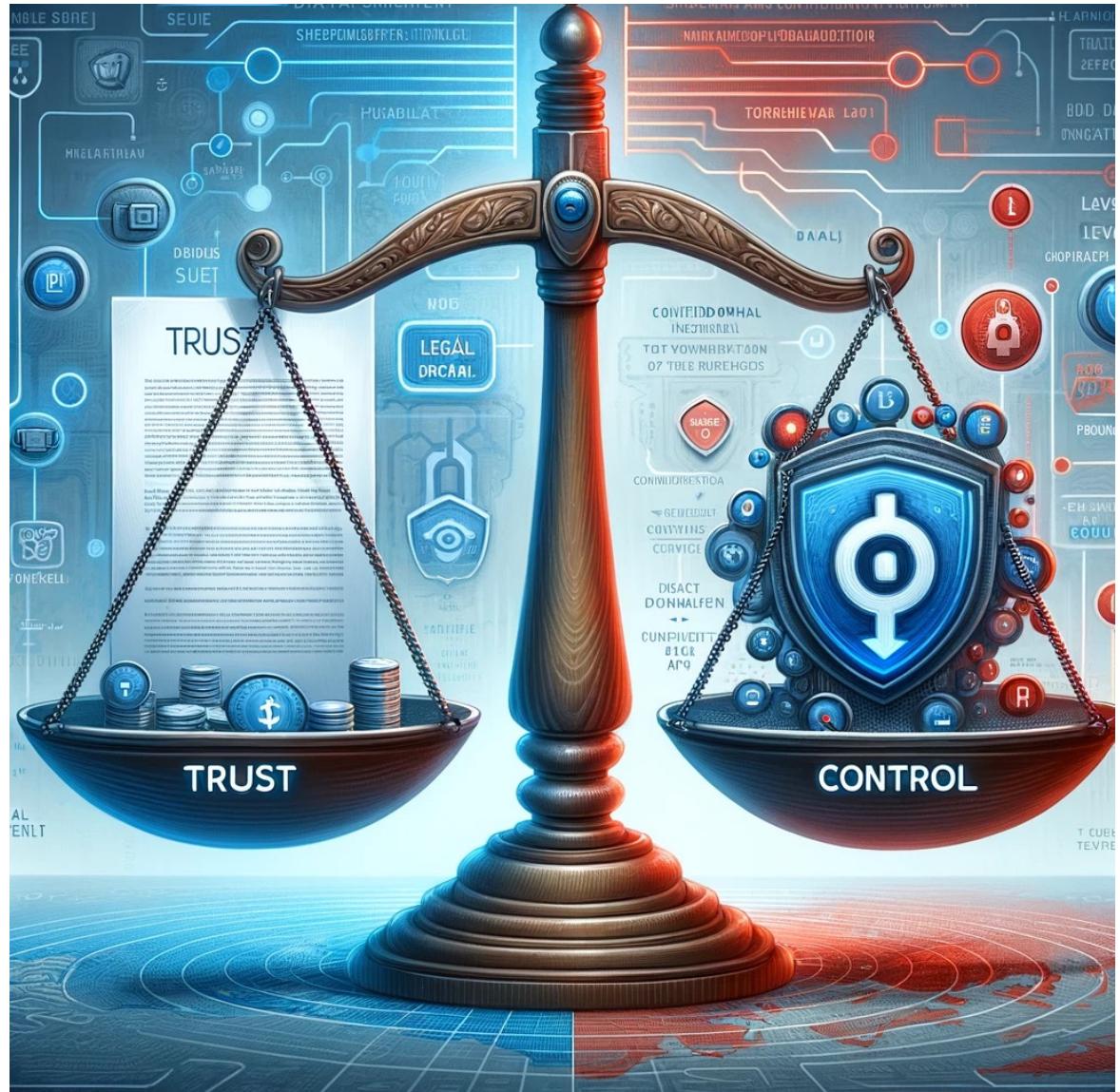


Healthy Relationships

Balancing
Trust and Control
when sharing
confidential information





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

Steinar Noem



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)

A close-up photograph of a person's hand holding a camera lens. The lens is positioned in front of a blurred background of a mountainous landscape with a body of water. The text of the slide is overlaid on the image, with the lens serving as a focal point.

