ICT-Innovation

How digital sovereignty and it-security can help pushing Europe forward

Prof. Reinhard POSCH
reinhard.posch@cio.gv.at

RISK ASSESSMENT / SECURITY & HACKTIVISM

Symantec employees fired for issuing rogue HTTPS certificate for Google

Unauthorized credential was trusted by all browsers, but Google never authorized it.

by **Dan Goodin** - Sep 21, 2015 9:35pm CEST

Symantec has fired an undisclosed number of employees after they were caught issuing unauthorized cryptographic certificates that made it possible to impersonate HTTPS-protected Google webpages.

"We learned on Wednesday that a small number of test certificates were inappropriately issued internally this week for three domains during product testing," Symantec officials wrote in a blog post published Friday. "All of these test certificates and keys were always within our control and were immediately revoked when we discovered the issue. There was no direct impact to any of the domains and never any danger to the Internet."

The post went on to say that the unnamed employees were terminated for failing to follow Symantec policies. Symantec officials didn't identify the three domains the test certificates covered, but in a separate blog post, Google researchers said Symantec's Thawte-branded certificate authority service issued an Extended Validation pre-certificate for the domains google.com and www.google.com.

"This pre-certificate was neither requested nor authorized by Google," they wrote.

DIGITAL SOVEREIGNTY – HOW IS IT ENDAGERED

jurisdiction aware IT and communication

switching mobile connections – floating cross jurisdiction to reduce cost

push notification – always on a leash

cloud storage – do we have to fear about IPR

document collaboration – in the cloud as you type

certificates and updates – who controls what you use

DEMOCRATIC MODEL – GOVERANCE BY HUGE COMPANIES

SAFE HARBOR

Europäischer Gerichtshof: Datentransfer von EU in USA ist unzulässig

BIRGIT RIEGLER

6. Oktober 2015, 15:02

Wiener Jurist Max Schrems sieht Urteil als Meilenstein – Experte erwartet weitreichende Konsequenzen für Unternehmen

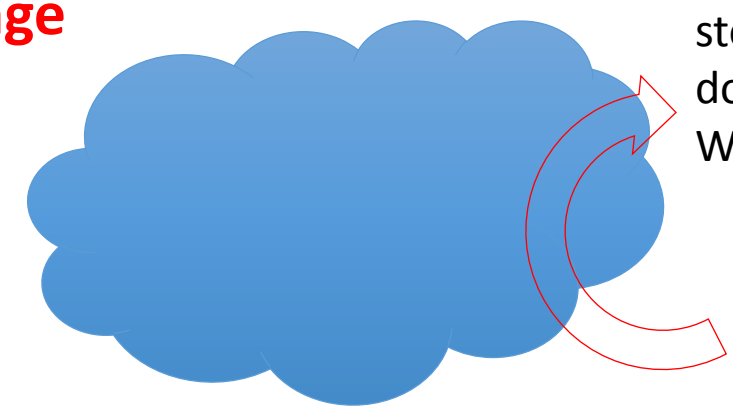
Der Europäische Gerichtshof hat am Dienstag das Safe-Harbor-Abkommen zwischen den USA und der EU für ungültig erklärt. Mit dem Abkommen wurde bisher festgehalten, dass personenbezogene Daten von EU-Bürgern in die USA übertragen und dort gespeichert werden dürfen. Die US-Unternehmen könnten dafür einen angemessenen Datenschutz bieten, hatte die EU-Kommission im Jahr 2000 entschieden. Nur gilt das seit den Enthüllungen rund um die NSA-Spionageaktivitäten nicht mehr, wie der Gerichtshof nun festgestellt hat.

SAFE HARBOR

EID – SECURITY – MOBILE DEVICES

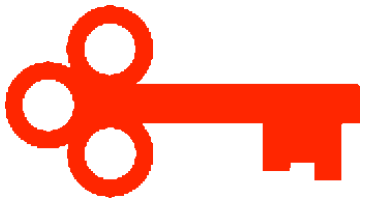
CLOUD

- **future**
- **challenge**



storage
documents - collaboration
WEB SERVICES

Tablet
Handy
Laptop
PC ...

