CLOUD SECURITY

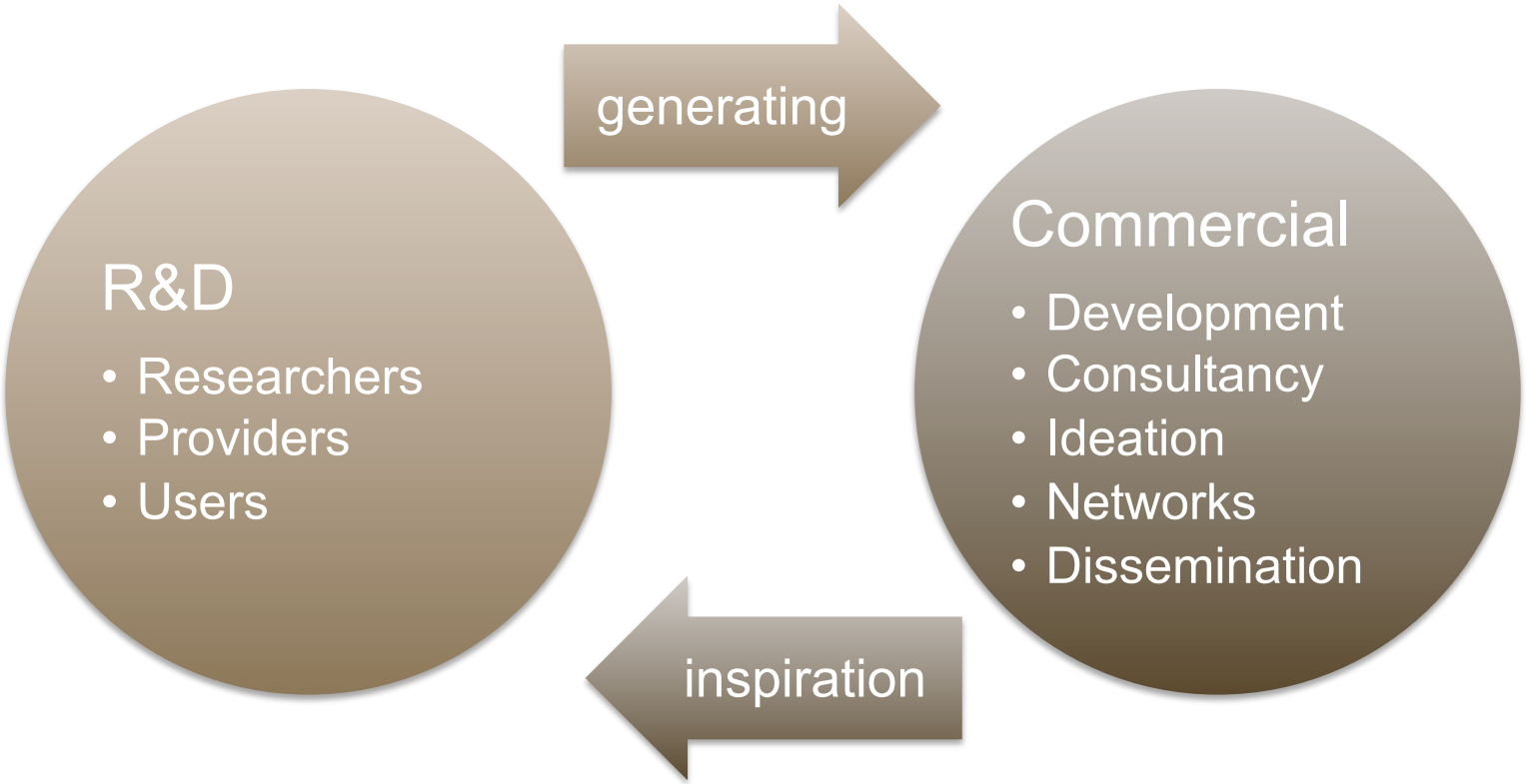
OR: HOW I LEARNED TO STOP WORRYING AND LOVE THE CLOUD

PUBLIC

Jakob I. Pagter
Alexandra Instituttet A/S

About ”Alexandra Instituttet A/S”

- Non-profit application oriented research institution – focus on IT
- GTS – Godkendt Teknologisk Service Institut
- 100+ employees



ALEXANDRA INSTITUTTET

Essential Characteristics of Cloud Computing

On-demand self-service

- provision computing capabilities automatically without requiring human interaction

Broad network access

- Capabilities are available over the network promote use by heterogeneous thin or thick client

Measured Service

Resource usage can be monitored, controlled, and reported, providing transparency

Rapid elasticity

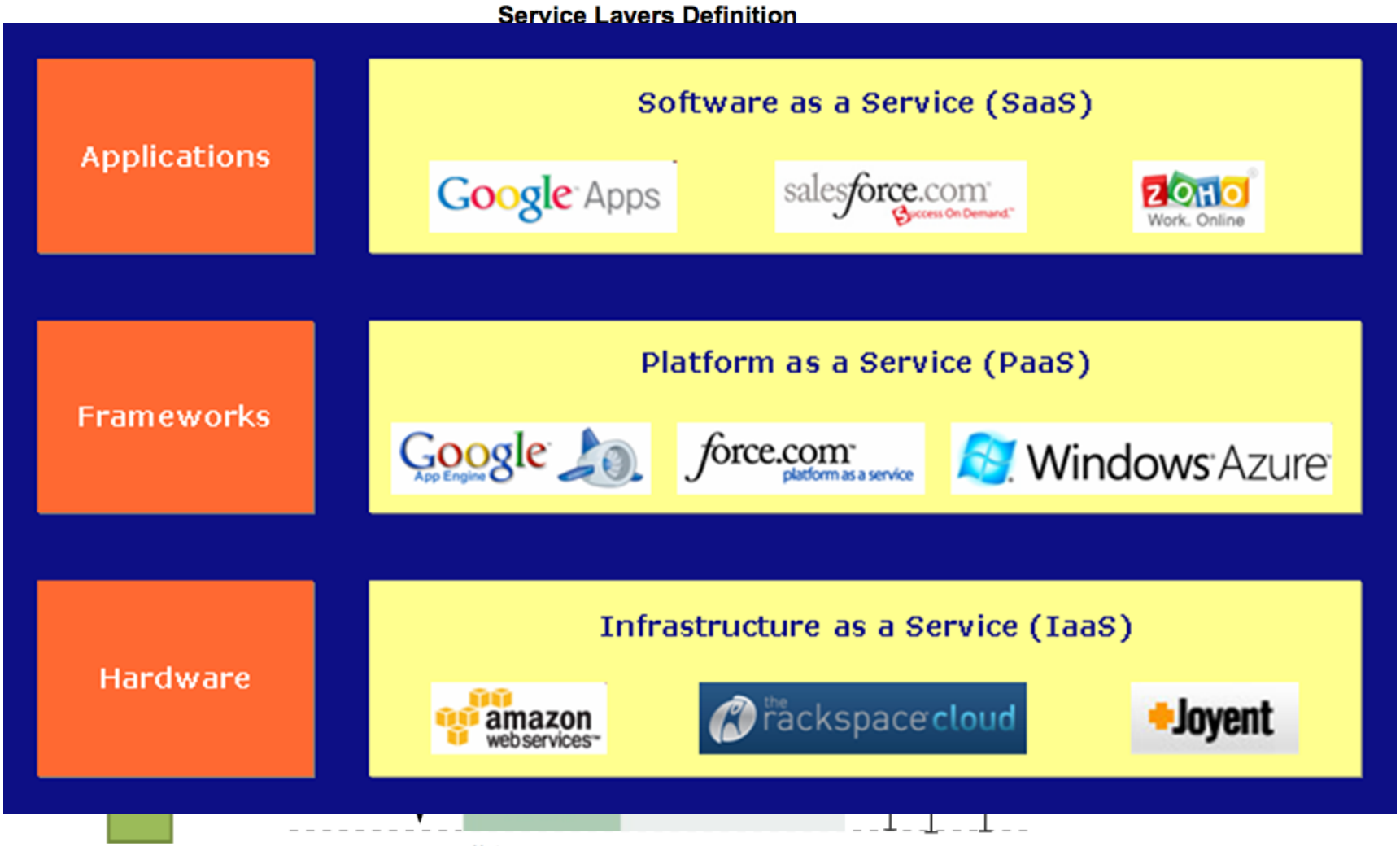
- Capabilities can be rapidly and elastically provisioned, automatically, to quickly scale out or rapidly scale in

