Privacy-Enhancing Technologies:
Anonymous Credentials and Pseudonym Systems

Anja Lehmann
IBM Research – Zurich

IBM

ROADMAP

Privacy-Enhancing Credentials

Privacy Attribute-Based Credential (P-ABCs)

Privacy-ABCs

Privacy-Preserving Credentials

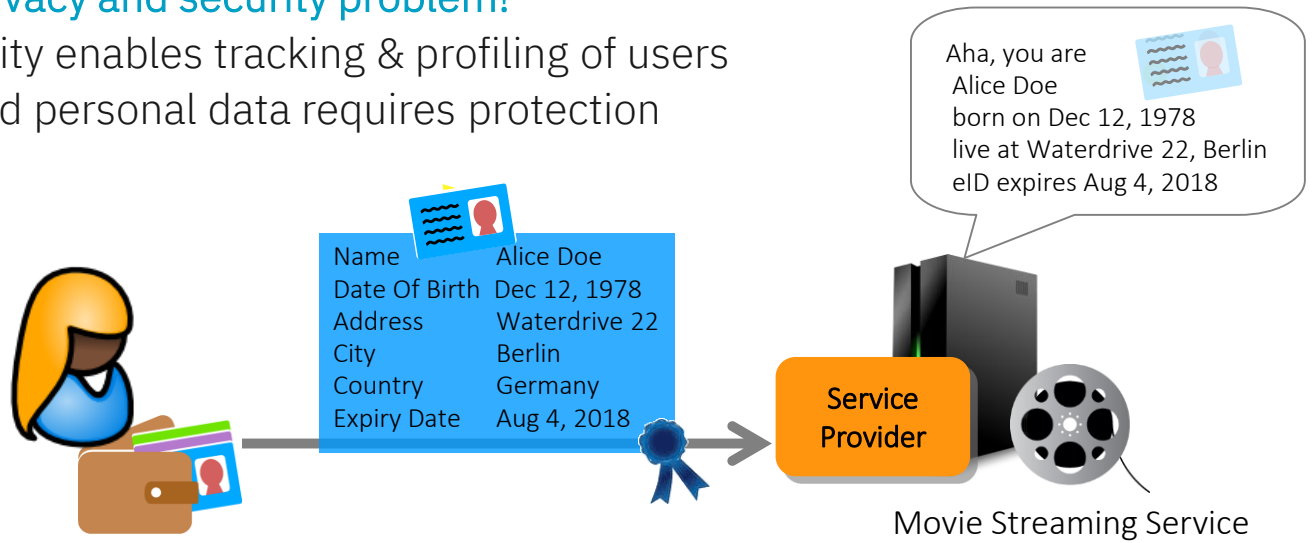
- Anonymous Credentials
  – privacy-preserving (user) authentication
- Pseudonym Systems
  – privacy-preserving & auditable data exchange

Strong User Authentication

- Strong (user) authentication via certificates / attribute-based credentials
  - Many European countries have or will introduce eID cards
  - Desirable for security, but detrimental for privacy
  - Existing schemes require full information disclosure & user is linkable in all transactions

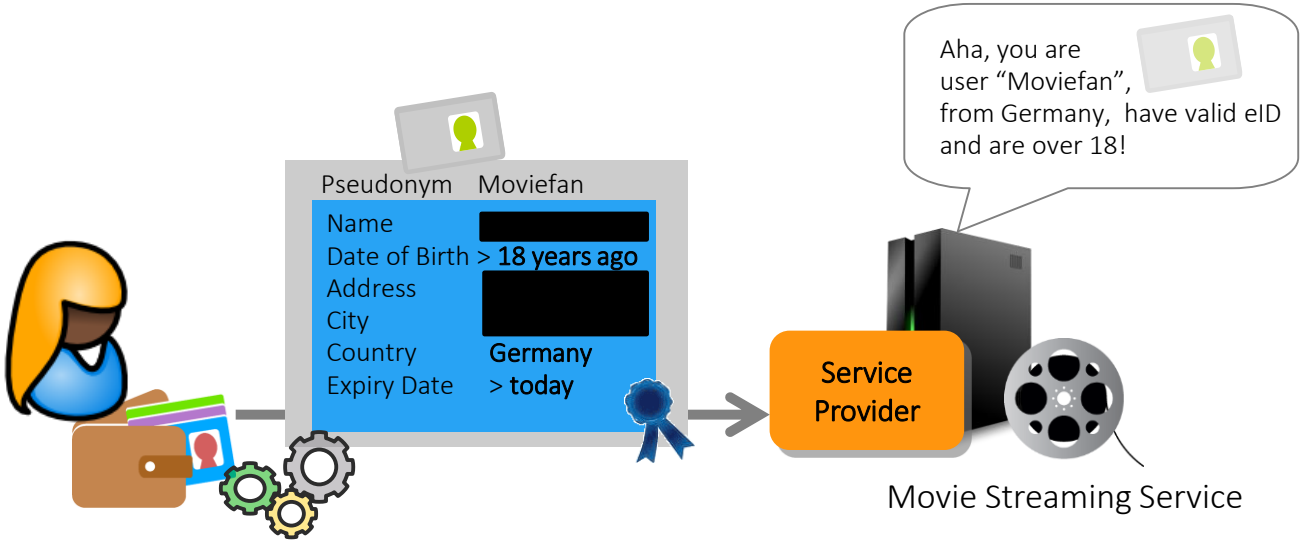
→ This is a privacy and security problem!

  - Linkability enables tracking & profiling of users
  - Acquired personal data requires protection



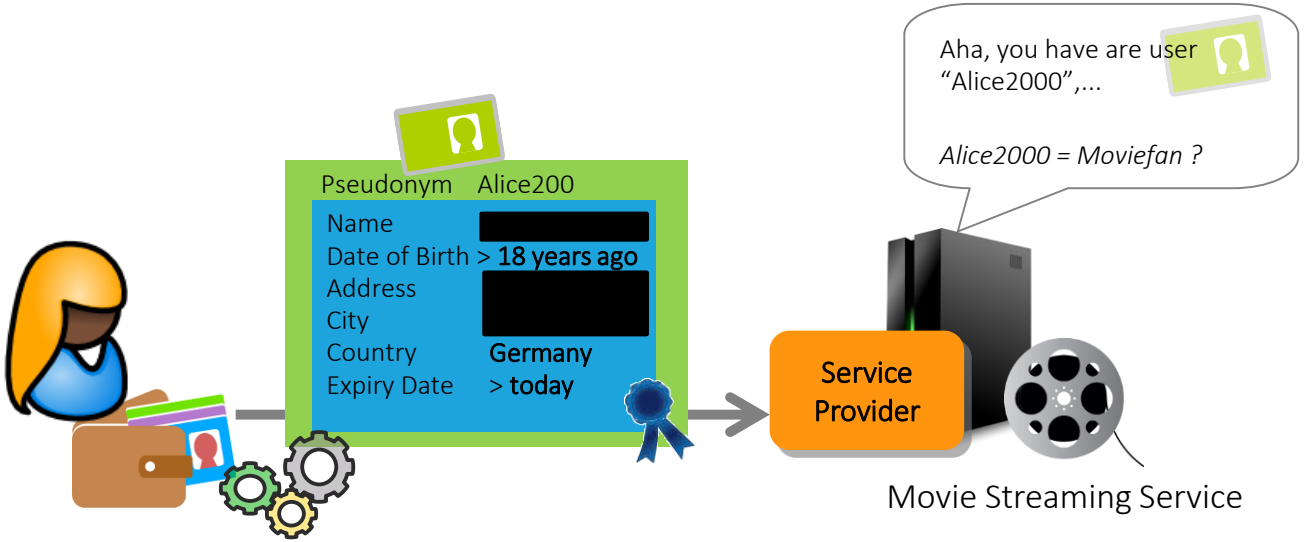
Strong & Privacy-Preserving User Authentication

- Envisioned by Chaum in 1981, first full scheme by Camenisch & Lysyanskaya in 2001
  - User can selectively disclose each attribute
  - User can prove predicates over the attributes, e.g., “I'm over 18”
  - Unlinkable authentication as default, linkability as an option



Strong & Privacy-Preserving User Authentication

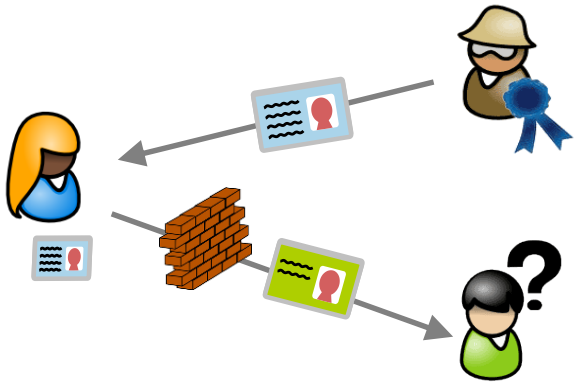
- Envisioned by Chaum in 1981, first full scheme by Camenisch & Lysyanskaya in 2001
  - User can selectively disclose each attribute
  - User can prove predicates over the attributes, e.g., “I'm over 18”
  - Unlinkable authentication as default, linkability as an option



Privacy-Enhancing Credentials | Existing Solutions

- Most prominent core-credential/signature schemes:

Identity Mixer (IBM)

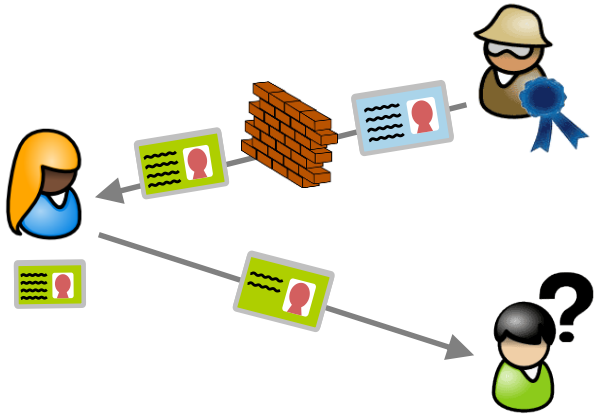


Multi-use credentials

Zero-Knowledge Proofs

Strong RSA, pairings (LRSW, qSDH)

U-Prove (Microsoft)



