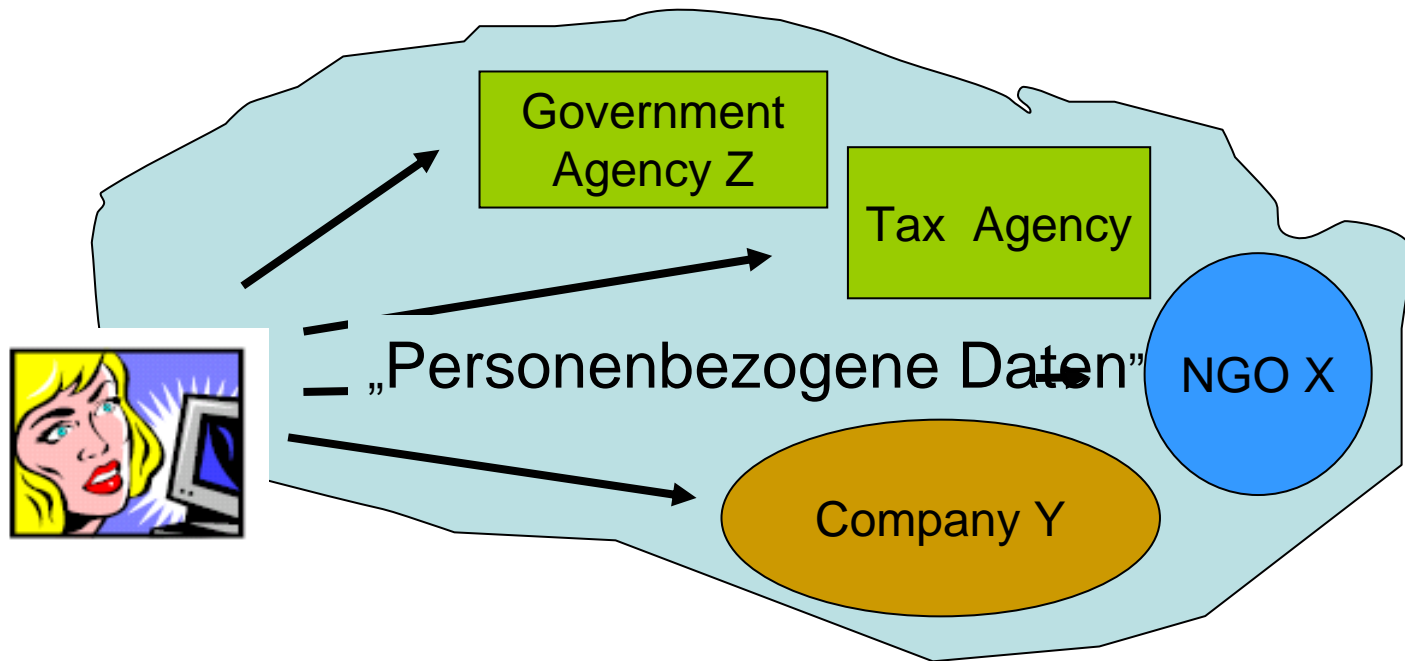


Anonymous Tax Declarations – Is this feasible?

