Regulatorily Aligned Consult-Scoped Anonymous Credentials with Accountable Transparency for EHDS-based Health Data Access

Mahdi Akil and Frank Pallas

Paris Lodron University of Salzburg

DPM Workshop

A consultation needs a limited record view

PARIS LODRON UNIVERSITÄT SALZBURG

- Dr. A at hospital H1 asks specialist Dr. B at hospital H2 for advice
- Dr. B needs **selected data** to answer one clinical question
- A portal or clinical summary may expose **more than the consultation needs**

Two laws pulling in opposite directions

- General Data Protection Regulation (GDPR): limit personal data to what is necessary
- European Health Data Space (EHDS), Article 9: information on who accessed which data, and when
- Our design keeps the specialist's identity hidden from the gateway and **recoverable by an auditor**

Article 9 applies in stages from March 2029 and March 2031, depending on data category.

Requirements

- **Minimal disclosure:**
  Reveal only what the gateway needs to enforce access
- **Delegation integrity:**
  Enrolled clinicians only, no impersonation or further delegation
- **Case-bound authorisation:**
  Require hospital approval for this case and purpose
- **Patient transparency:**
  Let patients find out who accessed which data, and when

Cryptographic building blocks

PARIS LODRON UNIVERSITÄT SALZBURG

- **Delegatable anonymous credentials** carry certified attributes and a limited delegation chain
- A **zero-knowledge proof** shows that the access conditions hold while hiding the secret values
- **Verifiable encryption** seals an identifier for the auditor and proves that it is the correct one

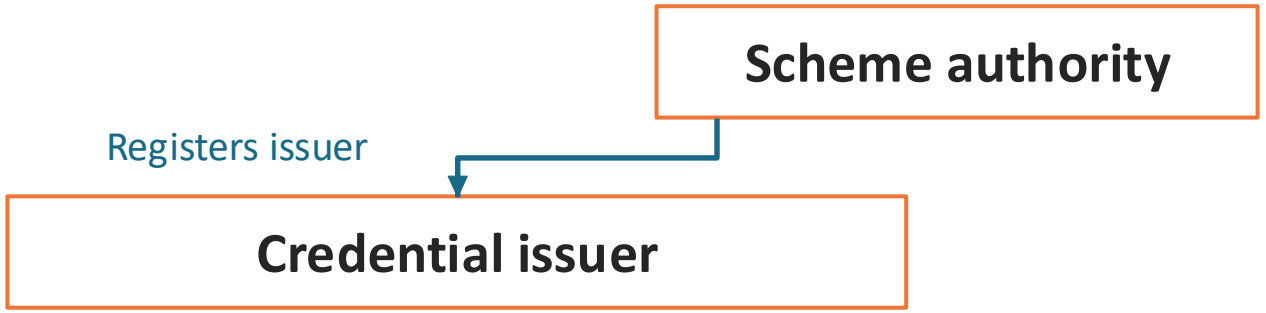
Scheme setup

PARIS LODRON UNIVERSITÄT SALZBURG

Scheme authority

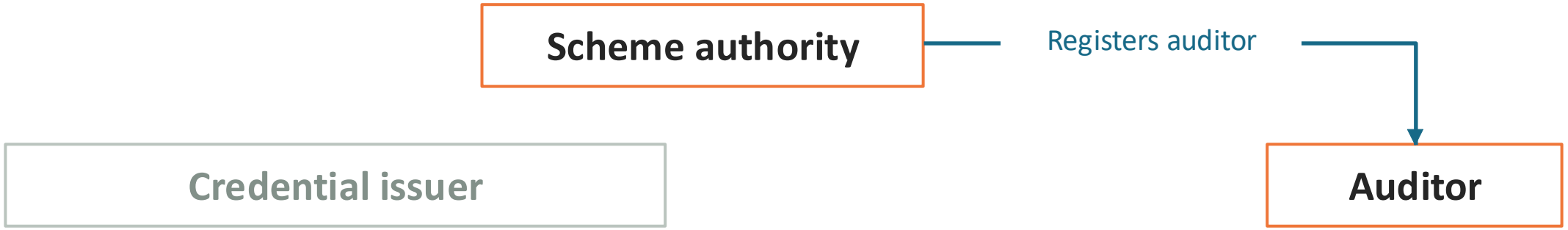
- The scheme authority registers the participating authorities and hospitals
- It publishes shared public parameters and trusted public keys

Scheme setup



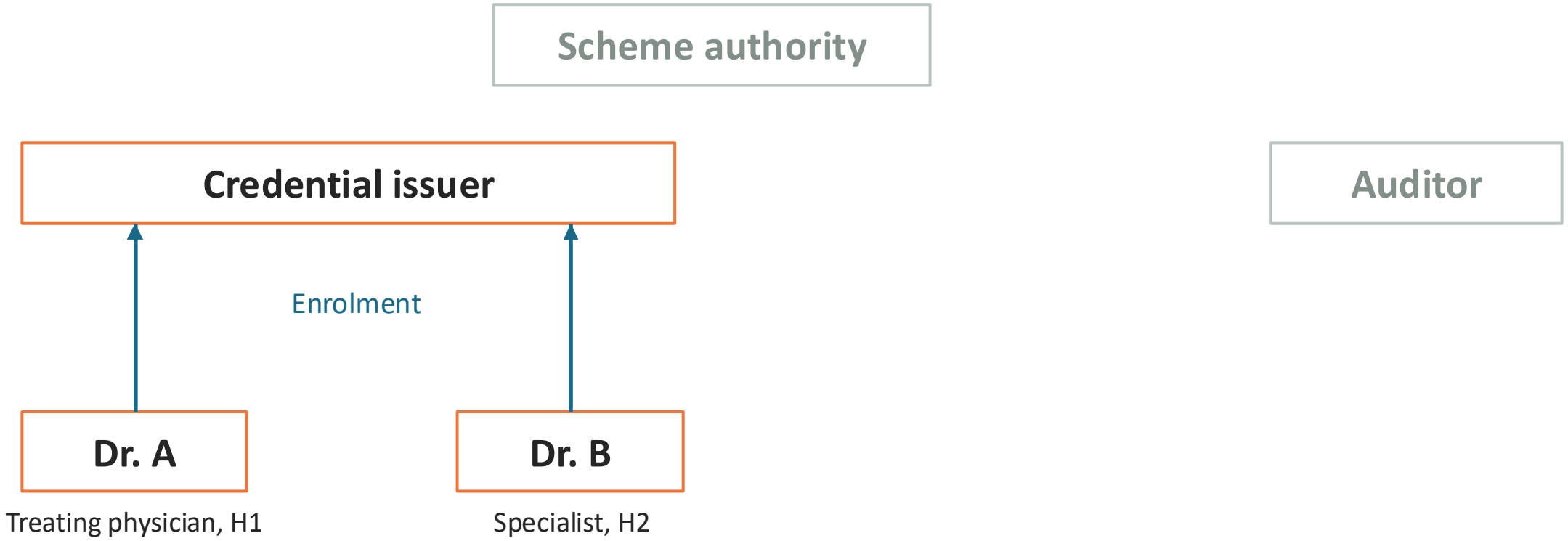
- The credential issuer enrols licensed clinicians
- It issues their clinician credentials and matching identity certificates