Resource pooling

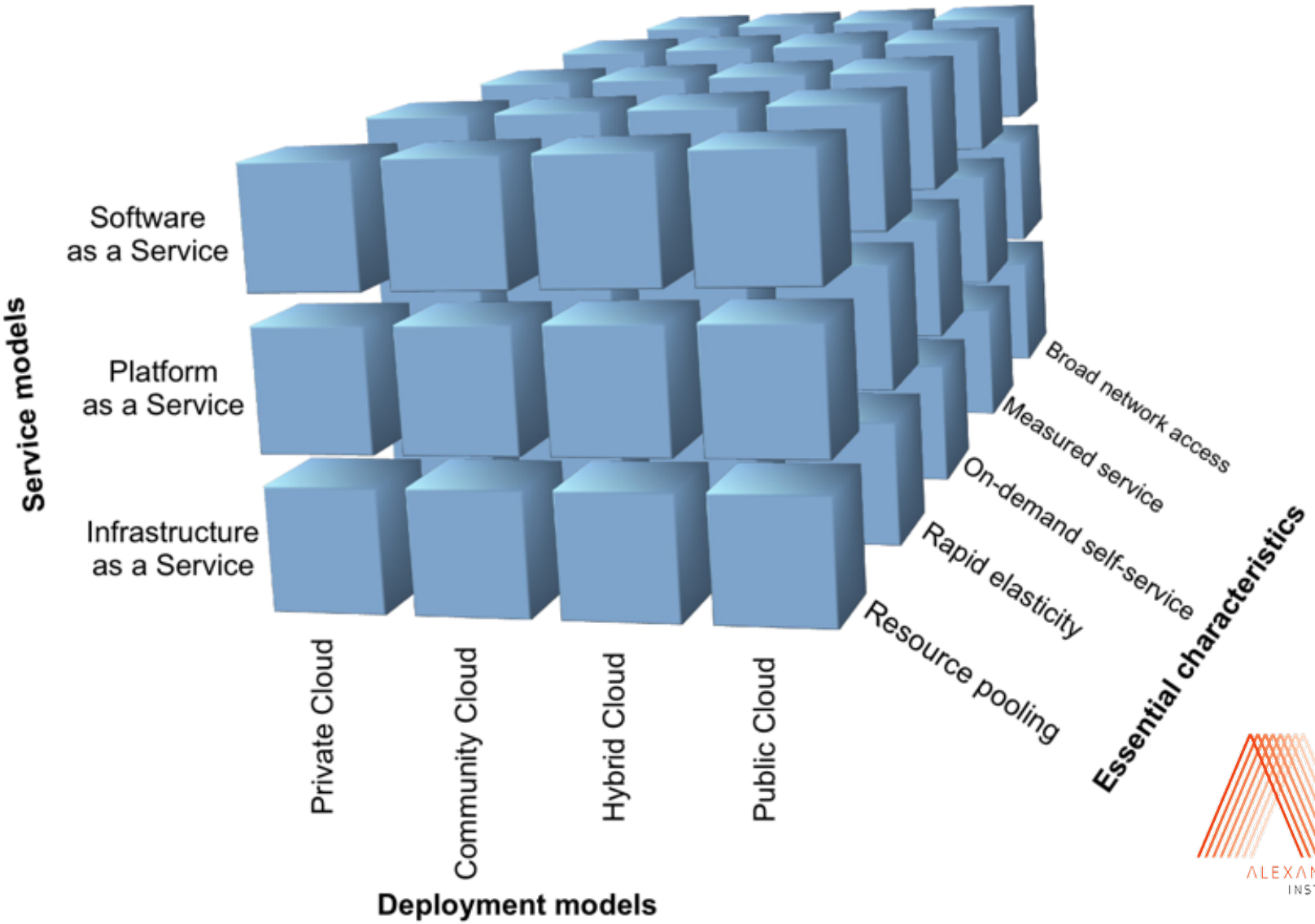
- A sense of location independence. customer has no control or knowledge over the location of the resources

ALEXANDRA INSTITUTTET

Cloud Service Models -



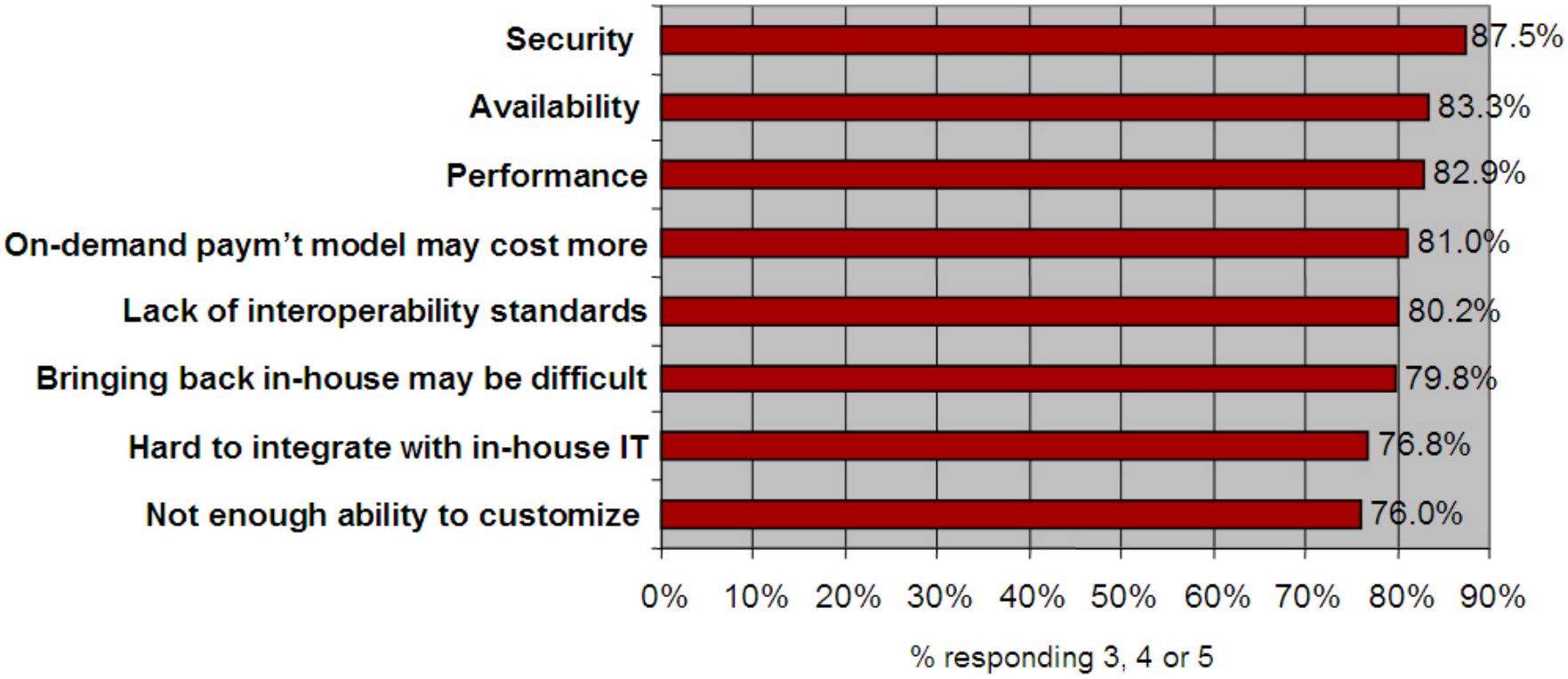
NIST Visual Model of Cloud Computing Definition