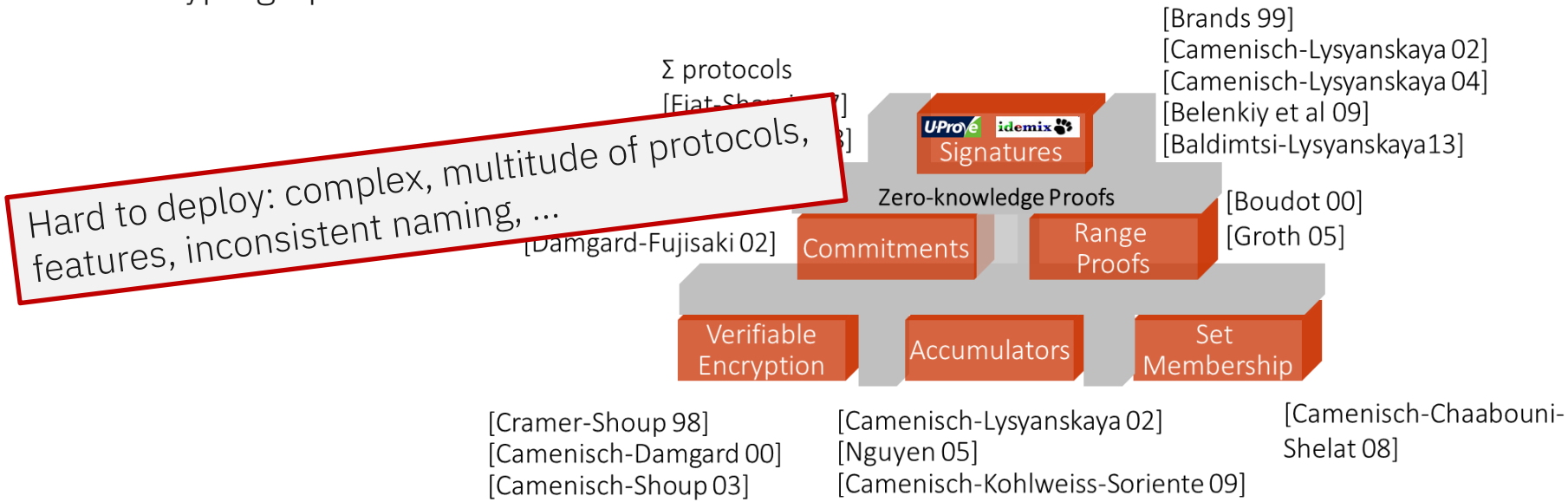
One-time use credentials
(multi-use via batch-issuance)

Blind Signatures

RSA, DL

Privacy-Enhancing Credentials | Extended Features

- Many more extensions & properties:
  - Revocation, multi-credential proofs, issuance with carry-over attributes, conditional disclosure, „symmetric“ credentials
- Various cryptographic realizations

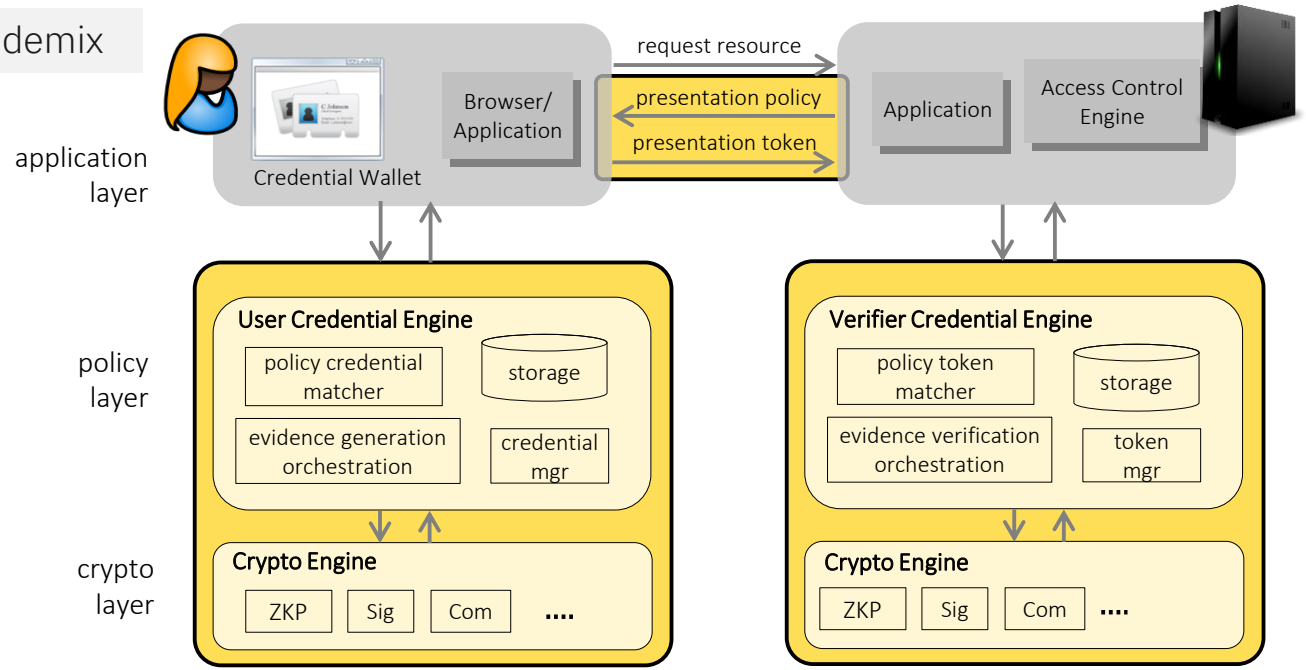


Privacy-Enhancing Credentials | Generic Framework

ABC4Trust (EU project)

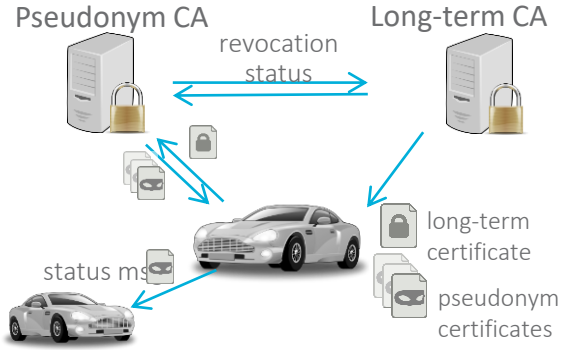
- Technology-independent & „easy-to-use“ framework
  - Comprehensive & standardized language framework
  - Technology-agnostic credential & policy handling on top of crypto engine
  - Generic, automated crypto engine

www.zurich.ibm.com/idemix



Privacy-Enhancing Credentials | New Applications

- V2X communication (vehicles (V2V) and infrastructure (V2I))
  - Security needs: authentication & privacy
  - Current approach: pseudonym CA
  - Privacy-credentials fit perfectly! (almost)



- Hardware-based device/user attestation (DAA)
  - Draft for FIDO standard
  - FIDO ("Fast IDentity Online") Alliance
    = industry consortium developing standardized strong user/device authentication

- Blockchain: “eternal” and public transaction ledger
  - Privacy credentials needed to avoid privacy nightmare
  - Identity Mixer being integrated into Hyperledger Fabric
  - IBM joined the Sovrin Foundation – decentralized digital identity network

HYPERLEDGER

ROADMAP

- Anonymous Credentials
  – privacy-preserving (user) authentication

Privacy-Enhancing Credentials

Privacy Attribute-Based Credential (P-ABCs)

Privacy-Preserving Credentials

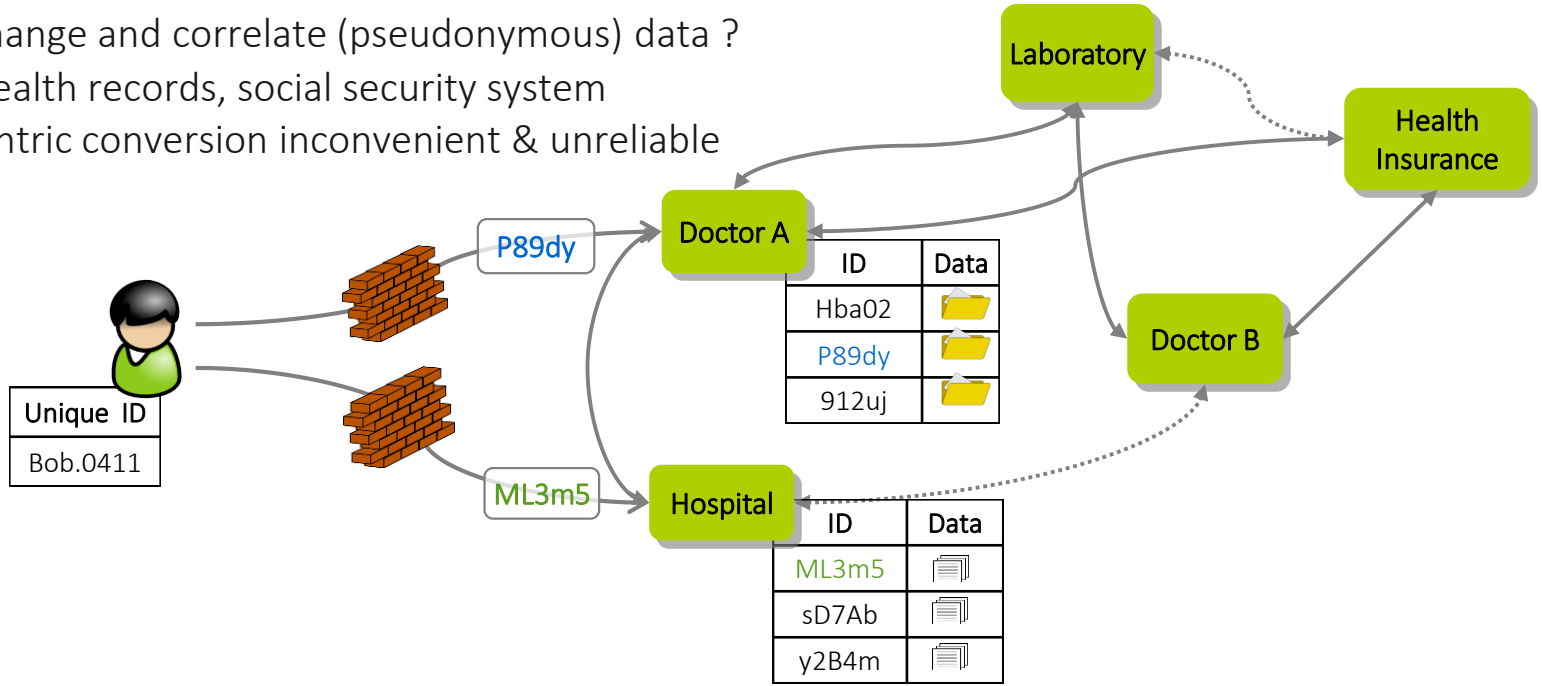
Privacy-ABCs

- Pseudonym Systems
  – privacy-preserving & auditable data exchange

[CL15] Camenisch, Lehmann. *(Un)linkable Pseudonyms for Governmental Databases*. CCS15.
[CL17] Camenisch, Lehmann. *Privacy-Preserving User-Auditable Pseudonym Systems*. IEEE EuroSP17.