Scheme setup



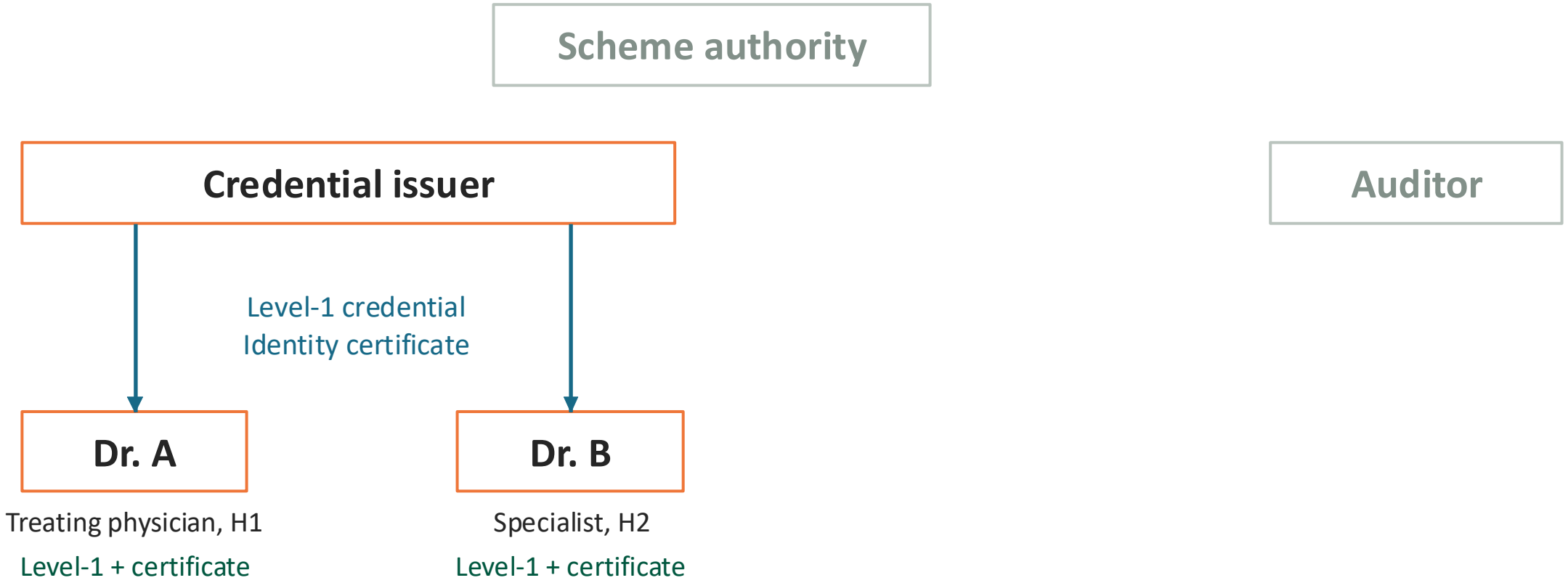
- The auditor holds the secret key for recovering logged clinician identities
- Everyone can encrypt an identifier with the auditor's public key

Clinician enrolment



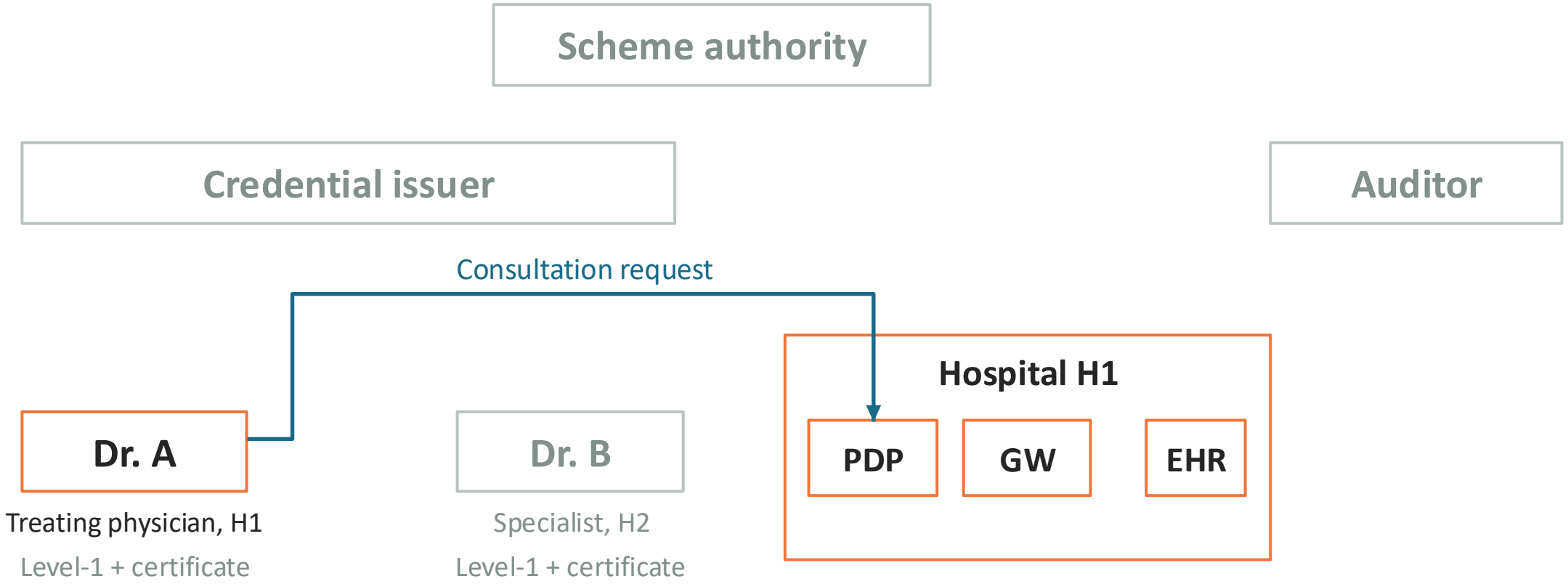
- Dr. A and Dr. B each enrol with the credential issuer
- The issuer checks their identity and professional eligibility

