



**Safeguarding Privacy  
Through Design of Information Systems**

**Dr. Stefan Brands**

**brands@cs.mcgill.ca, brands@credentica.com**

**October 1<sup>st</sup>, 2007**

**CREDENTICA**

# HIPAA Privacy Rule

credentica.com



- **Regulations for the use and disclosure of Protected Health Information (PHI)**
  - PHI = any information about health status, provision of health care, or payment for health care that can be linked to an individual
- **When a covered entity discloses PHI, it must make a reasonable effort to disclose only the minimum necessary information required to achieve its purpose**

# Problematic technical solutions

credentica.com



- **Provide only de-identified information**
  - Limited sets may not be effective & restrictive for research
  - Cannot do good statistical analysis without knowing all databases used in matching attempts (now and future ...)
  - Particularly problematic for longitudinal patient data
- **Privacy-preserving data matching: computing results without sharing data**
  - Providers must be queried online
  - Ongoing research problem (not generally practical)
- **Personal Electronic Health Record devices**
  - Data subject must be online and involved
  - Cannot do meaningful queries on aggregated data

# A better technical solution (?!)

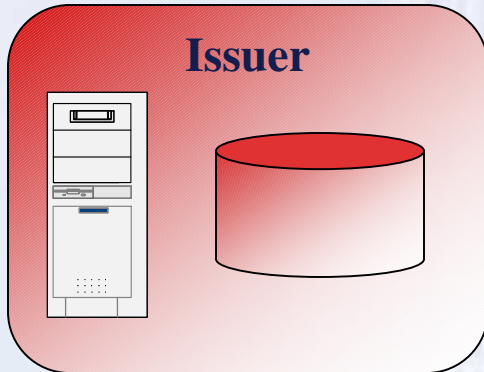
credentica.com



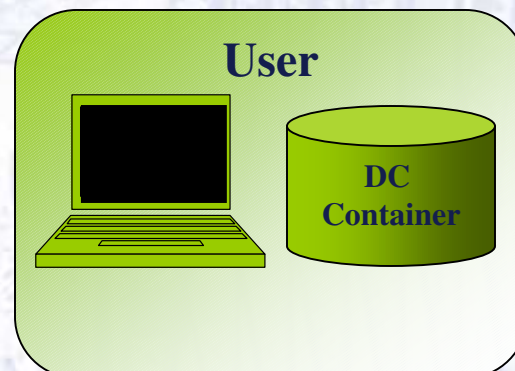
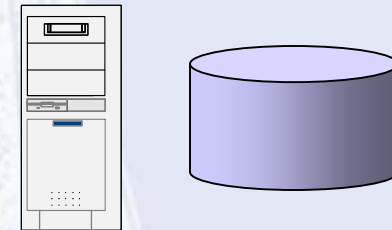
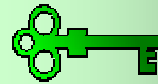
- **Independent Health Record Trusts (brokers trusted by data subjects / infomediaries)**
  - Can “minimally” respond to queries by researchers
  - Can collect user-verifiable audit trails
  - Personal record management tools
  - Can tie EHR to private keys held by data subjects
- **Challenge #1: Broker becomes honeypot**
  - Solution: extreme security measures, regulations, etc.
- **Challenge #2: Secure online access?**
  - Solution: strong authentication in single domain
- **Challenge #3: Authenticity and integrity of responses? (Digital signing defeats minimal disclosure & enables re-identification)**
  - Solution: cryptographic selective disclosure techniques

