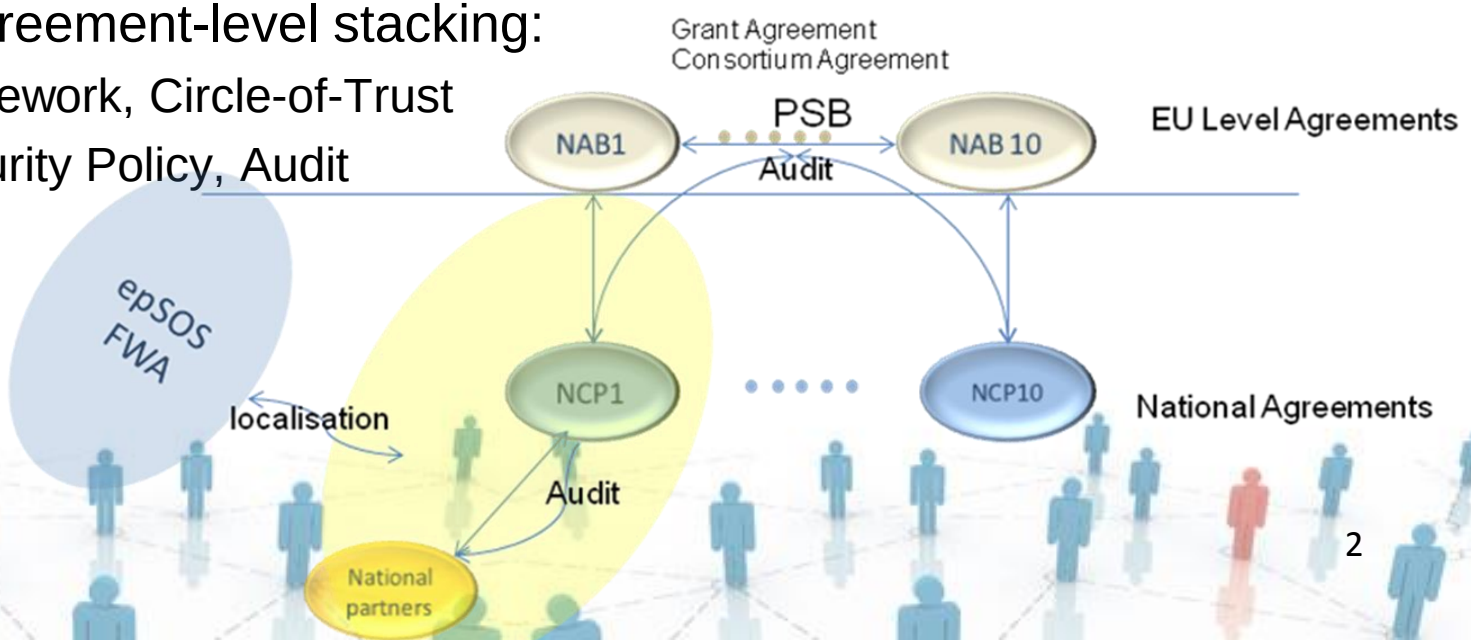
EpSOS eIdentification and Security Requirements