ALEXANDRA INSTITUTE

Q: Rate the challenges/issues of the 'cloud'/on-demand model

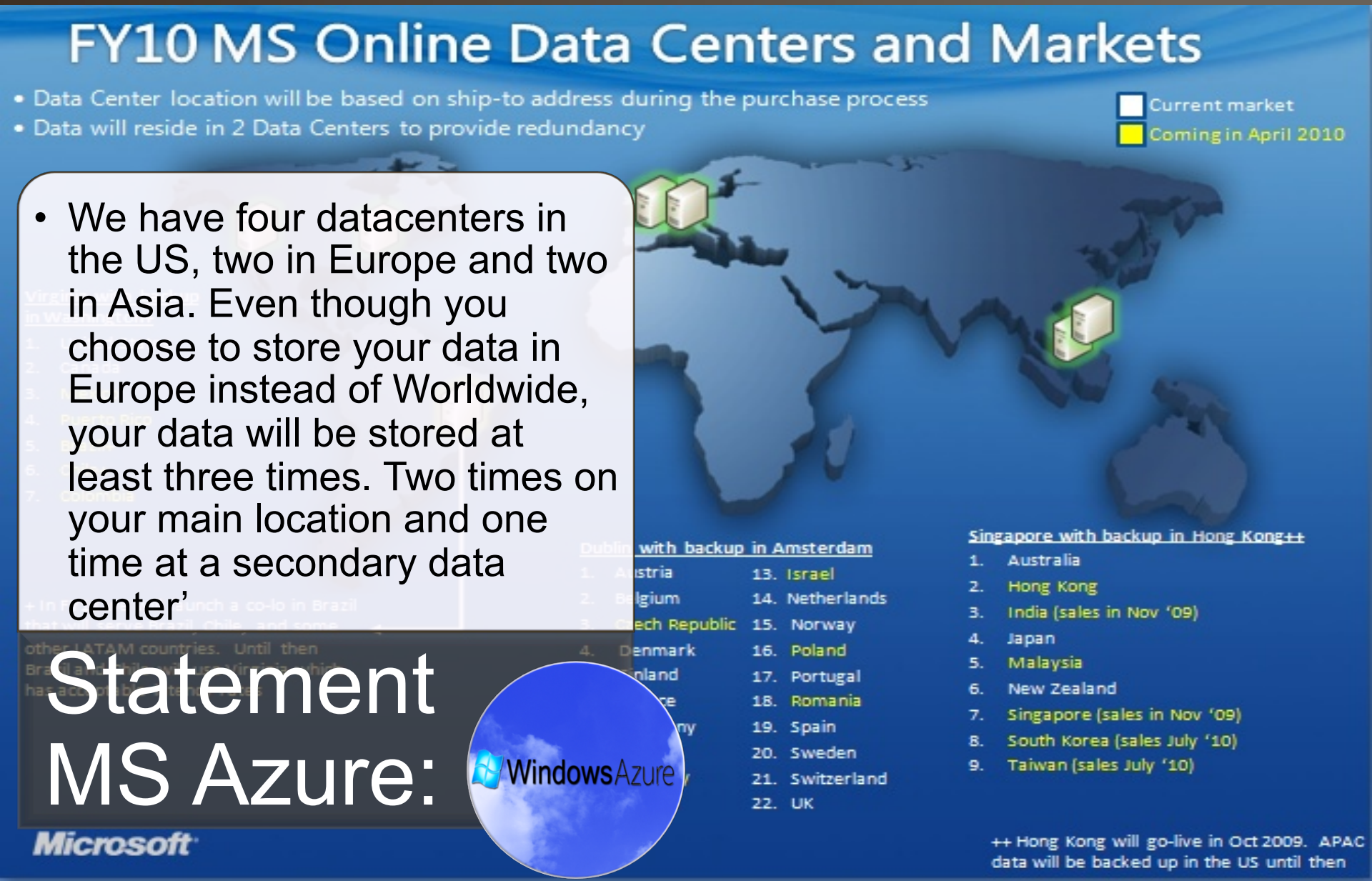
(Scale: 1 = Not at all concerned 5 = Very concerned)



Source: IDC Enterprise Panel, 3Q09, n = 263

ALEXANDRA INSTITUTTET

Governance and compliance



- We have four datacenters in the US, two in Europe and two in Asia. Even though you choose to store your data in Europe instead of Worldwide, your data will be stored at least three times. Two times on your main location and one time at a secondary data center'

Statement MS Azure:

COMPUTERWORLD

Subscribe to a Newsletter

Topics | News | In Depth | Reviews | Blogs | Opinion | Shark Tank

Government/ Industries | Financial Services | Gov't Legislation/Regulation | Health Care | IT Indus

Home > Government/Industries > Gov't Legislation/Regulation

News

EU upset by Microsoft warning on U.S. access to EU cloud

By Jennifer Baker

July 5, 2011 12:28 PM ET

1 Comment | Like 31

IDG News Service - Members of the European Parliament have demanded to know what lawmakers intend to do about the conflict between the European Union's Data Protection Directive and the U.S. Patriot Act.

The issue has been raised following Microsoft's admission last week that it may have to hand over European customers' data on a new cloud service to U.S. authorities. The company may also be compelled by the Patriot Act to keep details of any such data transfer secret. This is directly contrary to the European directive, which states that organizations must inform users when they disclose personal information.

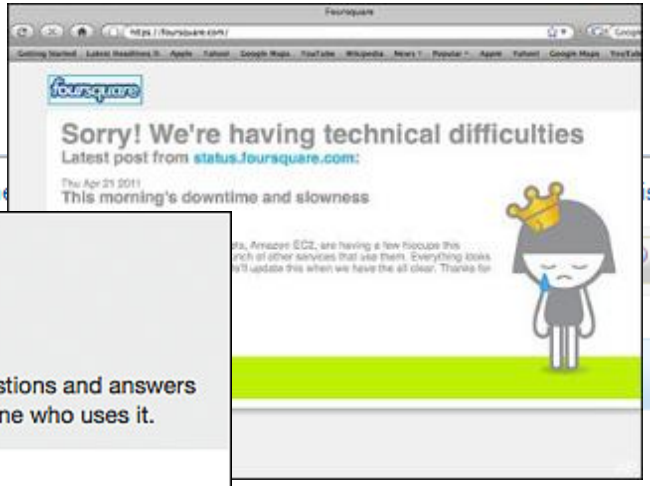
consider that the U.S. Patriot Act thus effectively
Protection? What will the Commission do
protection rules can be
take precedence
over
ment's
civil liberties comm

Note: MS first movers on EU standard contract clauses

ALEXANDRA INSTITUTTET

SLA's

http://aws.amazon.com/message/65648/



amazon web services™

Sign in to the AWS Manageme

AWS | Product

Quora

A continually improving collection of questions and answers created, edited, and organized by everyone who uses it.