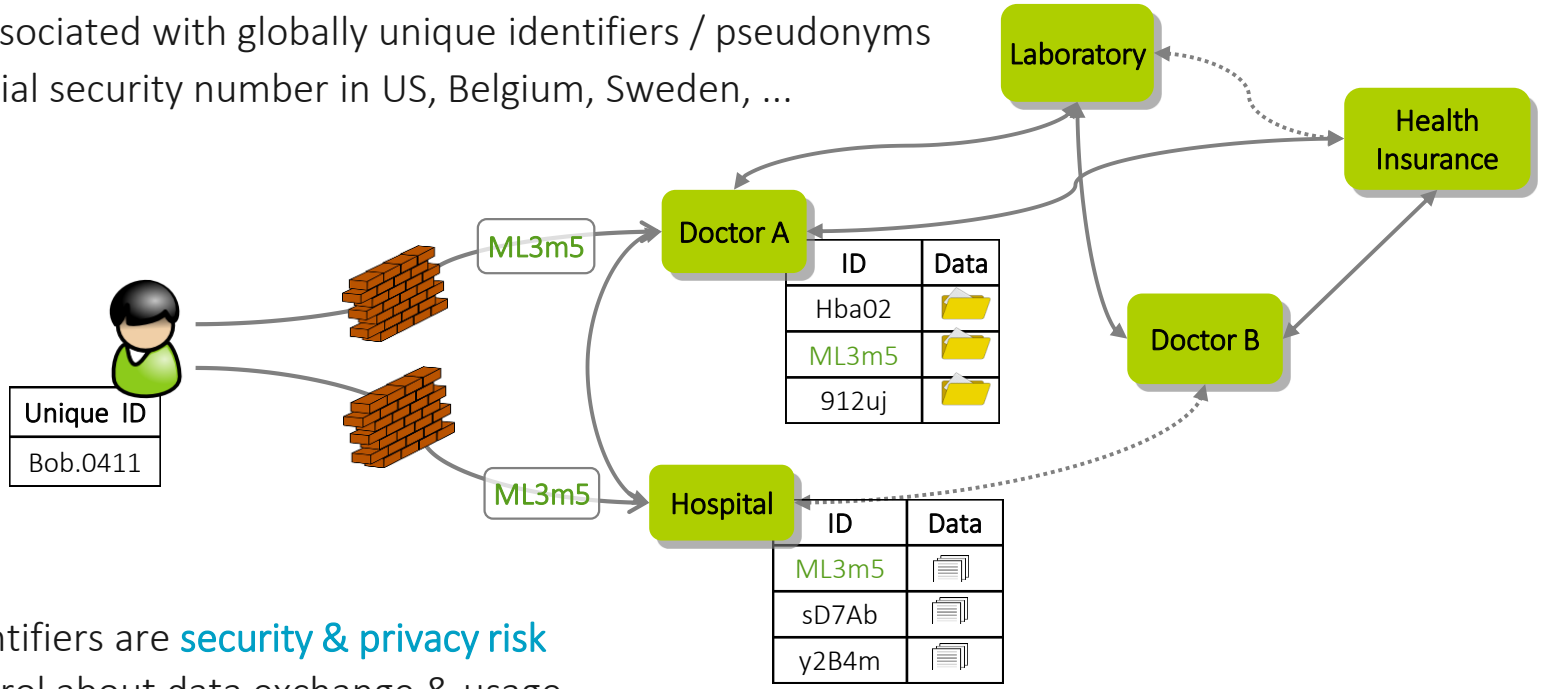
Pseudonym System | Motivation

- How to exchange and correlate (pseudonymous) data ?
  - E.g., eHealth records, social security system
  - User-centric conversion inconvenient & unreliable



Pseudonym System | Globally Unique Pseudonyms

- Data gets associated with globally unique identifiers / pseudonyms
  - E.g., social security number in US, Belgium, Sweden, ...

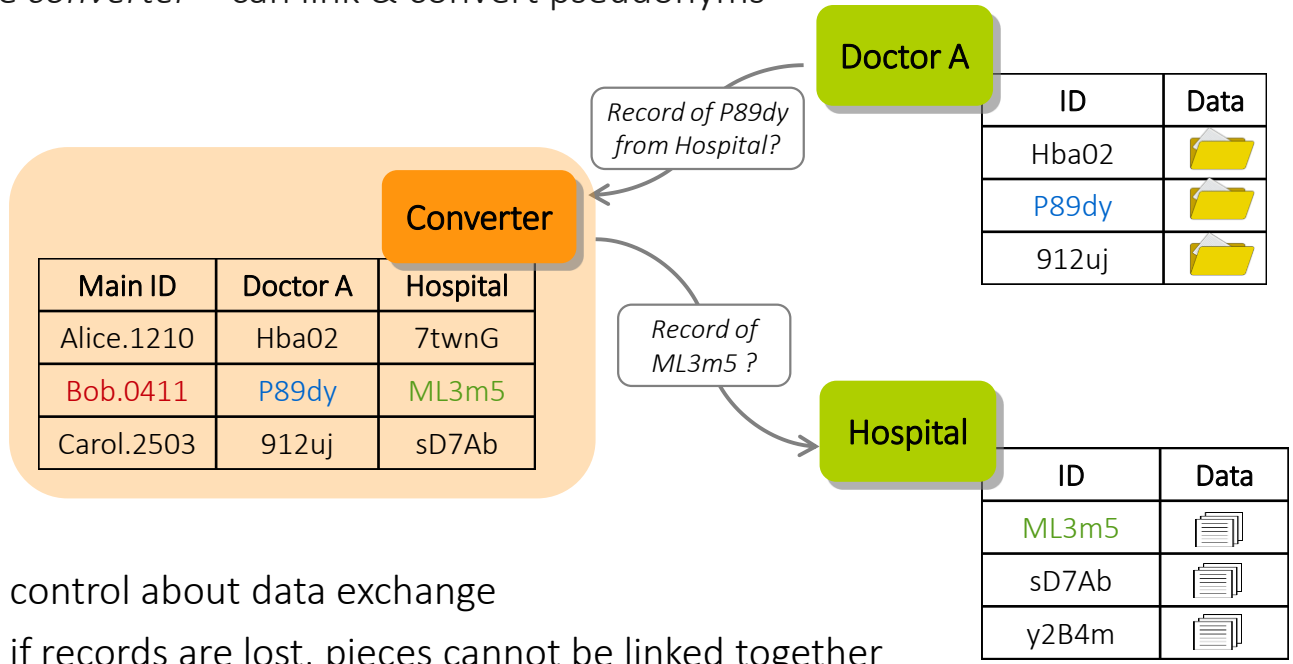


- Unique identifiers are security & privacy risk
  - no control about data exchange & usage
  - if associated data is lost, all pieces can be linked together
  - linkability of data allows re-identification of “anonymized” data (e.g. Netflix challenge)

Pseudonym System | Local Pseudonyms & *Trusted* Converter

- User data is associated with random looking local identifiers – the *pseudonyms*
- Only central entity – the *converter* – can link & convert pseudonyms

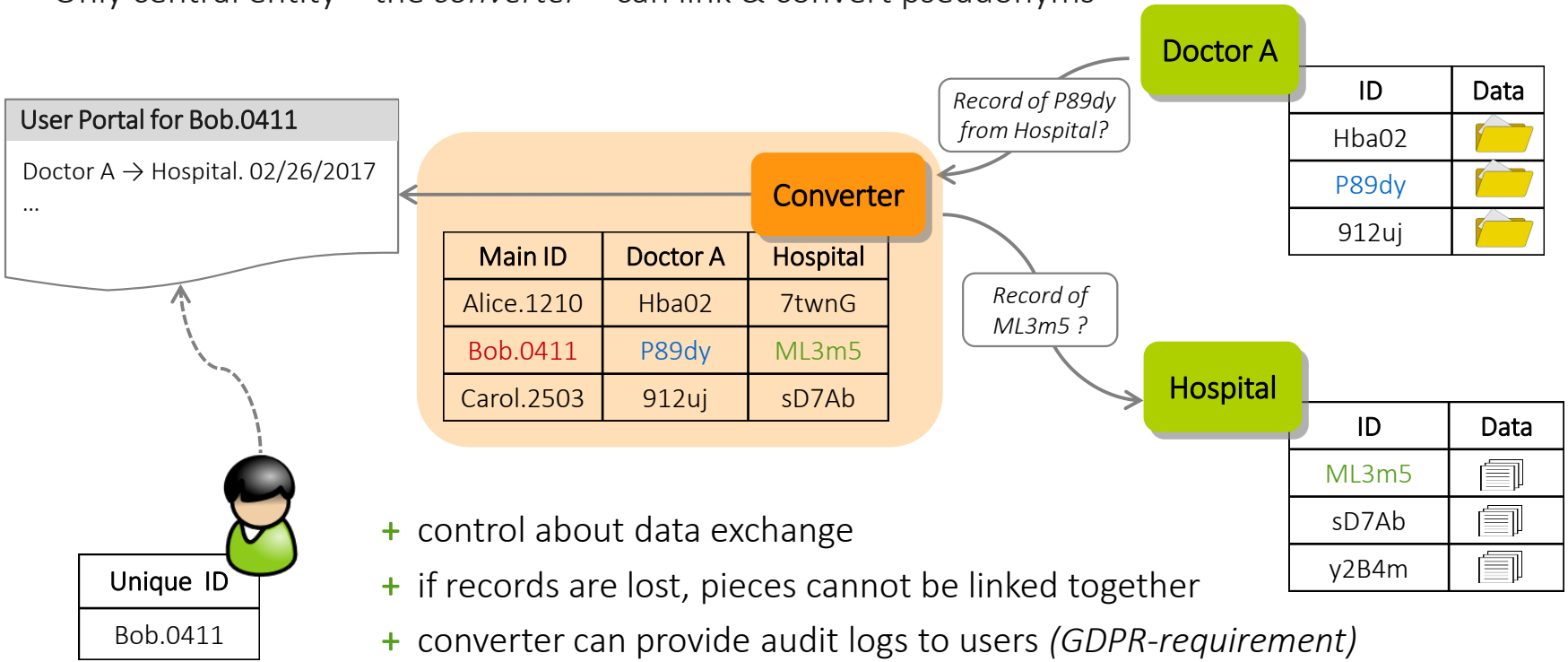
new Japan eID / social security number system (?)



