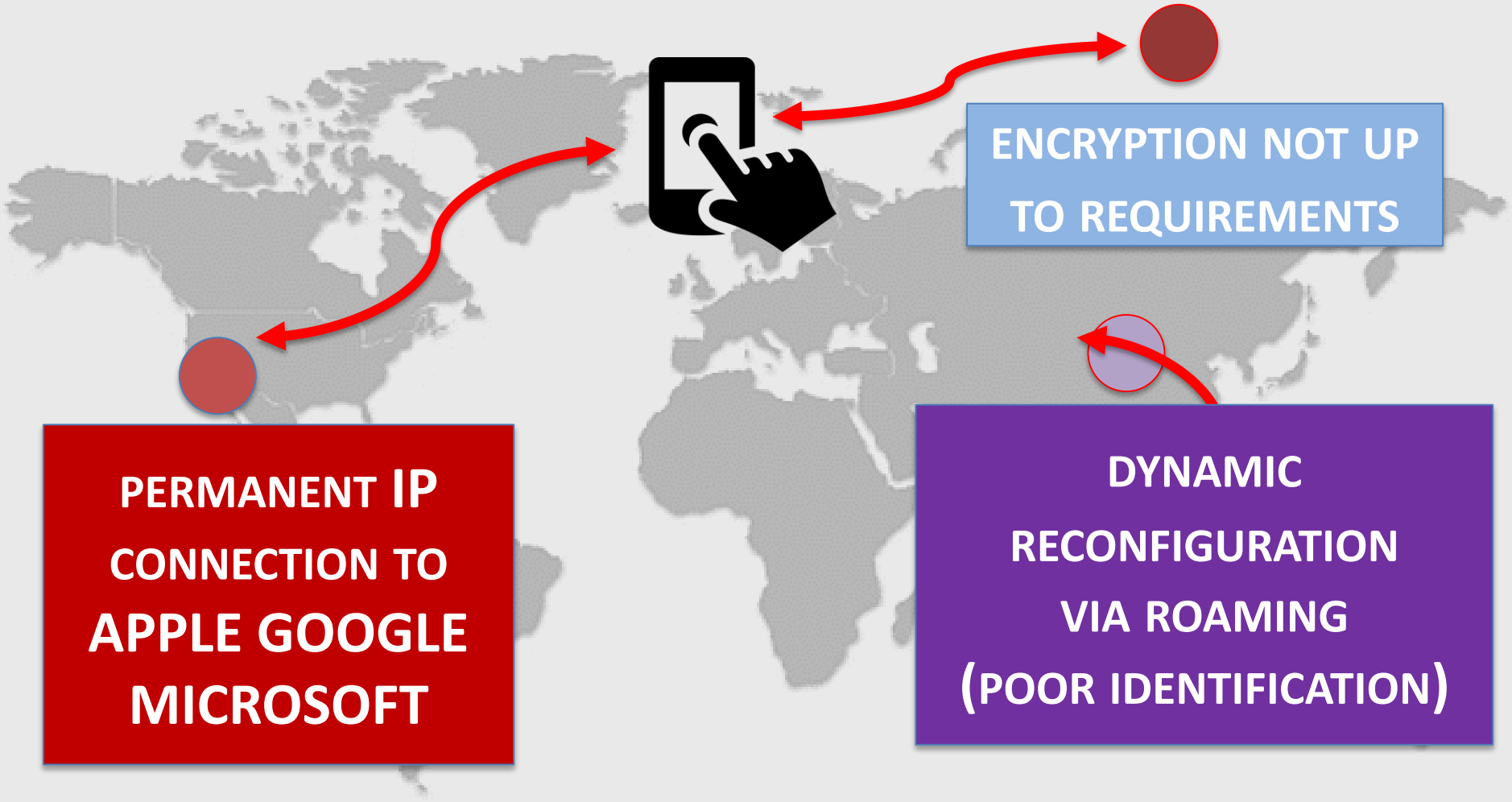
Identity and encryption tools to enable digital sovereignty

Prof. Dr. Reinhard Posch
CIO Federal Government
AUSTRIA

GOVERNANCE SOVEREIGNTY

ICT INCREASINGLY FACING MONOPOLIES BY GLOBAL INDUSTRY PLAYERS

MOBILITY CHALLENGING SECURITY



CONCEPTS DRIVEN BY LACK OF AWARENESS

ONLINE COLLABORATION AND CLOUD

?

which documents can be used in collaboration

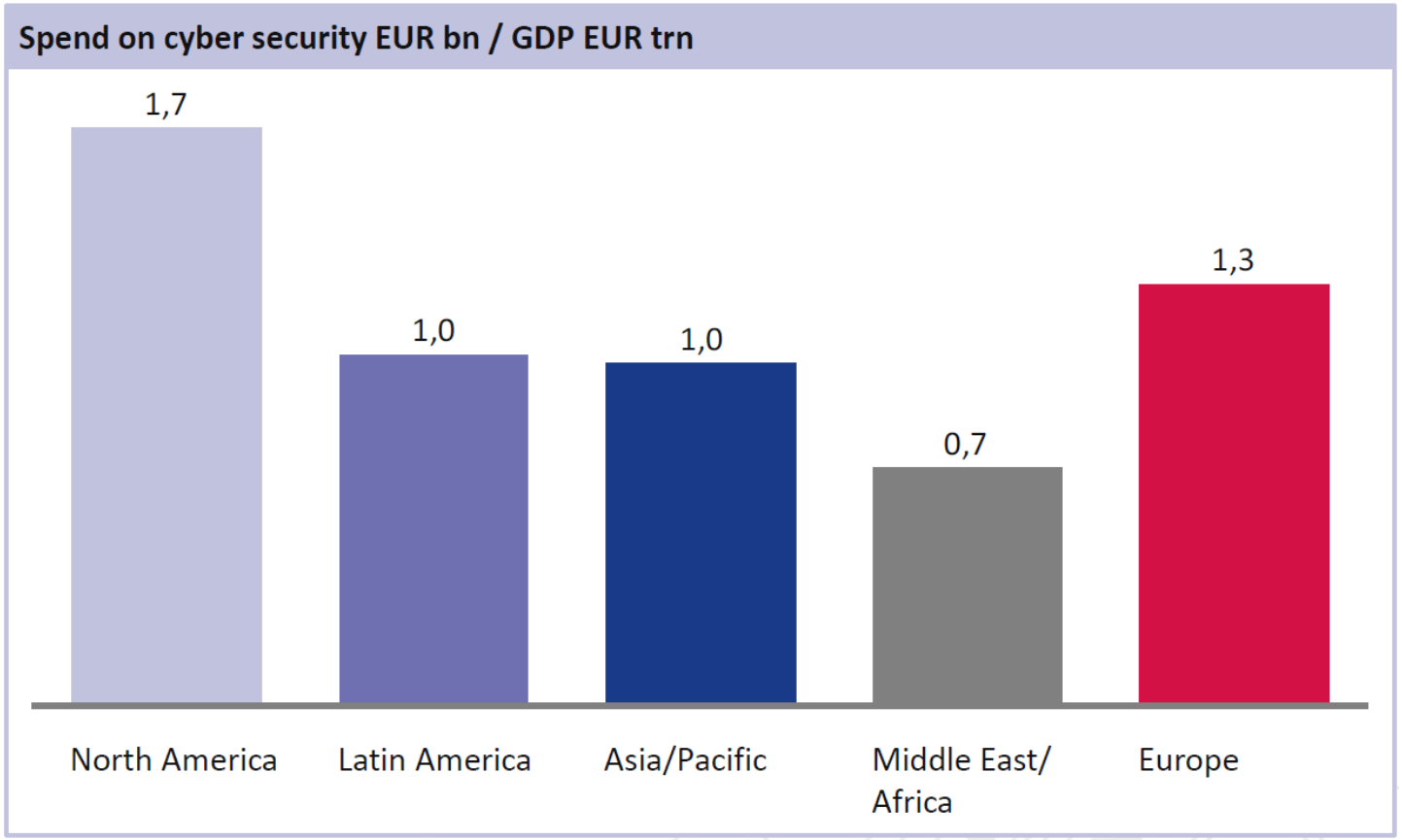
?