Reinhard Riedl, Andras Kiraly
University of Zurich

Digital Identity = union of all data related to a person



“The Citizen”: Control on who sees what

“The State”/“The Companies”: Integration of all citizen data

Well-known patterns for One-Stop-E-Government

- Anti-pattern: Data synchronization
- Pattern: SOA/POA with document services

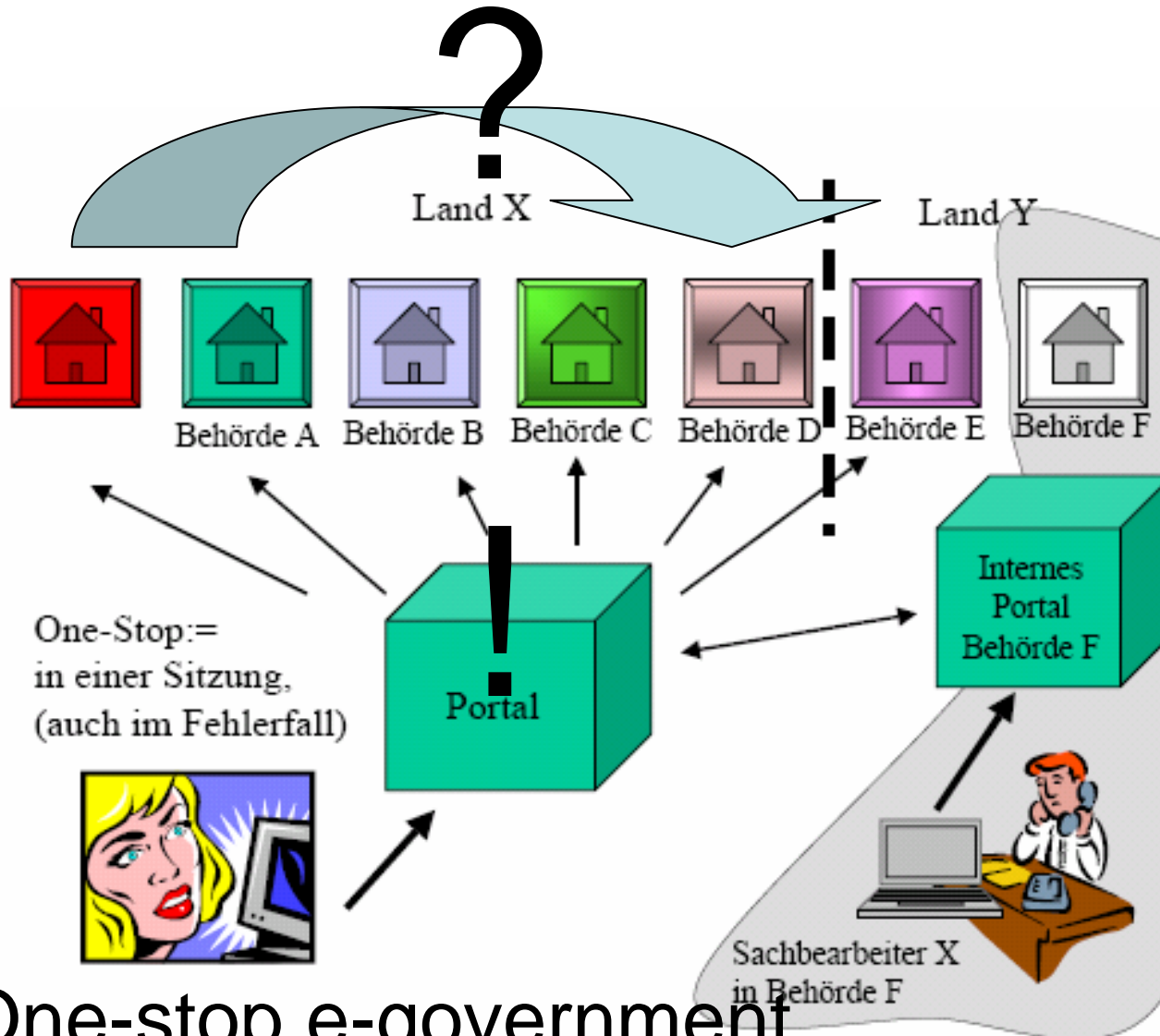
The vision is ...

- ... a digital representative, which is universally and globally usable for all forms of identity management (incl. delegation etc.) and which allows the citizen to control her data
- Far from today's reality!!!
 - Lots of basic question have not even been touched
 - Tendency that technicians and vendors decide on the future rights of citizens by creating legacies
 - Remember ... L'état c'est le peuple! That is, it should be democratic decisions which shape future digital identity management

