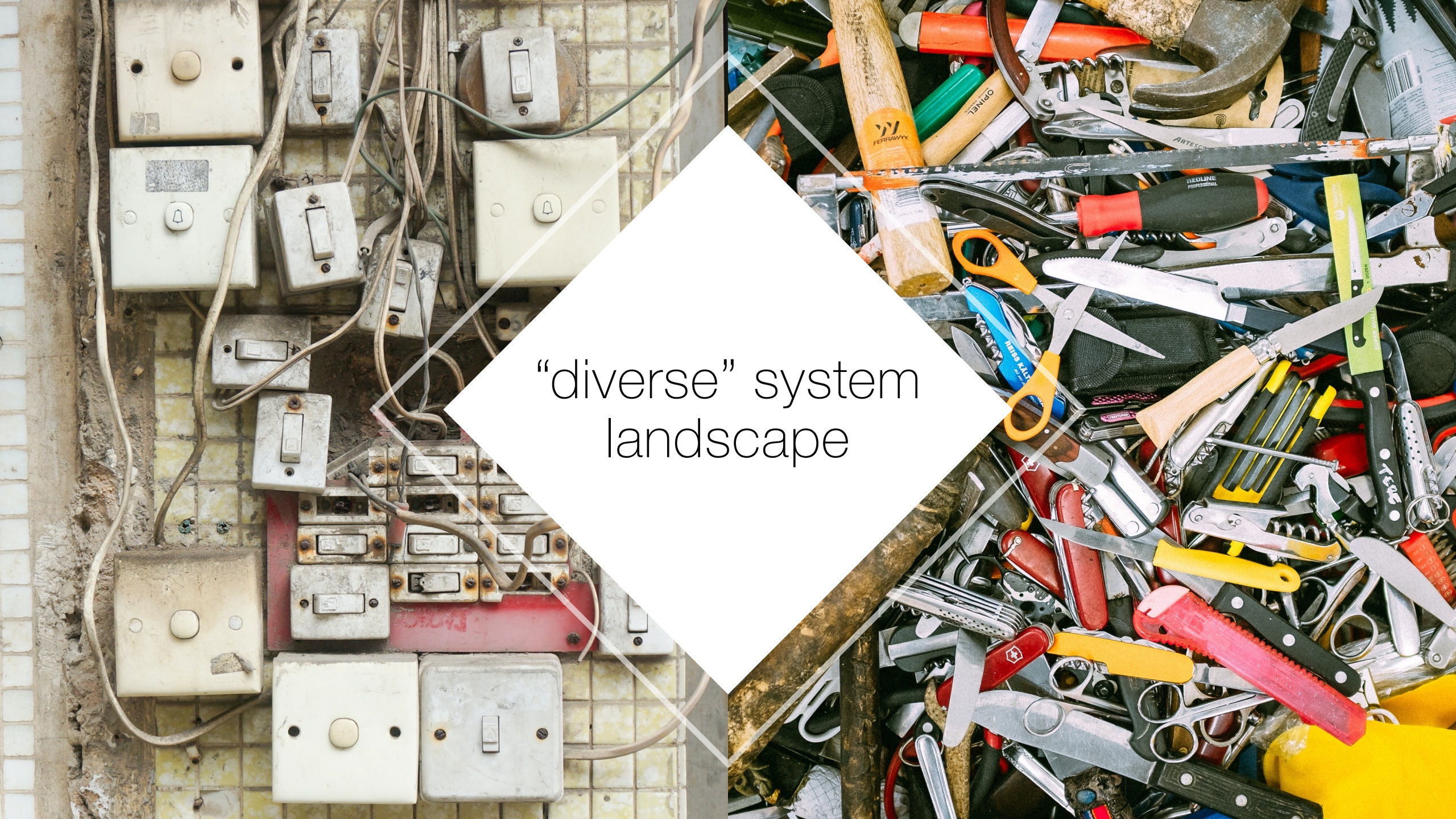
Digitalisation (not digitisation) is necessary



7000 health providers

sharing sharing health information between

500 000 health professionals



"diverse" system
landscape

Support for different data sharing patterns



Distributed data sharing



Centralized data sharing

THE CRUX... FINDING BALANCE BETWEEN

⇒ THE RIGHT TREATMENT AT THE RIGHT TIME

⇒ PREVENTING UNAUTHORIZED ACCESS





PRIVACY



PATIENT SAFETY



Control?