We're currently having an unexpected outage, and are working to get the site back up as soon as possible. Thanks for your patience.

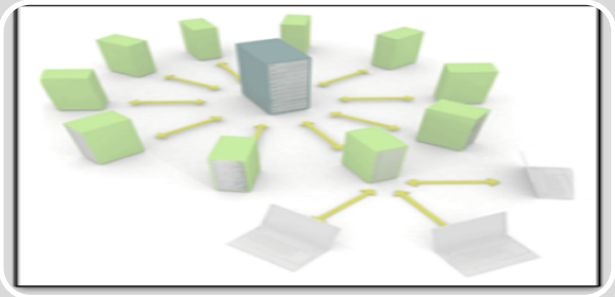
Summary of the Amazon EC … East Region

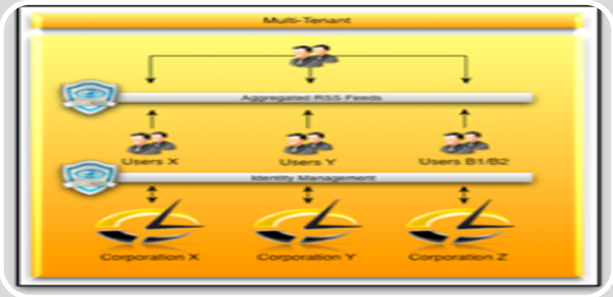
Amazon is currently experiencing a degradation. They are working on it. We are still waiting on them to get to our volumes. Sorry.

N… our customers about the
e… rvices, and what we are doing t
p… antly impacted by this event,
a… will improve the service for our
c…

T… volved a subset of the Amazon Elastic Block Store ("EBS") volumes in a single
A… unable to service read and write operations. In this document, we will refer to these
a… these affected volumes to also get "stuck" when they attempted to read or write to
t… EBS cluster in that Availability Zone, we disabled all control APIs (e.g. Create
V… shot) for EBS in the affected Availability Zone for much of the duration of the even
F… raded EBS cluster affected the EBS APIs and caused high error rates and latencies
fo… ion. As with any complicated operational issue, this one was caused by several root causes interacting with one another and therefore gives us many opportunities to protect the service against any similar event reoccurring.

Multi-Tenancy





Multi-Tenancy

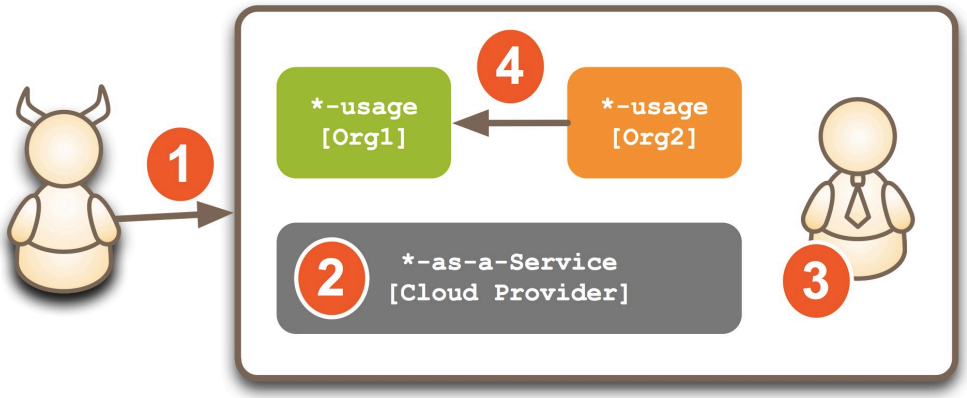
- one program, need to serve at the same time the number of consumer organizations (Tenants)

Separation

- Solution that supports Multi-Tenancy, capable of creating separation between the different Tenants

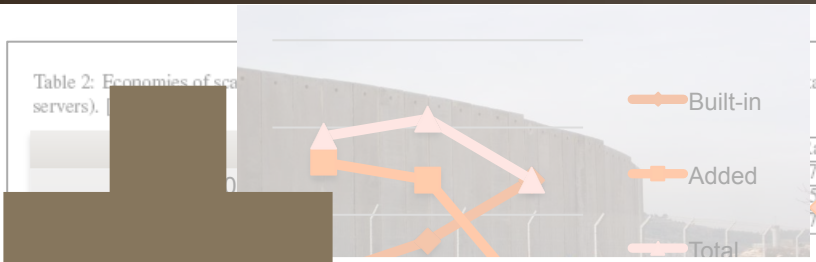
Technical attack vectors

1. Outsiders
2. Platform
3. Insiders
4. *Neighbours*



ALEXANDRA INSTITUTTET

Business pros (and cons!)