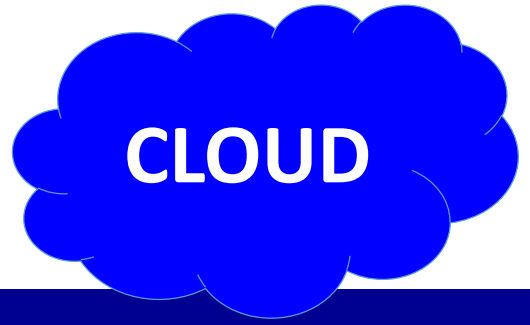


security services

identification
signature
encryption

eID – BASIS OF SOVEREIGNTY

BIG PLAYER IN THE CLOUD – EU LEGISLATION



- eIDaS assigns control on electronic identity and supervision to member states not to cloud provider
- technical and legal schemes with big PUBLIC CLOUDs need adjustments to comply with technical and legal requirements

A-SIT

no security without identity

- before defending interests we need to know and identify the partners
  - multi factor identification
  - crypto based identification
  - robust against replay
  - simple for users
  - broad acceptance

STORK – the root of EU eID

- assuming minimum security
- mutual recognition – technology, legal
- Interoperability – protocol
- for administration and private sector

model for eIDaS

A-SIT

BADUSB - ON ACCESSORIES THAT TURN EVIL

USB has become so commonplace that we rarely worry about its security implications. USB sticks undergo the occasional virus scan, but we consider USB to be otherwise perfectly safe – until now.

This talk introduces a new form of malware that operates from controller chips inside USB devices. USB sticks, as an example, can be reprogrammed to spoof various other device types in order to take control of a computer, exfiltrate data, or spy on the user.

We demonstrate a full system compromise from USB and a self-replicating USB virus not detectable with current defenses.

We then dive into the USB stack and assess where protection from USB malware can and should be anchored.

PRESENTED BY

Karsten Nohl & Jakob Lell

Im Rubber Ducky steckt ein progarmmierbarer Computer, der sich dem PC gegenüber als Tastatur ausgibt.

NO SECURITY WITHOUT HRDWARE
NO SOVEREIGNTY W/O HW SUPPORT

BASIC NEEDS MUST NOT FADE AWAY WITH CLOUD

- **user** and **services** need to know about jurisdictions for data in rest and in transit
  - **NOT YET EVIDENT IN PRACTICAL SITUATIONS**
- **user** and **services** need to make sure that they are the only ones having access to content
  - **IMPORTANCE BECAME EVIDENT ALONG WITH RECENT SITUATIONS**
- **law enforcement and interception** may be needed on a national level
  - **STILL UNSOLVED AND HARDLY EVER DISCUSSED FOR GOVERNMENT DATA CROSS BORDER**

A-SIT

JURISDICTION MATTERS WITH LIABILITY

- users need to keep control and possibly choice
- relevant jurisdictions to be known at the time of communication
- availability at all services to allow taking advantage
- needed to assign responsibilities