Clinician enrolment



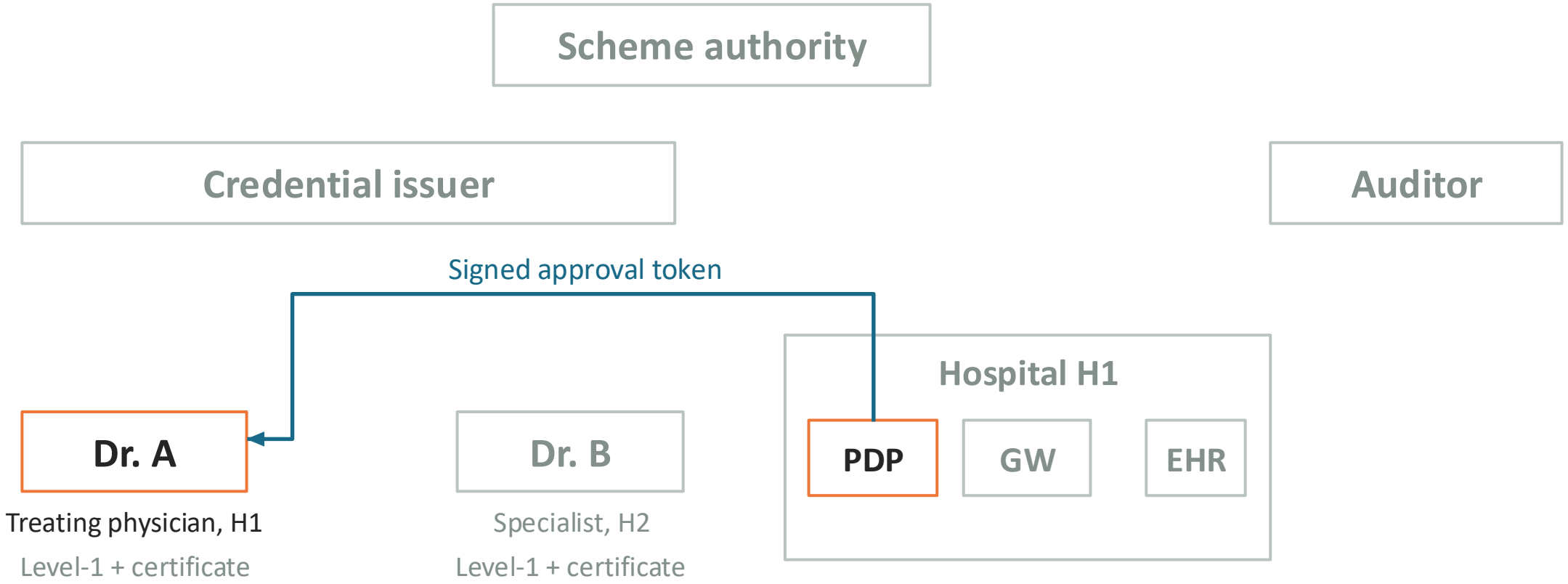
- Each doctor receives a Level-1 credential and a matching identity certificate
- Both bind the same clinician identifier and public key

Hospital approval



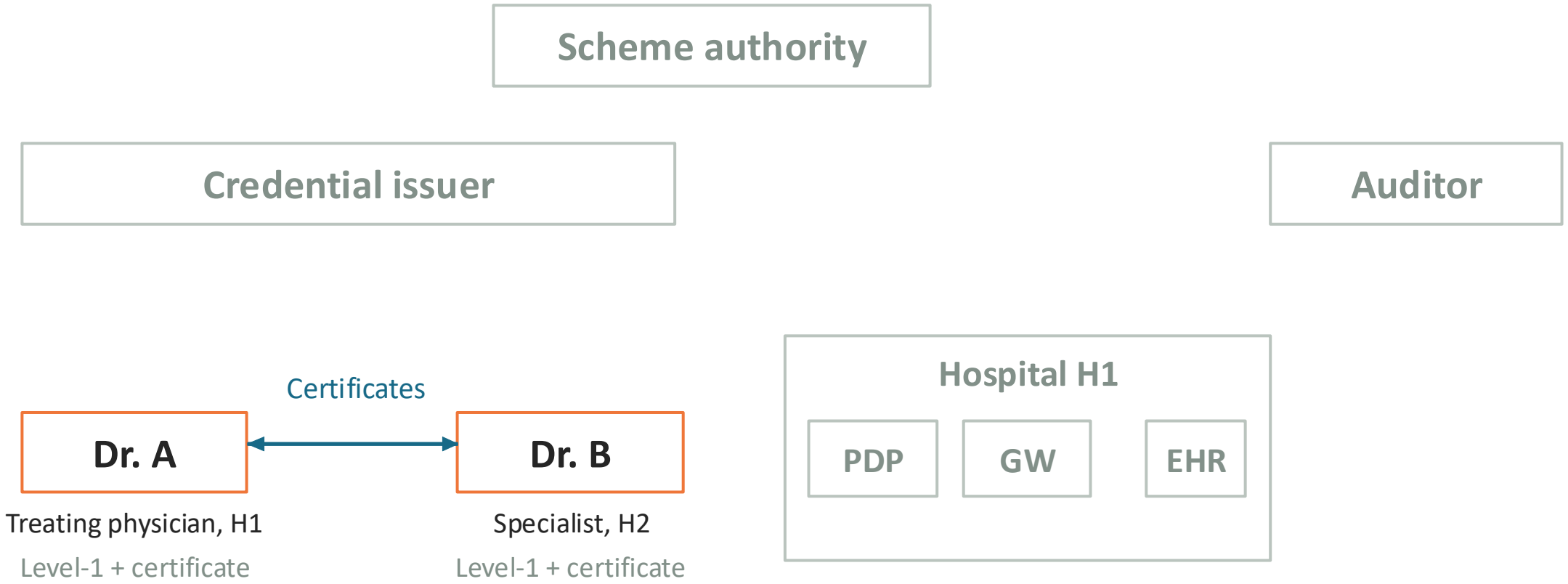
- Dr. A asks the policy decision point to authorise the consultation
- Request: Dr. A's public key, case, data categories, expiry and purpose