Today I will talk about
Our Journey in
making the sharing of confidential
information using http possible in Norway



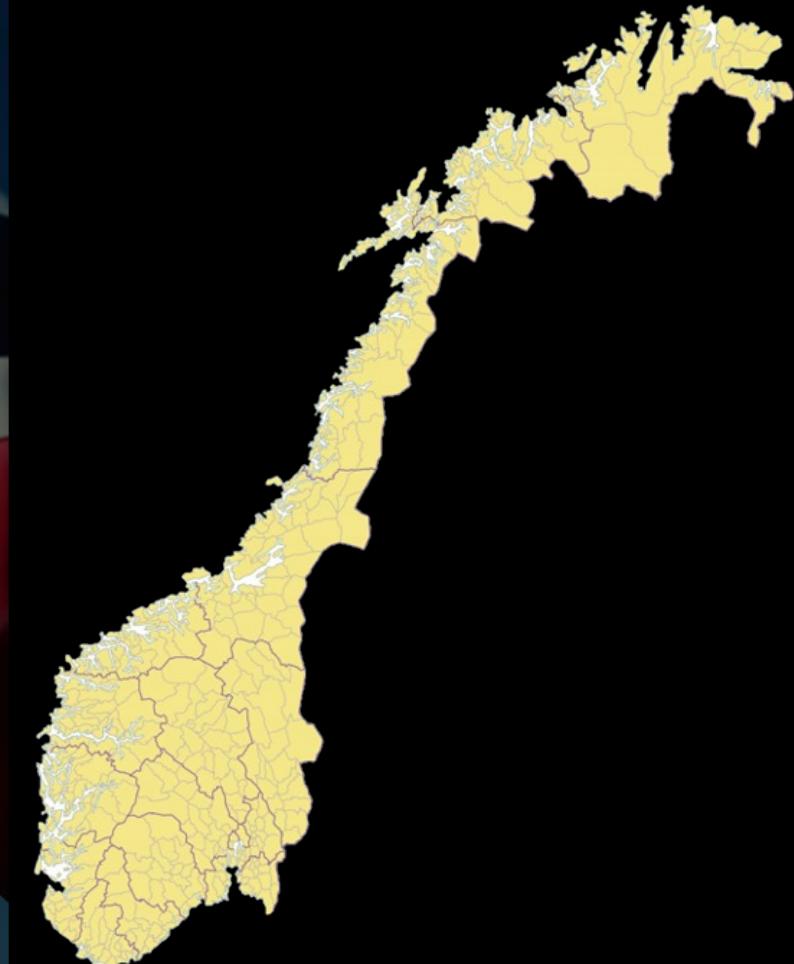
Key take-aways from this talk (my message to you)