Economies of scale

Fate-sharing

Cost

Agility

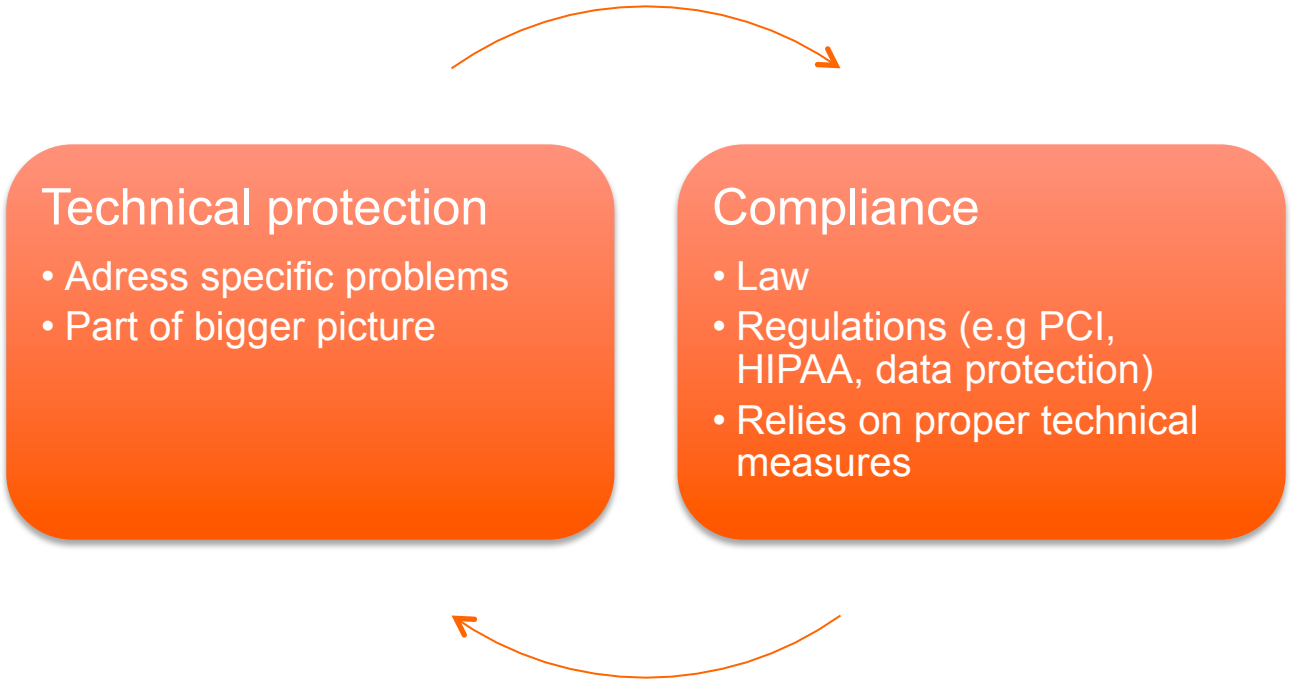
Innovation

Location/ Compliance

SLA's

Multi-tennancy/ Virtualization

Two problems

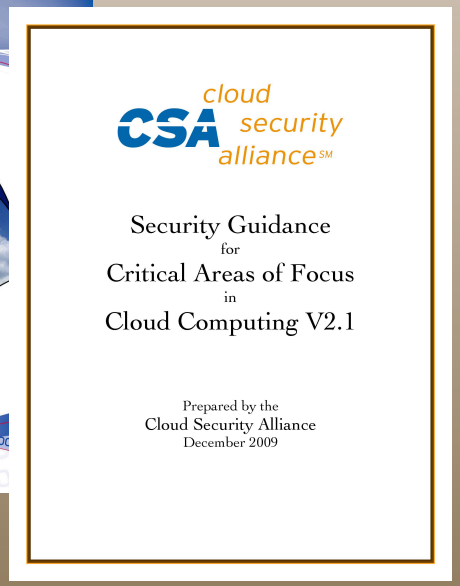


ALEXANDRA INSTITUTTET

Two approaches

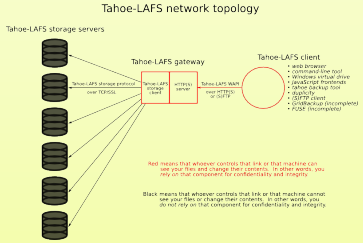
Ide → Vurdering → Analyse → Realisering → SLA'ing → Security by design

SLA'ing



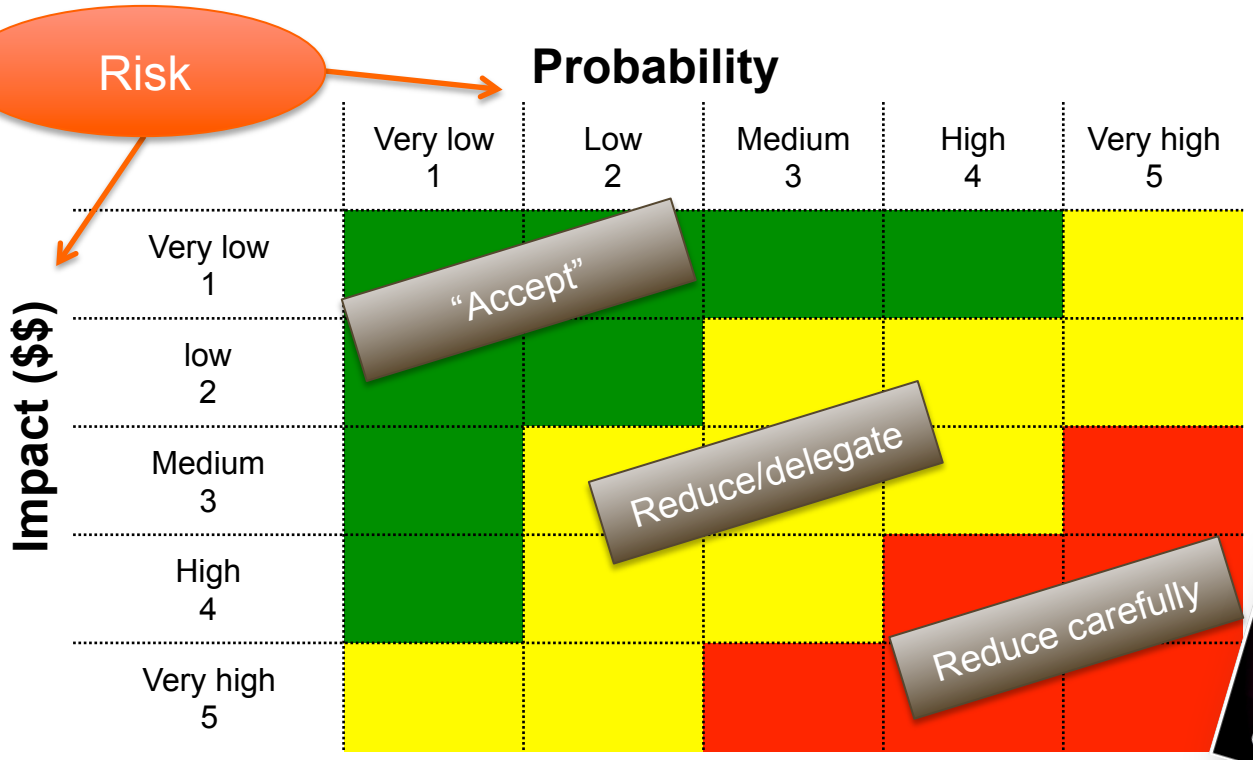
Security by design

- Adapt to user capabilities
- Exploit existing protection
- Divide-and-conquer



ALEXANDRA INSTITUTTET

But first – “go old school”



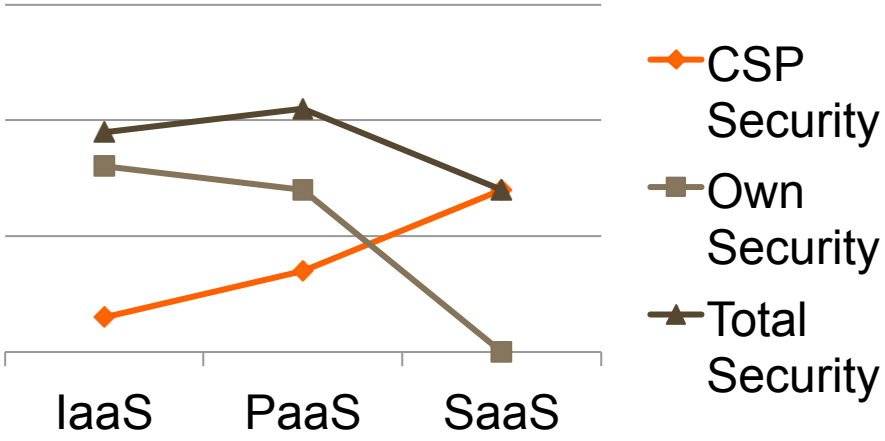
Good security is *business driven*!

Good analysis is *knowledge driven*!

ALEXANDRA INSTITUTTET

Security by design using cryptography

- Adapt to user capabilities
- Exploit existing protection
  - Understand first!
- Divide-and-conquer
  - Trust, classification, …



- Understand context
  - Protection level <-> key sizes
  - What does and doesn't crypto provide
  - When aren't data encrypted
- Don't DIY
- Protect the key!

ALEXANDRA INSTITUTTET

Context – key sizes!