how to handle the critical rest

?

safe harbor

SPENDING ON CYBER SECURITY



SOURCE: Cyber-security market size in Europe – Gartner 2014, IMF 2013

HOW TO REINFORCE TRUST ?

The Seattle Times
Winner of Nine Pulitzer Prizes

Business / Technology

Home | News | Business & Tech | Sports | Entertainment | Food | Living | Homes | Travel | Opinion

Originally published July 31, 2014 at 11:44 AM | Page modified August 1, 2014 at 6:28 AM

NY judge: US warrant can reach Microsoft email in Ireland

U.S. law enforcement can force Microsoft Corp. to turn over emails it stores in Ireland, a judge ruled in a case that technology companies have rallied around as they pursue billions of dollars in data storage business abroad.

Share:

Recommend 15

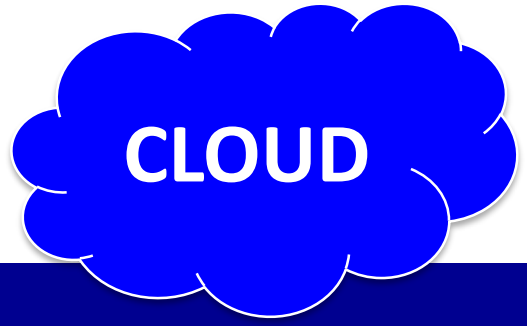
4 Comments

E-mail article

Print

A-SIT

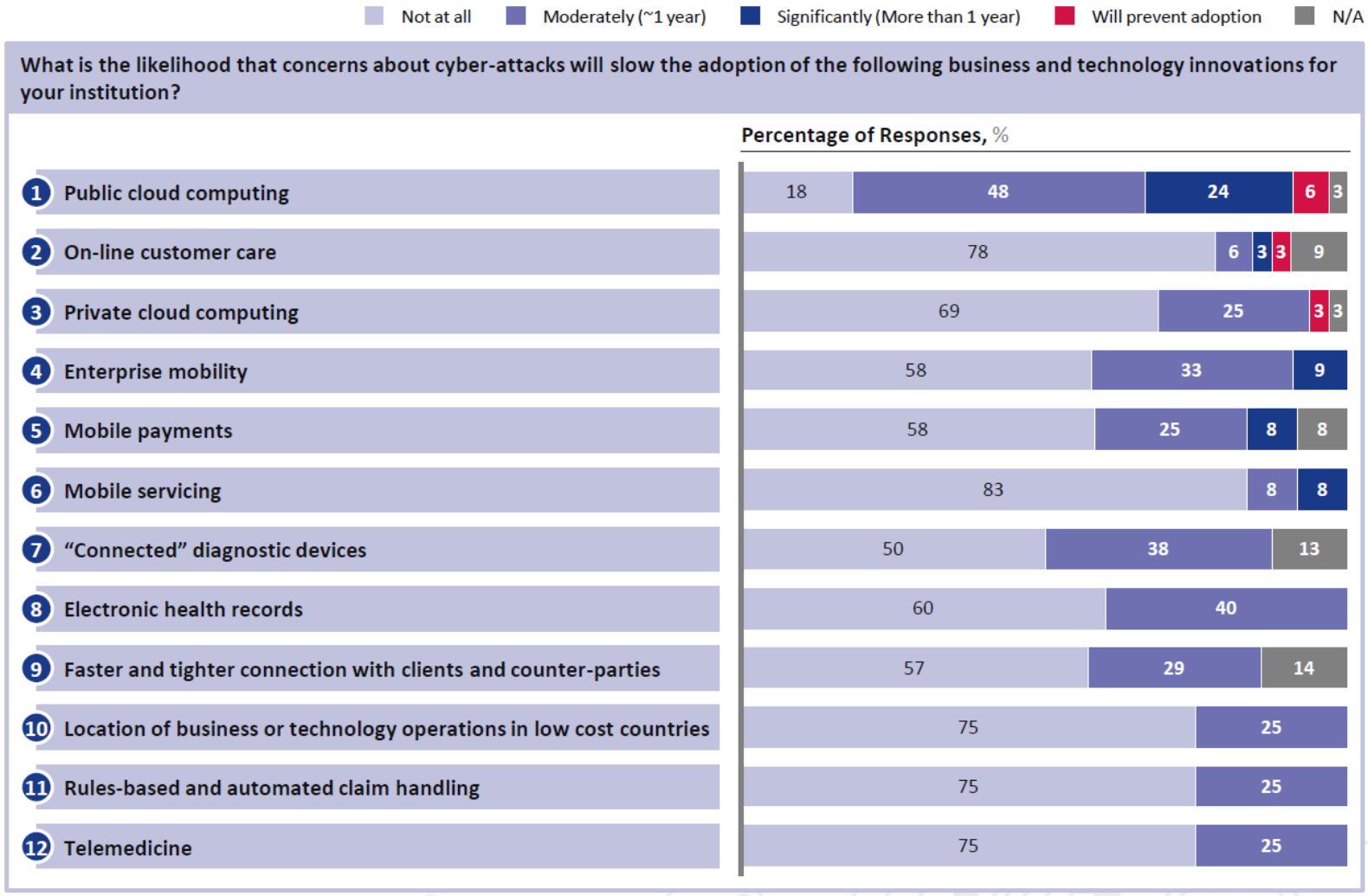
CLOUD NEEDS A BIG EFFORT



- eIDaS defines governance for electronic identities as a duty of member states. in reality cloud providers still claim eID governance
- mechanisms with major PUBLIC CLOUDs are not ready for European administrations – neither technologically nor legally

SECURITY CONCERNS SLOWING DOWN?