COMPULRORY SECURITY SUITES
DNSSEC + TLS w CLIENT CERTIFICATE
PROVIDER INFRASTRUCTURE ENHANCEMENTS

A-SIT

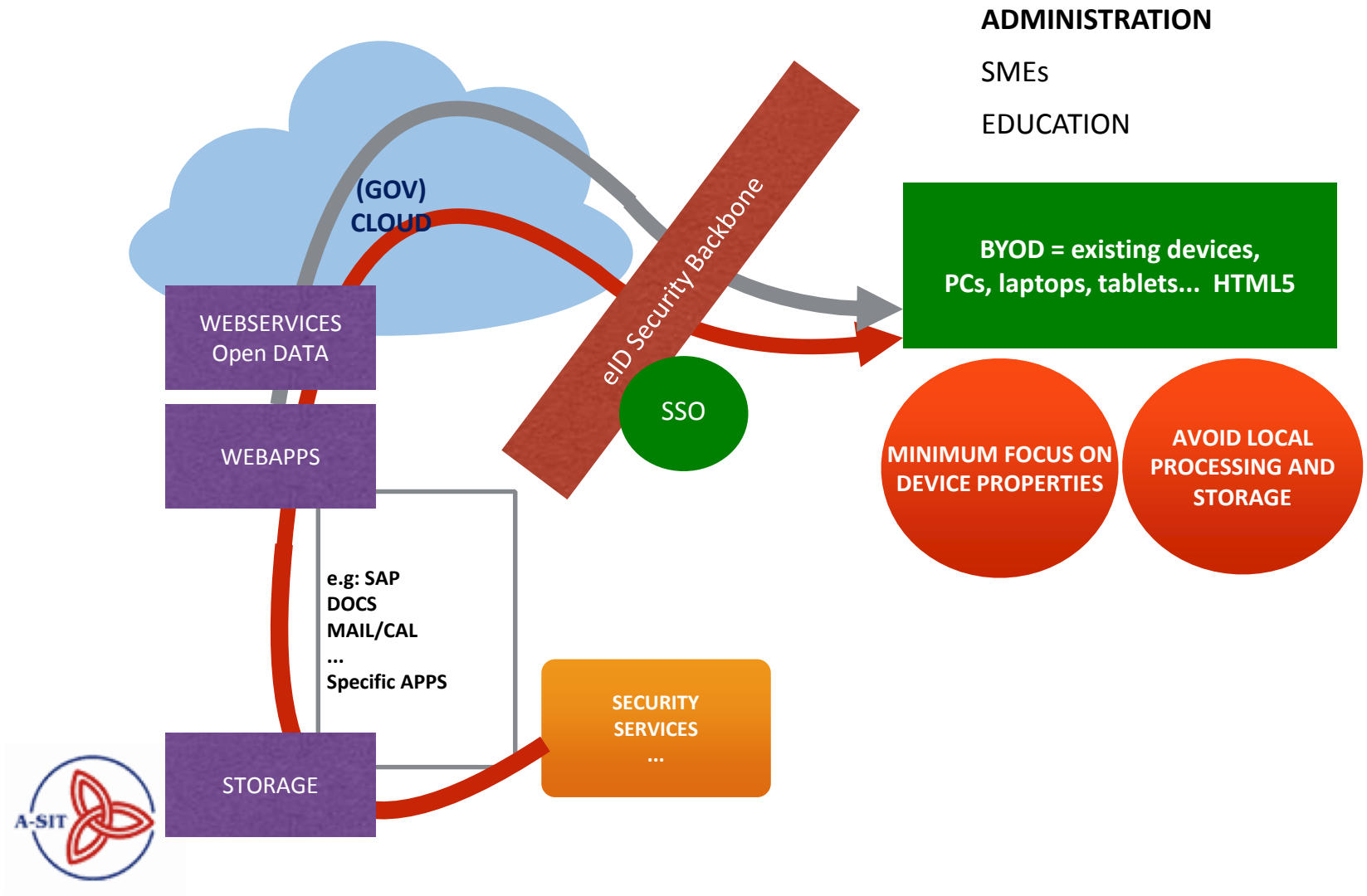
The Seattle Times
Winner of Nine Pulitzer Prizes

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.