Trust?





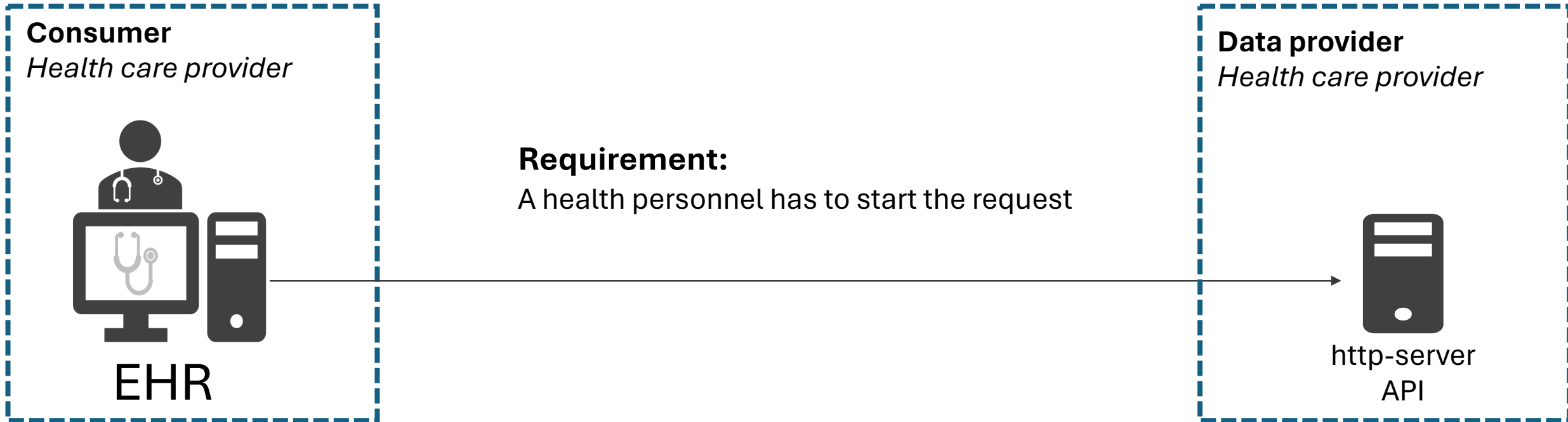
Our journey




Context

EHR software calling http-server API

The http-response message contains confidential information



Assumptions/requirements

A person's silhouette stands in a room, looking at a large, menacing shadow of a bear on the wall. A potted plant is visible on the right side of the room.