Massimiliano Masi

SEG, SEG-II, 3.A, 3.7

epSOS Principles

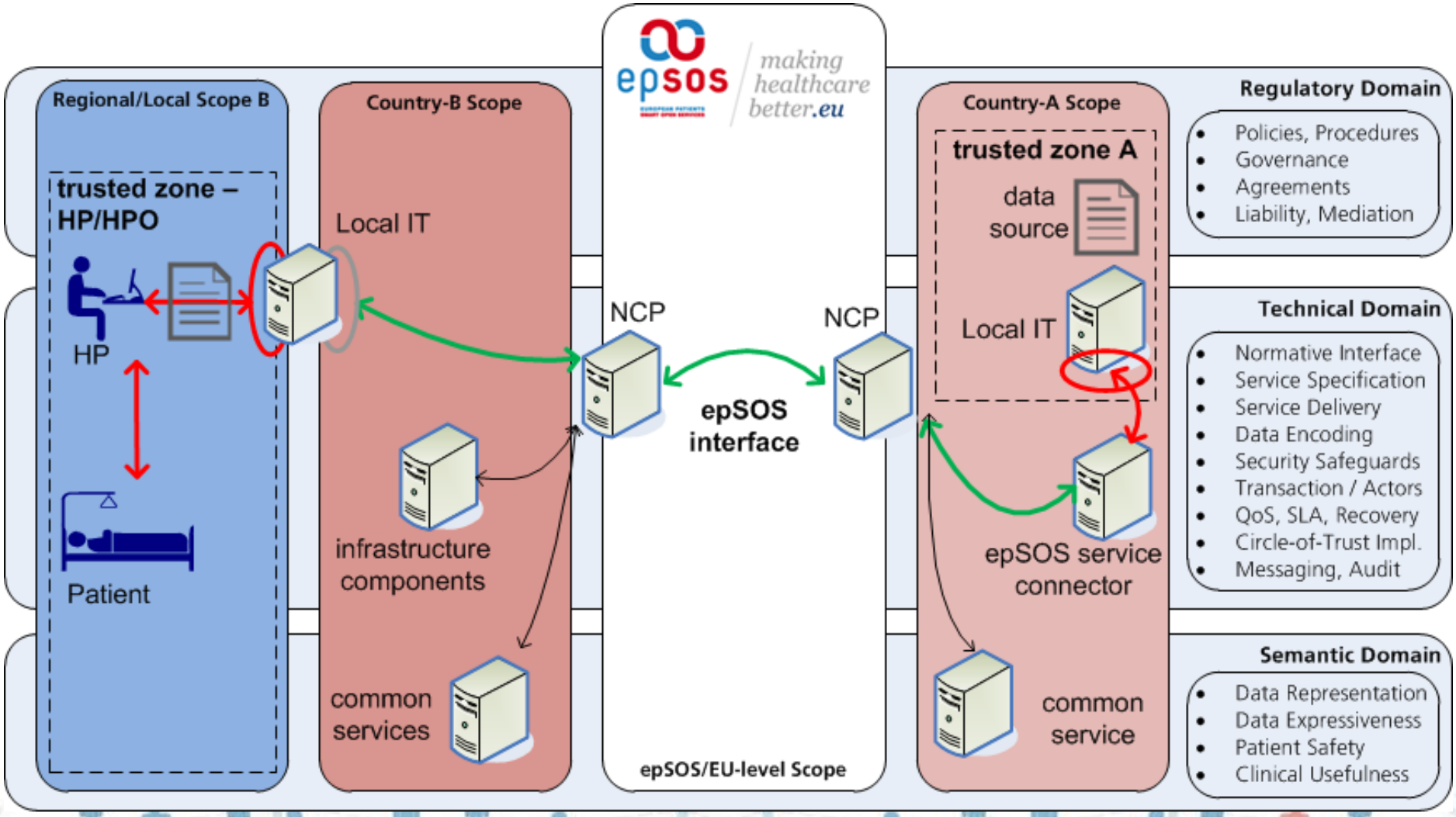
- health care is a sovereign concern of PN‘s:
  - Legal and technical decisions are made in common
  - Interoperability agreements are in place to define such concepts as common data sets to be exchanged, semantic and technical specifications, Circle of Trust and Security Policies as well as the epSOS legal FWA
  - PN’s may tailor (localise) local agreements’ implementation in so much as it will stay compliant to the essential requirements
  - policy-/agreement-level stacking:
    1. framework, Circle-of-Trust
    2. Security Policy, Audit
    3. etc.



Cornerstones of epSOS Architecture

- non-intrusive towards sovereign health infrastructures:
  - acknowledgment of disparity between regulatory domains
- decoupling of Business and Security Architecture:
  - strong separation through layering of architecture (ECCF)
  - brokered trust paradigm, security demands by countries
- Service Orientation with focus on Interoperability:
  - architecture abstraction through layering, profile focus
- high flexibility concerning component orchestration:
  - self-sustained, interchangeable components
  - interceptor model for introduction of extended components