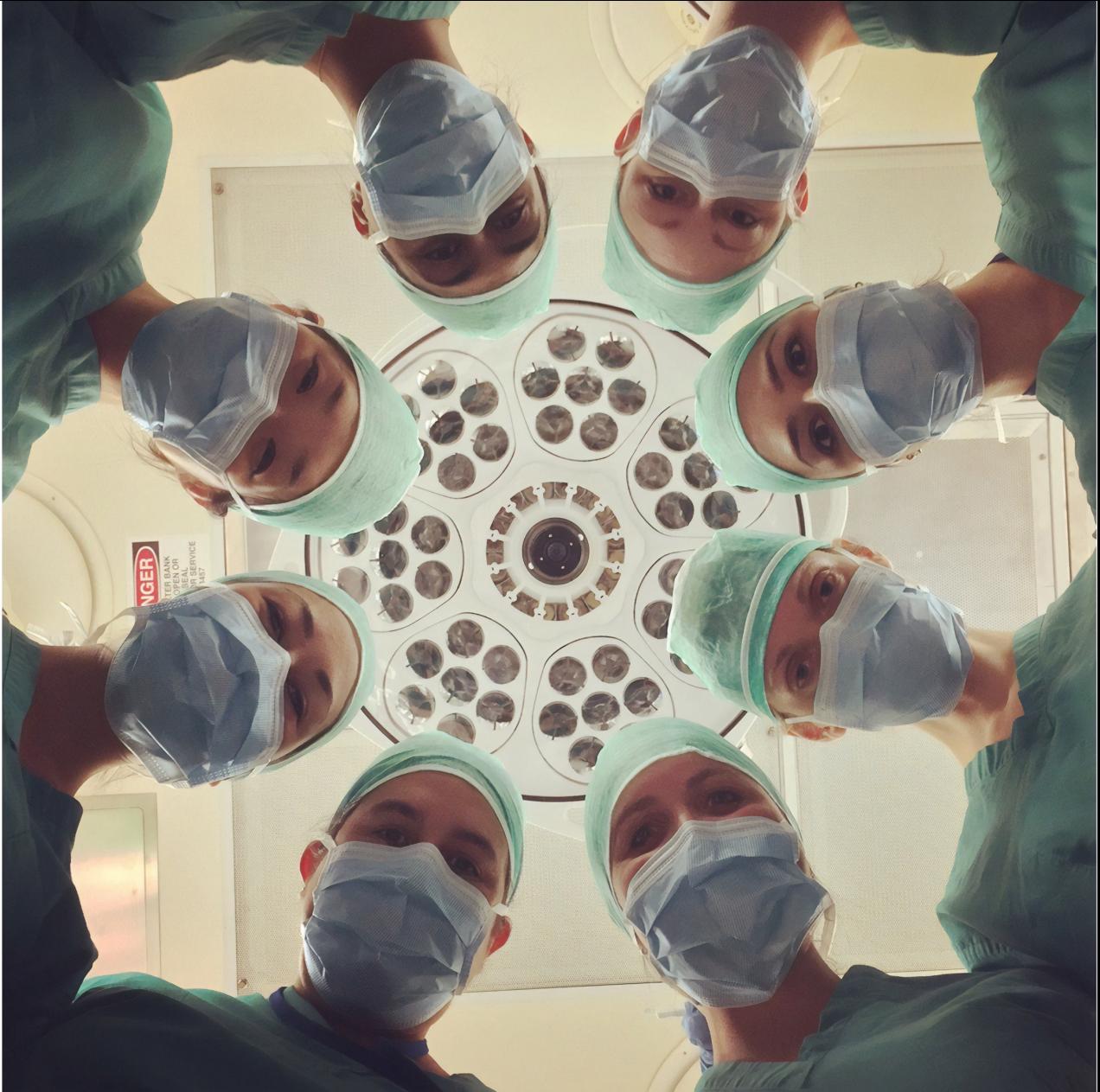
- Understand the underlying needs and requirements better – spend time on analysis before crafting solutions
- Legal requirements are shades of gray, not black/white
- We are over-complicating authorization!