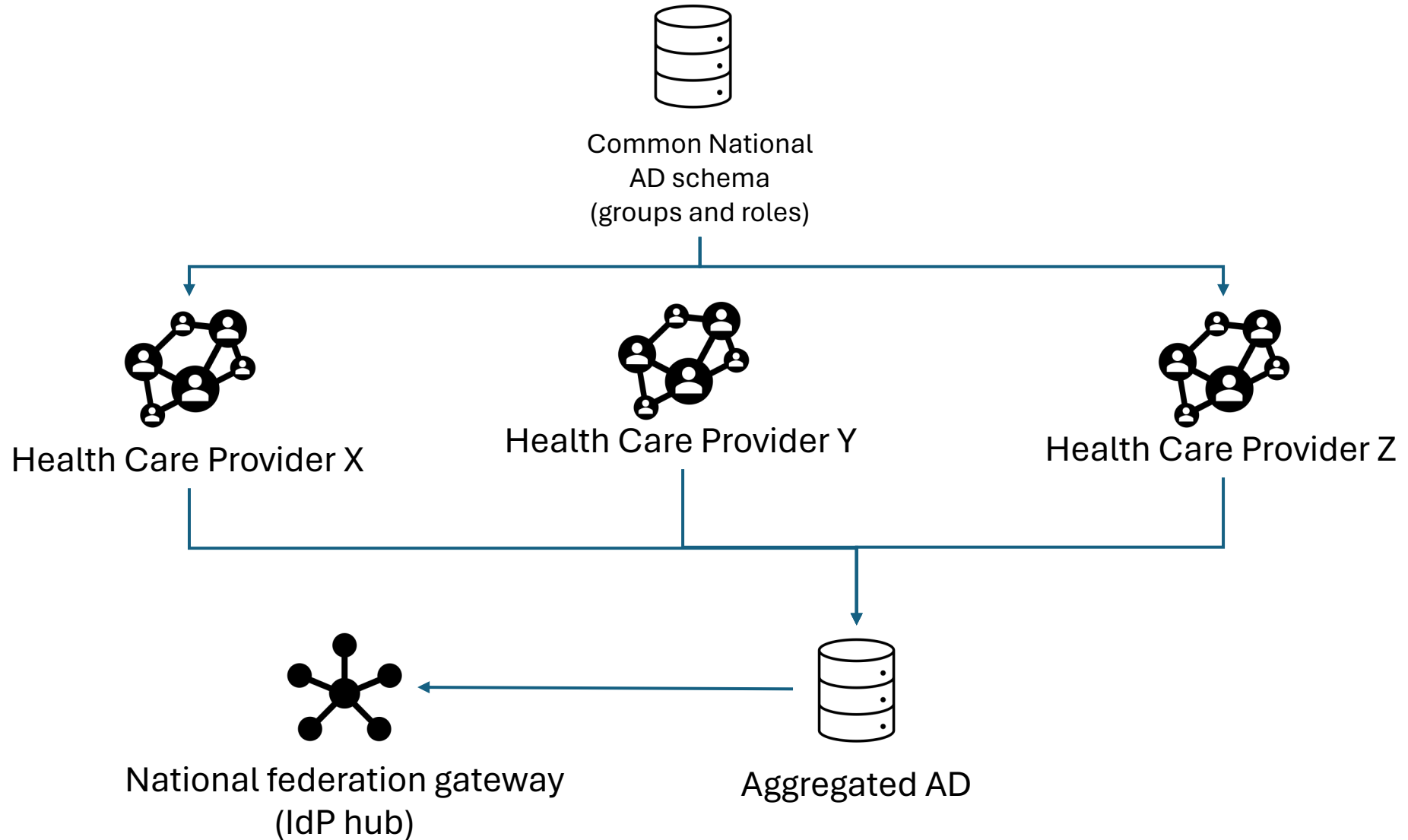
Access control for every request to an API

Authorization for the API must comply with the same rules as on the EHR

The motivation is risk (and fear)