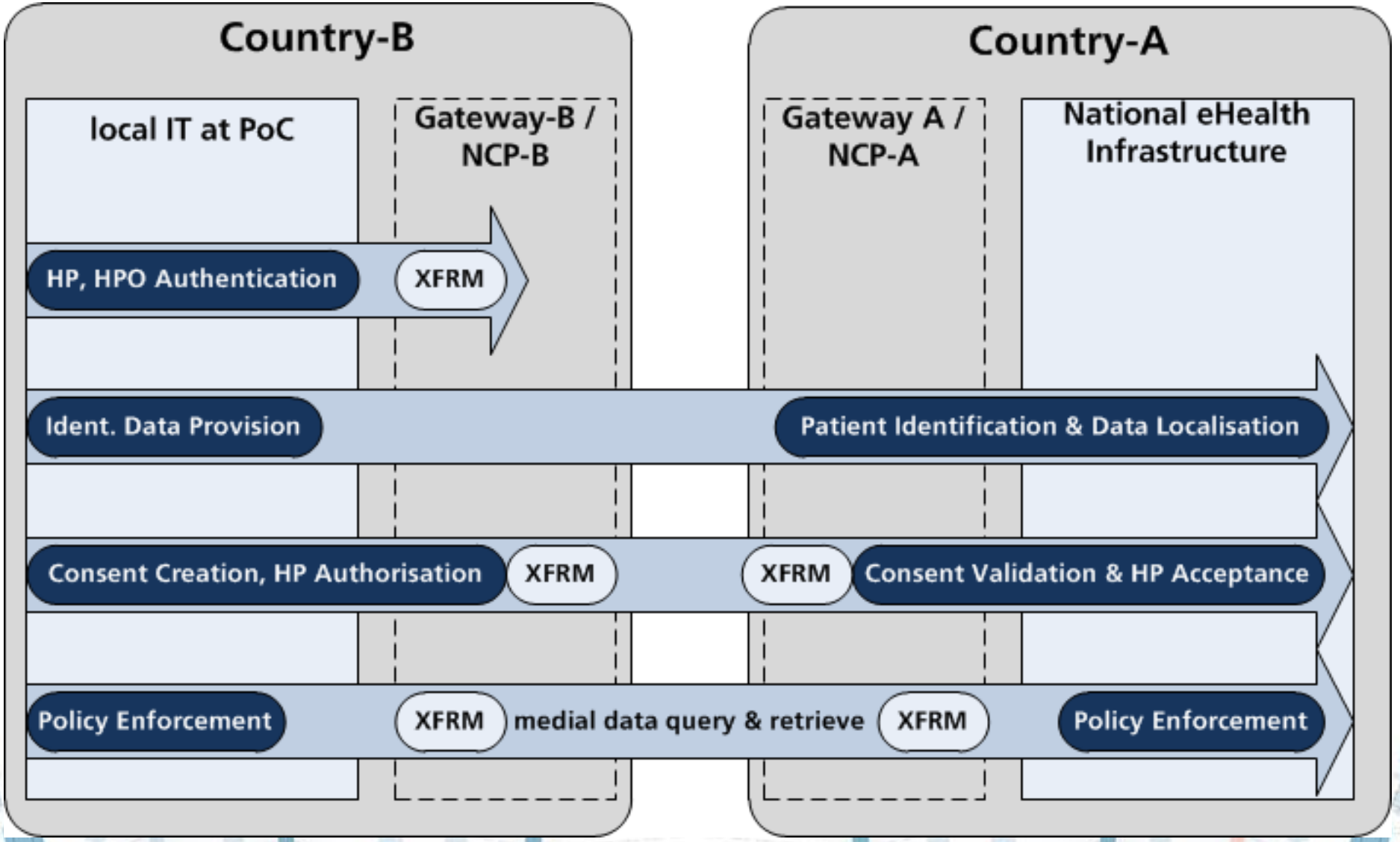
epSOS Architecture Composition



„Heart“ of epSOS: National Contact Point (NCP)

- epSOS is founded on a partial brokered trust paradigm:
  - each MS only directly trusts its **own** NCP and **own** HP’s
  - each medical disclosure decision is **always** made in country-A
  - double-role mapping for roles
- the NCP’s act in several roles:
  - enforcement point for **x-border procedures and governance**
  - **legal umbrella** for each Member State, delimiting its boundaries
  - trust anchors and terminators:
    - as brokered “mutual” AuthN providers, trust assurances, and audit trail
  - technical “**glue**” for national interfaces, protocols, and formats
  - as “**semantic bridges**” that perform schema and code translation