# Digital Credentials life-cycle

credentica.com

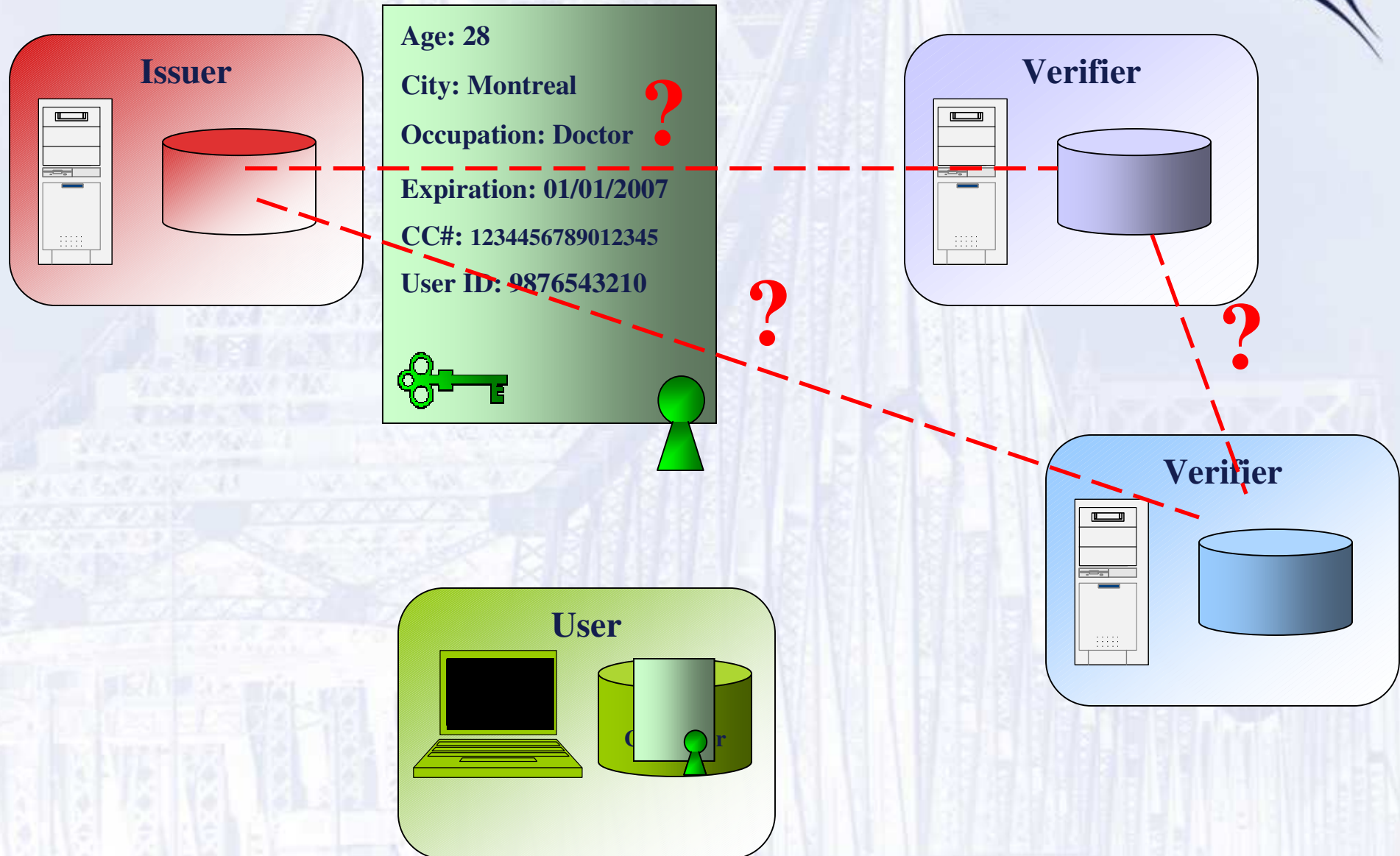


**Age: 28**  
**City: Montreal**  
**Occupation: Doctor**  
**Expiration: 01/01/2007**  
**CC#: 1234456789012345**  
**User ID: 9876543210**