FIRST CONCEPT: RBAC

Common National LDAP schema



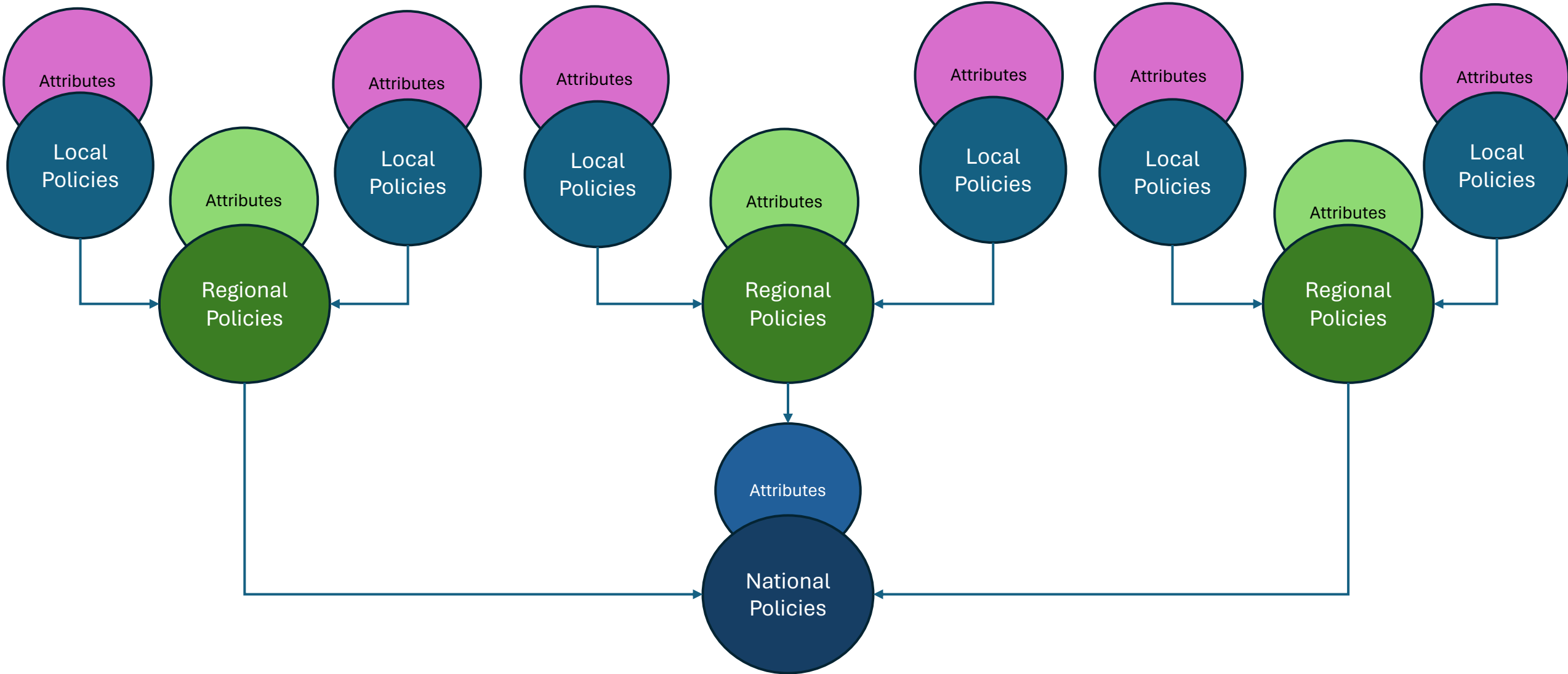
Good idea #1 vs reality

- Very different schemas in the sector
 - Different roles at different health care providers
 - No standard naming
- Too high technical complexity



SECOND CONCEPT: ABAC

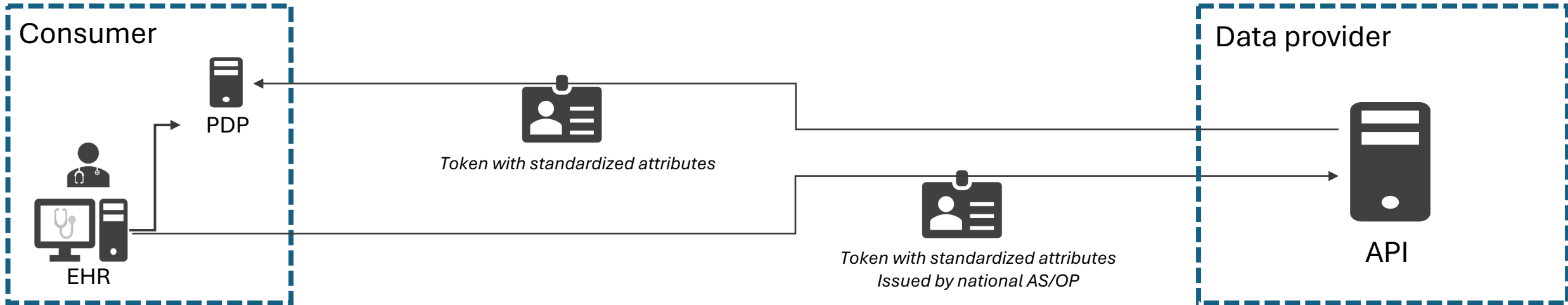
Aggregating Policies and Standardizing attributes