CLOUD



A-SIT

IDENTITY IS THE CORE OF SECURITY

- we need to have identities of entities before we can save their interests
  - multi factor – baseline of security
  - crypto identity – the only way in large systems
  - replay must be impossible
  - user will only buy in, if it is simple
  - broad acceptance is key

eID MUST SERVE USER'S NEEDS

- increasingly tablets and mobiles are used
- this results a different paradigm – no external devices.
- when it comes to take-up comfort is the key issue

- the Austrian response is the mobile signature and eID. "CITIZEN CARD"

CITIZEN CARD – the functionality (§ 4 Abs. 1 E-GovG)

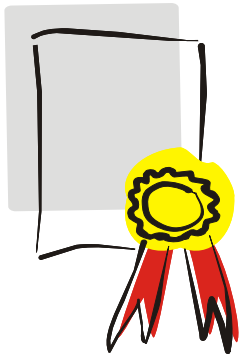
the „citizen card“ is about

- the **unique identity** of the applicant
  - the **authenticity** of the electronic application (so that legal validity conforms to a process in writing)...

therefore it is:

→**E-ID** and

→**signature** in the electronic domain



eID using a mobile phone

qualified signature

A-TRUST einfach sicher

Vergleichswert: 7gqSgCgSTF

Signaturdaten anzeigen

TAN: bqz48n

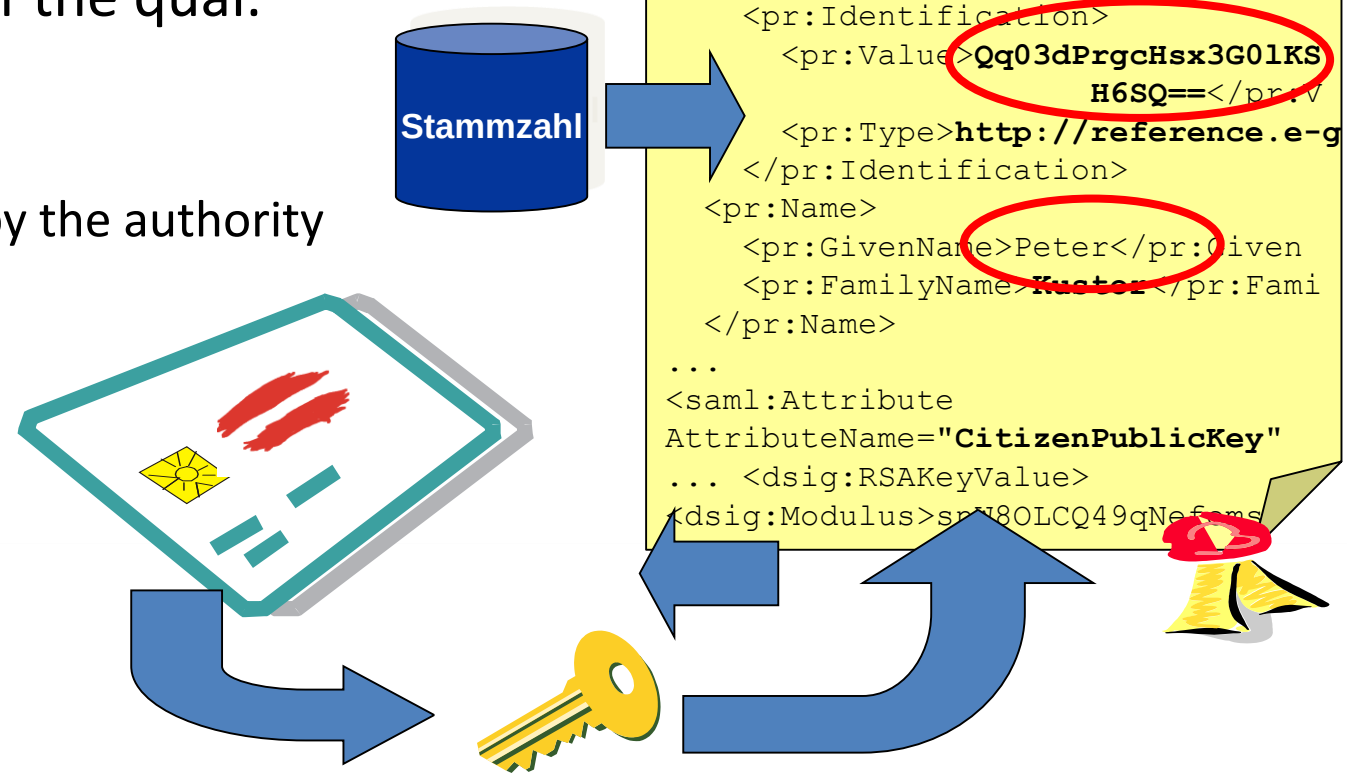
Signieren

Hilfe

A-SIT

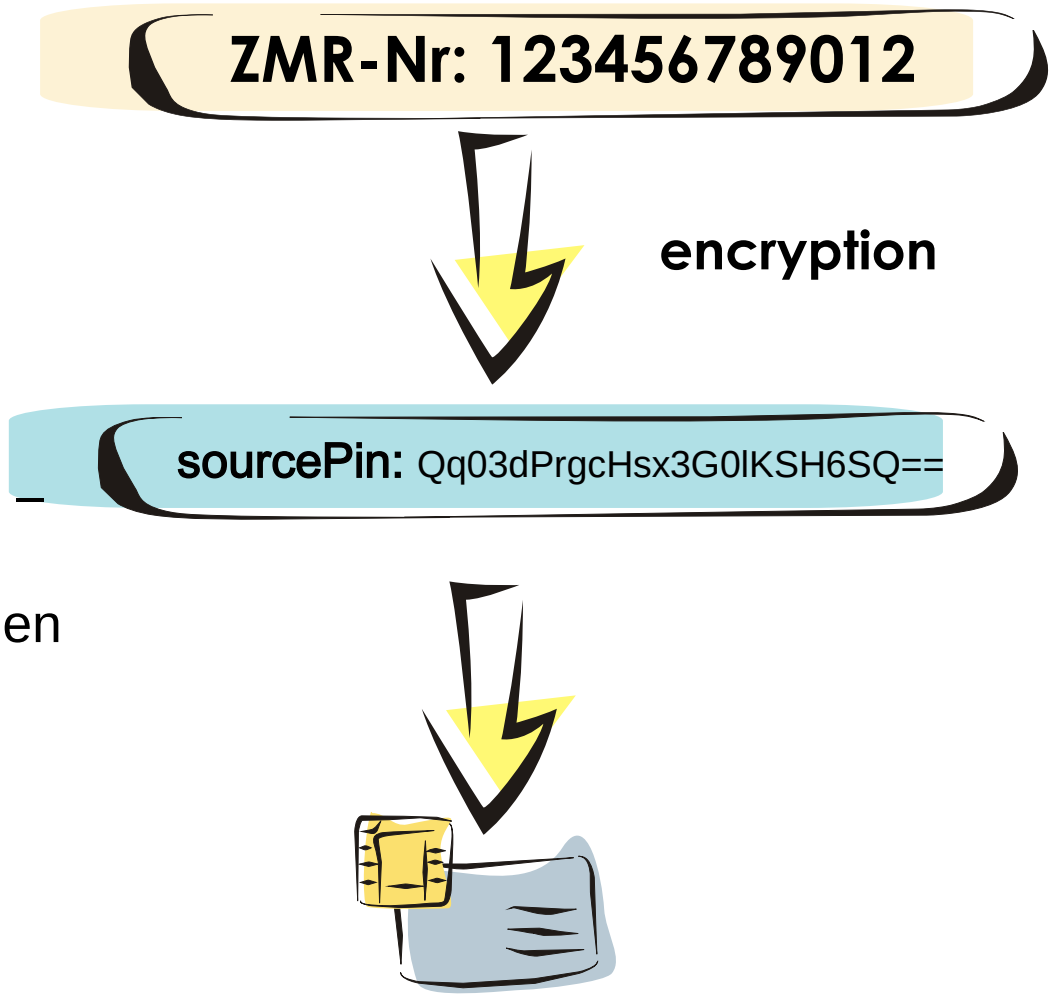
how to bind to the person

- XML data within the secure hardware:
  - –name and birthdate
  - –unique identifier “sourcePin”
  - –public key of the qual.
  - –signature
  - –
- this XML is signed by the authority
- StZRegBeh



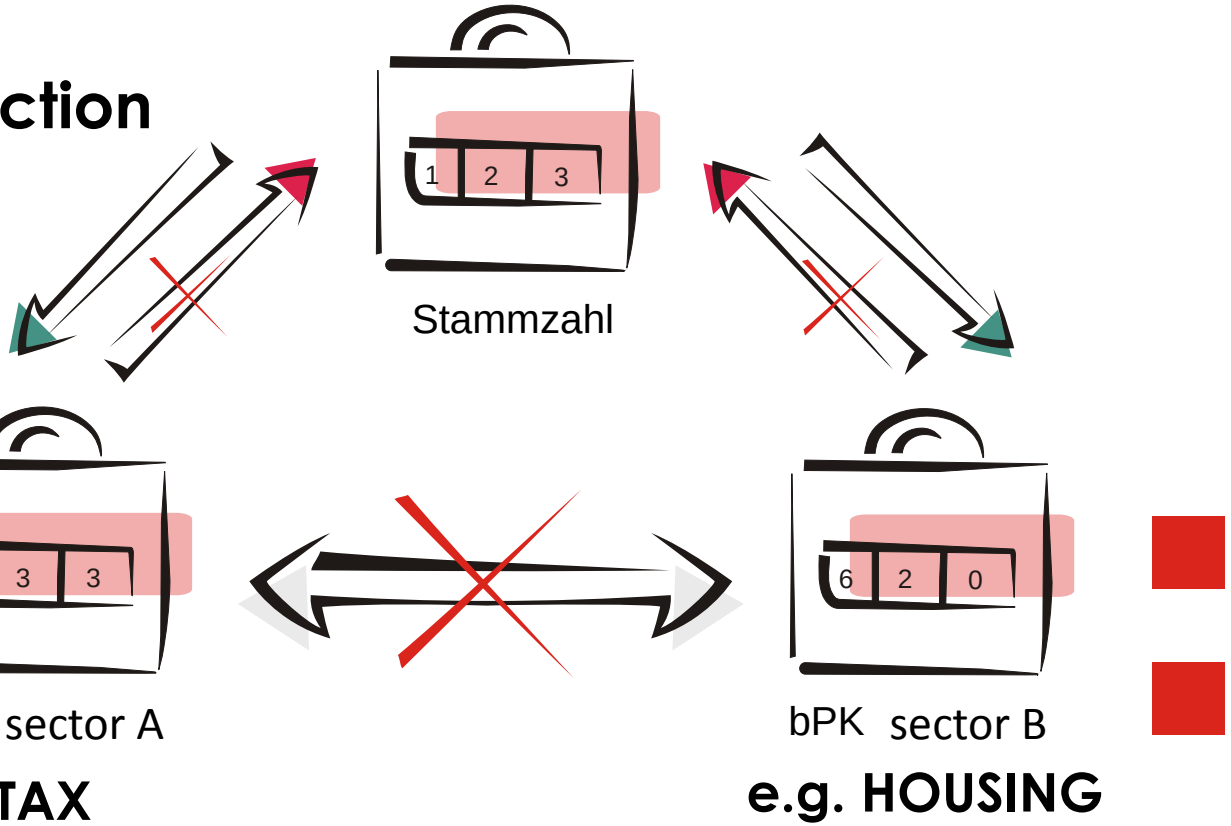
how to get the sourcePin (SP)