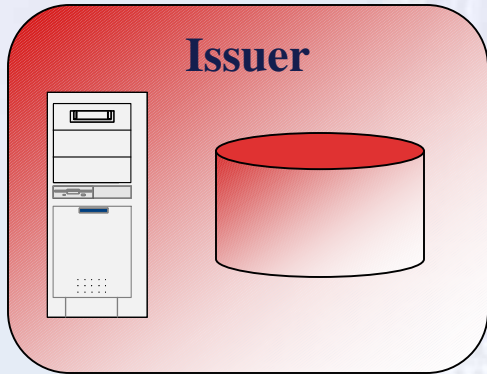
# Digital Credentials life-cycle

credentica.com

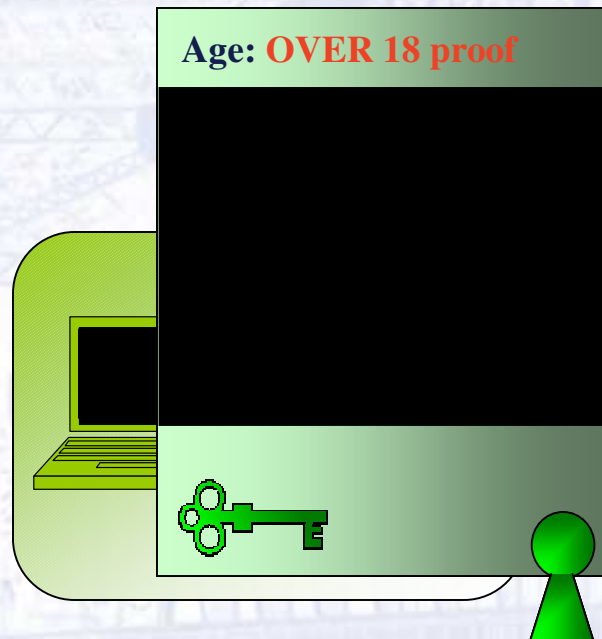
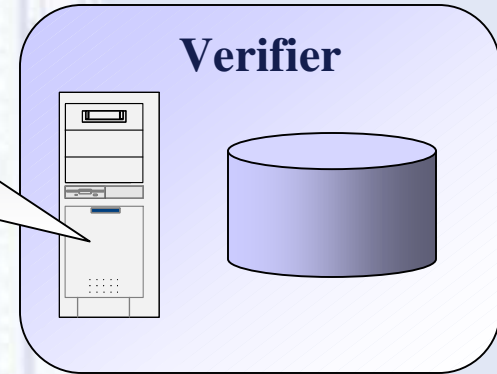


# Selective disclosure

credentica.com

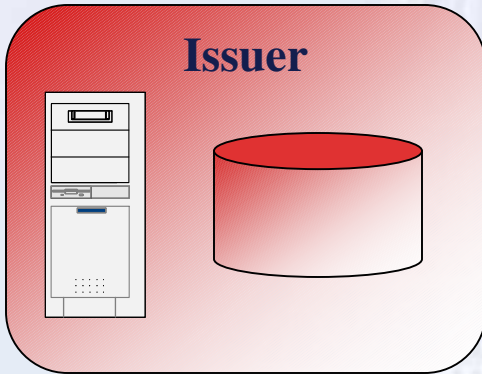


Prove that you are over 18

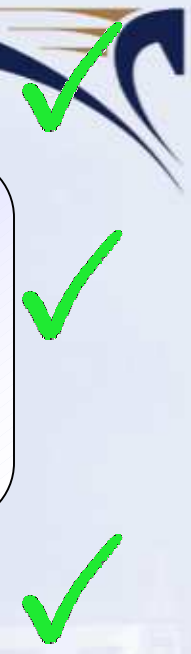
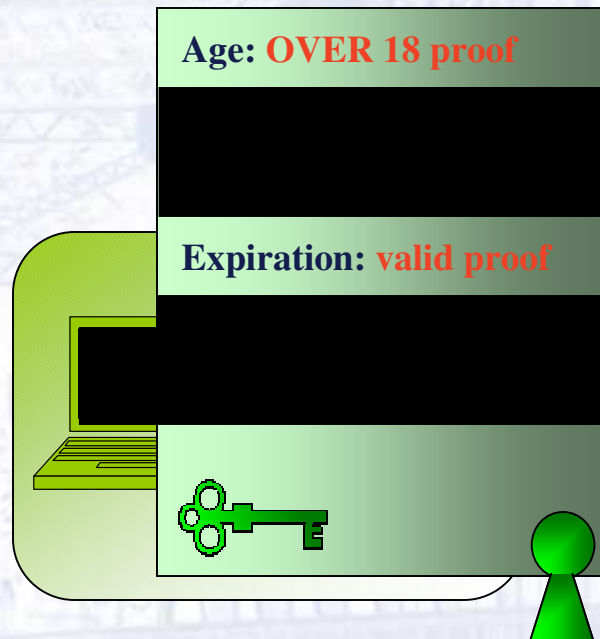
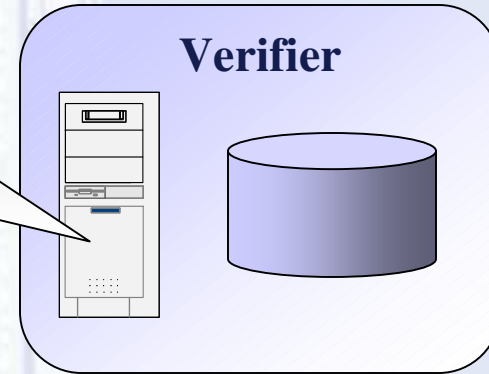