Hospital approval



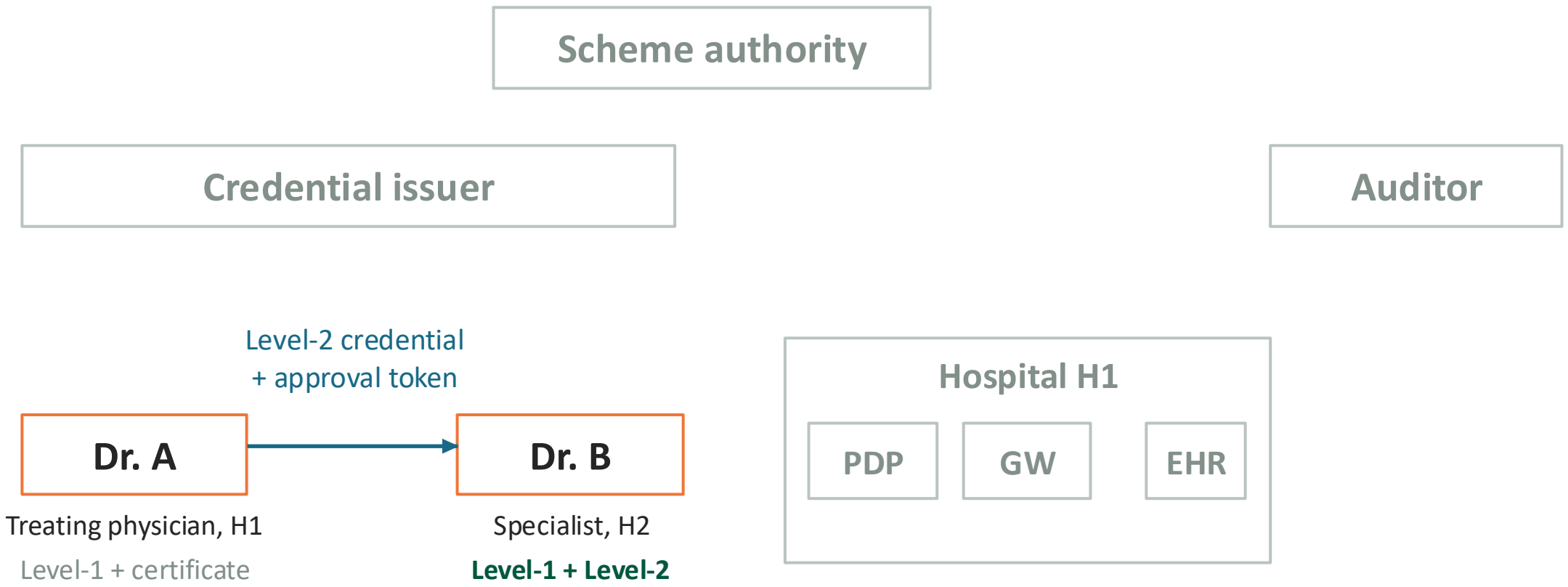
- The policy decision point returns a signed authorisation token
- It binds Dr. A to the approved case, data categories, expiry and purpose

Consultation delegation



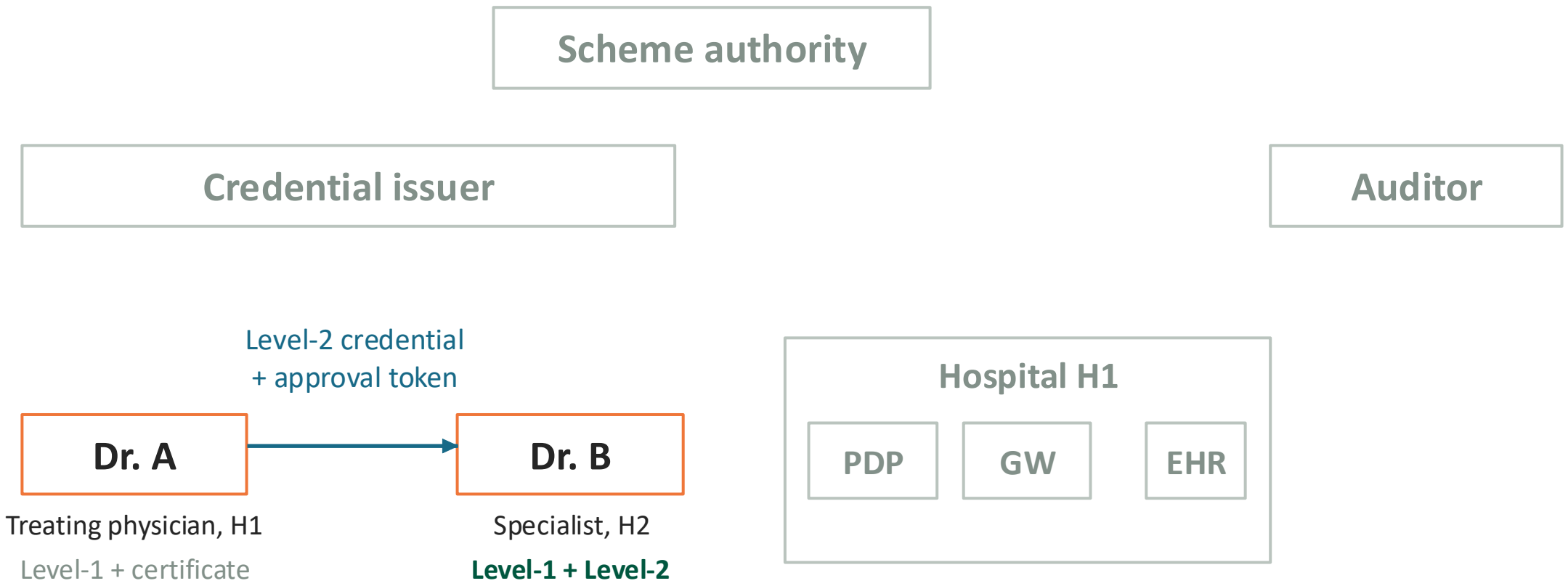
- The doctors exchange identity certificates over a secure clinical channel
- Dr. A checks Dr. B's identifier, public key and control of the matching key