Level	Protection	Symmetric	Asymmetric	Hash
1	Attacks in "real-time" by individuals *Only acceptable for authentication tag size*	32	-	-
2	Very short-term protection against small organizations *Should not be used for confidentiality in new systems*	64	816	128
3	Short-term protection against medium organizations, medium-term protection against small organizations	72	1008	144
4	Very short-term protection against agencies, long-term protection against small organizations *Smallest general-purpose level, 2-key 3DES restricted to 2^{40} plaintext/ciphertexts, protection from 2009 to 2012*	80	1248	160
5	Legacy standard level *2-key 3DES restricted to 10^6 plaintext/ciphertexts, protection from 2009 to 2020*	96	1776	192
6	Medium-term protection *3-key 3DES, protection from 2009 to 2030*	112	2432	224
7	Long-term protection *Generic application-independent recommendation, protection from 2009 to 2040*	128	3248	256
8	"Foreseeable future" *Good protection against quantum computers*	256	15424	512

Baseret på www.keylength.com

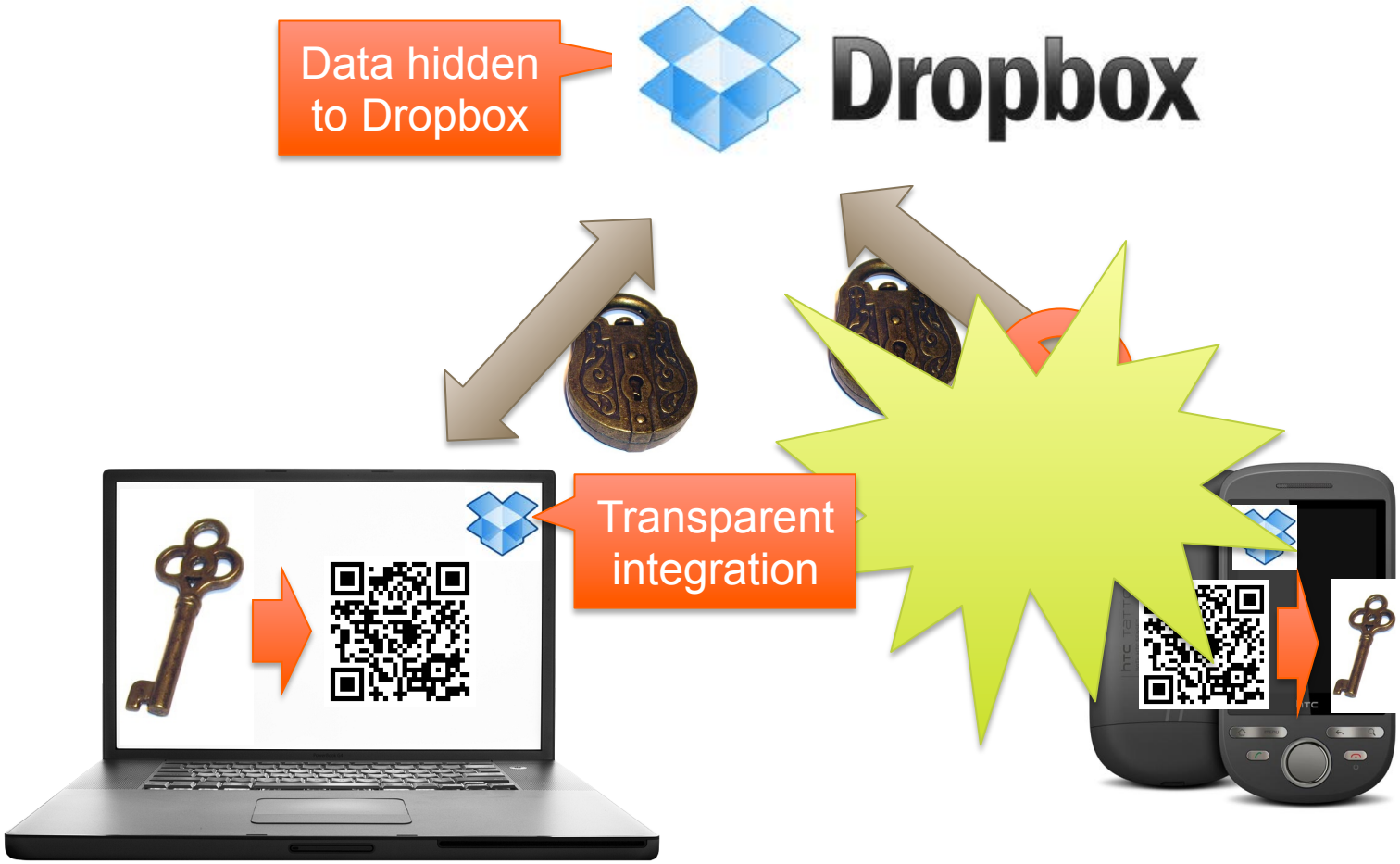
ALEXANDRA INSTITUTTET

Crypto check/wish list

- Client-side encryption
- No trust in third parties
- Minimal user responsibility
- Full functionality

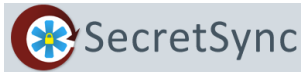
ALEXANDRA INSTITUTTET

Dropbox case study



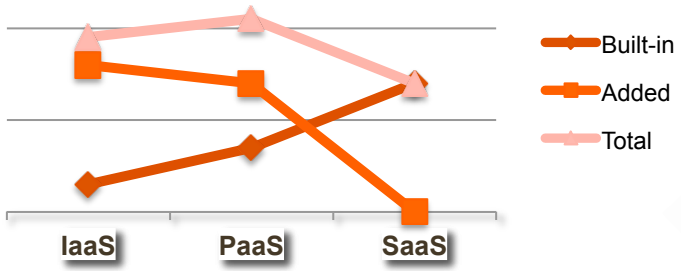
ALEXANDRA INSTITUTTET

Storage-as-a-Service



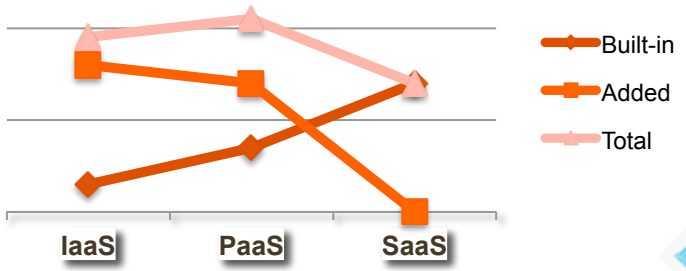
Solution	DYI	Boxcryptor	Secretsync	completely privatefiles	Tahoe
Service(s)	Anything	dropbox	dropbox	box	Any storage
Client-side encryption	yes	Yes/ password based!	yes	yes	yes
Trust in third parties	no	no	yes	yes	Divide-and-conquer
Minimal user responsibility	no	no	(yes)	(yes)	no
Full functionality	no	no	no	no	no

IaaS/PaaS



Solution	DYI	Porticor	CipherCloud	Tahoe
Service(s)	Anything	AWS	Salesforce etc.	Any storage
Client-side encryption	yes	yes	yes	yes
Trust in third parties	no	Divide-and-conquer	no	Divide-and-conquer
Minimal user responsibility	no	yes	yes	no
Full functionality	no	no	tokenization	no

SaaS



Solution	DYI	Ciphercloud	Voltage
Service(s)	Nope!	Salesforce etc.	SaaS eg. PCI
Client-side encryption	yes	yes	yes
Trust in third parties	no	no	no
Minimal user responsibility	no	yes	yes
Full functionality	no	tokenization	tokenization