- SP = encrypted using the ZMR (register of inhabitants)
- only the authority can encrypt and calculate SP
- SP is protected on the card
- the authority does not store SP – only calculates from ZMR
- the key is only to be used by then authority to calculate sector specific identifiers bPK



identifying a person in a sector bPK

one way function



e.g. TAX

e.g. HOUSING

bPK-A → bPK-B NO WAY

STORK – the eID trigger

- considering minimum security
- mutual recognition
  technology level and legally
- focus on an interoperability-protocol
- applicable for public and private

serves as a model for eIDaS

A-SIT

HOW TO REACH COMPREHENSIVE SECURITY

- **service transition – E-MAIL to WEB, FACEBOOK to APP etc.**
  - this is a major area of risk as security is generally lowered here
- **eID lacks of technical security**
  - e.g. most cloud providers offer USERID PASSWORT thus open for phishing and more
- **awareness is key but no tool to win the battle**
  - experience has shown that awareness can keep the situation stable – AT THE BEST
- **liabilities and contracts care more about services than users**
  - the effect: public services mostly stay away from cloud

eID PLUS IMPROVING CONTRACTS
A PROMISING COMBINATION FOR SUCCESS

CLOUD NEEDS TO RESPECT THE NEEDS

- **user and services** need to know the jurisdiction of partners and transactions
  - **THIS IS IN MANY WAYS UNCLEAR**
- **user and services** must have the sole control over data
  - **APPLICABLE JURISDICTION PLAYS A MAJOR ROLE AS SEEN IN THE RECENT PAST**
- **there is also a need for lawful access**
  - **AMONG JURISDICTIONS ESPECIALLY WHEN MIXED WITH PRIVATE SECTOR THIS IS AN OPEN QUESTION**

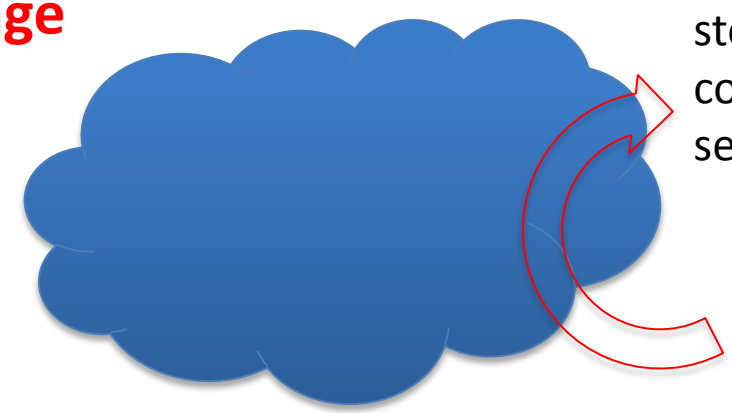
LIABILITY - JURISDICTION

- user need information, choice and control
- the need comes up at the point in time of intended communication
- transparent information about jurisdictions should be available with all services on request
- responsibility for providing such information needs to be evident

eID – SECURITY – MOBILE DEVICES

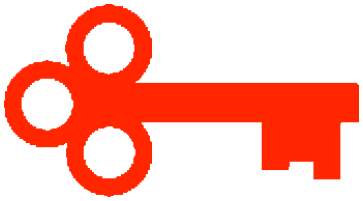
CLOUD

- future
- challenge



storage
collaboration
services

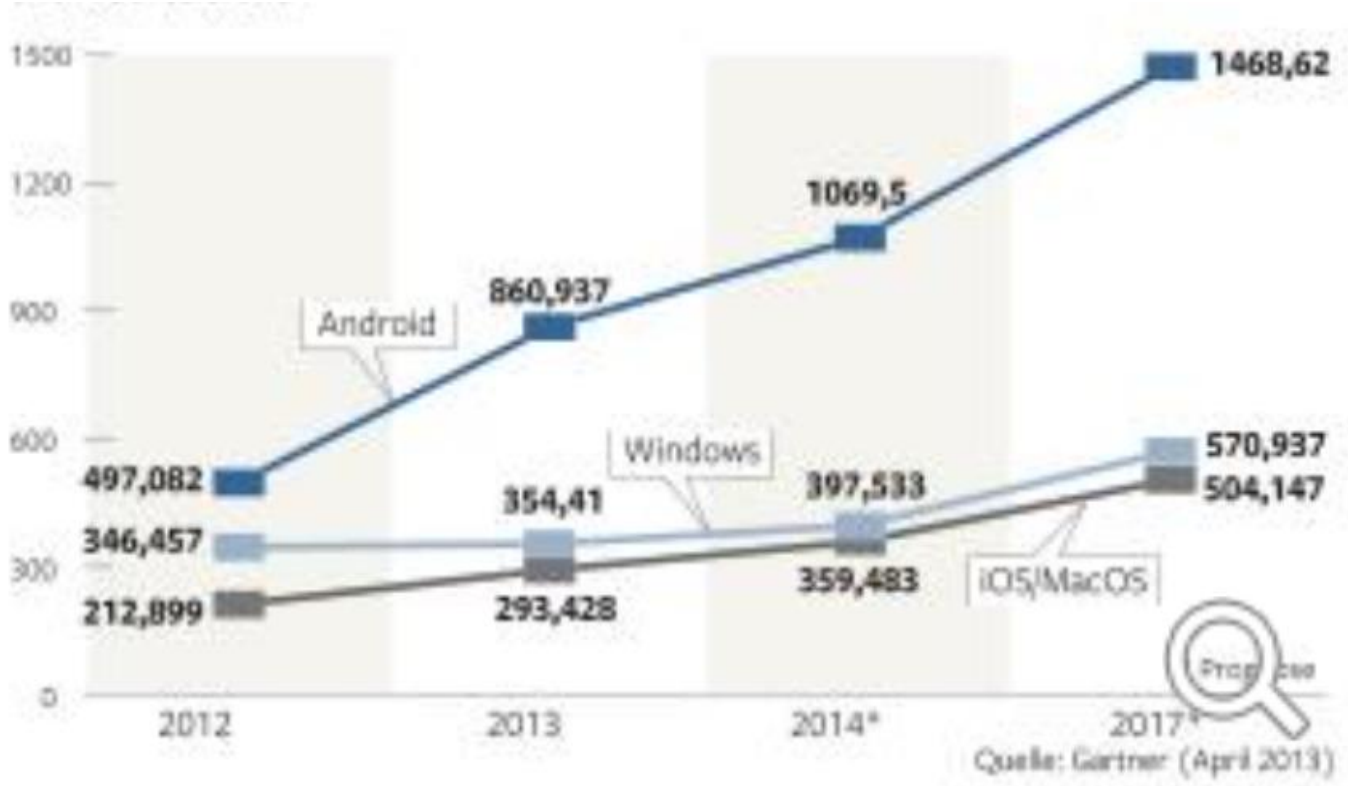
Tablet
Mobile
Laptop
PC ...



security service

eID
Signature
encryption

MOBILE DEVICES



THE LEAST SECURE IS THE MOST SUCCESSFUL?