# Selective disclosure

credentica.com

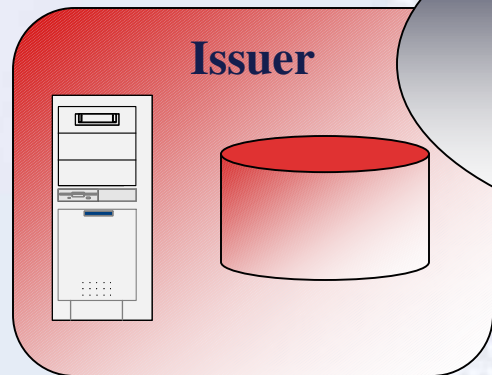


Prove that you are over 18 and that the Digital Credential has not expired

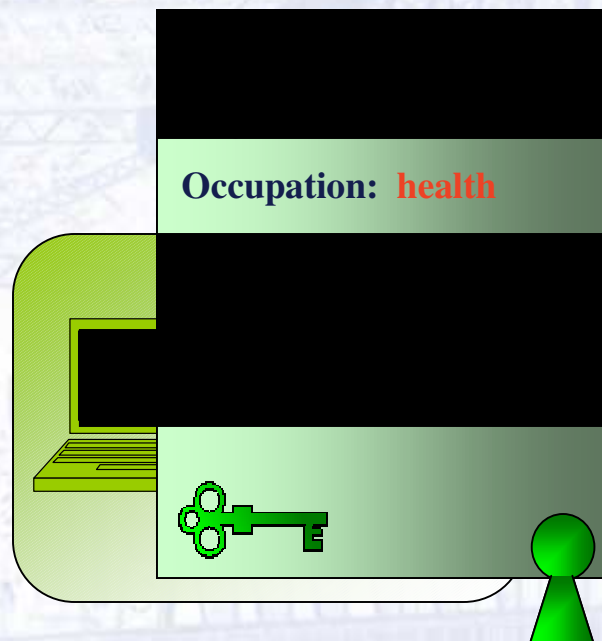
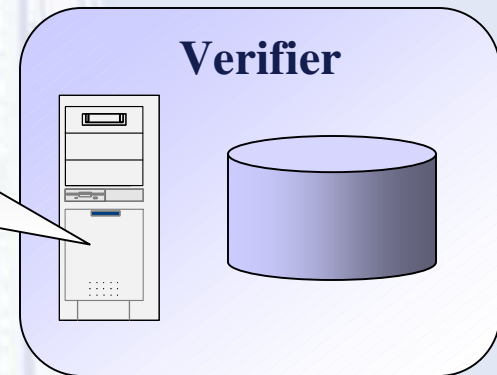


# Selective disclosure

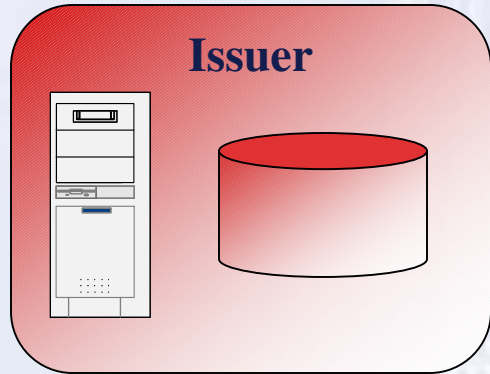
credentica.com



Prove that you are a doctor, a pharmacist, or a medical insurer



# Transcript forwarding



A doctor visited me