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)

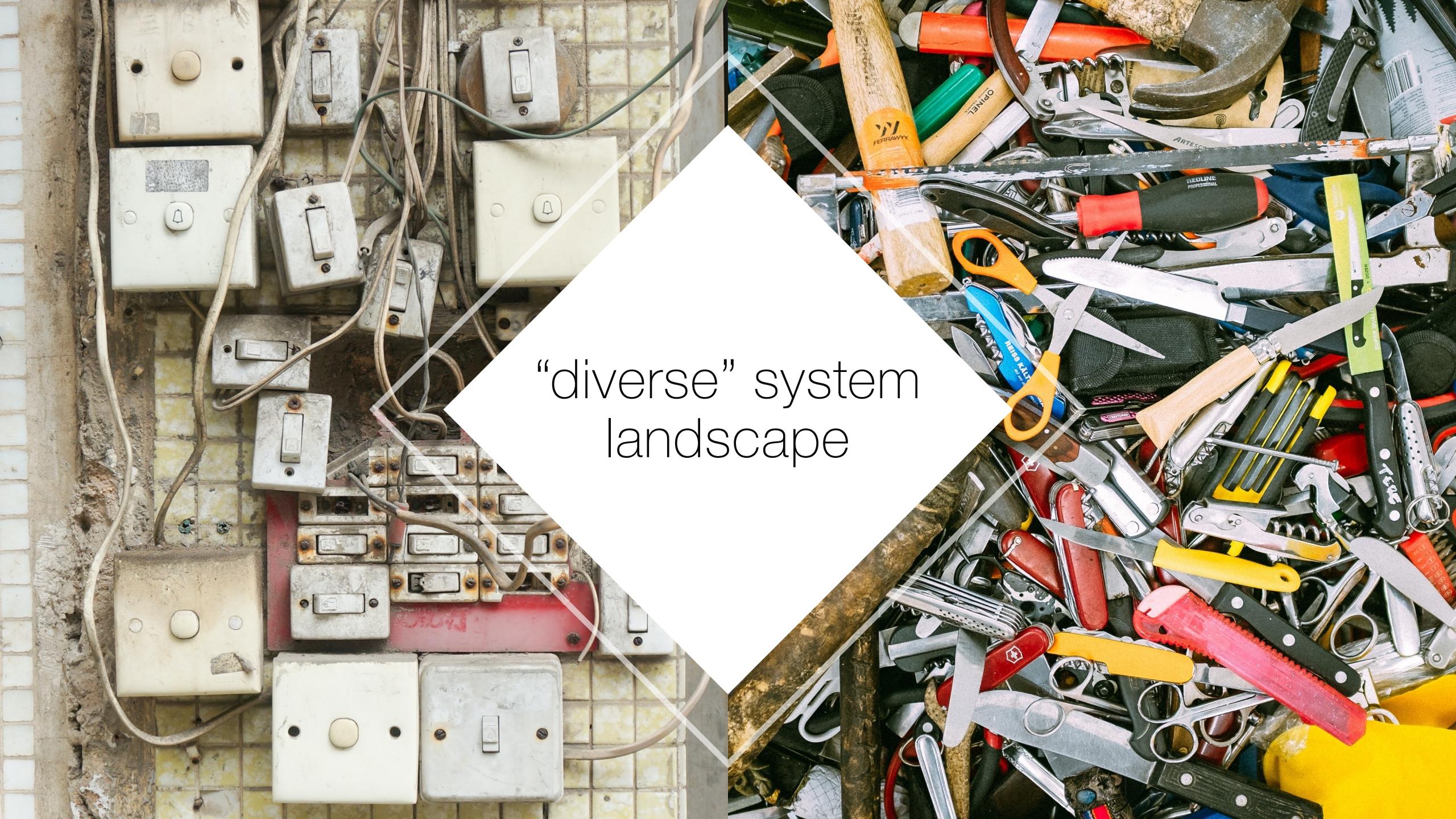
Digitalisation (not digitisation) is necessary