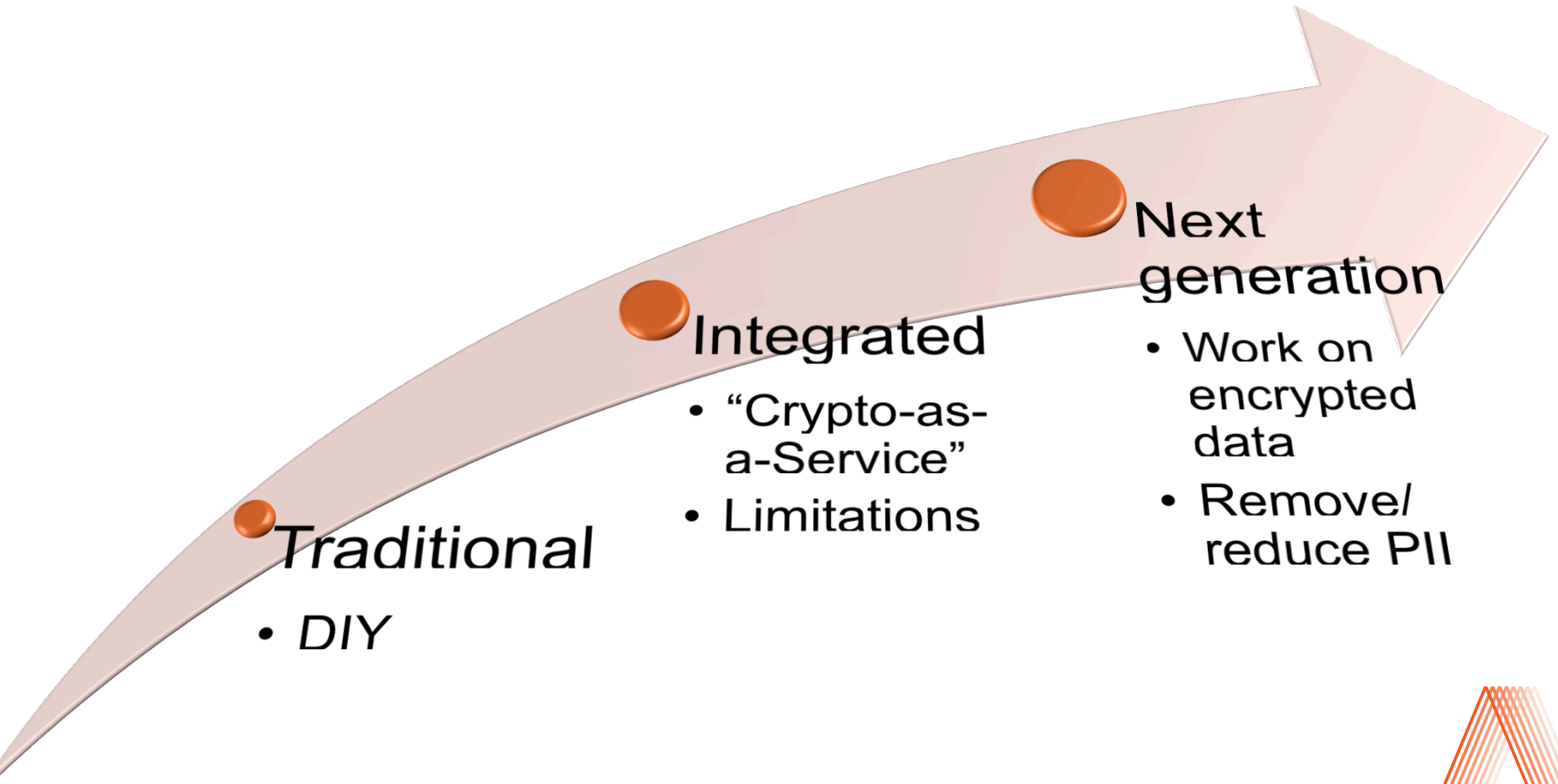
ALEXANDRA INSTITUTTET

Summary

- Client-side encryption
- No trust in third parties
- Minimal user responsibility
- Full functionality