A-SIT

challenges

- guarantee for a security perimeter
- map the security requirements into CLOUD
- map the security requirements into SERVICES
- ensure responsibilities and awareness

CRYPTO and the CLOUD

KEEPING USABILITY AND CONVENIENCE

OBSERVING NATIONAL INTERESTS

MANAGING THE COMPLEXITY

RESEARCH TO CLOSE THE OPEN ISSUES

CRYPTO UNDER NATIONAL CONTROL

KEEPING CONTROL OF COST AND EFFICIENCY

DATA PROTECTION AND SECURITY MIGHT ALLOW EUROPE TO APPROACH COMPETITIVENESS IN CLOUD COMPUTING.

A-SIT

PRODUCT CYCLE

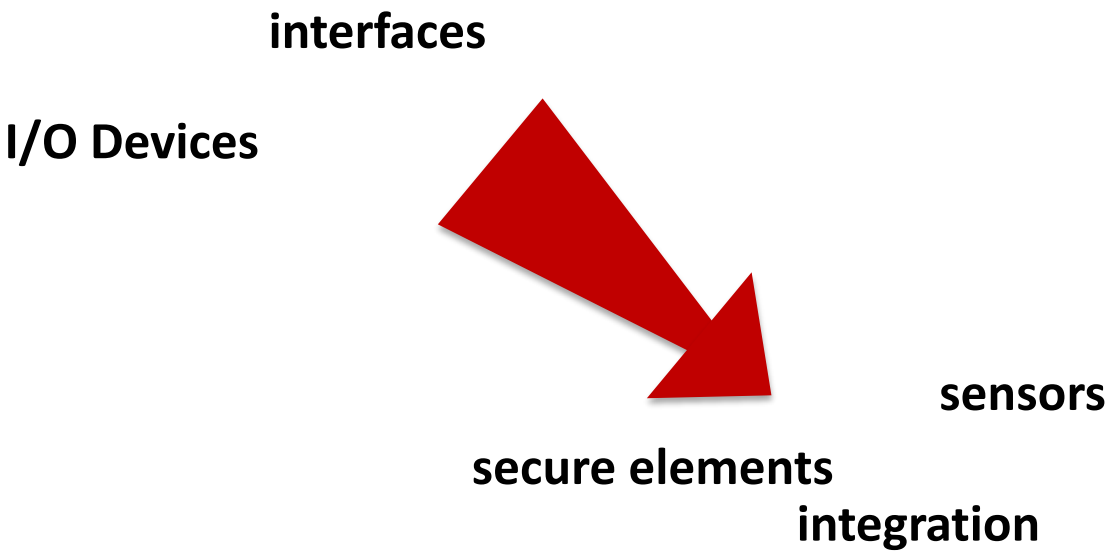
innovation **product** **regulation** **standards**

industry push to shorten

industry push to avoid hurdles

how are users empowered with their interest to shorten the period until standards are available ???

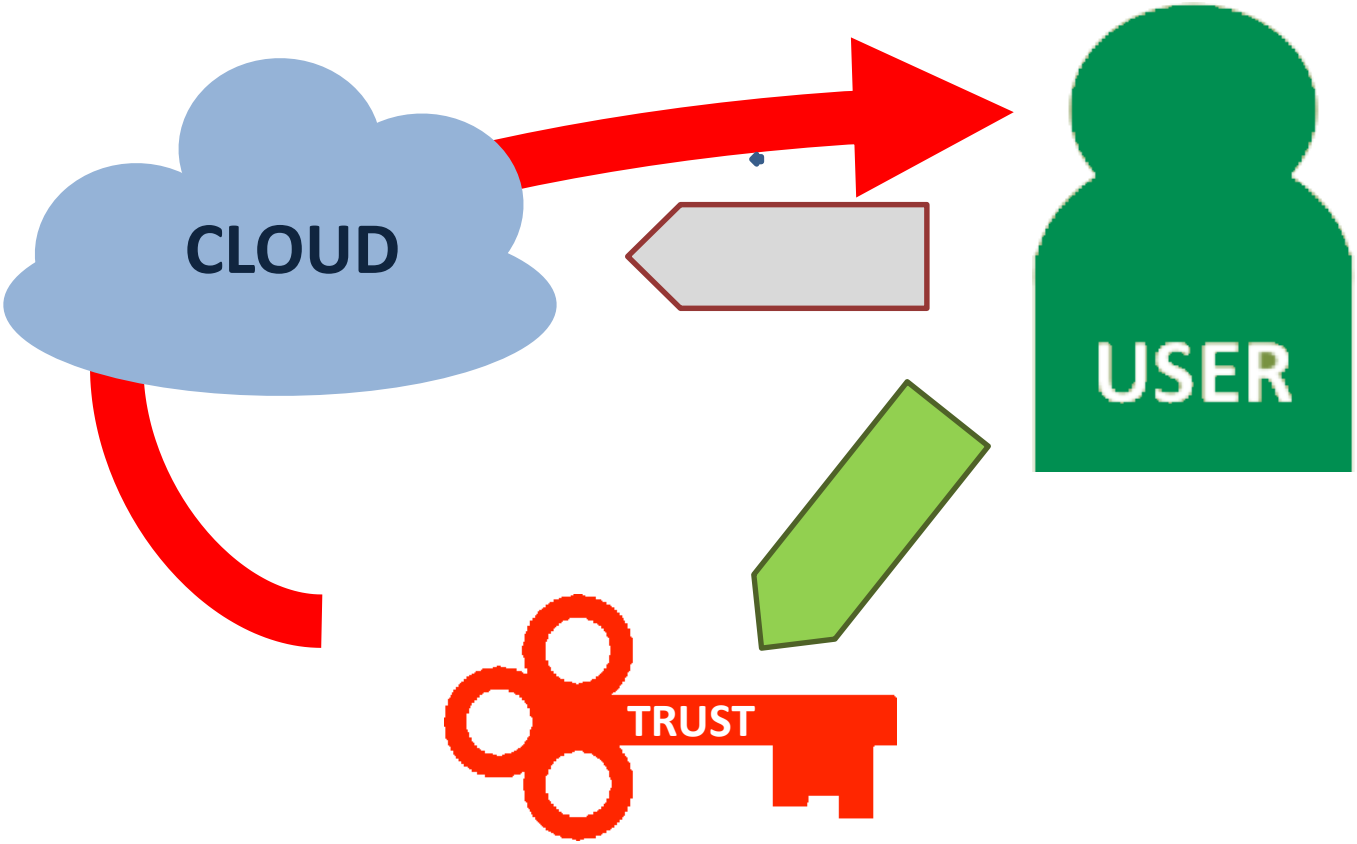
TECHNOLOGY – MOBILITY



the concept and the usability do not allow peripherals in practice.
Devices will be used as they are sold for the whole cycle.