7000 health providers

sharing 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?



A photograph of a person from behind, wearing a bright red puffy jacket, standing on a snowy slope. They are looking towards a majestic, snow-capped mountain range under a clear blue sky. The central peak is particularly sharp and prominent, resembling the Matterhorn. The scene is bathed in the warm light of either sunrise or sunset.

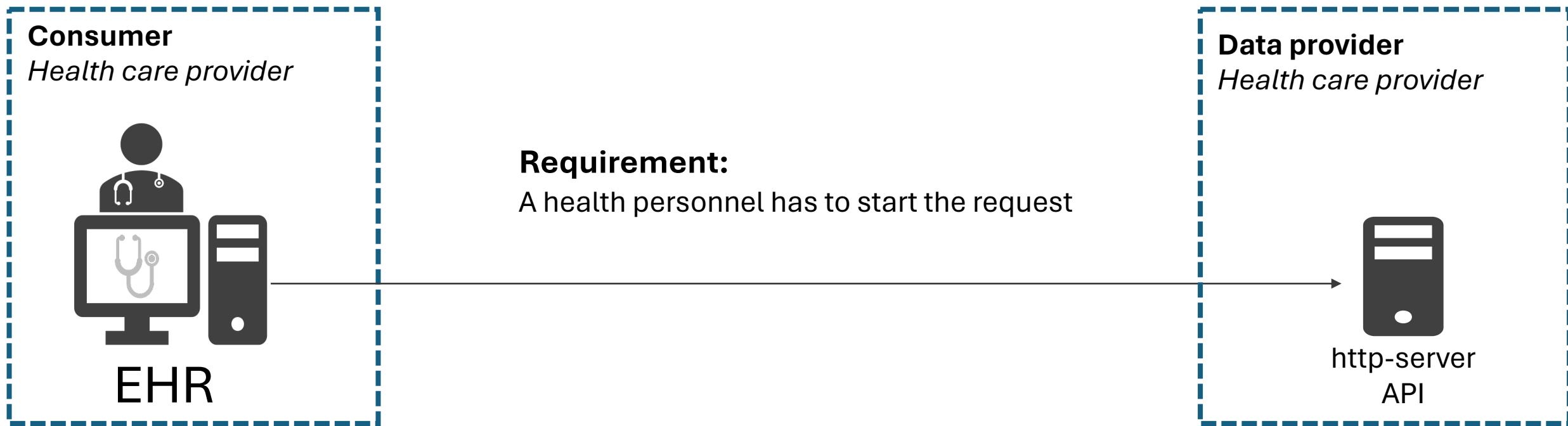
Our journey



Context

EHR software calling http-server API

The http-response message contains confidential information



Assumptions/requirements

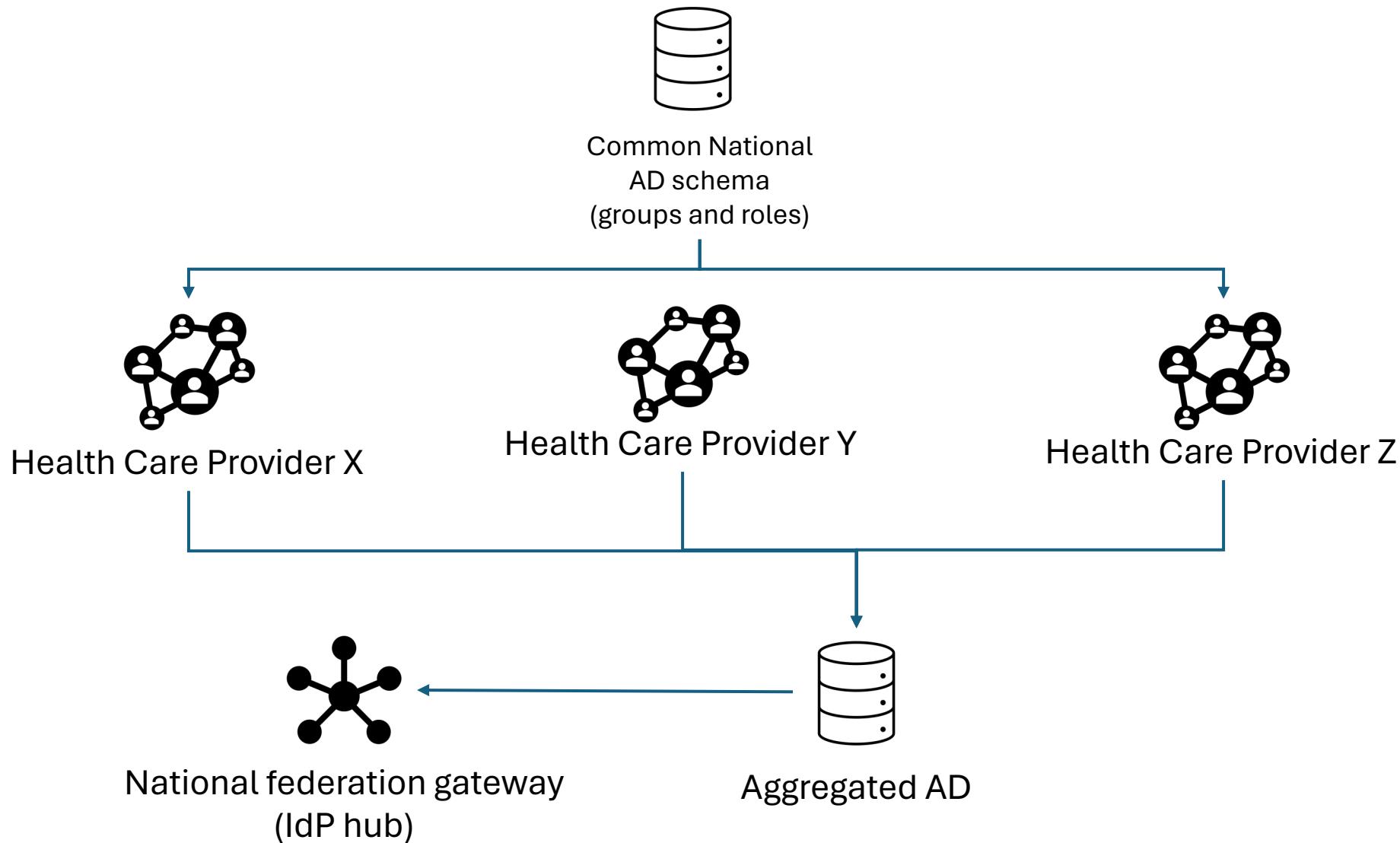
Access control for every request to an API