Consultation delegation



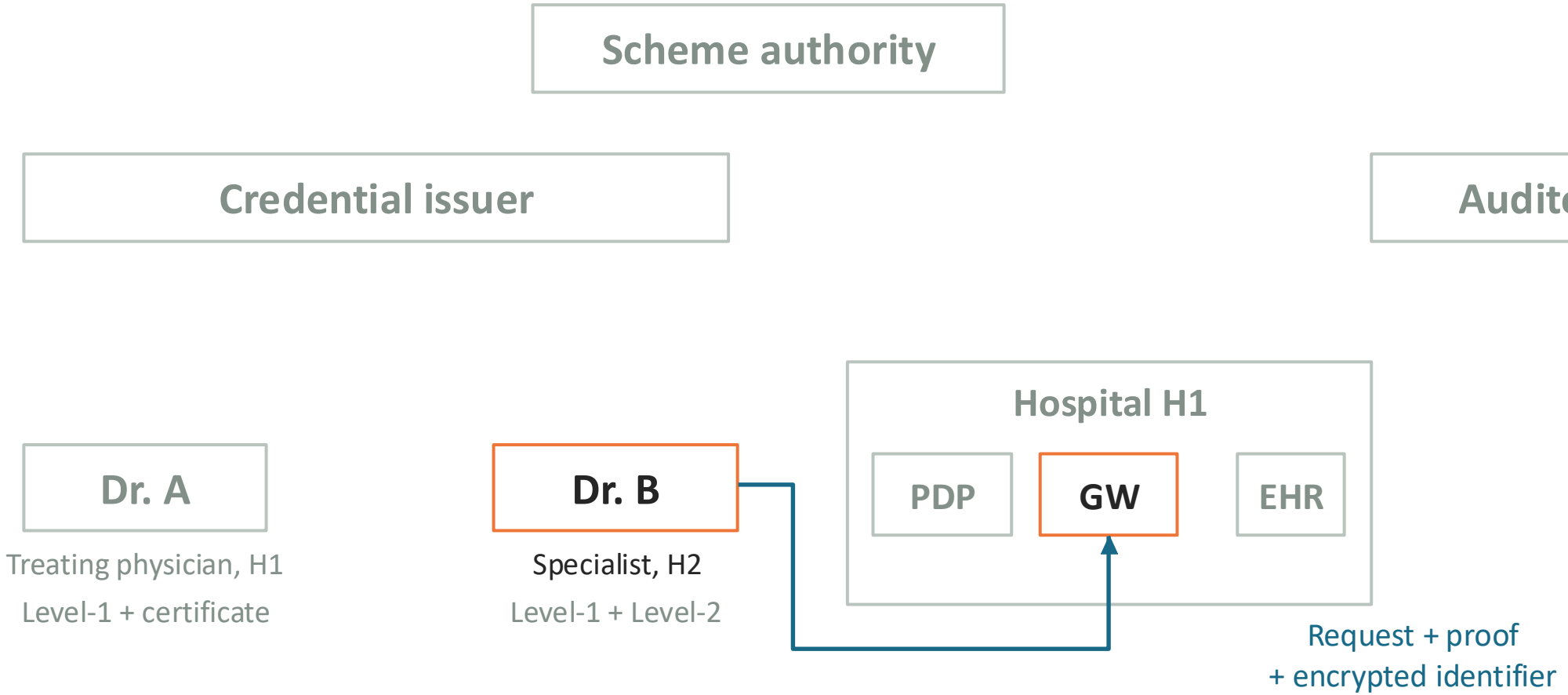
- Dr. A signs a Level-2 credential bound to Dr. B and the hospital's approval
- Dr. B checks it and keeps it alongside the original Level-1 credential

Delegated credential contents



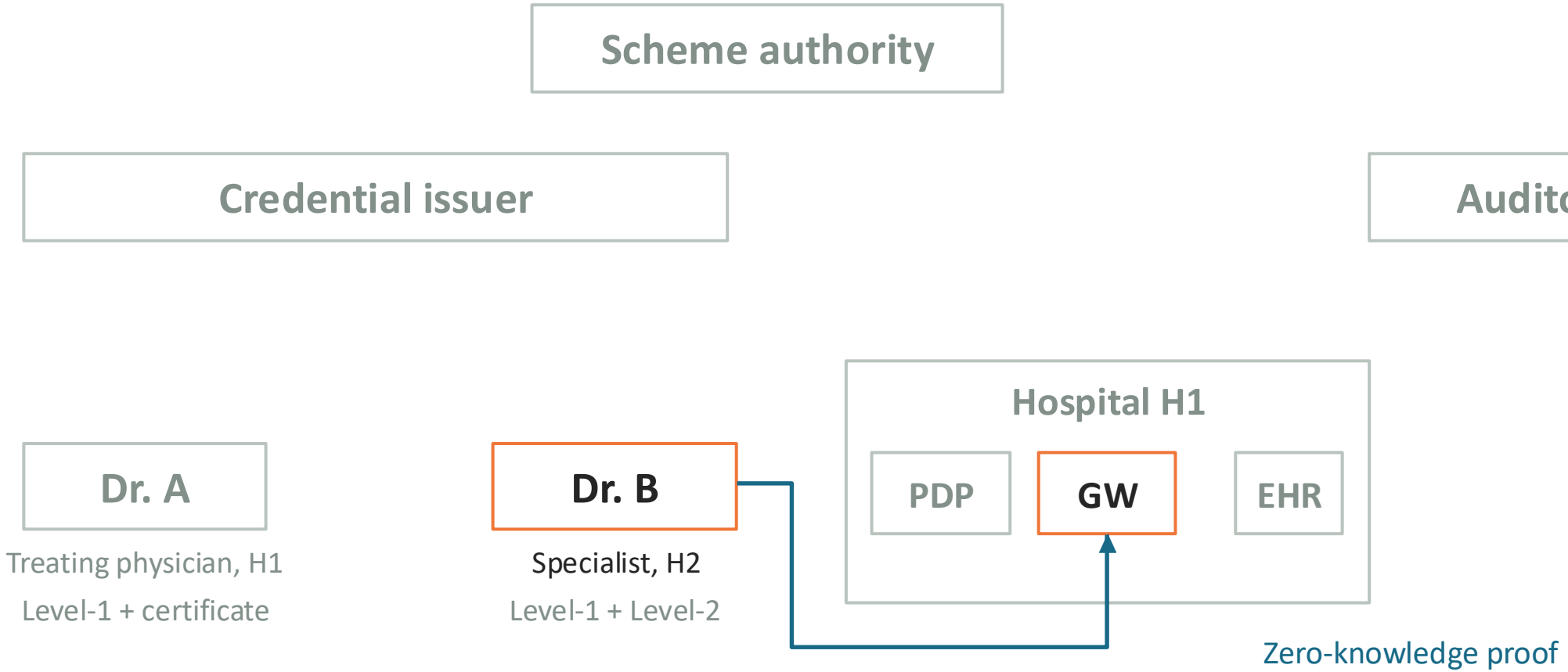
- **Recipient:** Dr. B's identifier and public key
- **Access limits:** patient case, hash of permitted data categories and expiry
- **Approval binding:** hash of the signed hospital authorisation token