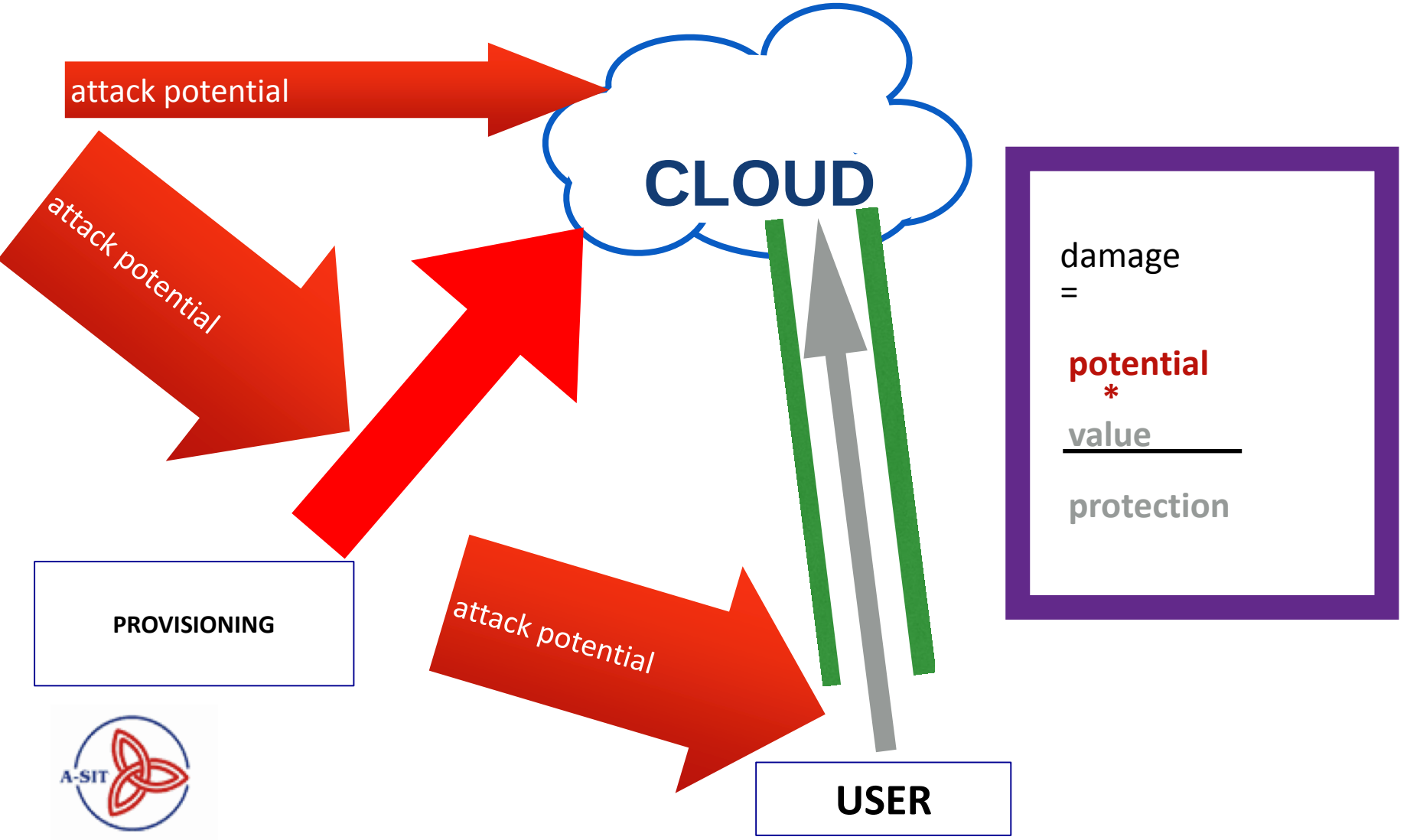
A-SIT

CLOUD AND TRUST



TRUST NEEDS TO BE ALLOCATED WITHIN THE SPHERE

CLOUD AND RISK



CLOUD : DOCUMENT COLLABORATION

DIGITAL:AUSTRIA

Office 365

Google Docs

Live Documents
Office for the Internet Generation

?

THERE HAS BEEN A SUBSTANTIAL CHANGE OVER THE LAST YEARS

CONTINUITY?

LOCK IN?