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



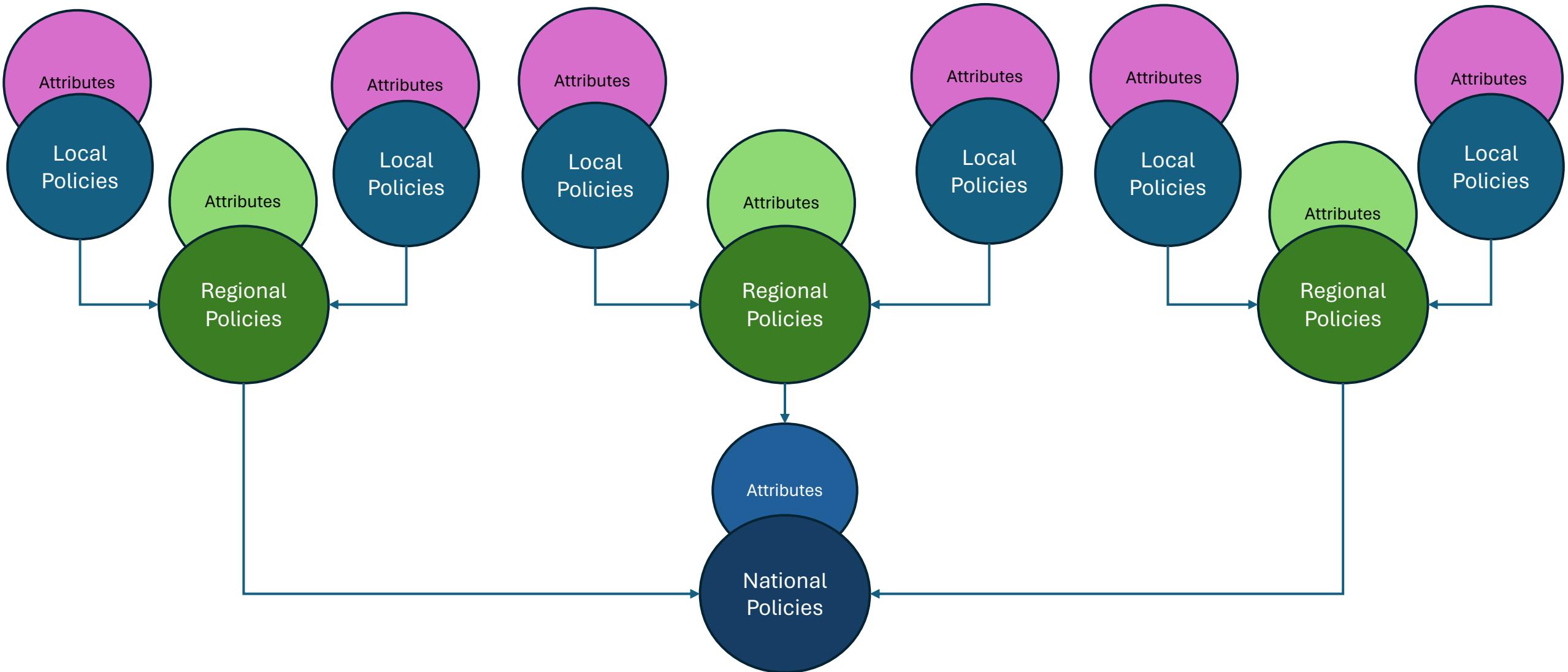
Good idea #1 vs reality

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



SECOND CONCEPT: ABAC

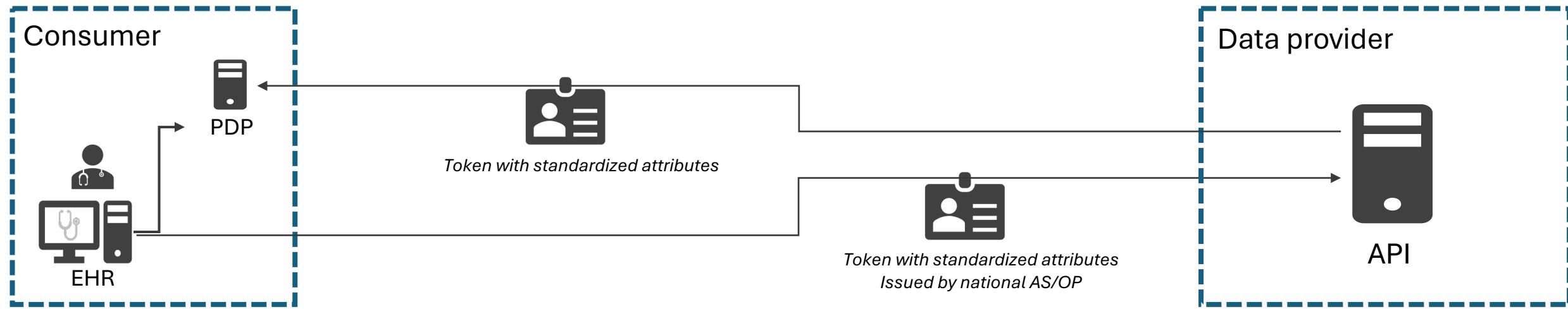
Aggregating Policies and Standardizing attributes