epSOS Interaction Patterns



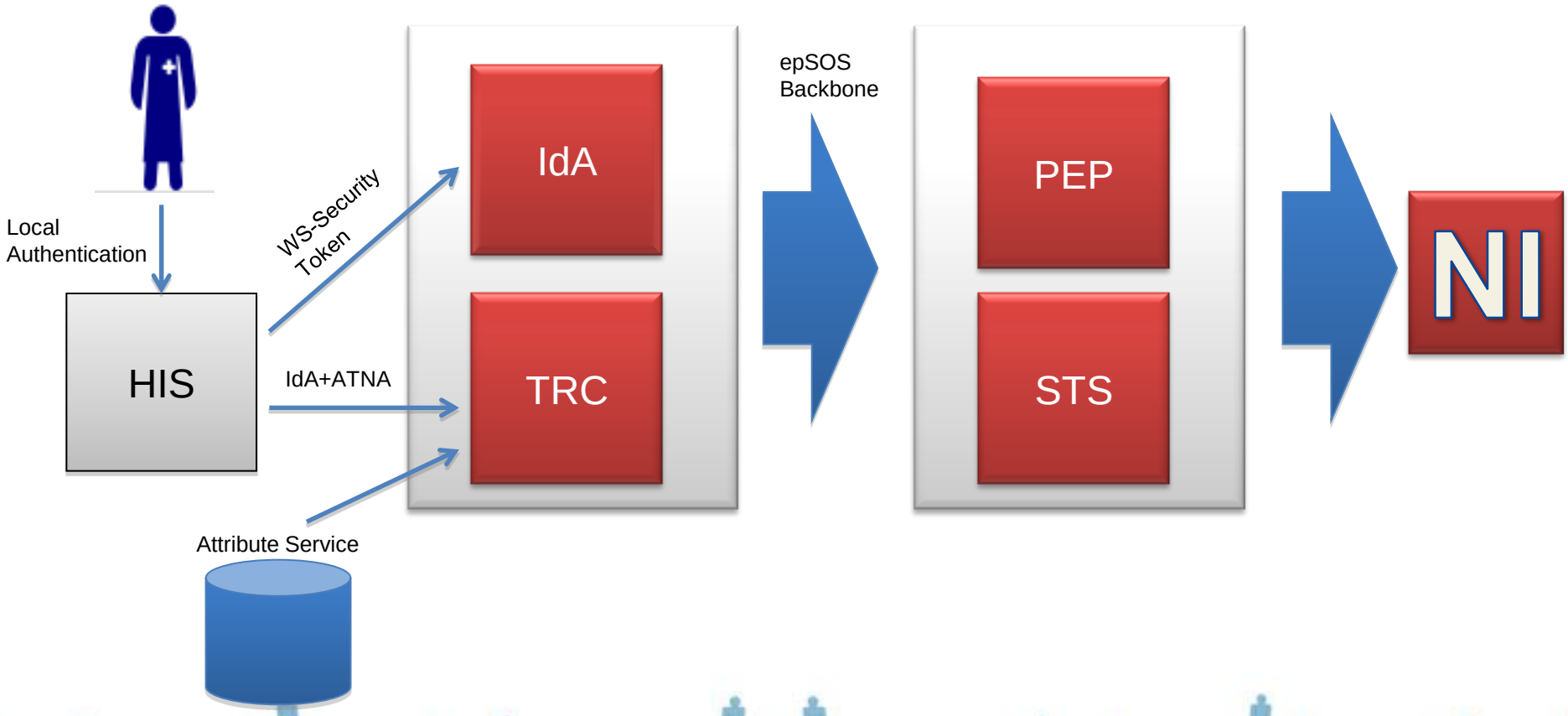
Application of eID within epSOS

- epSOS is operating trust relationships:
  - trust bootstrapping by PN contracts and agreements
  - circle of Trust as shared common regulatory framework
  - mediated, brokered trust between active participants
  - technically encoded as two dependent SAML assertions:
    - Identity Assertion (IdA) asserting the HP **identity**, attributes
    - Treatment Relationship Confirmation asserting the **context**
    - **Sender-vouches** mechanism preserving legal national responsibility