+ control about data exchange
+ if records are lost, pieces cannot be linked together

Pseudonym System | Local Pseudonyms & *Trusted* Converter

- User data is associated with random looking local identifiers – the *pseudonyms*
- Only central entity – the *converter* – can link & convert pseudonyms



\+ control about data exchange

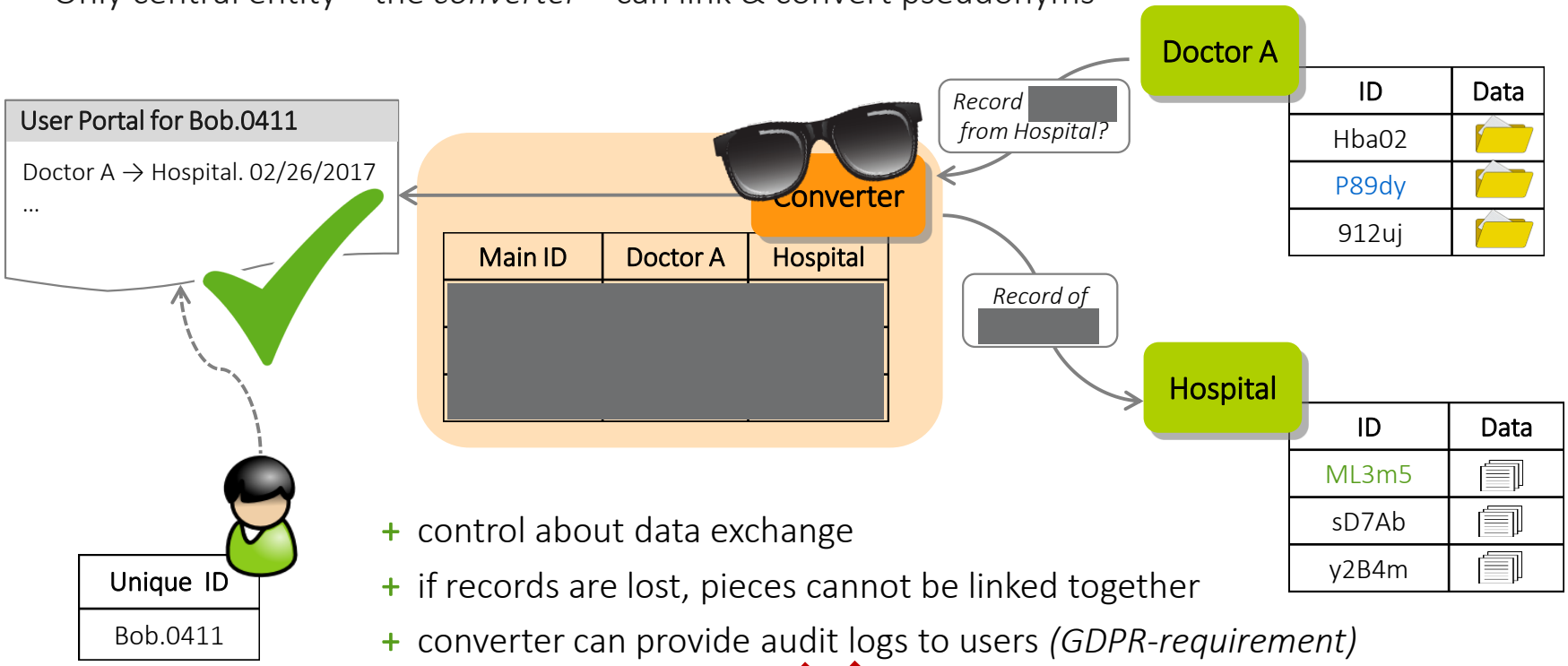
\+ if records are lost, pieces cannot be linked together

\+ converter can provide audit logs to users *(GDPR-requirement)*

– converter learns all request & knows all correlations

Pseudonym System | Local Pseudonyms & *Oblivious* Converter

- User data is associated with random looking local identifiers – the *pseudonyms*
- Only central entity – the *converter* – can link & convert pseudonyms



\+ control about data exchange

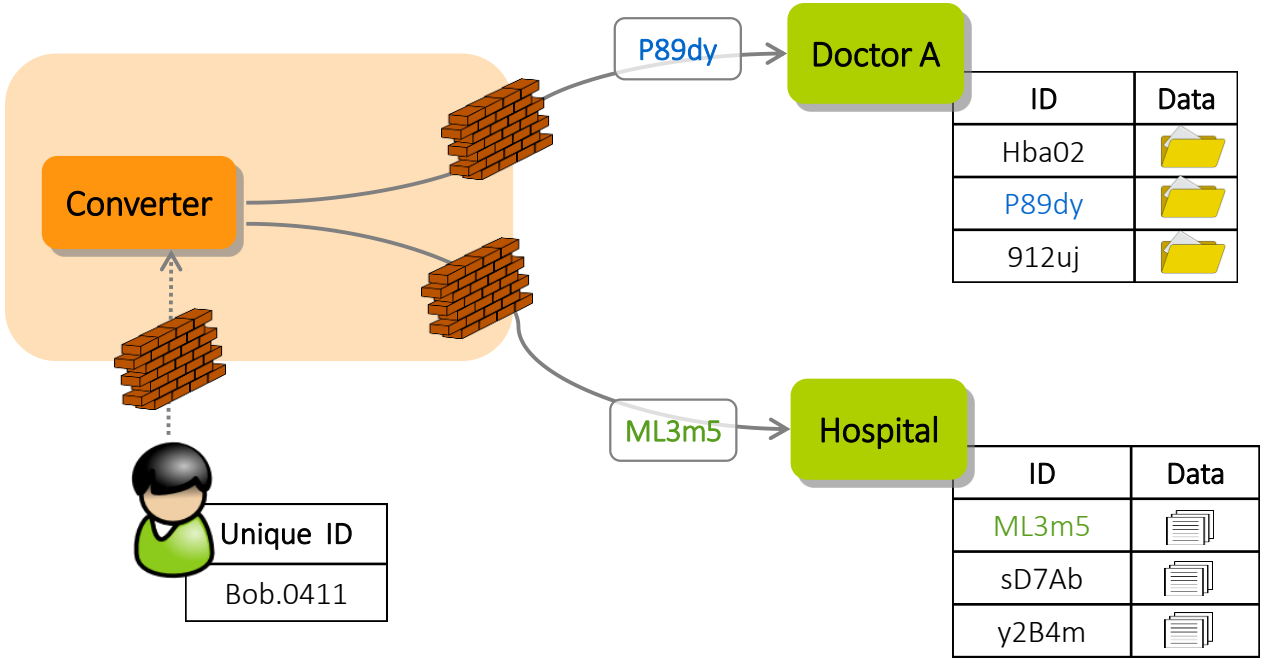
\+ if records are lost, pieces cannot be linked together

\+ converter can provide audit logs to users *(GDPR-requirement)*

– converter learns all requests & knows all correlations

(Un)linkable Pseudonyms | Pseudonym Generation

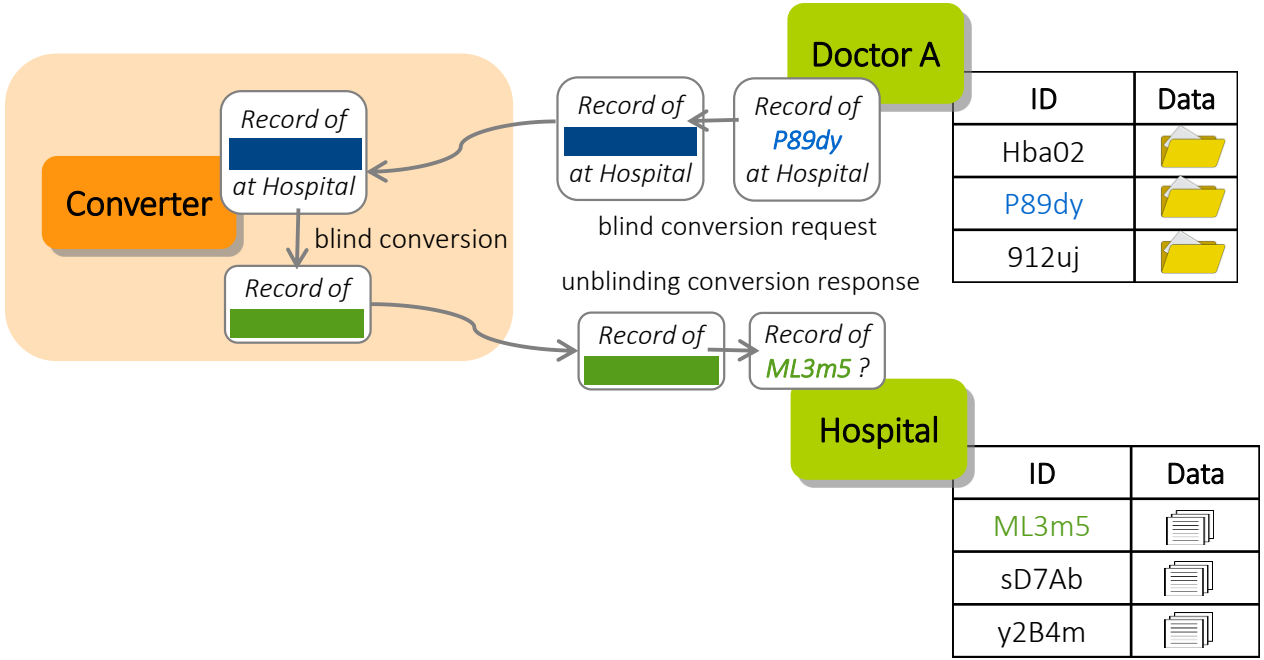
- User, converter & server jointly derive pseudonyms from unique identifiers



- [CL15] generation triggered by converter, knows unique IDs
- [CL17] oblivious pseudonym generation triggered by user