CLOUD : COMMUNICATION AND TRUST



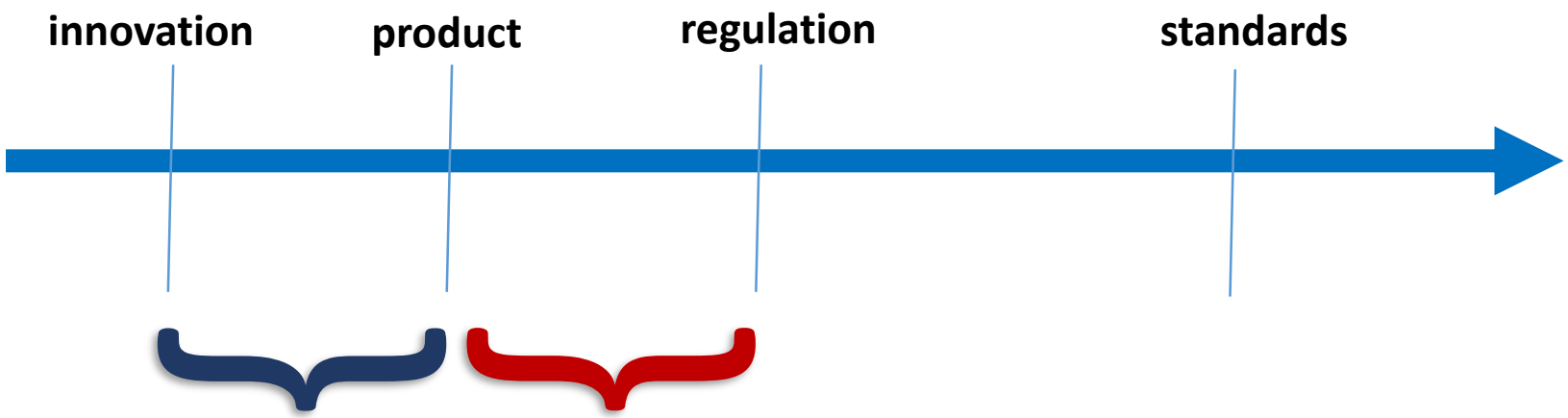
CRYPTO and CLOUD

EUROPE COULD PLAY A COMPETENT ROLE

A-SIT

TECHNOLOGY – PRODUCTS – RULES

implementation – cycle

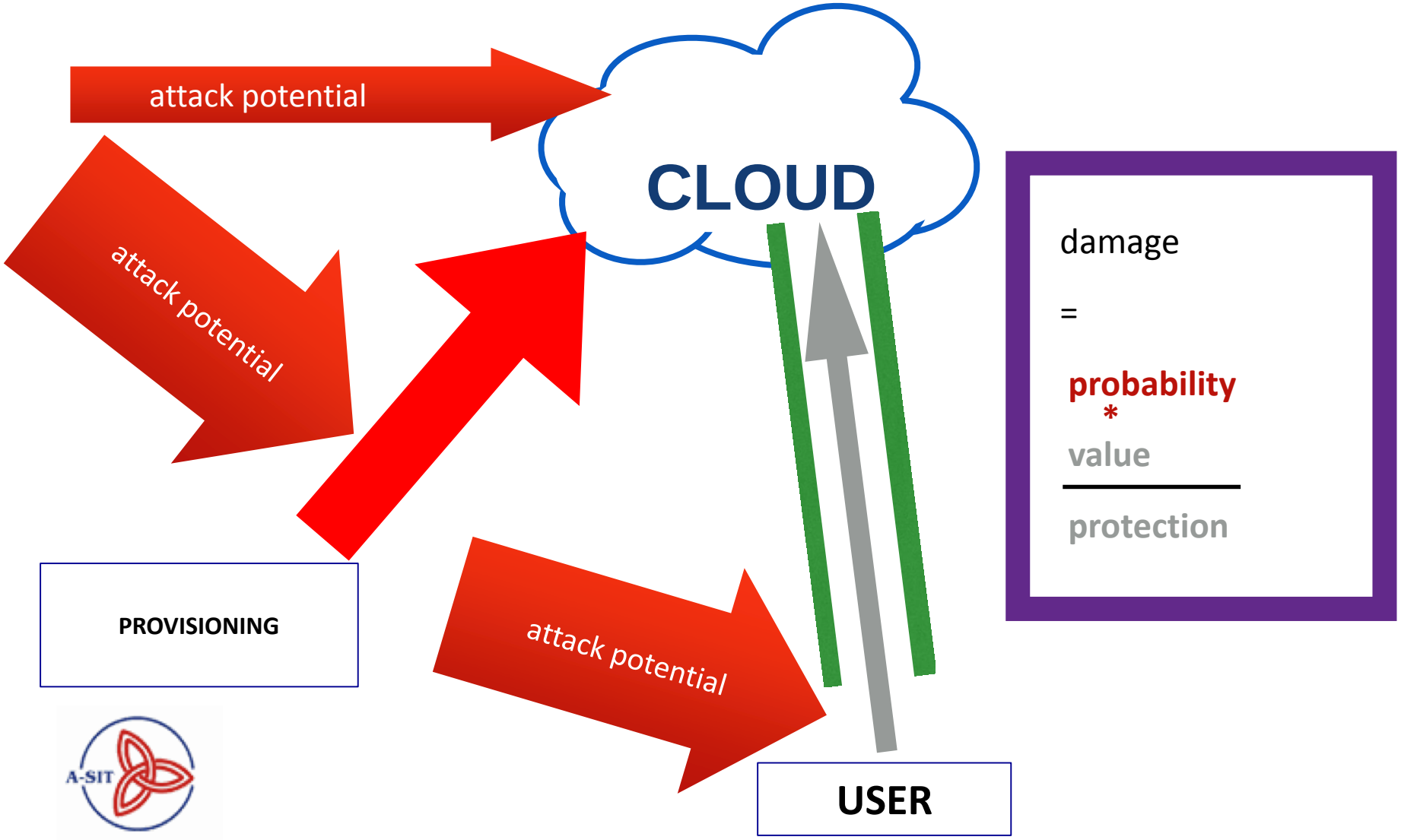


Industry to care for an as short as possible interval

industry pushing to avoid hurdles

who empowers users to be able to minimize the time to standards??