What Dr. B sends



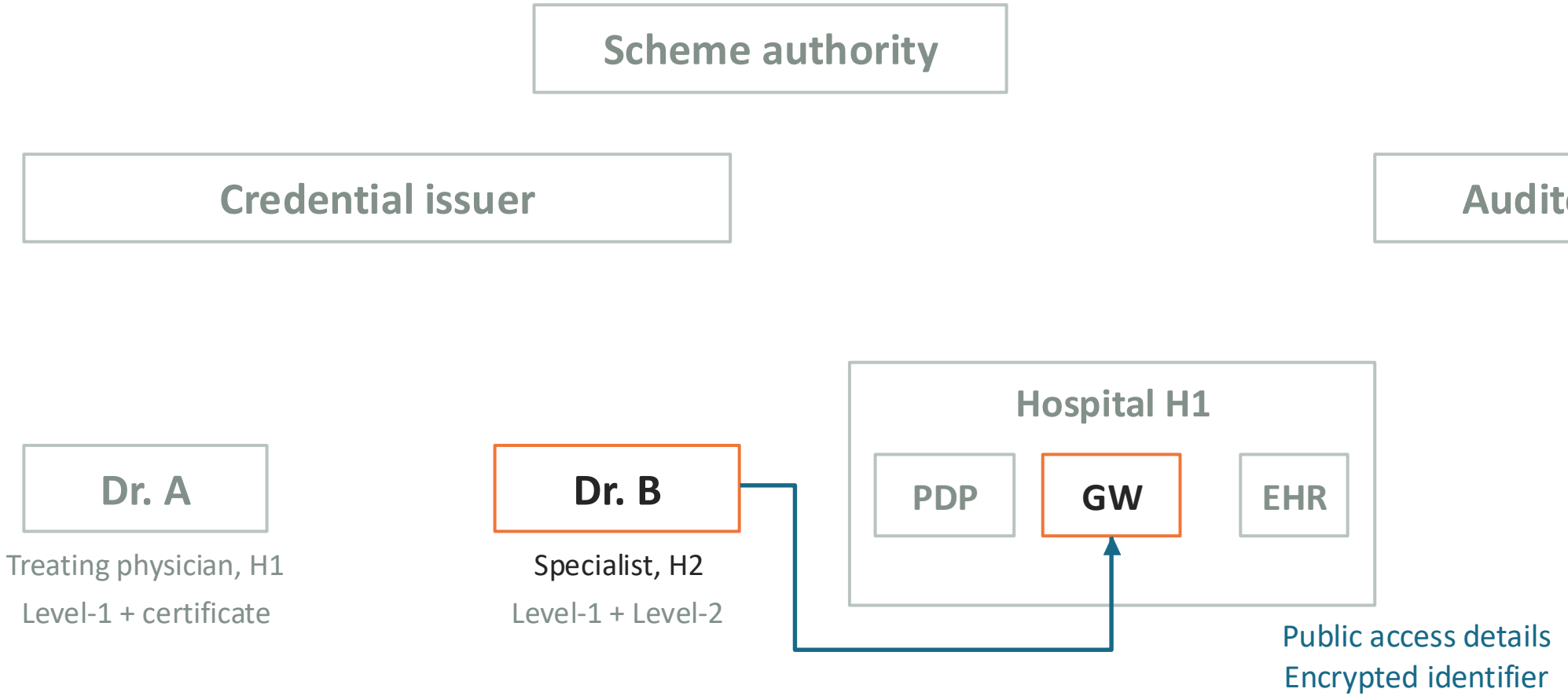
- **Request:** case, requested category, permitted category set, expiry and timestamp
- **Signed hospital approval**, including purpose and Dr. A's public key
- **Zero-knowledge proof** and Dr. B's identifier **encrypted for the auditor**

What the proof establishes



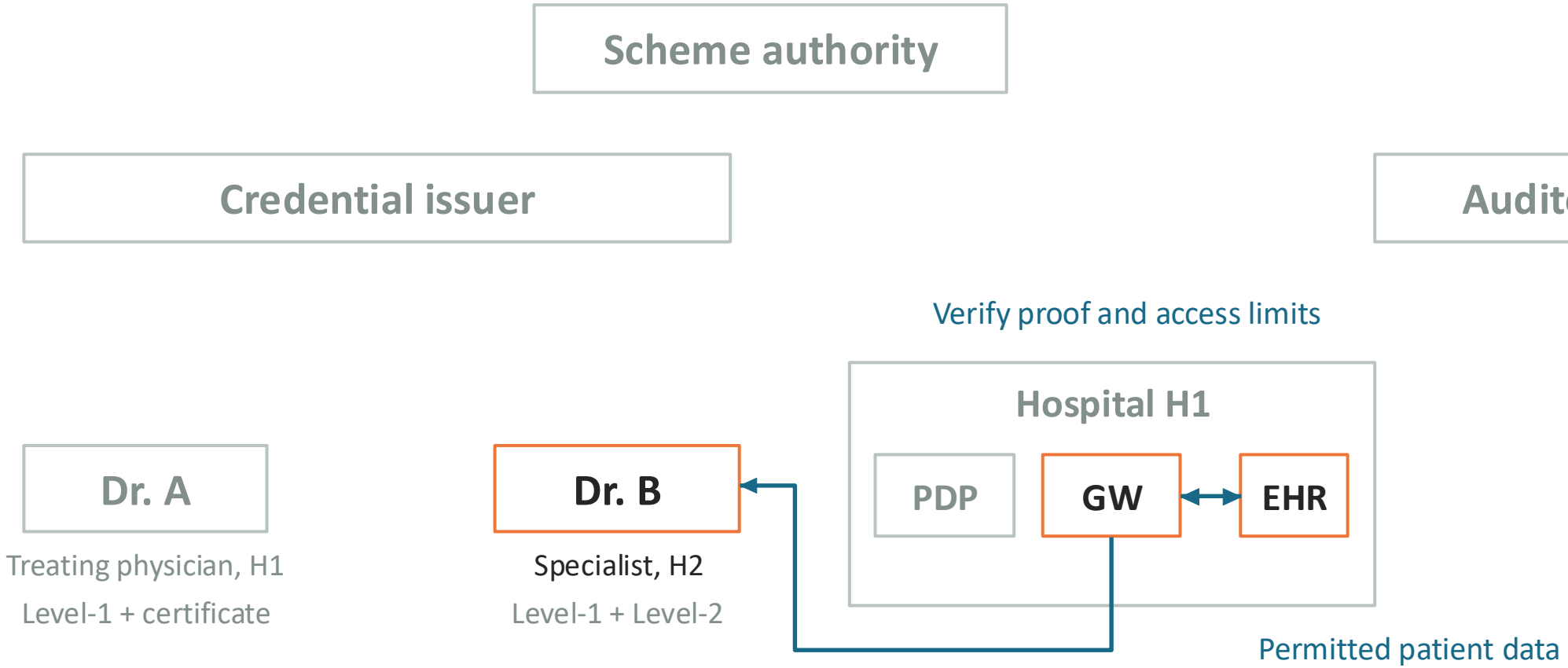
- **Valid clinician credential** and knowledge of Dr. B's credential secret
- **Valid delegation** for the same key, matching hospital approval and access limits
- **Same identifier** in Dr. B's own credential, the delegation and the encrypted identifier