POSSIBLE ABAC-PATTERNS

Calling a PDP at the consumer

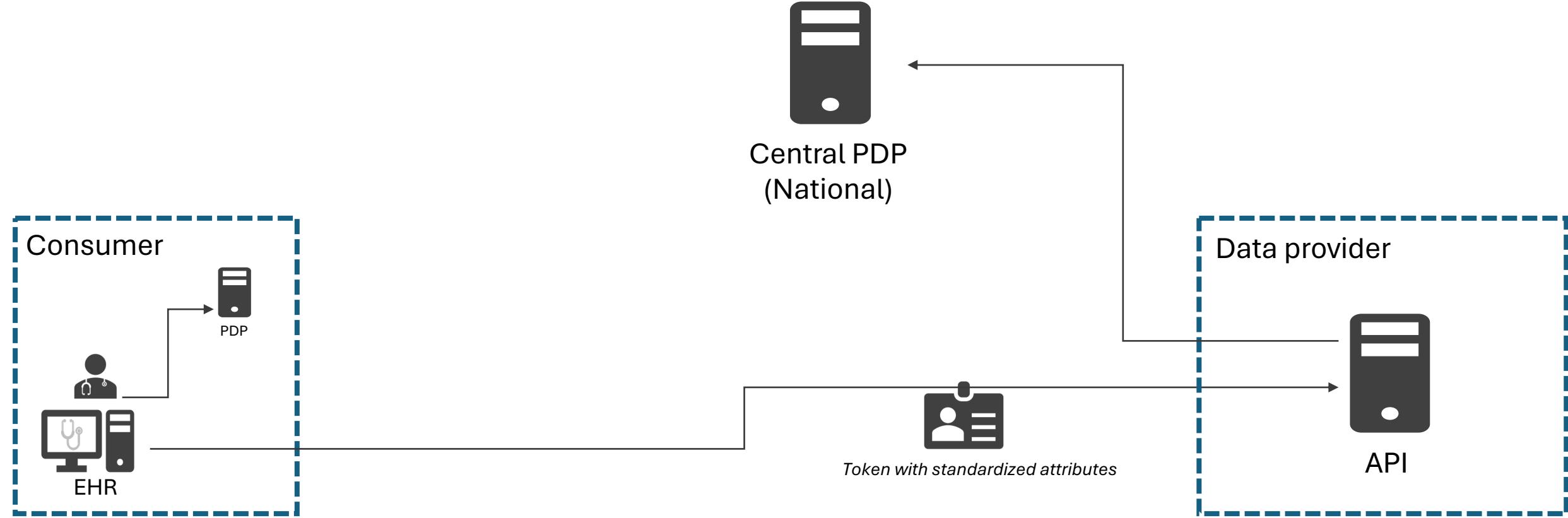
The consumer decides access



POSSIBLE ABAC-PATTERNS

Calling a centralized PDP

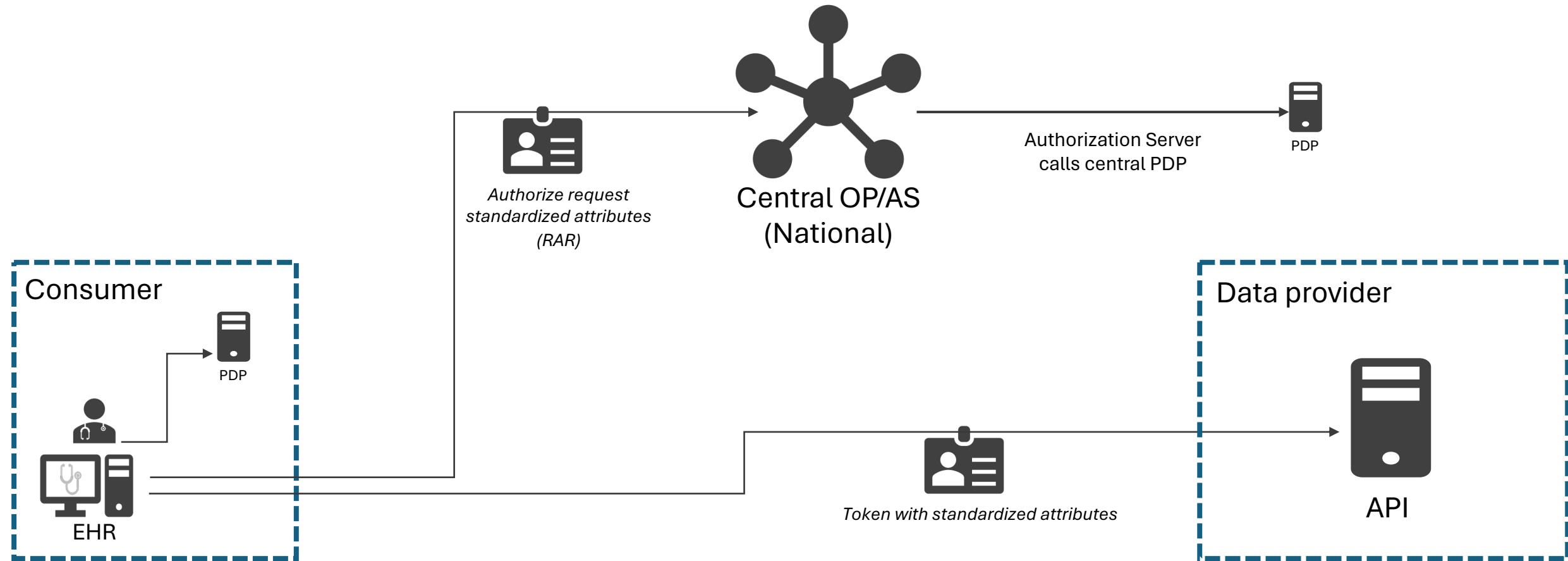
The central PDP decides access



POSSIBLE ABAC-PATTERNS

Utilizing the OAuth Authorize request

The central OP/AS calls national PDP



Good idea #2 vs reality

- Not every health care provider had ABAC
- No existing standards for attributes
- Conflicting policies
- Too high complexity in administrating the policies



A dramatic, high-contrast photograph of a large, cracked eggshell being tilted. A thick stream of dark, viscous liquid is pouring out from a metal bucket at the top. The eggshell is heavily textured with deep, irregular cracks. The liquid is splashing onto a pile of dark, jagged rocks on the ground. In the background, a vast, desolate landscape stretches to a distant horizon under a clear sky with a few small birds flying.