POSSIBLE ABAC-PATTERNS

Calling a PDP at the consumer

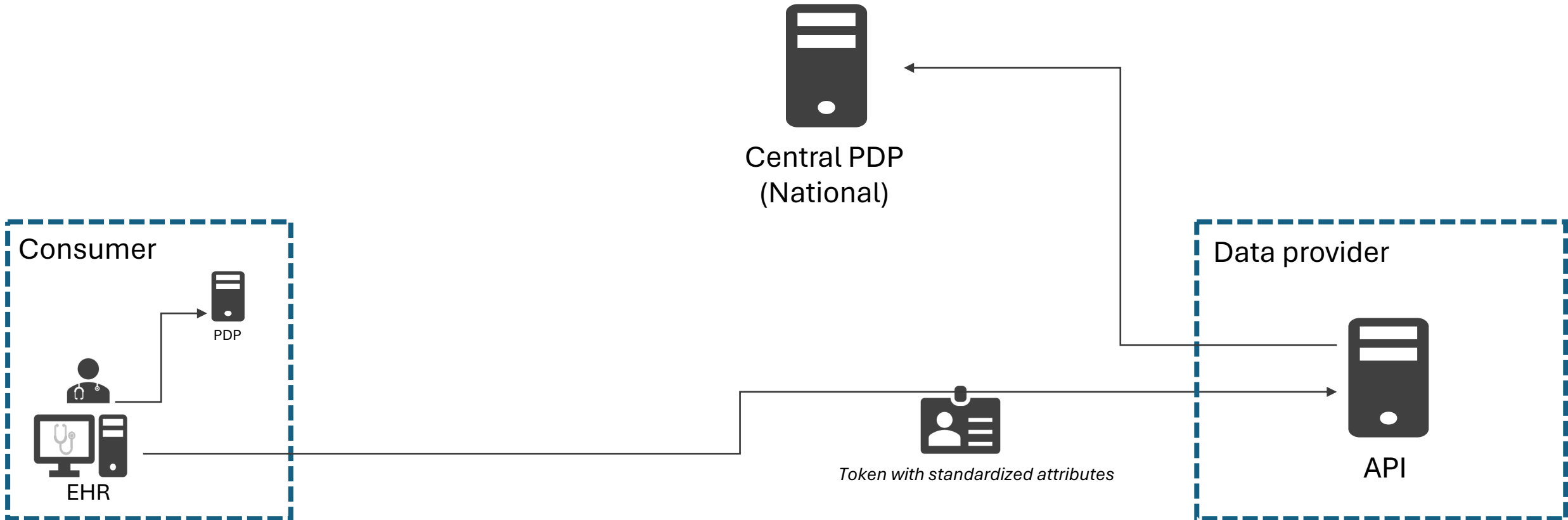
The consumer decides access



POSSIBLE ABAC-PATTERNS

Calling a centralized PDP

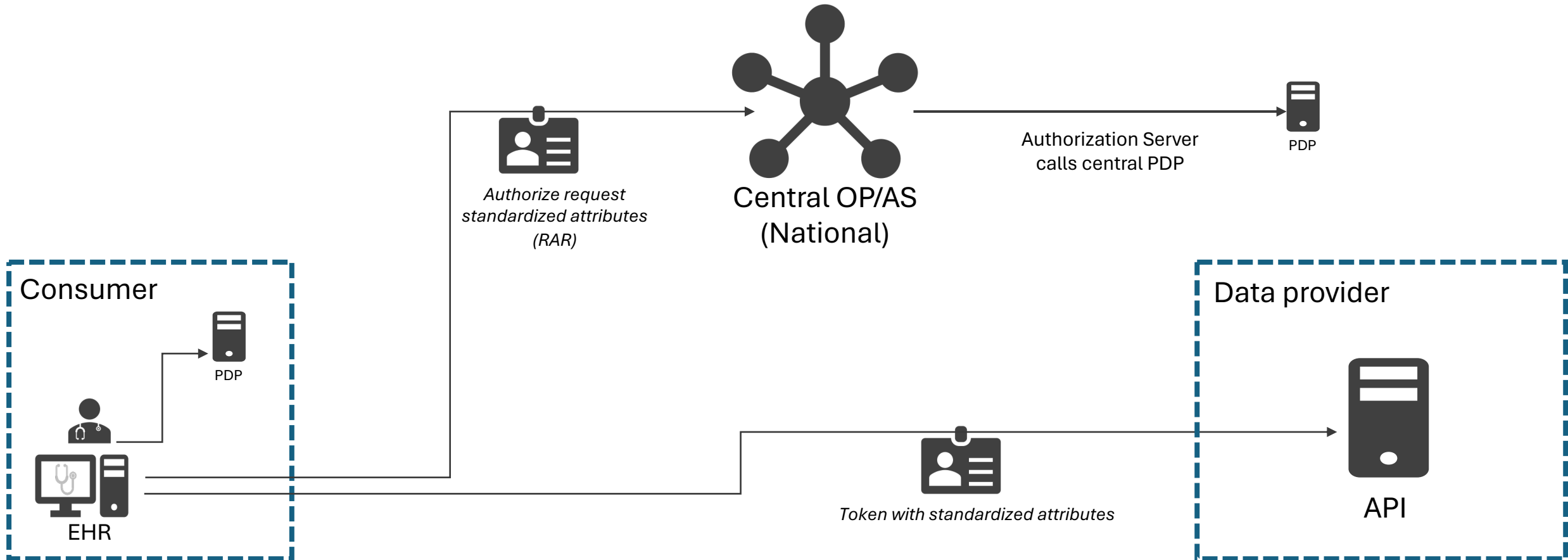
The central PDP decides access



POSSIBLE ABAC-PATTERNS

Utilizing the OAuth Authorize request

The central OP/AS calls national PDP



A surreal image featuring a man in a dark suit standing on a rocky shore, holding a large, cracked globe. The globe is tilted, and a thick stream of water is pouring out from its top. The background shows a vast, flat landscape under a bright sky with several birds flying. The overall mood is one of environmental crisis or global failure.

BUMMER..
DOOMED FOR FAILIURE?

next attempt..

FROM CONTROL TO TRUST

A “trust model” based on policies and agreements

The precondition:

- The consumer has legal basis and legitimate interest

The essence:

- The consumer authorizes the health personnel
 - Substantiates legitimate interest
- Establish a national “data sharing club” (membership)
 - Identity verification for legal entities
 - Authentication and authorization using OAuth 2.0
 - High focus on security where it makes sense (FAPI 2.0)
- Focus on accountability instead of authorization





The Norwegian *Health Network*

“The data sharing Club”

(Already existed)

Just needs to be adjusted

Central tasks of the health network

Substantiate legal basis and legitimate interest

- Is the software used by a health professional?
- Is the software used at a health institution?
- Has the health institution agreed to the terms
- Is the software used in the treatment of patients?

Accountability (non-repudiation)

- Is there a high LoA for the identities?
 - The person
 - The software
 - The legal entity

Security

- Is there a low probability that the transport is compromised?
- Is there a low probability that the protocols are compromised?
- Is there a low probability that the software is compromised?
 - Public client or confidential client?
 - E.g. Javascript client or backend

Innovations and decisions

B2B delegation

- Move away from Enterprise Certificates
- Replaced by explicit B2B delegation
 - using national authorization server
- Verification of delegation in national AS