What the gateway can see



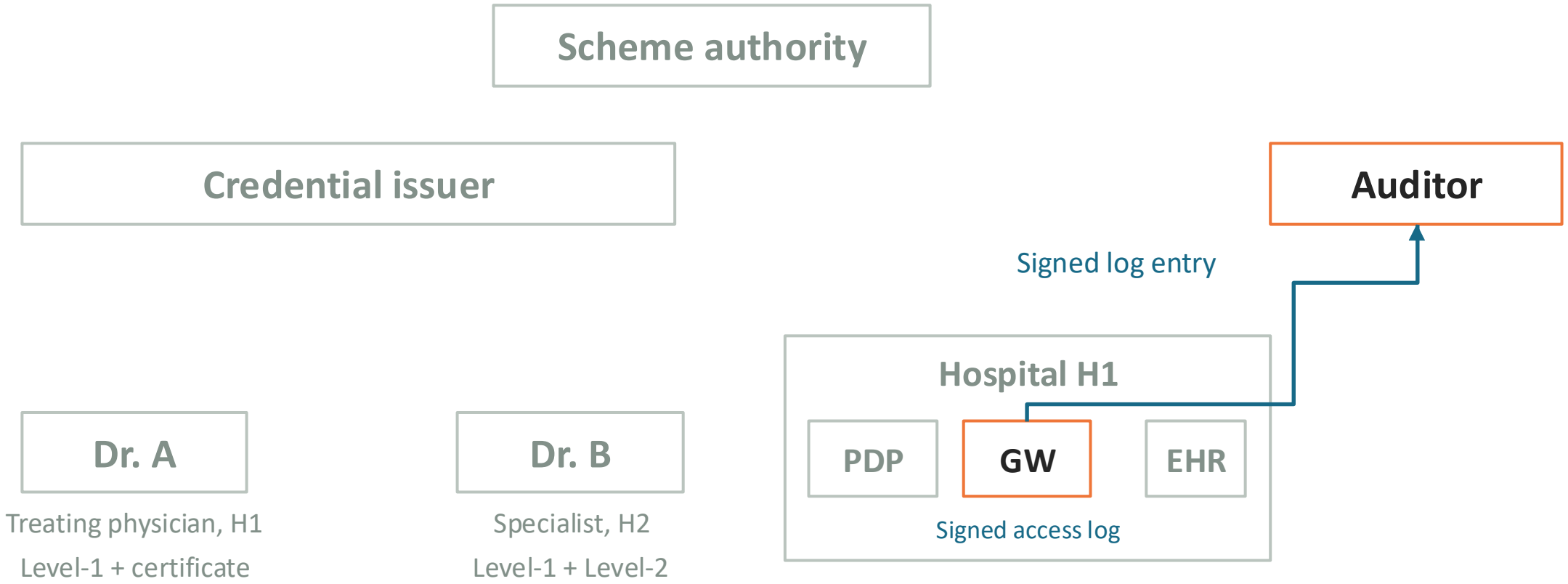
- **Visible:** case, requested category, permitted category set, expiry and access time
- Visible: approval token, purpose, Dr. A's key, proof and encrypted identifier
- **Hidden:** Dr. B's identifier, public key, secret key and credential signatures

Gateway checks and response



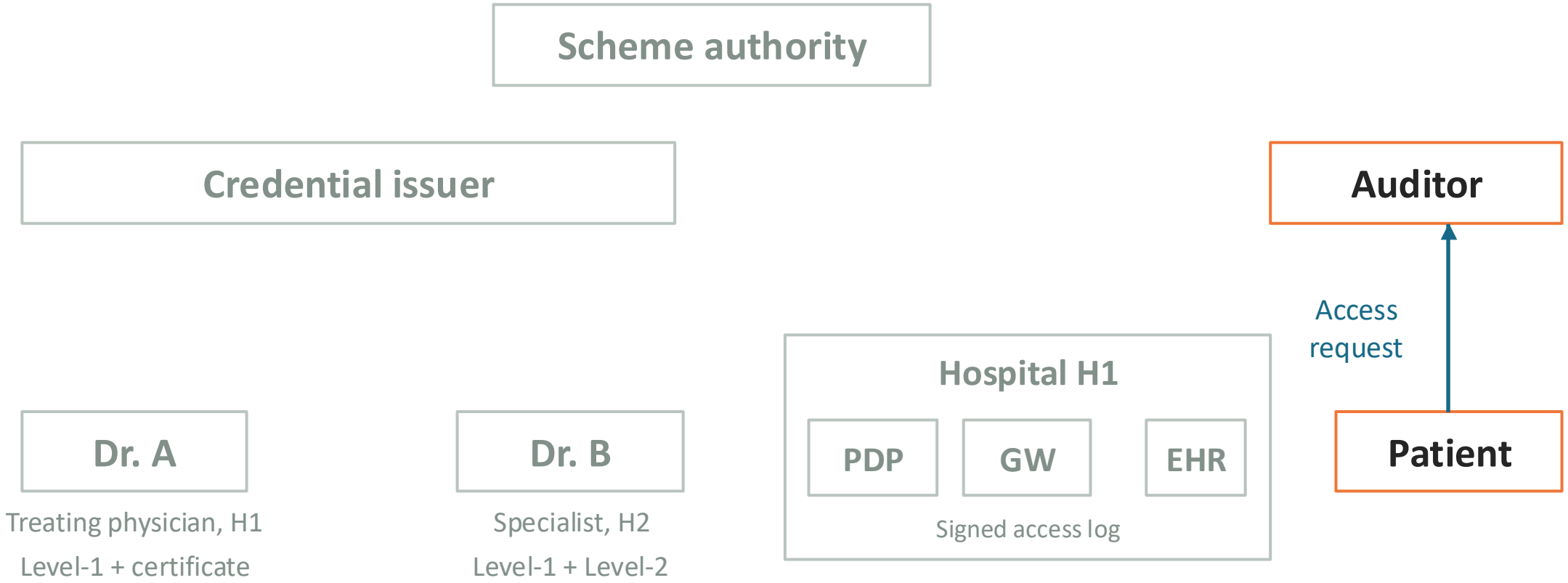
- **GW checks** the approval, permitted category, expiry, timestamp and replay protection
- GW **records the access** and returns only the **permitted patient data**