Privacy protection = context conservation/protection

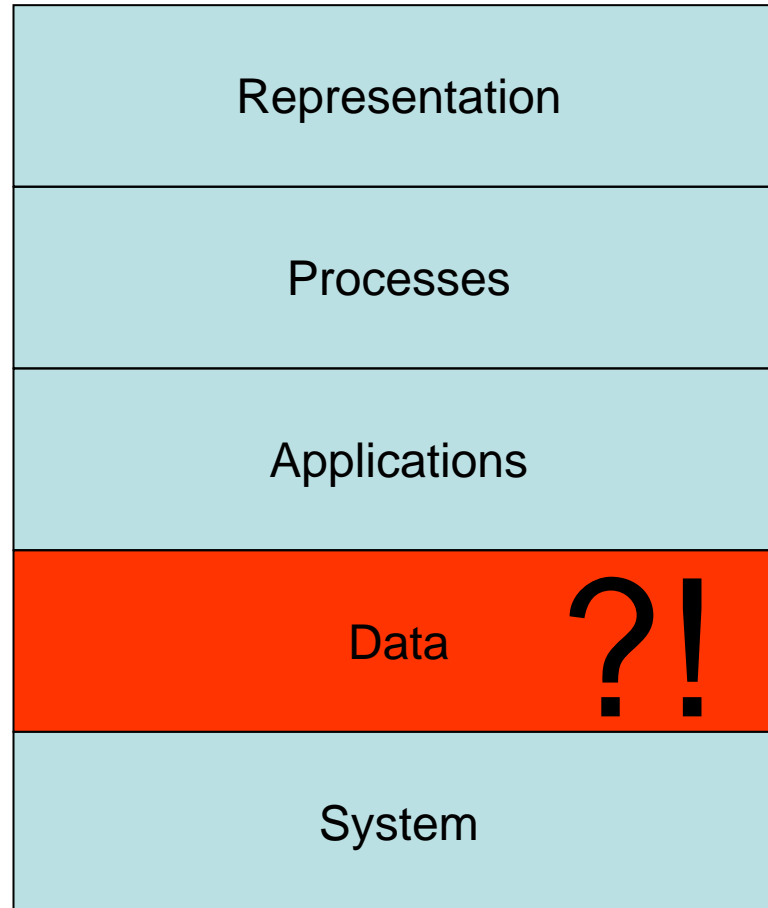
- Data protection principle:
systematic data collection requires a justified case & explicit reason
 - Size and quality must be adequate for the data usage context
- In general, the transfer of data from context to another is forbidden
 - The “information” represented by data and the “quality” of data depend on the context
- Postmodern reality:
each individual lives in many different “societies”
 - It is not admissible to automatically exchange / synchronize data between them
 - A key risk for the citizen is the propagation of mistakes and the misinterpretation of data

Context conservation in e-gov?!



One-stop e-government

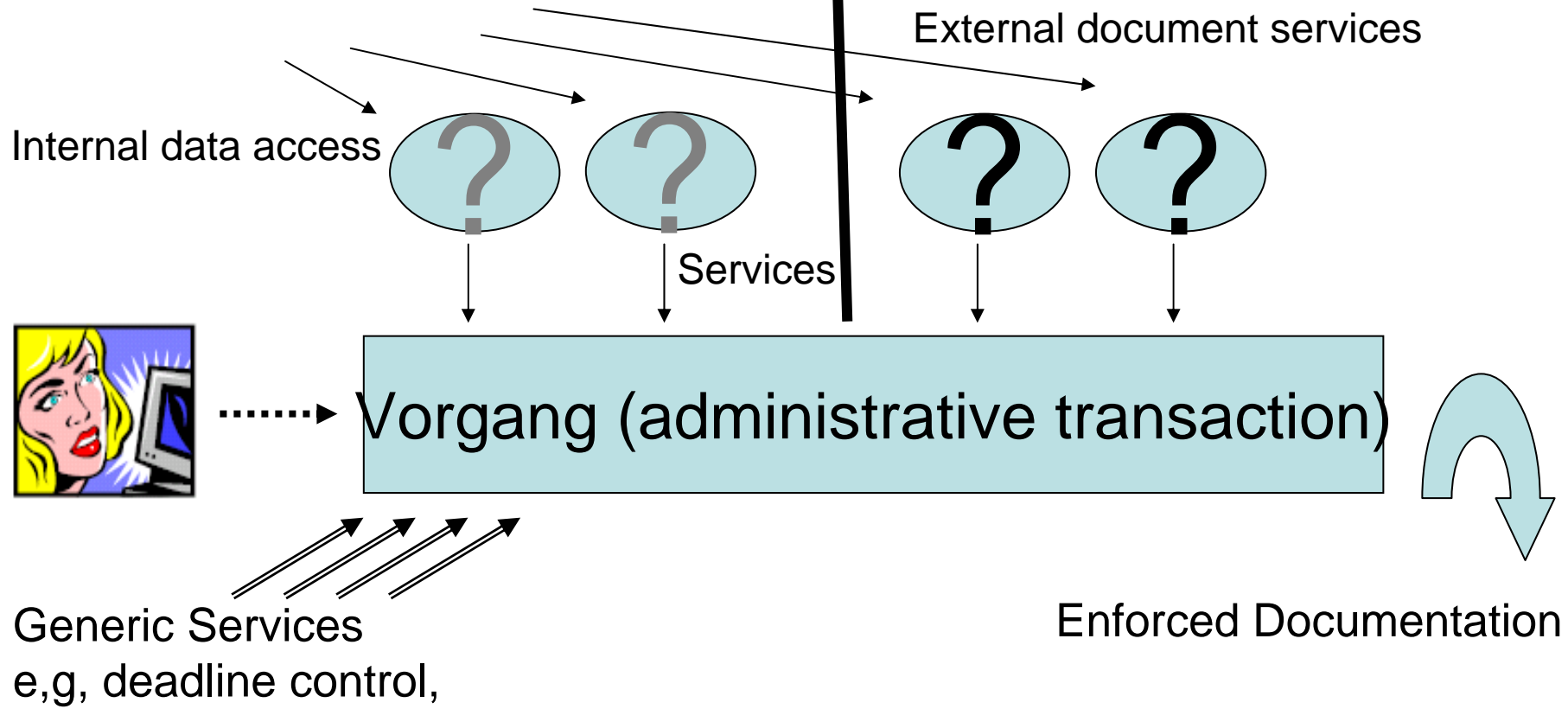
Context conversation in e-gov ?!



