Plan

- Introduction
- Analytic approach
- A new generic solution
- Conclusions

Introduction

- Privacy is a critical issue in many emerging applications
- Legislation:
  - A/RES/45/95, 95/46/CE, 2002/58/EC, 98/1165, ...
- Implementation:
  - Social security data in the US → Symmetric Keys
  - Medical data in France → Secret keys
  - Cancer data in Germany → Hybrid encryption (IDEA/RSA)
  - Statistical data in Switzerland → Hybrid encryption
- But... most of these solutions are developed empirically

Analytic approach

- Is it possible to develop a generic solution?

A new generic solution

Conclusions

Objectives & Requirements

Solutions characterization

Solutions
Methodology: needs

- **What?**
  - Express the User expectations, ...
    - Form not very explicit

- **Examples**
  - Both directly and indirectly nominative data should be anonymized
  - Using personal data → The patient consent
    - ...

Methodology: objectives

- **Anonymization objectives**
  - Reversibility → encryption
  - Irreversibility → one-way hash function
    - (once replaced by anonymous codes, the original nominative data are no longer recoverable)
  - Inversibility → disanonymization ⇒ exceptional procedure

- **Examples**
  - Medical data transmission & storage ⇒ Reversibility
  - Focused epidemiological studies ⇒ Inversibility
    - (sometimes, authorities ⇒ medical examiner, the inspector-doctor or a trustworthy advisory committee ⇒ need to re-identify the patients in some particular situations)

Methodology: requirements

- **Anonymization requirements**
  - Linking
    - (associating in time and space, one or several codes to the same patient)
      - temporal (always, sometimes, never)
      - spatial (international, national, régional, local)
  - Robustness
    - (concern exclusively illicit disanonymization)
      - reversion robustness
        - e.g., if the used cryptographic technique is not strong enough
      - inference robustness
        - e.g., age * sex * month of discharge from hospital ⇒ enough to identify a person
  - Example
    - Medical data transmission & storage ⇒ Reversion robustness

Methodology: solutions characterization

- **Type**
  - organizational procedure, Access control
  - cryptographic algorithm
  - one-way function

- **Plurality**
  - mono / double / multiple anonymizations

- **Interoperability**
  - Transcoding (manually)
  - translating (mathematically)
    - Anonymization system ⇒ another one
  - transposing (automatically)
Plan

- Objectives
  - Reversibility
  - Linking
  - Robustness

- Requirements
  - Type
  - Plurality
  - Interoperability

Analytic approach:

- A new generic solution
  - General scheme
  - Discussion

Conclusions

- Objectives
  - Reversibility
  - Linking
  - Robustness

- Requirements
  - Type
  - Plurality
  - Interoperability

- NEEDS

- SOLUTION CHOICE

Our solution: general scheme

- Hospital
- Processing center (project)
- End user

\[(T1) \rightarrow ID_{pat/Proj} = H(ID_{proj} / ID_{pat}) \]
\[(T2) \rightarrow ID_{auth(pat/Proj)} = (ID_{pat/Proj} \times K_{sk}) \]

Our solution: benefits?

- Generic, systematic and adaptable to different needs
  - The protection of the patient anonymous ID
    - Smart cards are sufficiently tamper-resistant,
    - \(ID_{pat}\) is randomly generated into the card
    - keep secret the patient identifier
    - \(H(ID_{proj} / ID_{pat})\) is calculated into the card
    - Protect the critical part of our process
  - No critical secret for all the population
    - The user anonymous ID depend only on (patient, project)
    - The anonymous ID differs from a project to another
    - The IDs are located in different places
    - The keys are held by different persons
  - The explicit patient consent
    - Use of the anonymized data
    - Reversing the anonymity

Our solution: discussion

- Regulating the data inversion
Our solution: Flexibility

- Merging data belonging to several establishments
  - Need: easily link data concerning every patient that has been treated in these hospitals

<table>
<thead>
<tr>
<th>Hospital A</th>
<th>Hospital B</th>
</tr>
</thead>
<tbody>
<tr>
<td>({IDA\text{pat}{Proj}} K_{\text{hospA}})</td>
<td>({IDA\text{pat}{Proj}} K_{\text{hospB}})</td>
</tr>
<tr>
<td>(K_{\text{hospA}})</td>
<td>(K_{\text{hospA}})</td>
</tr>
<tr>
<td>(K_{\text{hospAB}})</td>
<td>(K_{\text{hospAB}})</td>
</tr>
</tbody>
</table>

Encryption

Decryption

Conclusion

- Analytic approach
  - needs → Objectives → Requirements → Solutions
- Anonymization
  - Generic solution
    - Some privacy needs can be met by using smartcards

But also ...

- Organizational solutions
  - Risk analysis
  - Security policy
- Technical solutions
  - Suitable architecture
  - Access control mechanisms
  - IDS
  - ...

Plan

- Introduction
- Analytic approach
- A new generic solution
  - Conclusions

Thank you!

Questions?

Remarks?

Comments?

Advises?