Access logging



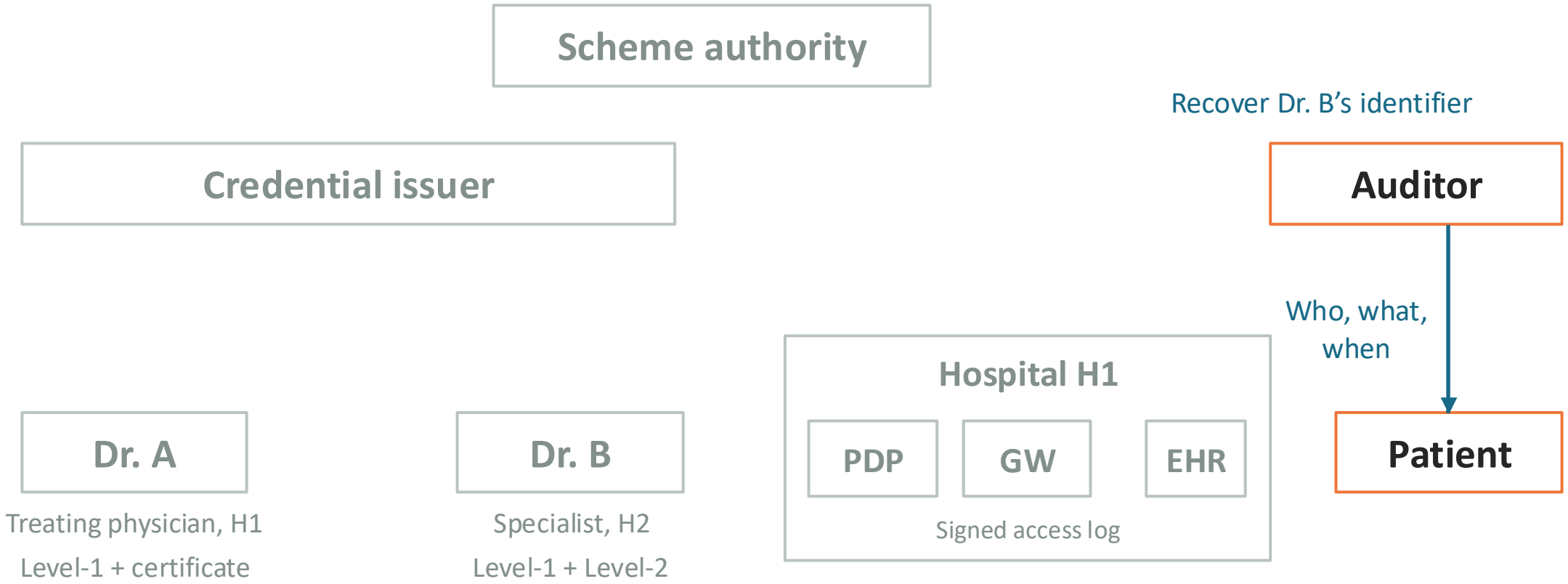
- GW signs a log entry containing the case, data category, time and encrypted identifier
- GW stores the entry and forwards it to the auditor

Patient transparency



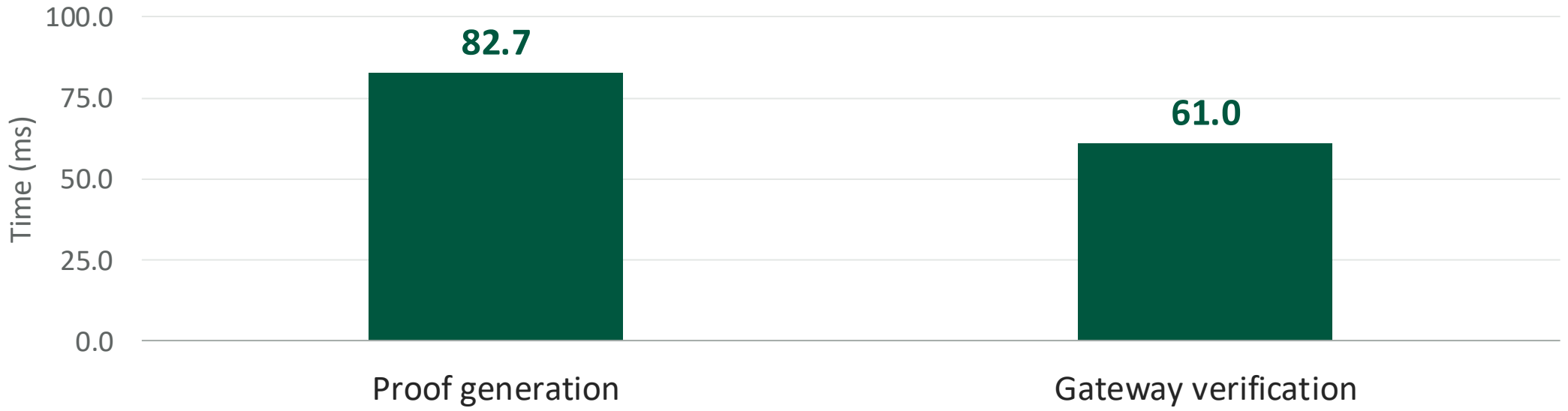
- The patient requests information about access to their records
- The auditor authenticates the patient and retrieves the relevant entries

Patient transparency



- Under the identity-resolution policy, the auditor decrypts Dr. B's identifier
- The patient receives who accessed which data, and when

Cost of the access proof



About 144 ms in total, with identity escrow accounting for about 90%

Discussion and open work

- What should patients see by default, and when should a doctor’s identity be resolved?
- Several independent approvals could reduce reliance on one auditor
- Formal security proof and a complete health-record prototype remain future work

Conclusion

- Consult access combines professional eligibility with **explicit case authorisation**
- The proof **binds the accessing specialist's identity** to the encrypted audit record
- The design joins minimal routine disclosure with a patient-facing path to accountability

Conclusion

- Consult access combines professional eligibility with **explicit case authorisation**
- The proof **binds the accessing specialist's identity** to the encrypted audit record
- The design joins minimal routine disclosure with a patient-facing path to accountability

Thank you!

Questions & Discussions