CLOUD AND RISK



innovation and digital sovereignty

industry taking innovation to products

avoiding the selling to overseas

industry 4.0

Data protection?
Security?
Applications?
Sovereignty?

THE FUTURE OF DOCUMENTS

Office 365

Google Docs

Live Documents
Office for the Internet Generation

?

EDITING DOCUMENTS
THE CHANGE IS ON THE WAY

CONTINUITY?

LOCK IN?

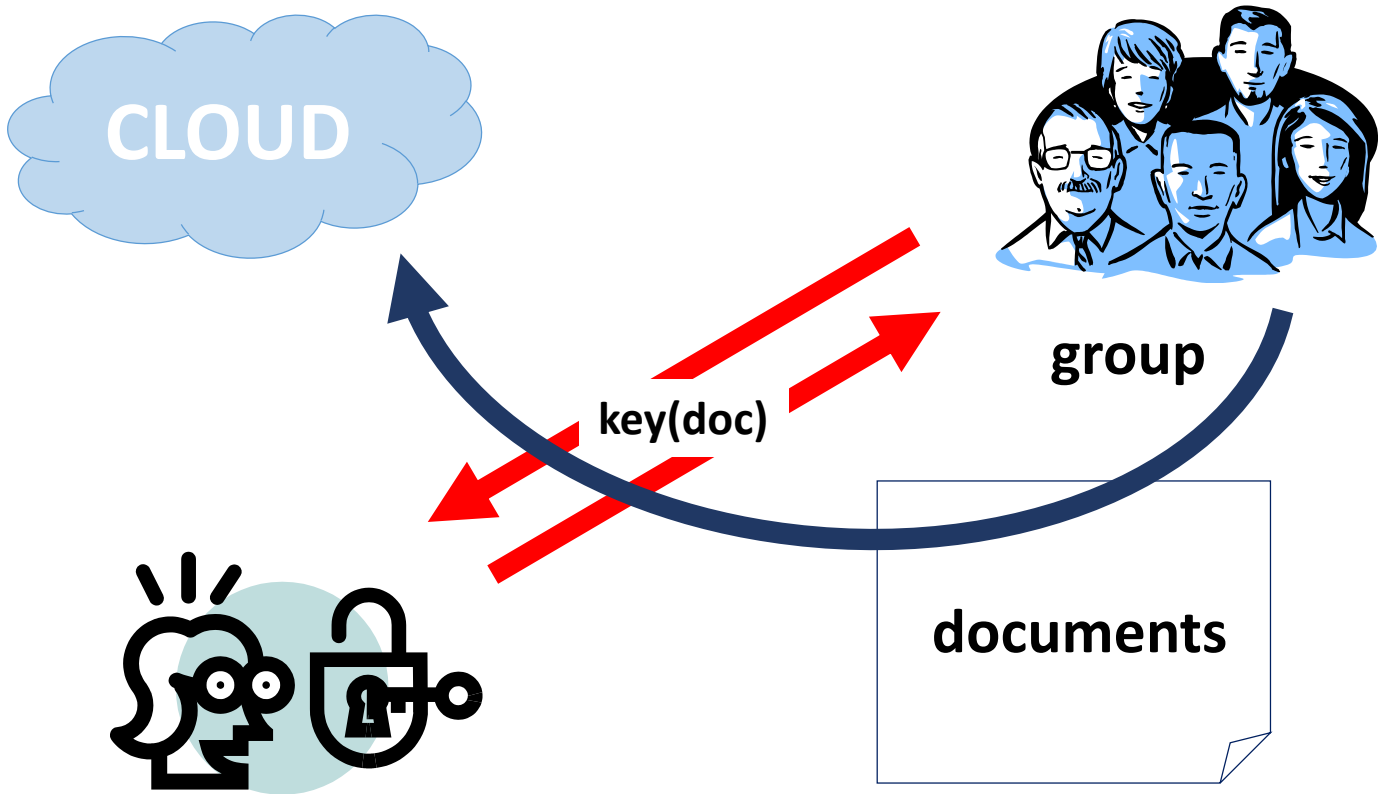
STANDARDS?