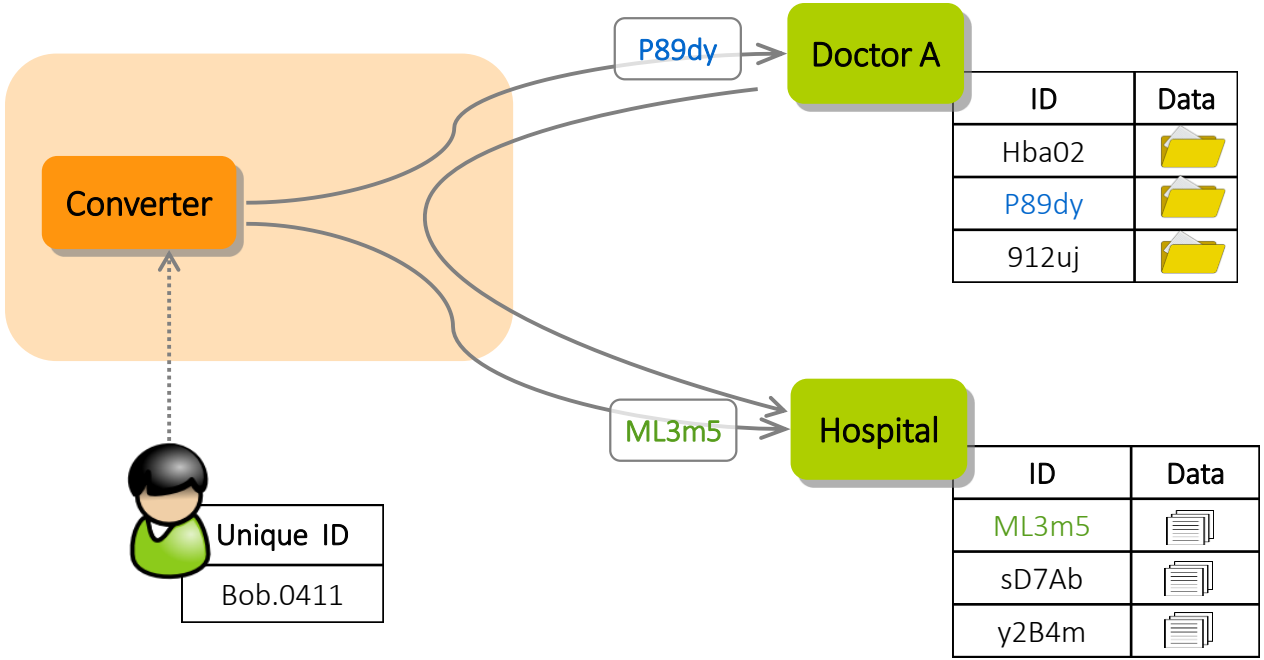
(Un)linkable Pseudonyms | Pseudonym Conversion

- Only converter can link & convert pseudonyms, but does so in a blind way



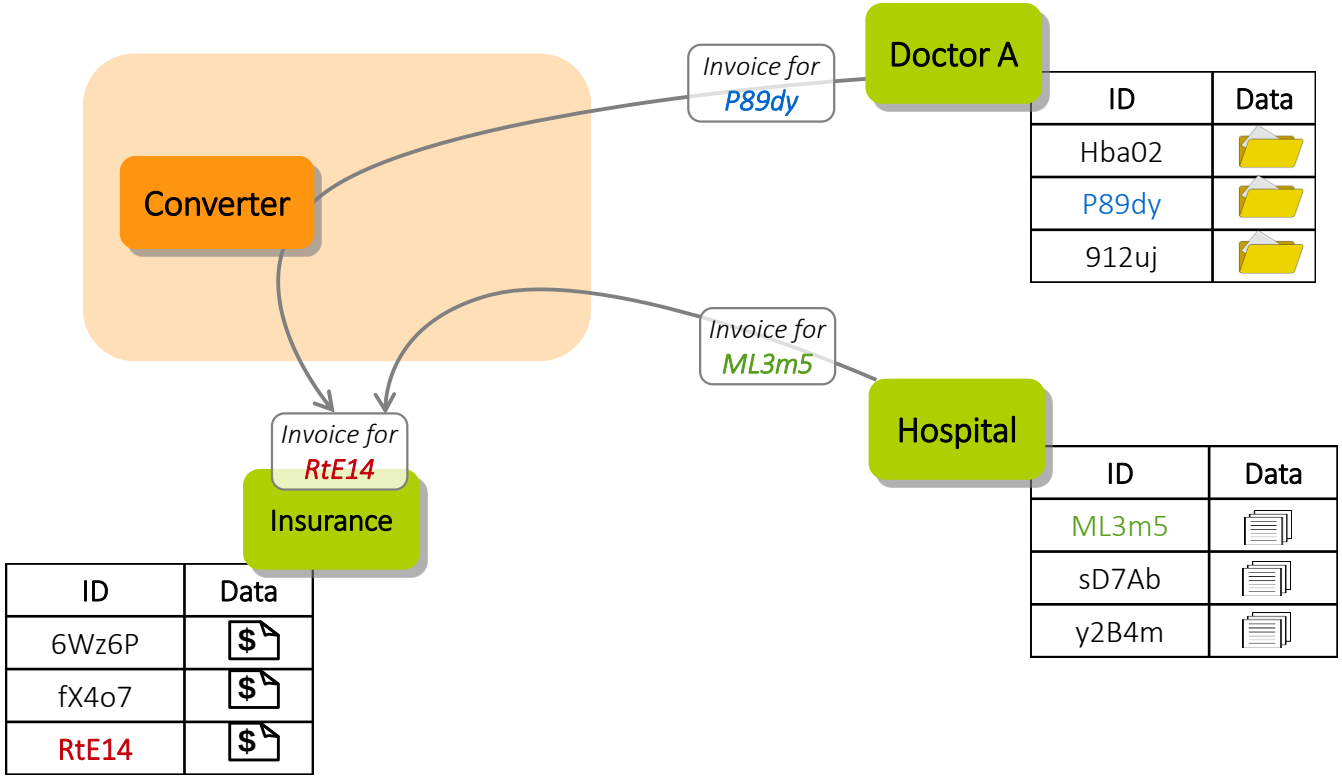
(Un)linkable Pseudonyms | Consistency

- pseudonym generation is deterministic & consistent with blind conversion



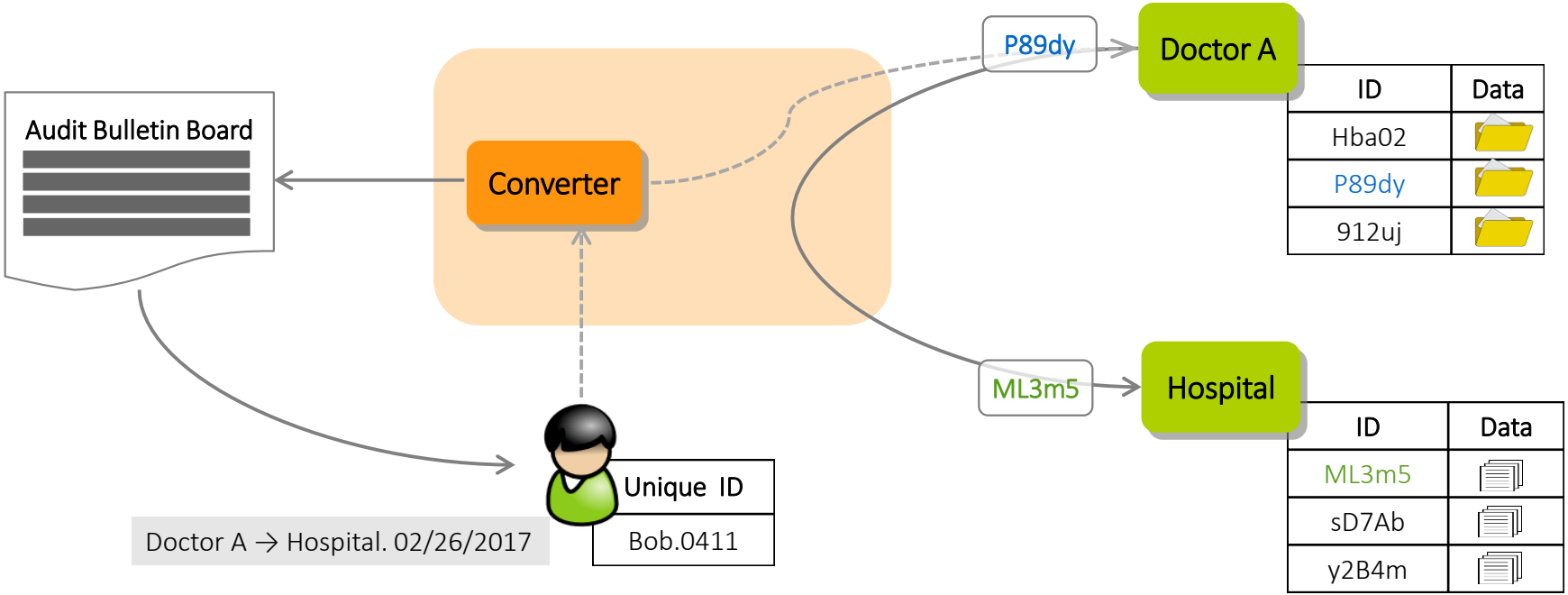
(Un)linkable Pseudonyms | Consistency

- pseudonym conversions are transitive, unlinkable data can be aggregated



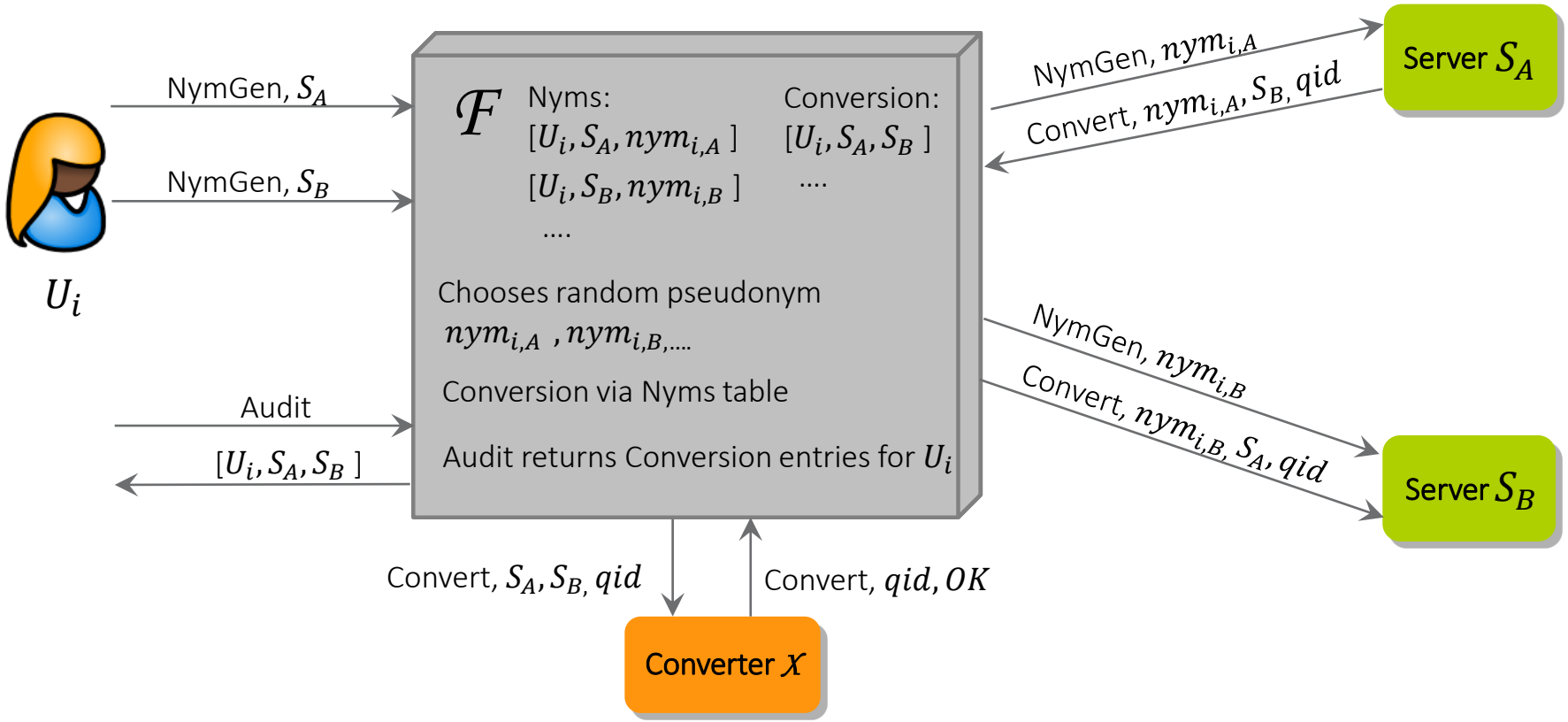
(Un)linkable Pseudonyms | User Audits

- [CL17] every pseudonym conversion triggers blind generation of audit log entry



(Un)linkable Pseudonyms | Security Model

- Universal composability (UC) model convenient & **simple** for privacy-preserving systems