epSOS Secure Invocation Pattern

- Initialise Circle-of-Trust (VPN, Mut.AuthN, ATNA, SecPol)
- Initialize a business security context in country-B:
  - HP Authentication through national managed IdA
  - Patient Identification / Authentication
  - HP Authorization and role mapping
- Encapsulate full security context within SAML assertions:
  - Health professional identity assertion
  - TRC assertion
- Relay the security context with each business transaction
- Initialise a provider security context in country-A:
  - Patient consent & privacy policy (IdA, TRC, XSPA, LoA, Policies)

epSOS Identity Assertion Life Cycle



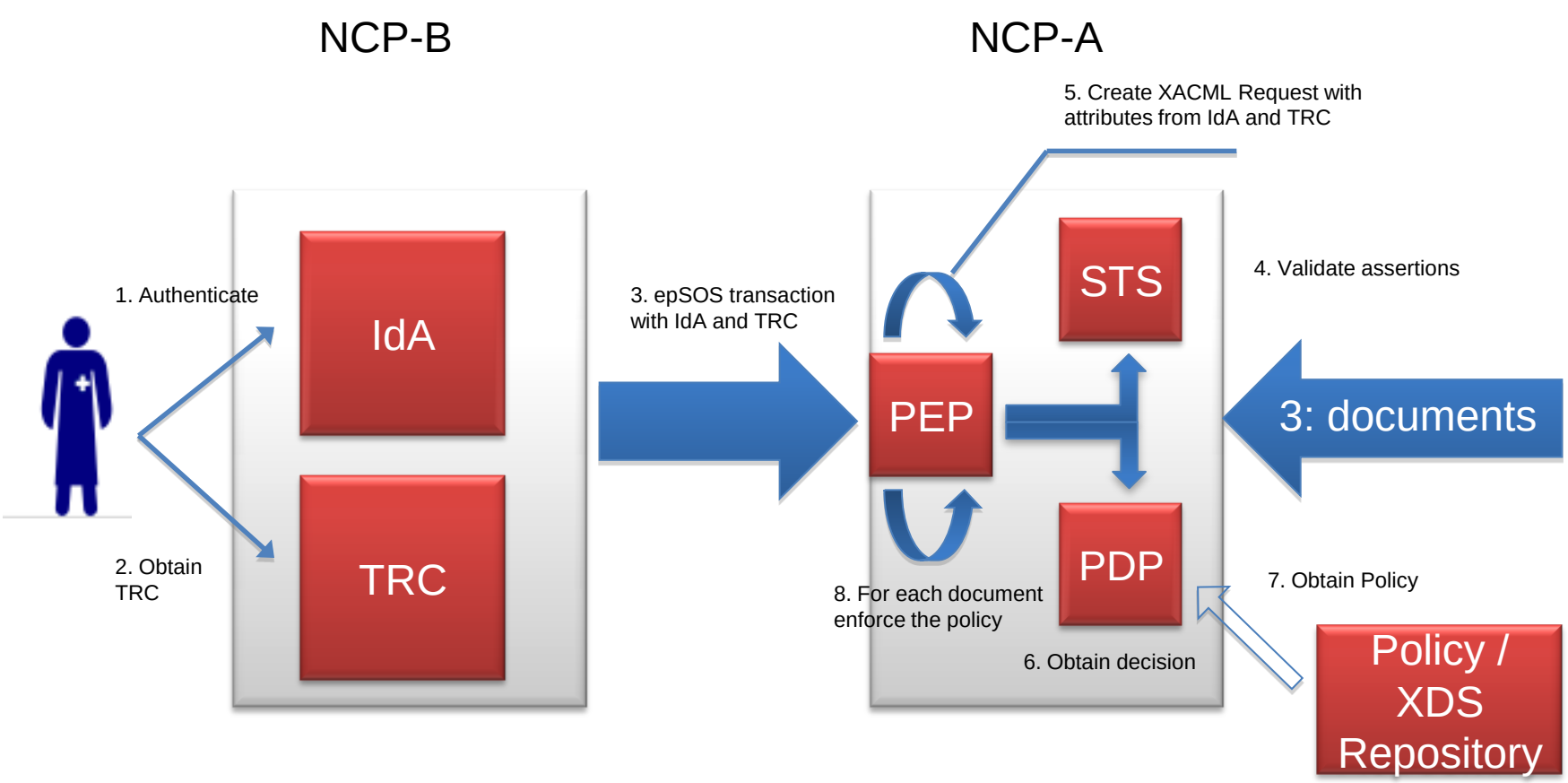
Patient Consent

- **informed consent - two shades:**
  - fundamental consent prerequisite for participation in epSOS in any case (*the patient need to opt-in*)