ALTERNATIVES?

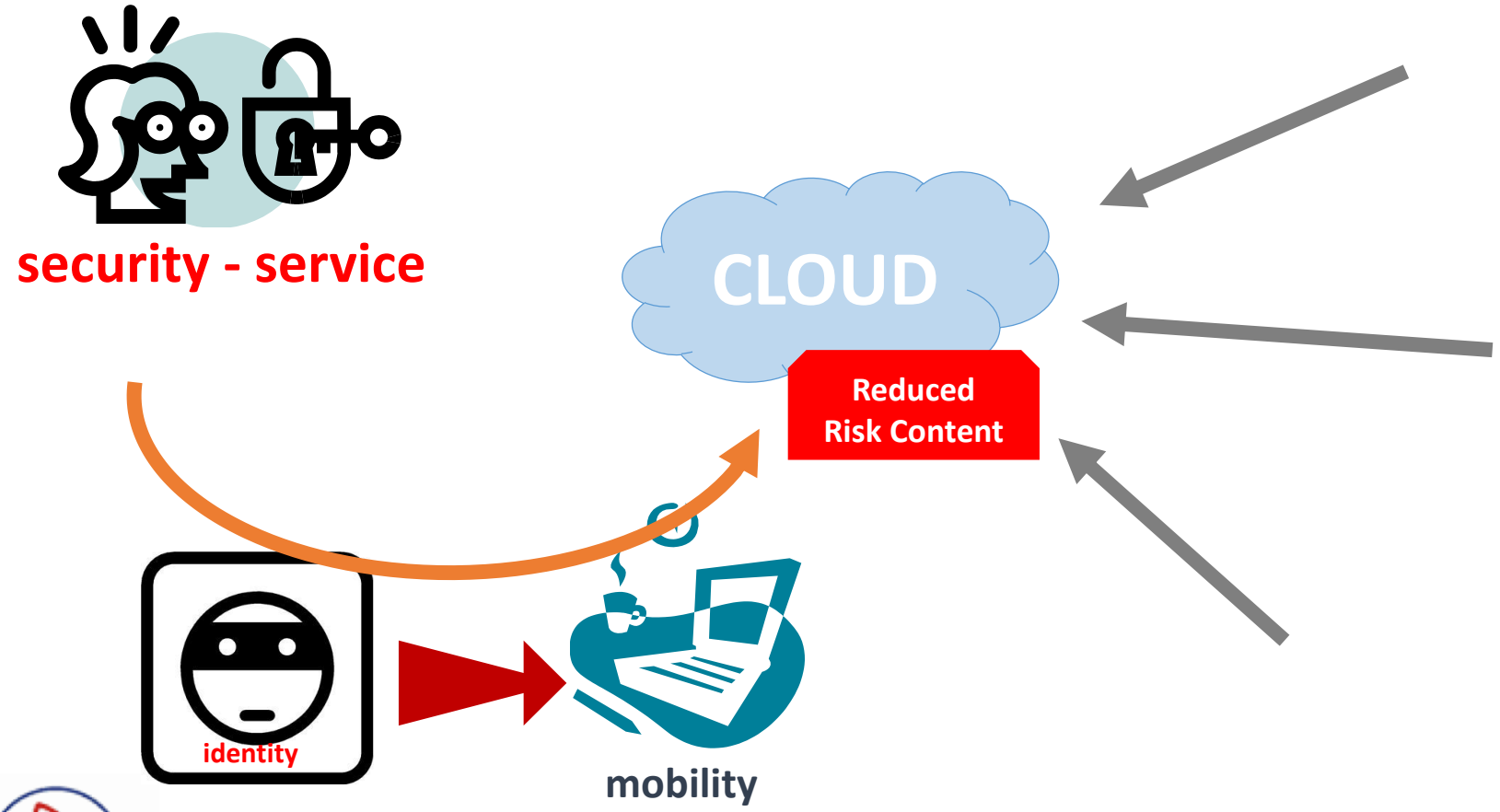
WHAT DOES THIS MEAN TO OTHER SYSTEMS?