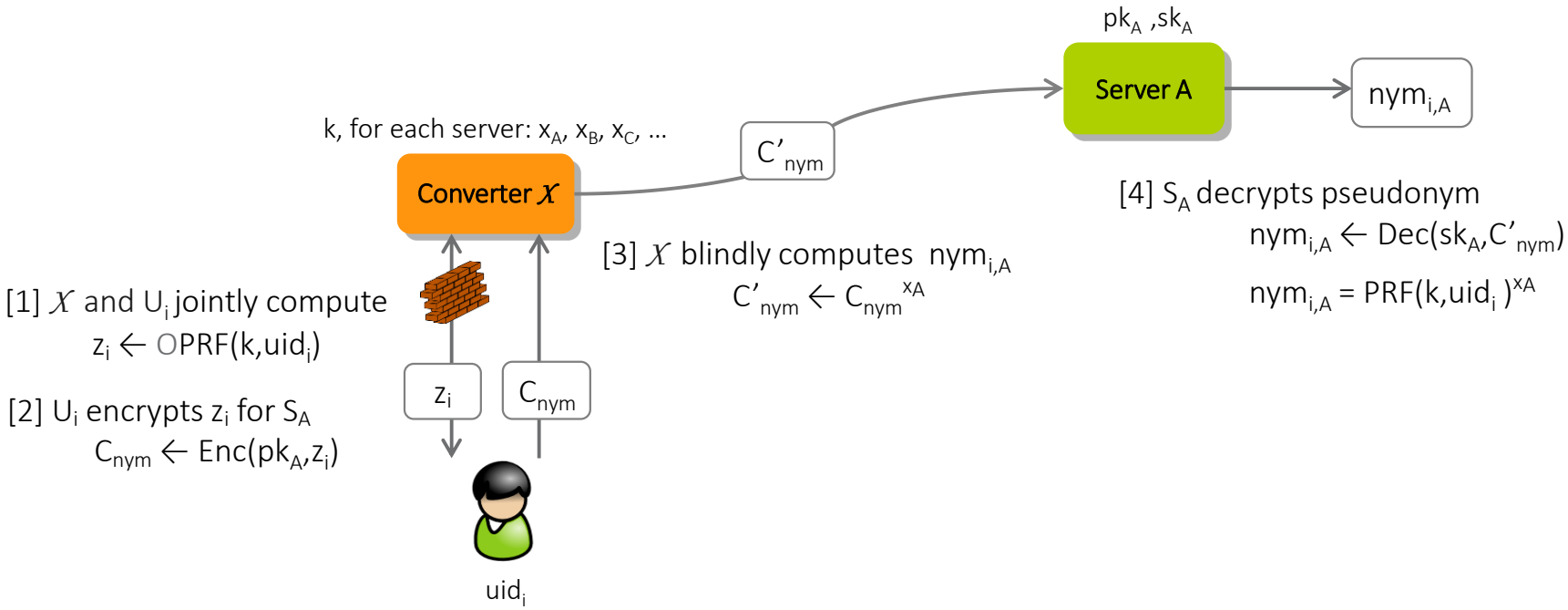


Our Protocol

- high-level idea of convertible pseudonyms
- adding (efficient) auditability
- security against active adversaries

High-level Idea | Pseudonym Generation

Core Idea
Generation: $\mathcal{X}$ blindly computes $nym_{i,A} \leftarrow PRF(k,uid_i)^{xA}$



High-level Idea | Pseudonym Conversion

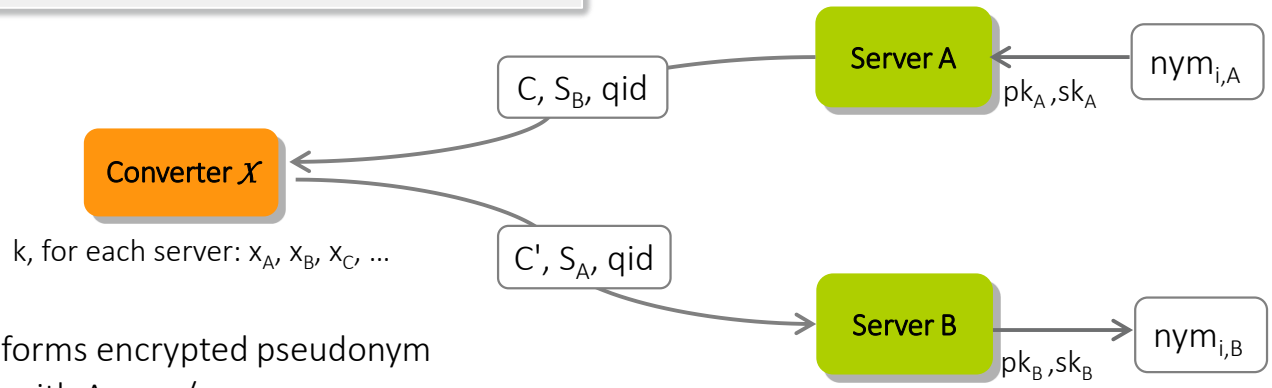
Core Idea

Generation: $\mathcal{X}$ blindly computes $nym_{i,A} \leftarrow PRF(k,uid_i)^{xA}$

Conversion: $\mathcal{X}$ blindly computes $nym_{i,B} \leftarrow nym_{i,A}^{xB\,/\,xA}$