BUMMER..
DOOMED FOR FAILURE?

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



A photograph of an antique book with a light green cloth cover. The words "MEMBERSHIP ROLL" are printed in a dark, serif font on the front cover. The book is bound in worn, dark leather at the spine and corners. It sits on a wooden chair with vertical slats. The book is open, showing aged, yellowish-brown pages.

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

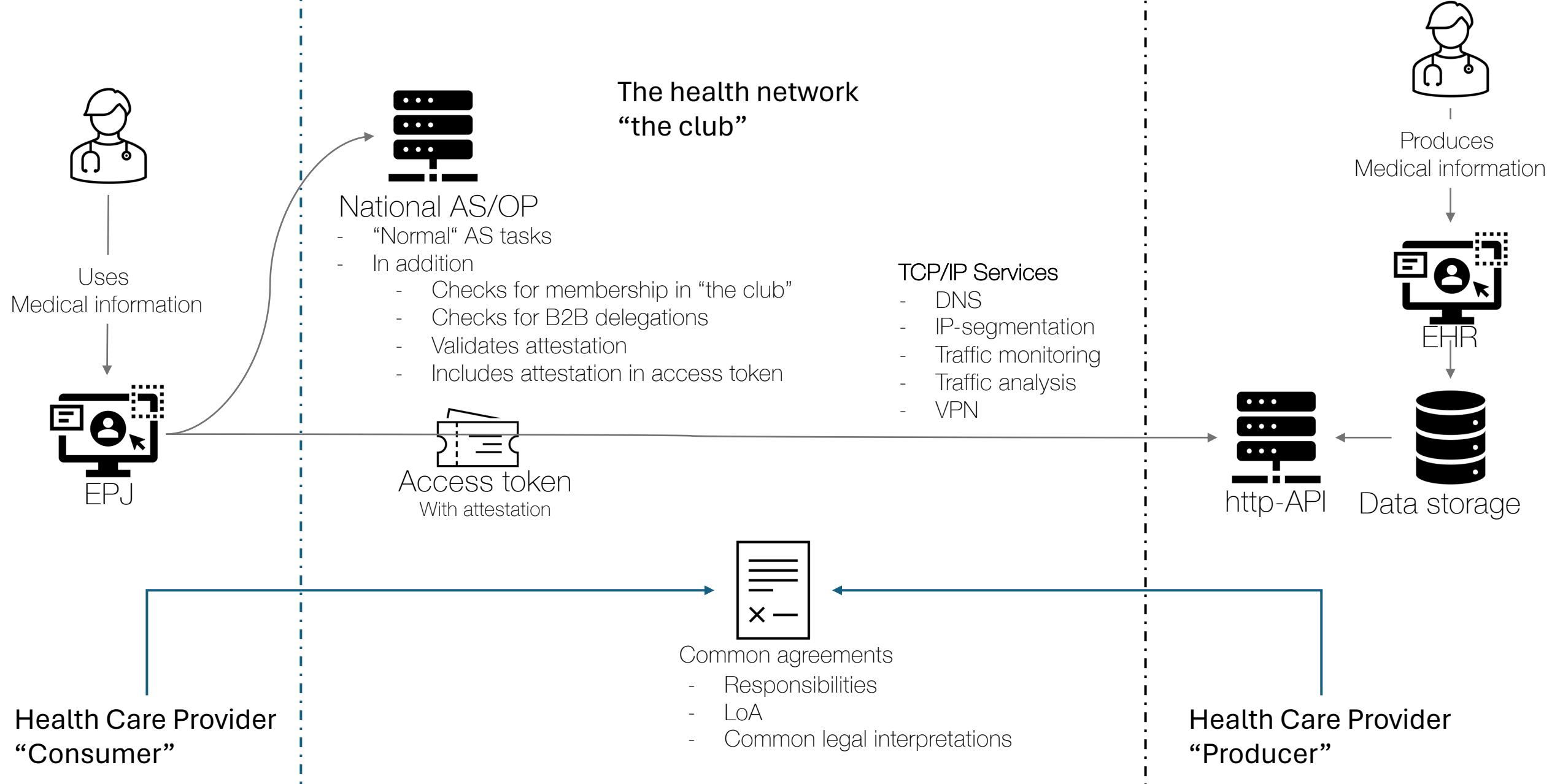
B2B delegation

- Move away from Enterprise Certificates
 - Replaced by explicit B2B delegation
 - using national authorization server
 - Verification of delegation in national AS
-
- 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
-
- FAPI 2.0 security profile
 - OAuth 2.1

Attestation of legitimate interest

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

Our data sharing trust framework



WALLETS?

main learning

LEGITIMATE INTEREST CAN'T BE DEDUCED