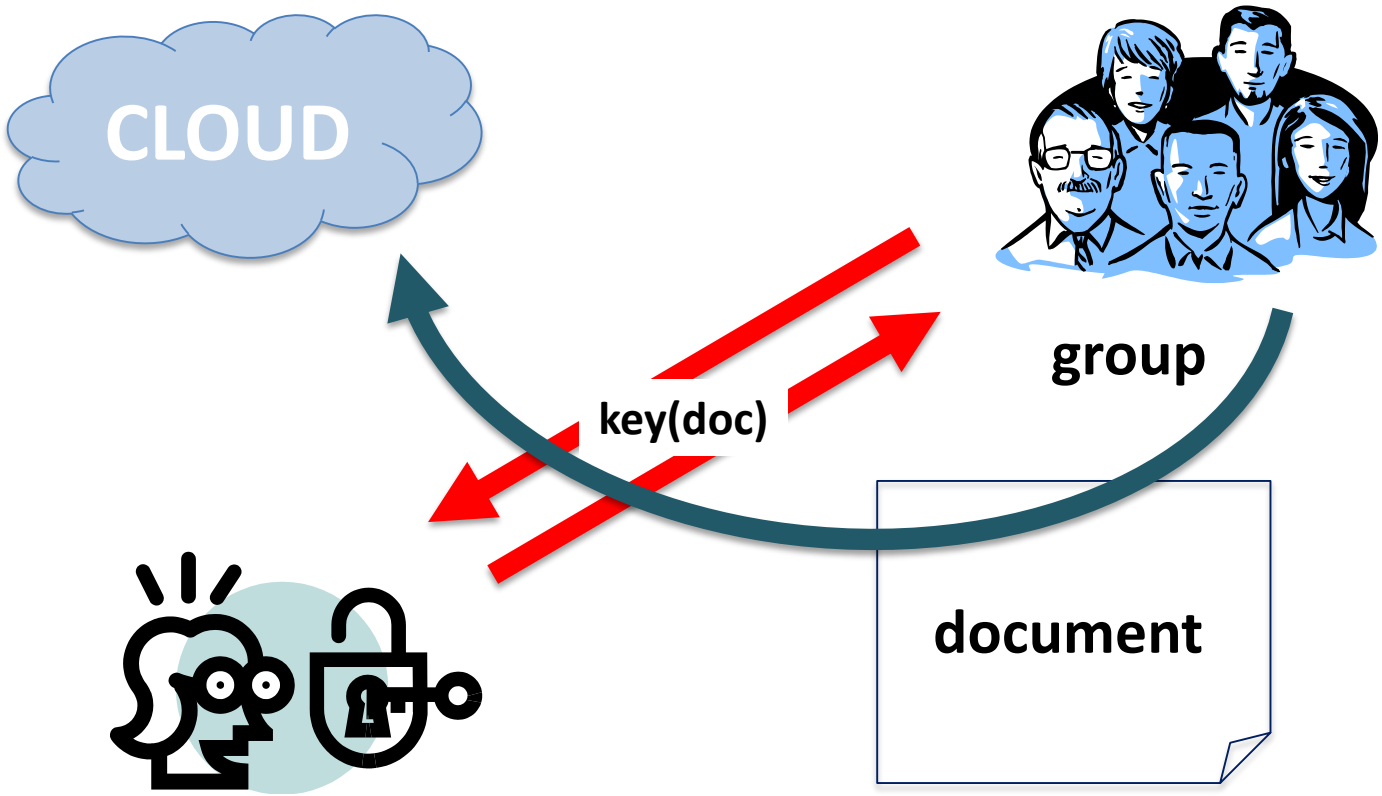
STANDARDS?

ALTERNATIVES?

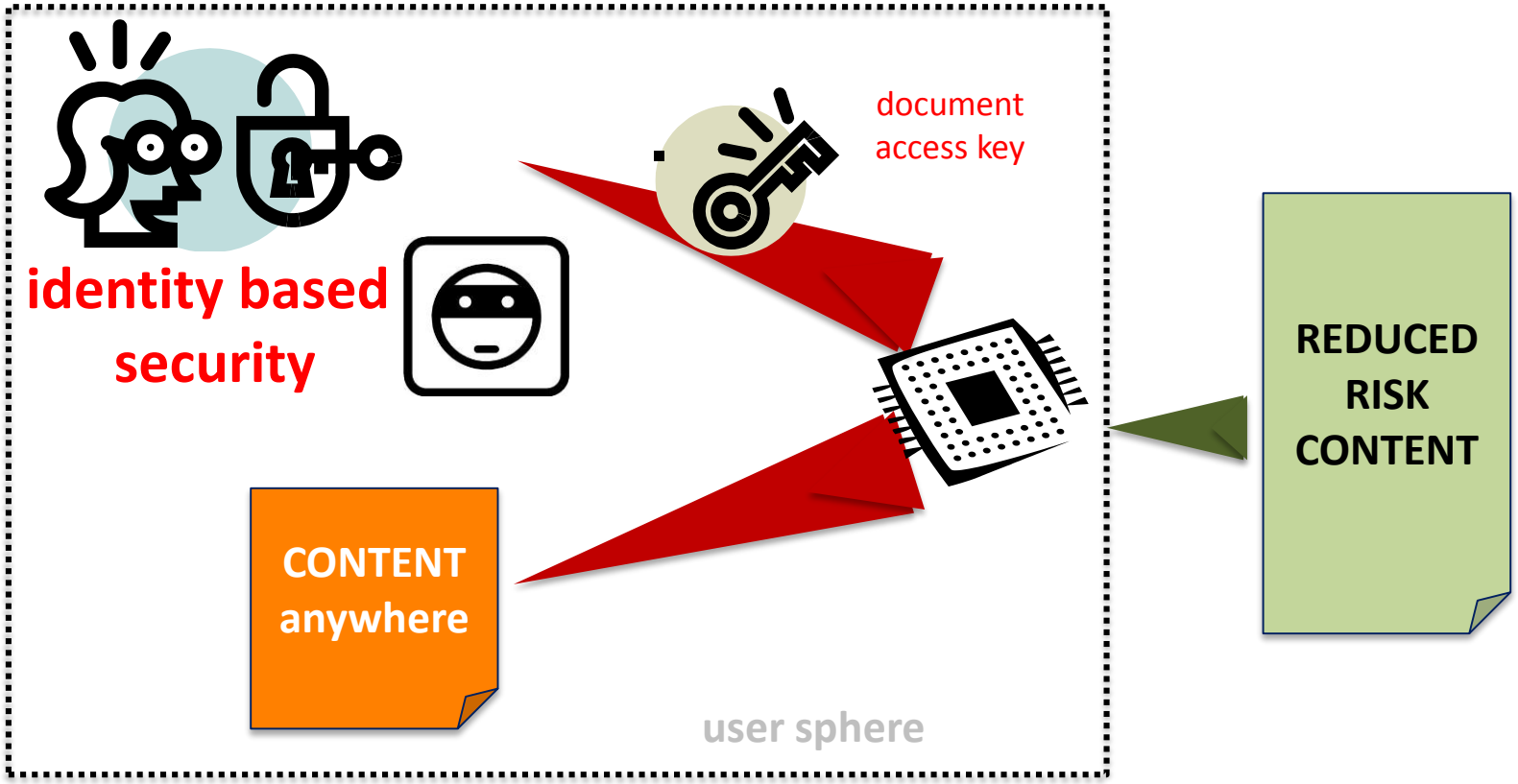
IMPACT ON OTHER SYSTEMS?

A-SIT

documents – collaboration



REDUCED RISK CONTENT



key per document:

$key(Doc_i) \neq key(Doc_j)$ if $i \neq j$

→ key per document use!

cyber security has a strong relation to prosperity
identity is the core of sovereignty
CLOUD opens up new dimensions but is a major security challenge at the same time
for the time being only security services in within the users security perimeter can preserve trust
documents and collaboration needs a specific focus to meet security and legal conformity

THANK YOU FOR LISTENING

REINHARD.POSCH@A-SIT.AT

A-SIT