- **consent is manifested by IHE BPPC representation:**
  - two fundamental and mandatory policies: *Opt-In*, *Opt-Out*
  - BPPC CDA document contains a reference to the given consent
  - the communicated consent is a template that enables the CoA to act according to their own legislation without introducing regulatory mismatch
  - consent/policy stacking encouraged to formalise enforcement of national law

- **The consent is rendered using a XACMLv2 policy:**
  - obtains required decision attributes from the SAML IdA, TRC, NSP
  - contains rules for each epSOS role, purpose of use, action, permission
  - Can be stored in a XACML Policy Repository using OASIS WS-Trust / SAMLv2 Profile for XACMLv2

eID-propelled Consent Enforcement



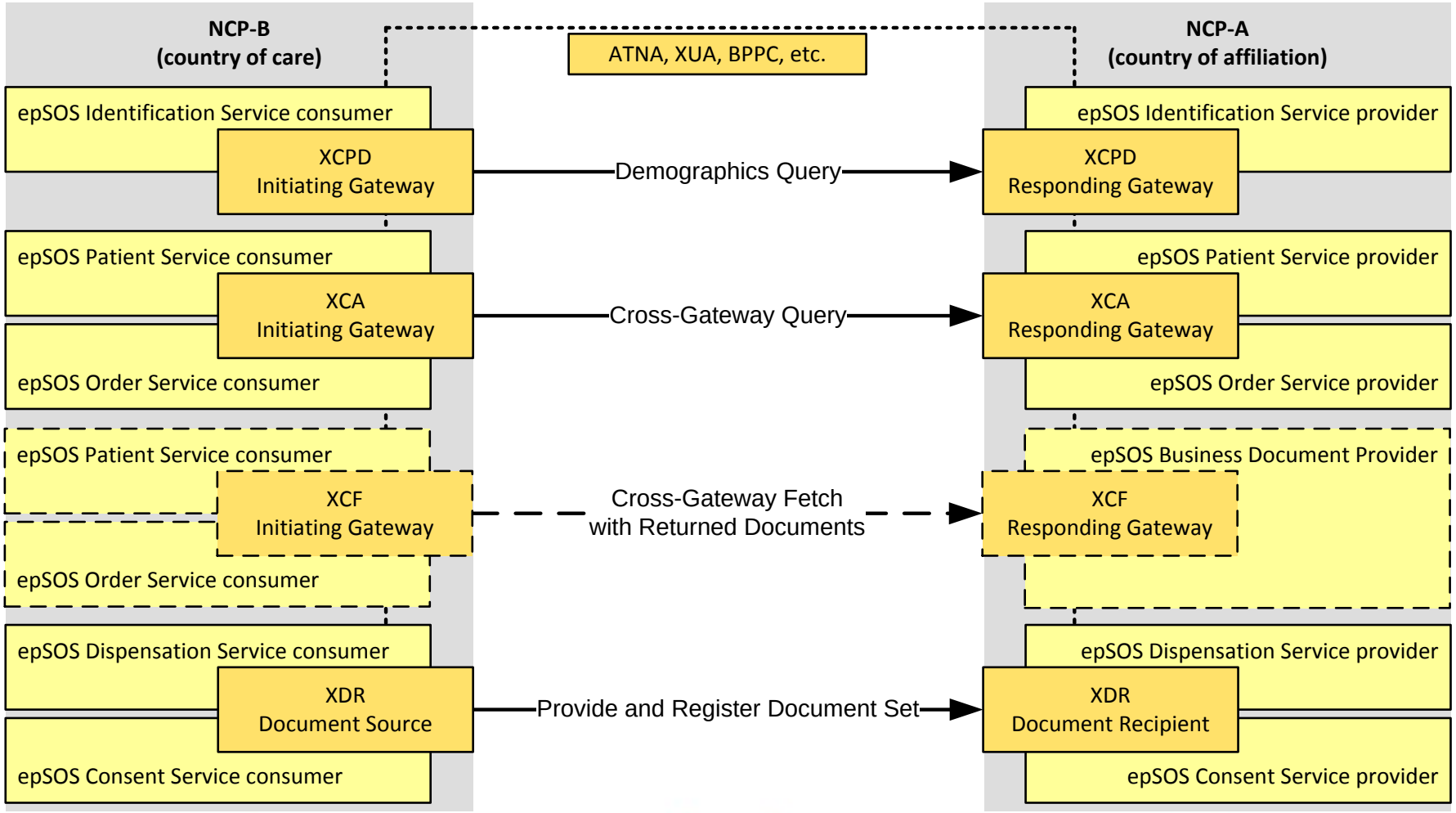
Challenges for comprehensive eID

- digital signatures in e-Health not yet fully operational:
  - usually at least one involved party is **unknown beforehand**
  - few HP possess **signature/encryption** means ready for eID regulation
  - patients can well be **identified** abroad but hardly **authenticated** with their existing national eID material
  - **disharmonic national regulations** cause further complexity:
    - patient-controlled health data remaining fully opaque to national systems
    - HP-initiated and -controlled health data with little to not patient interaction
    - proprietary, advanced or qualified signature requirements, human subjects only, no x-border exposition legally acceptable, etc., etc.
  - strong need for pre- and post-processing (translation, data conditioning, data export constraints) hinders traditional eID by digital signature and encryption
  - hard- and software incompatibility, different token carriers, etc.

Path to technical InterOp: Profiling

- common services within epSOS were profiled for:
  - interoperability assurances across systems and countries
  - „testability“, substitutes, and certification streamlining
  - exploiting already existing InterOp test-beds and activities
  - ➢ benefitting from off-the-shelf and plug-in components
- candidates for immediate application within epSOS:
  - XCPD, XDR, ATNA, BPPC, CDA, XACML, XSPA, TSL, etc.
  - reality check of new approaches: NSL, template consent
- candidates with adaption needs:
  - XCA, XUA, BPPC, community agreements, trust elevation
  - epSOS tried hard to reuse, not to replace or deprecate