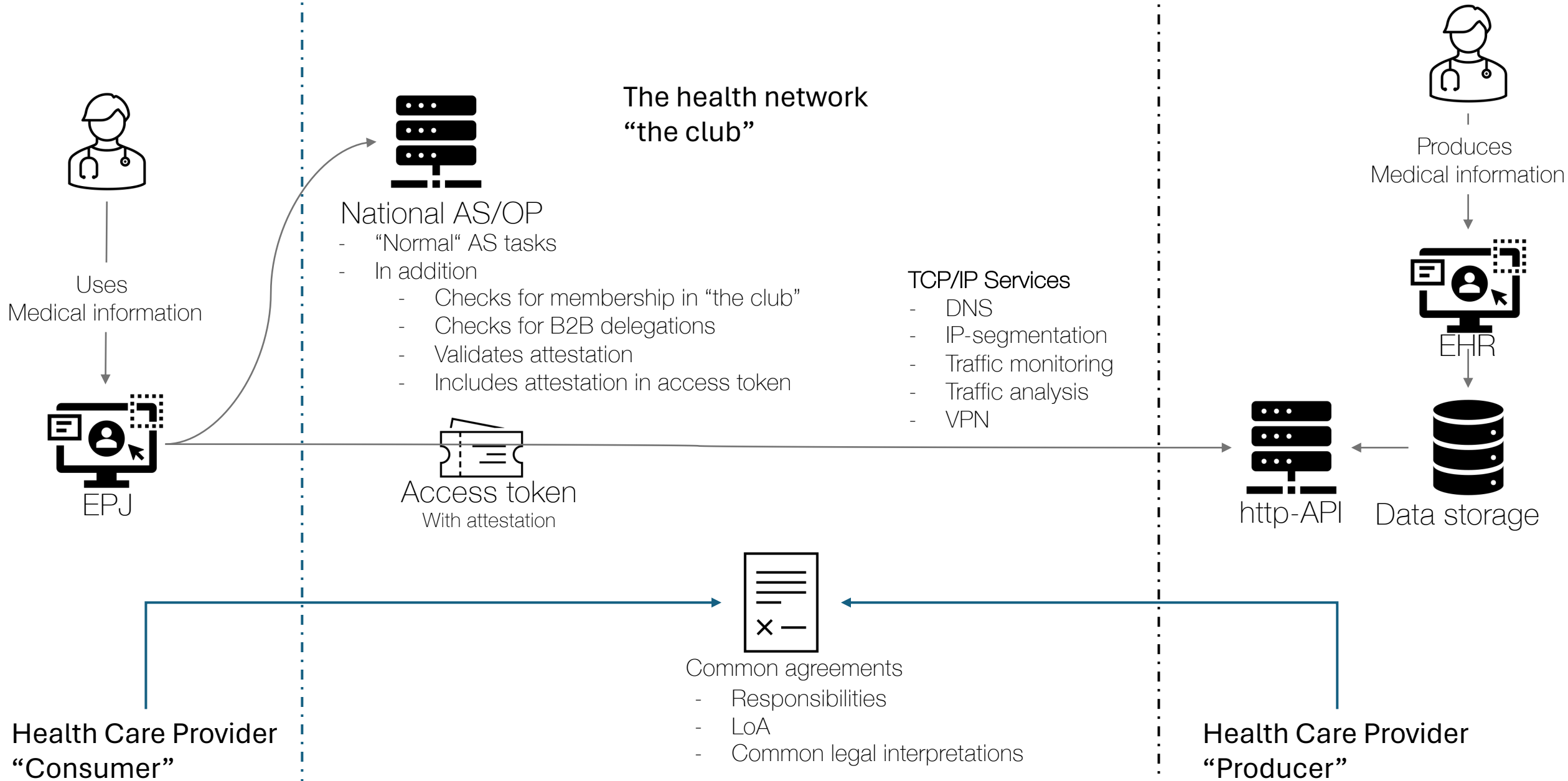
Attestation of legitimate interest

- The data consumer attests that the health personnel has a legitimate interest in the patient information
- The attestation is transferred to the national authorization server
- The attest is included in access tokens

Adopting the «latest and greatest» of protocol extensions and security

- FAPI 2.0 security profile
- OAuth 2.1

Our data sharing trust framework



WALLETS?

main learning

LEGITIMATE INTEREST CAN'T BE DEDUCED