Government Application Integration (GAI)

Context conversation in e-gov ?!

Information procurement with
GAI und Document-Services



Integrated administrative transaction processing

Maximal solution to the context transfer problem = anonymity

- Trustworthy anonymity
 - Proof of the evidence of statements about the validity of partial digital identities, which do not contain the name of the person or any other information to identify her
- Non-traceability
 - Impossibility to associate different such proofs
 - No possibility to identify a person through the enriched context of a whole trace
- Revocation
 - Linking of a trustworthy anonymous identity to a person within a given context

Anonymity reduces actors to their certified roles

- Privacy protection through minimal size of personal data and maximal quality
 - Possible practical use for citizen request to the administration, for solution-oriented brainstorming, etc.
- No border-line between anonymous and non-anonymous identity
 - The personal data delivered by one side are tailored to the actual necessities of the context
- Data protection law “would” imply: anonymity where it is admissible!

Anonymity can be practically implemented

- We have performed case studies and experiments with a prototypical implementation
 - Credential technology plus mix networks
 - Scenario: SOA/POA one-stop e-government (with Web-service orchestration)
 - Scenario: Virtual campus scenario (with mobile service access)
- Result: It works if and only if anonymity on the higher level protocols is enough
 - Mobile access may break the non-traceability

A-ACID Transactions

- **ACID** = **A**tomicity, **C**onsistency, **ser**ializability (isolation), and **D**uration
 - A commit takes place after it is guaranteed that all sub-transactions can be performed
- **A-ACID** = **A**nonymous **ACID**
 - Anonymous owner: all data processes refer to exactly one anonymous person
 - Before a commit can take place a trace is generated by a trustworthy revocation instance to verify that is only one person
 - The revocation instance replies the request for tracing with “yes (one person)” or “no”

Applied A-ACID

- “Testbed” for Gedankenexperimente ...
 - Based on the technological feasibility of the concept we ask for the conditions defining the legal and organizational feasibility
 - Focusing in particular on applications of **limited revocations**
- For example: **anonymous tax declaration** ...
 1. The citizen obtains anonymous income certificates and delivers them together with her tax declaration anonymously to the tax office
 2. The tax office proceeds as usual (e.g. optimistic algorithm with risk thresholds and manual exception handling)
 3. Before it issues the result (e.g. vorläufiger Bescheid), it asks the national certification authority to trace the anonymity
 4. If the certification authority confirms that all certificates relate to the same person, the result is issued, otherwise the citizen is requested to explain ...

This requires some legal and organizational change plus a corresponding technological and organizational infrastructure, but in principle it works.

This would fail, because of the challenging knowledge management process.

Testbed for Gedankenexperimente

- Applications of AACID transactions are largely straightforward if no good will is needed from third parties who provide the anonymous of certificates
 - If such a good will is indeed needed, the rights have to enforced by anonymity revocation of the third party, and this gets us into an organizational mess
 - Consequently, in practice it would be much easier to realize anonymous tax declarations than to realize anonymous applications for financial support from the state
- Anonymous duties are easier to implement than anonymous rights
 - Due to the different complexity of the legal and the organizational change required