[1] S_A encrypts $nym_{i,A}$ under S_B's key

$C \leftarrow Enc(pk_B, nym_{i,A})$



[2] $\mathcal{X}$ blindly transforms encrypted pseudonym

$C' \leftarrow C^{\Delta}$ with $\Delta = x_B / x_A$

$C' = Enc(pk_B, nym_{i,A})^{xB\,/\,xA}$

$= Enc(pk_B, PRF(k,uid_i)^{xA})^{xB\,/\,xA}$

$= Enc(pk_B, PRF(k,uid_i)^{xB})$

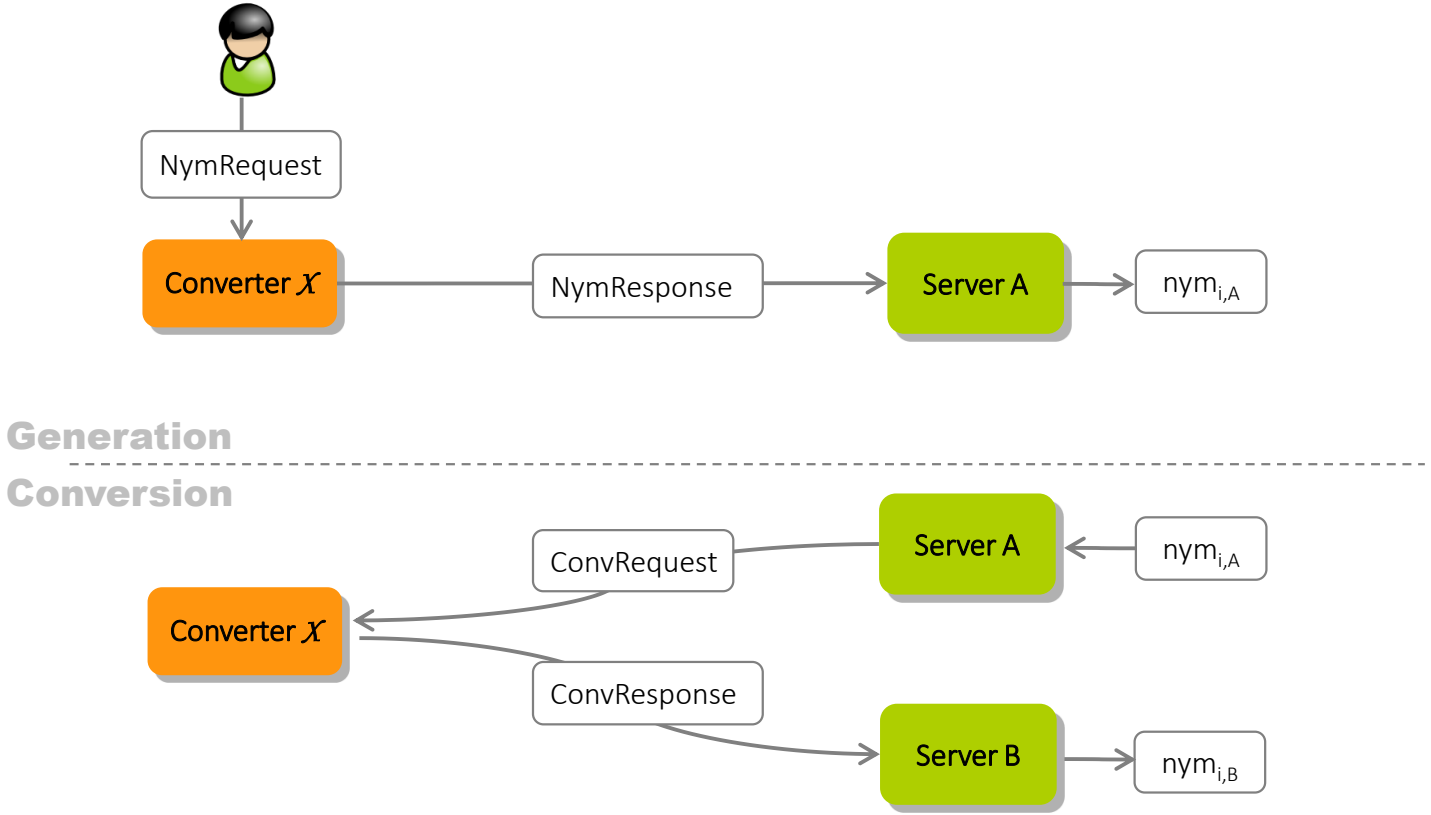
$= Enc(pk_B, nym_{i,B})$

[3] S_B decrypts converted pseudonym

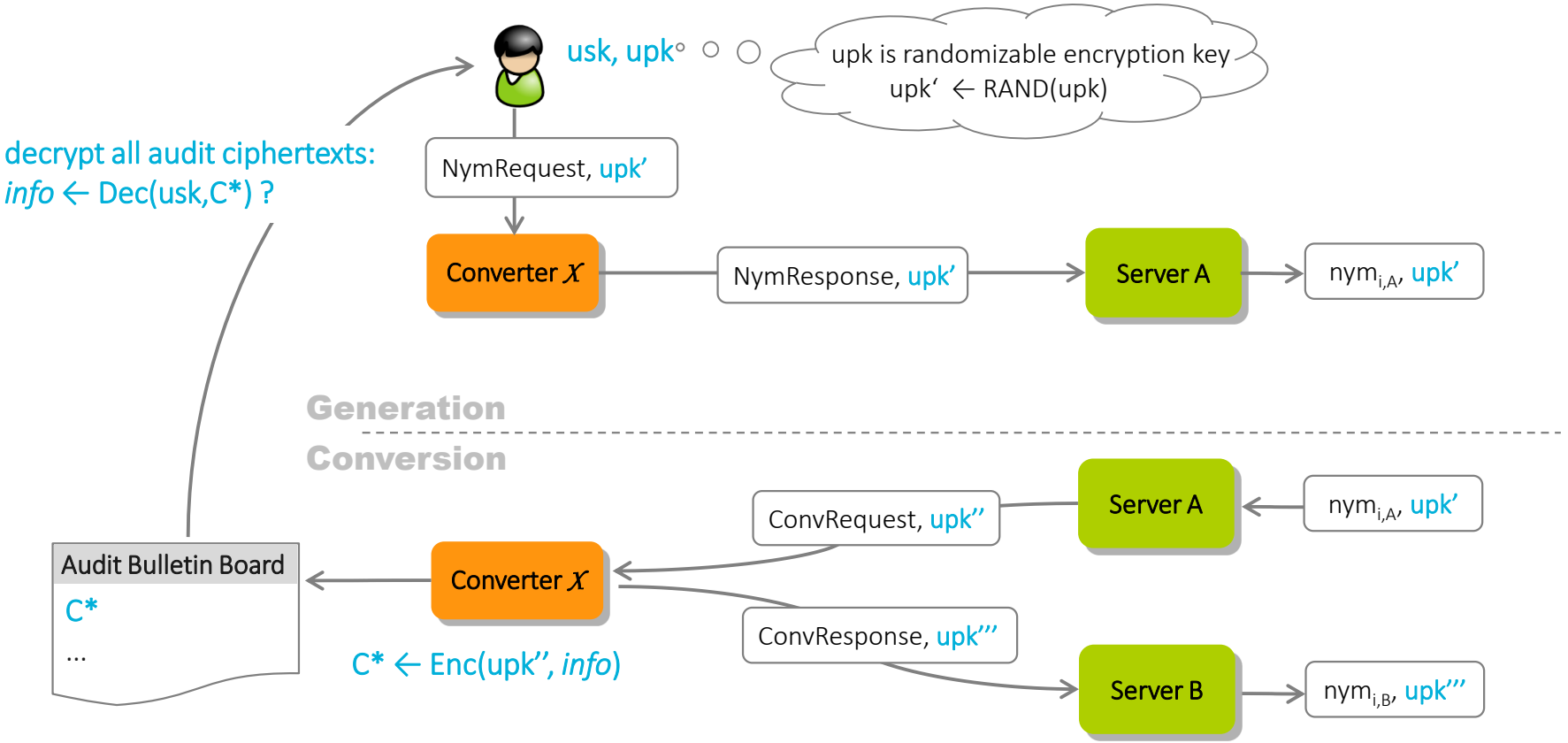
$nym_{i,B} \leftarrow Dec(sk_B, C')$

$nym_{i,B} = PRF(k,uid_i)^{xB}$

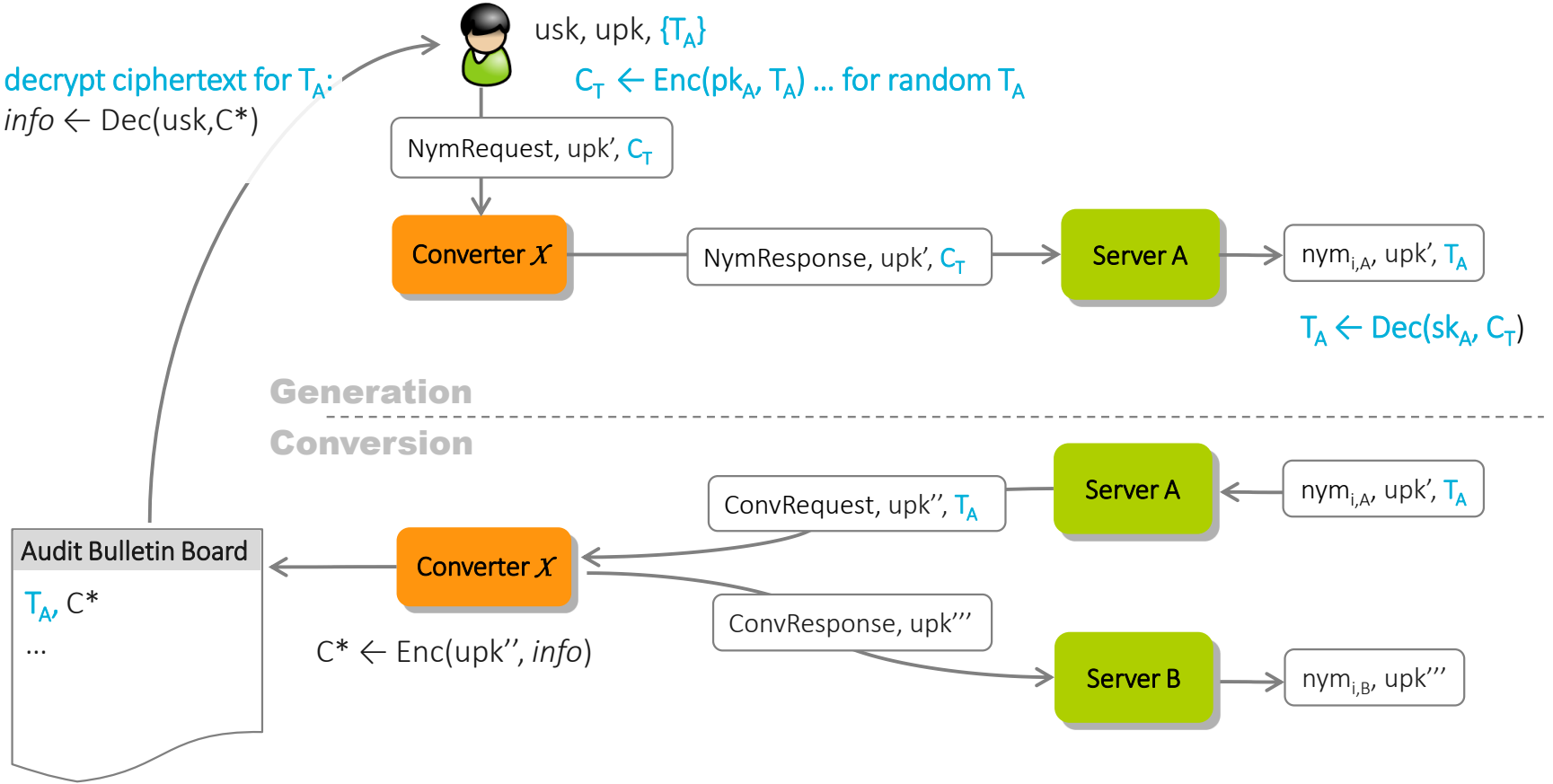
High-level Idea | Overview



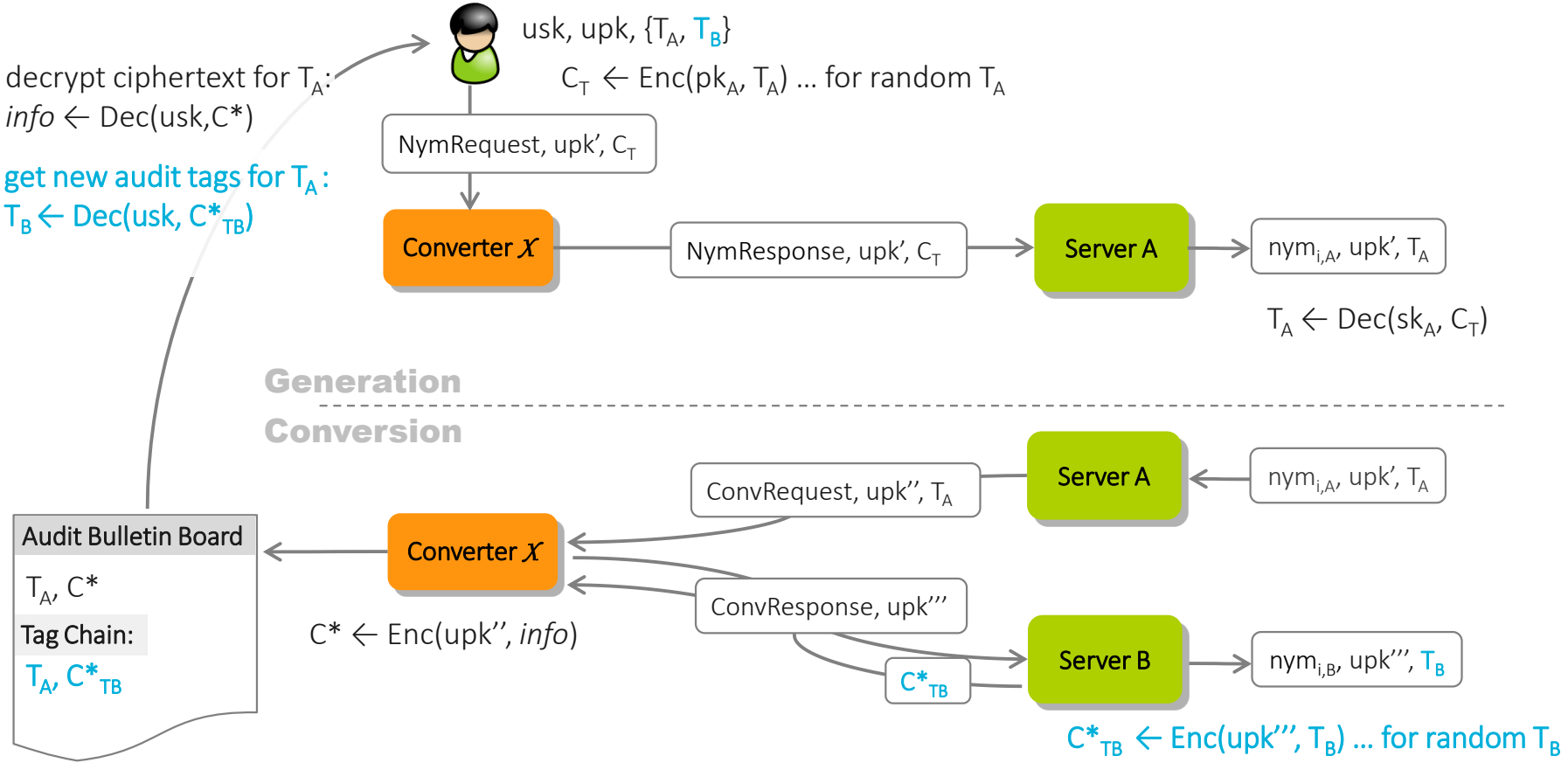
High-level Idea | Adding Auditability



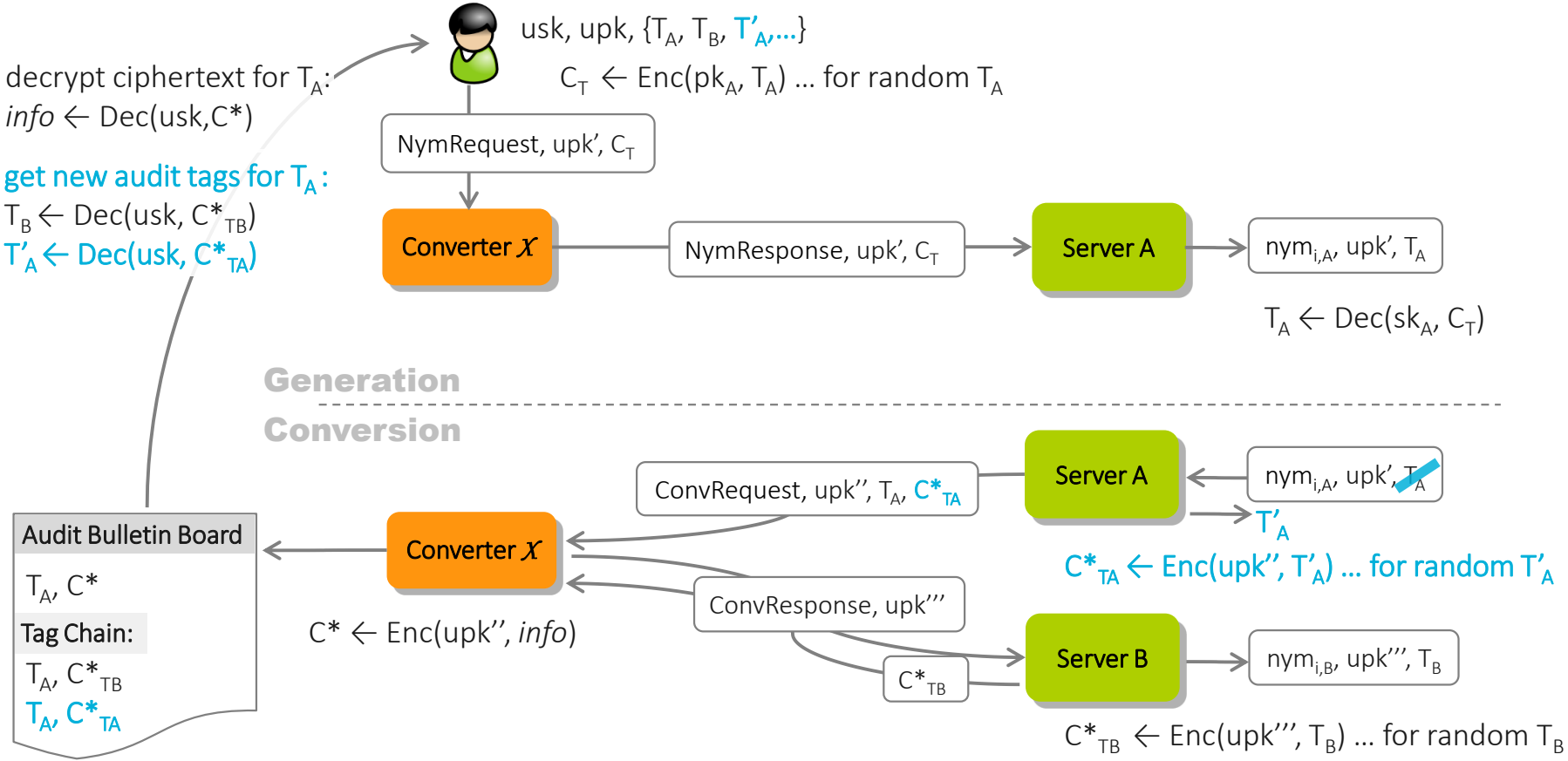
High-level Idea | Adding *Efficient* Auditability (via Audit Tags)



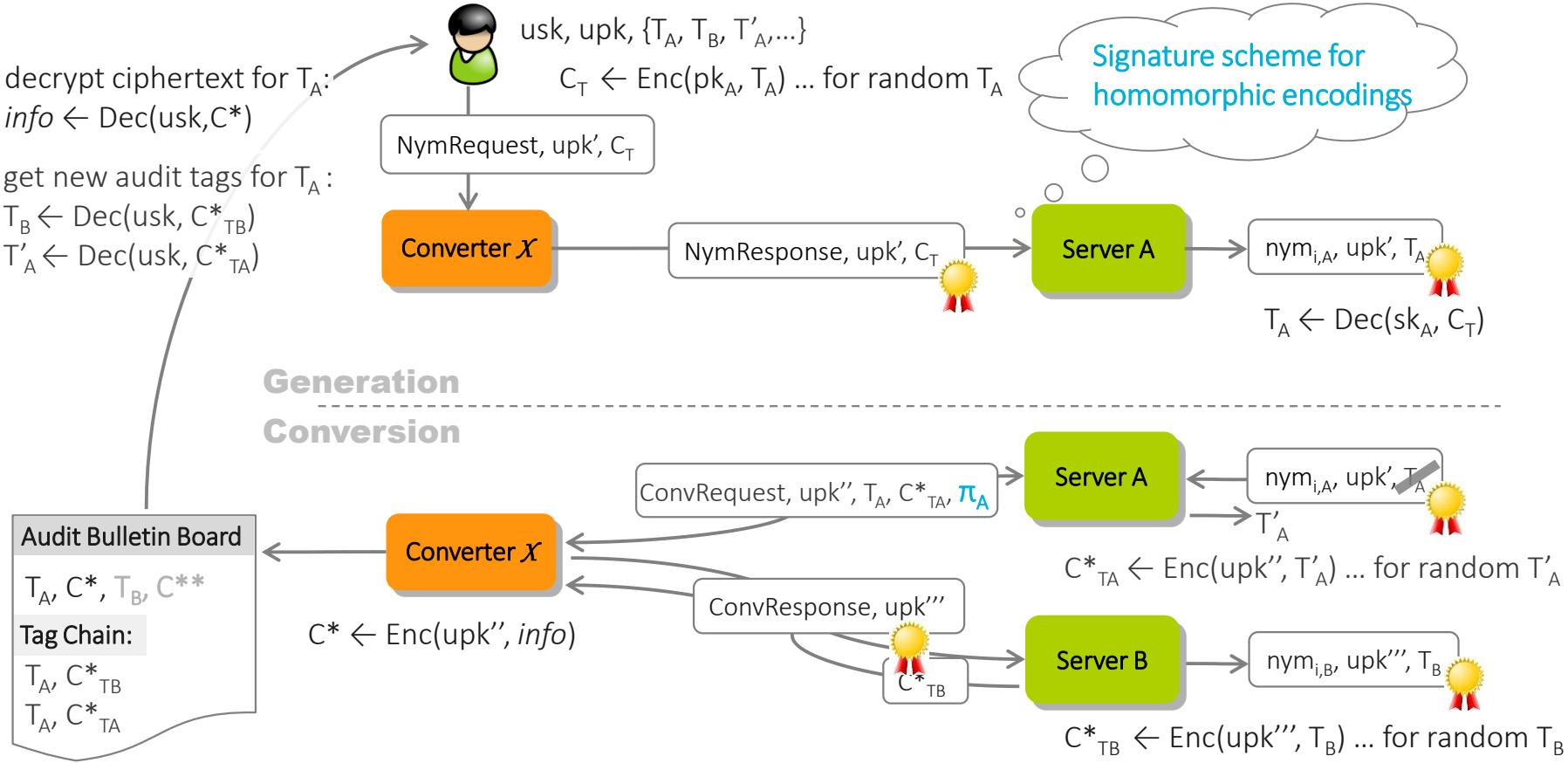
High-level Idea | Adding *Efficient* Auditability (via Audit Tags)



High-level Idea | Adding *Efficient* Auditability (via Audit Tags)



High-level Idea | Security against Active Adversaries



(Un)linkable & Auditable Pseudonyms | Security & Efficiency

- Provably secure construction in the Universal Composability (UC) framework based on
  - homomorphic encryption scheme (ElGamal encryption)
  - homomorphic encryption scheme with re-randomizable public keys (ElGamal-based)
  - oblivious pseudorandom function with committed outputs (based on Dodis-Yampolskiy-PRF)
  - signature scheme for homomorphic encoding functions (based on Groth signature scheme)
  - zero-knowledge proofs (Fiat-Shamir NIZKs)
  - commitment scheme (ElGamal based)
  - DDH

- Secure against actively corrupt users & servers, and honest-but-curious converter
  - (w/o audits even fully corrupt converter [CL15])

- Concrete instantiation ~50ms computational time per party for conversion

Summary

- Mature privacy-enhancing technologies exist – privacy and functionality are not exclusive
- Linkability crucial for utility, but also weakens privacy
  - Paradigm shift: unlinkability per default, linkability only when necessary
  - Controlled, selective linkability & enforced transparency
- GDPR creates a great practical demand for privacy-preserving mechanisms
  – data minimisation, consent enforcement, auditability, ...
- „Crypto Magic“ needs education and dissemination!

Thanks! Questions?

anj@zurich.ibm.com