  - however, epSOS was facing challenges (RLUS, Security)
  - ➢ motivating adaptions by innovation, and new profiles

Profiles in epSOS: Example IHE



What is achieved:

- establishment of EU-wide "**mediation beacons**":
  - 11 operational NCP's with exchange of real data
  - more within pre-pilot NCP's in final tests
- technical InterOp between Participating Nations:
  - **possible, feasible, and beneficial**
- stimulation of PN extensions to InterOp ecosystem:
  - DK, GR, FR: HP portal usability enhancements
  - ES: regionally distributed system and data
  - FR: smart-card security for HP AuthN/AuthZ
  - DE, AT: cross-border patient-centric security

What is in progress:

- organisational/regulatory streamlining:
  - alignment of x-border HC **Standard Operating Procedures**, security, privacy provisions
- infrastructure innovation and advanced piloting:
  - exceptional circumstances: x-border trust elevation (who you are, what you have, what you know, in which context)
- Stimulation of a sustainable ecosystem:
  - eHGI (etc.) for PN penetration and patient acceptance
  - Industry for sustainability and market development
  - Open Source initiative for accessibility (OpenNCP)

Conclusions

- EpSOS uses EU-specific technology (TSL), as well as consolidated standards from IHE, HL7, OASIS, and W3C
  - XCF, XUA, BPPC from IHE. SAML, XSPA, from OASIS. CDA from HL7, SOAP from W3C
- eID in epSOS: digital signature can't be used now to authenticate principals
  - Technical disharmonies (on hardware and software)
  - Recap what eID is: smartcards, card readers, rfid, NFC, phones, middleware: interoperability required
- Patient identification and authentication is very disharmonic
  - Achieved using IHE XCPD
  - No cryptographic evidence (hardware and software): eSignature directive?

Conclusions

- epSOS is already using the eID Trusted Service List technology
  - Once eID Regulation will be in force, alignments may be required (qualified properties, mandatory use of CRL/OCSP in MS, use of eID for non-human principals).
  - EpSOS did it first baby steps: more work in a bigger audience is welcome
- The foreign data controller is not capable to confirm the HP authentication, due to Brokered Trust. Even with cryptographic material
  - NCPs are using the *sender-vouches* mechanism. The IdA and TRC are *supporting tokens:* no need to use delegation

Thank You!

Contact: massi@tiani-spirit.com