A-SIT

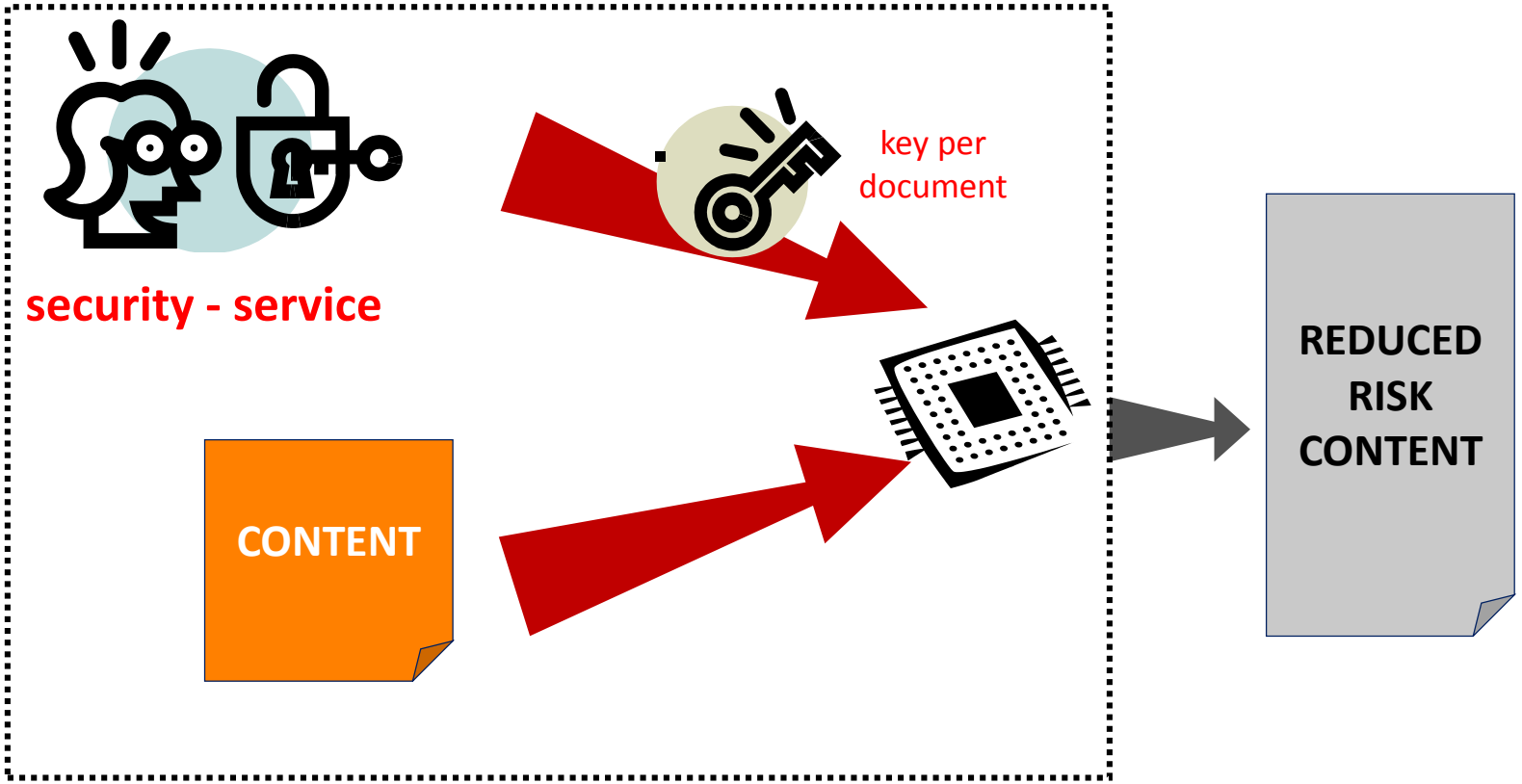
documents – collaboration



USER – GOVERNANCE – CONTROL



REDUCED RISK CONTENT



document per key

key(Doc$_i$) ≠ key(Doc$_j$) falls i ≠ j

REDUCED RISK CONTENT

→calendar (… tasks)	SMIME
→mail	SMIME
→documents	SMIME
→collaboration	??????

security has to be bound to identity in all cases!

TTIP – SAFE HARBOR

TTIP – WILL THE PUZZLE FIT?

we certainly need a closer look

WHAT NOW

chaos or chance?

A-SIT

SECURITY= STRENGTH * TAKE-UP

If we miss out on one – we loose
If we loose this formula – we loose the game