ALEXANDRA INSTITUTTET

Crypto evolution



ALEXANDRA INSTITUTTET

More fancy abbreviations

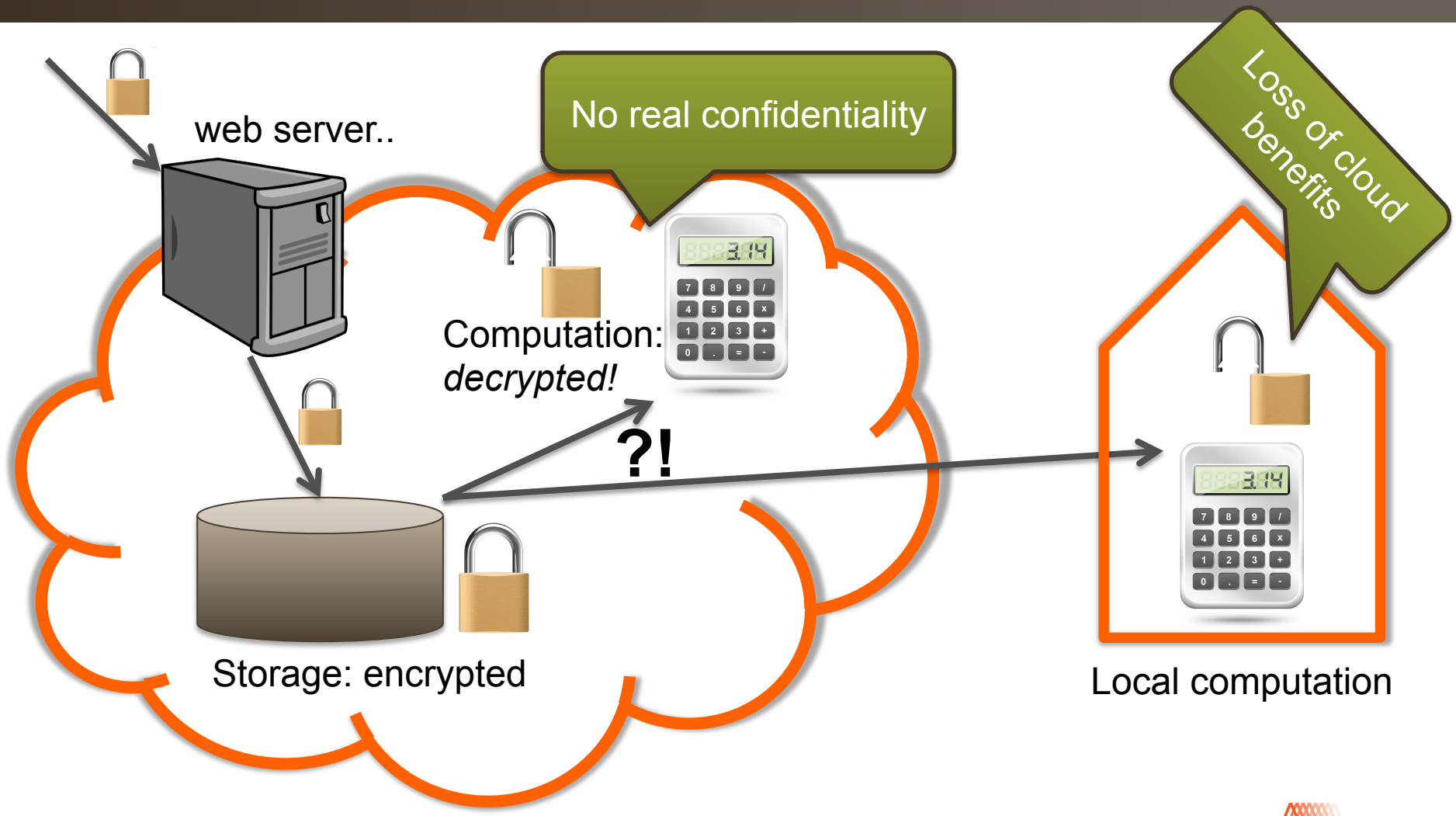
SMC

- Secure Multiparty Computation
- Research since ’78
- “Practical” since 2008

ABC

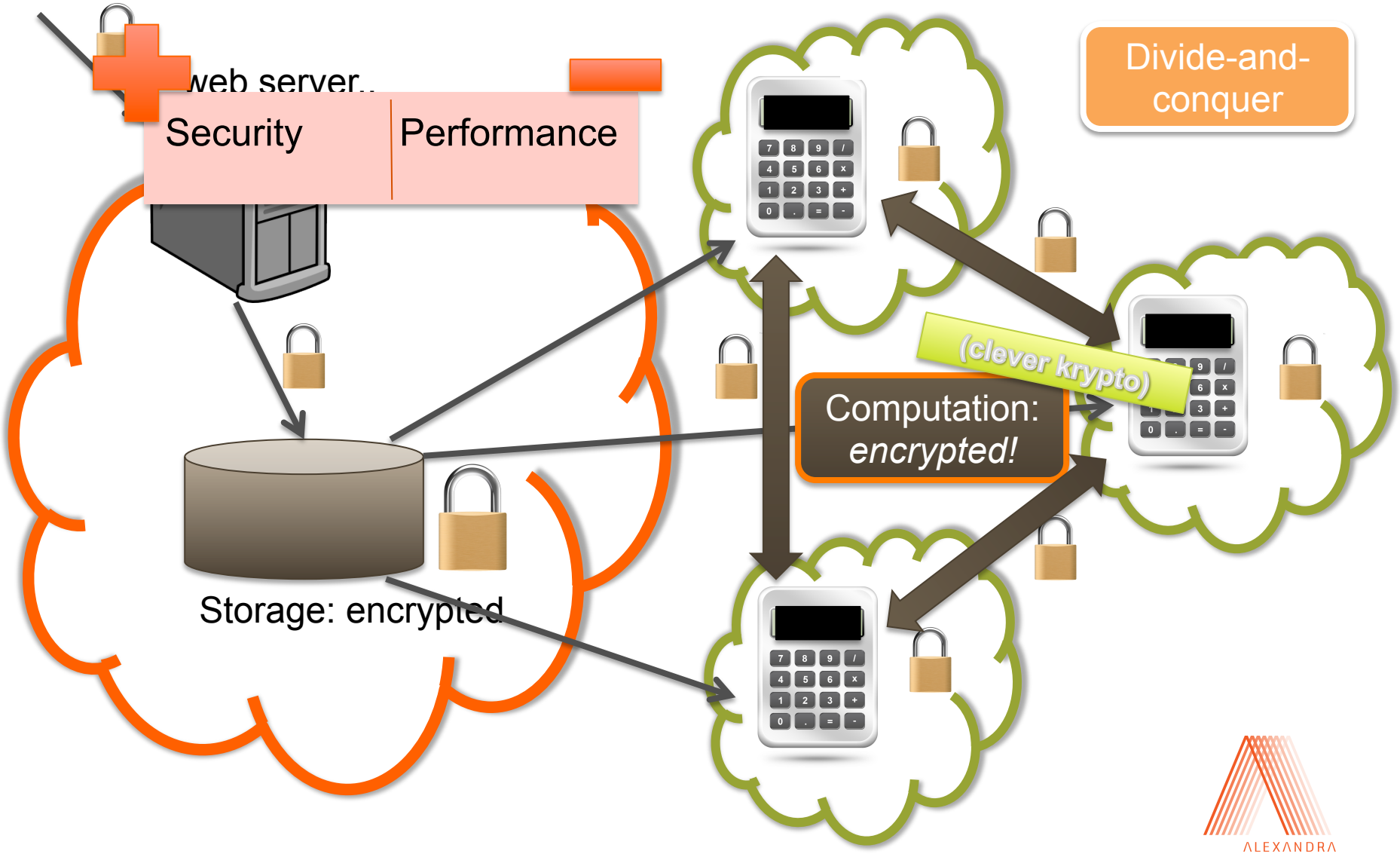
- Attribute-Based Credentials
- Research since at least ’83 (blind signatures)
- Software “previews” available: U-Prove (Microsoft) + IdentityMixer (IBM)

SMC: Shallow confidentiality



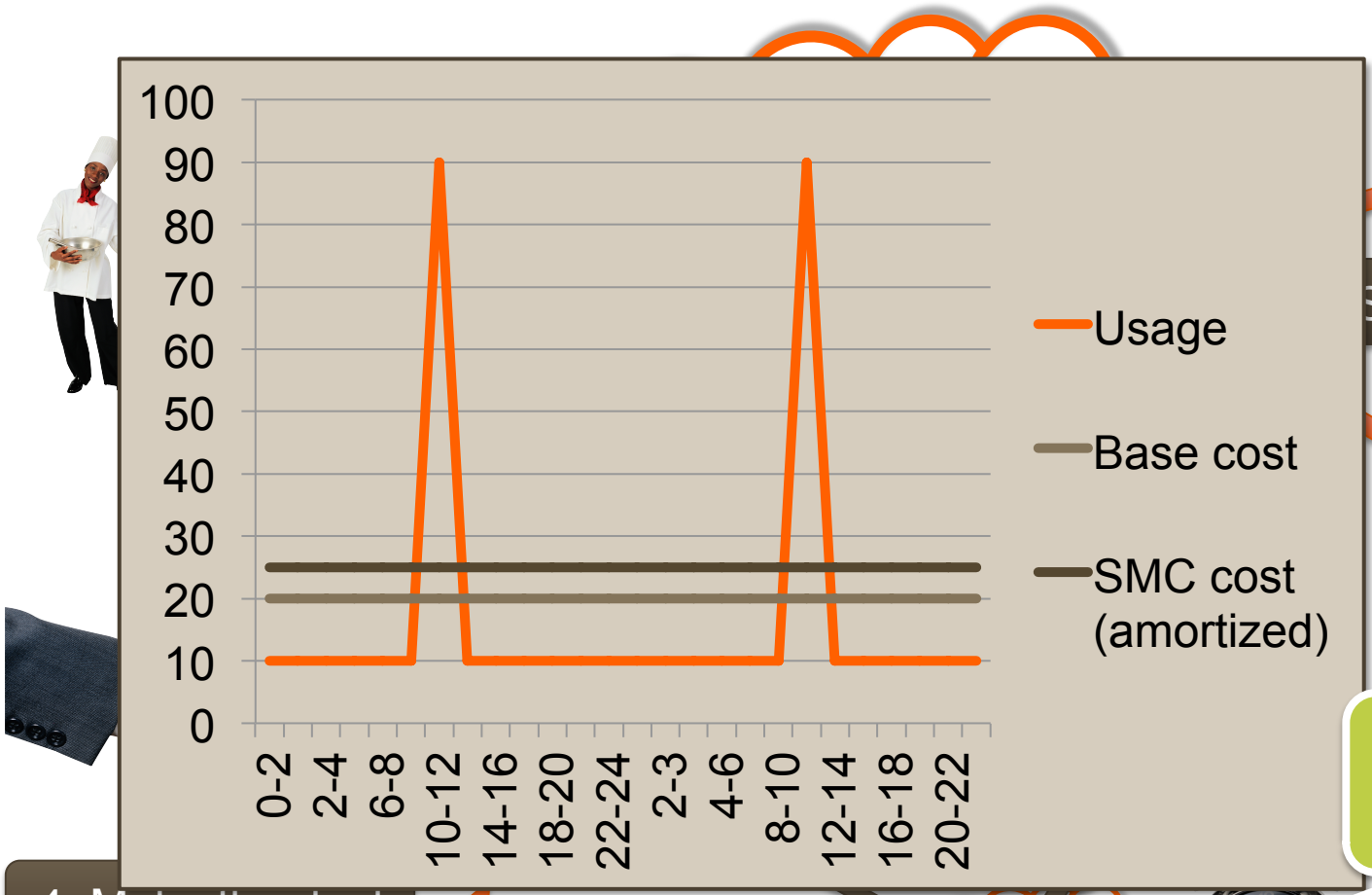
ALEXANDRA INSTITUTTET

SMC: Deep confidentiality



ALEXANDRA INSTITUTTET

SMC: energiauktion.dk (via partisia.com)



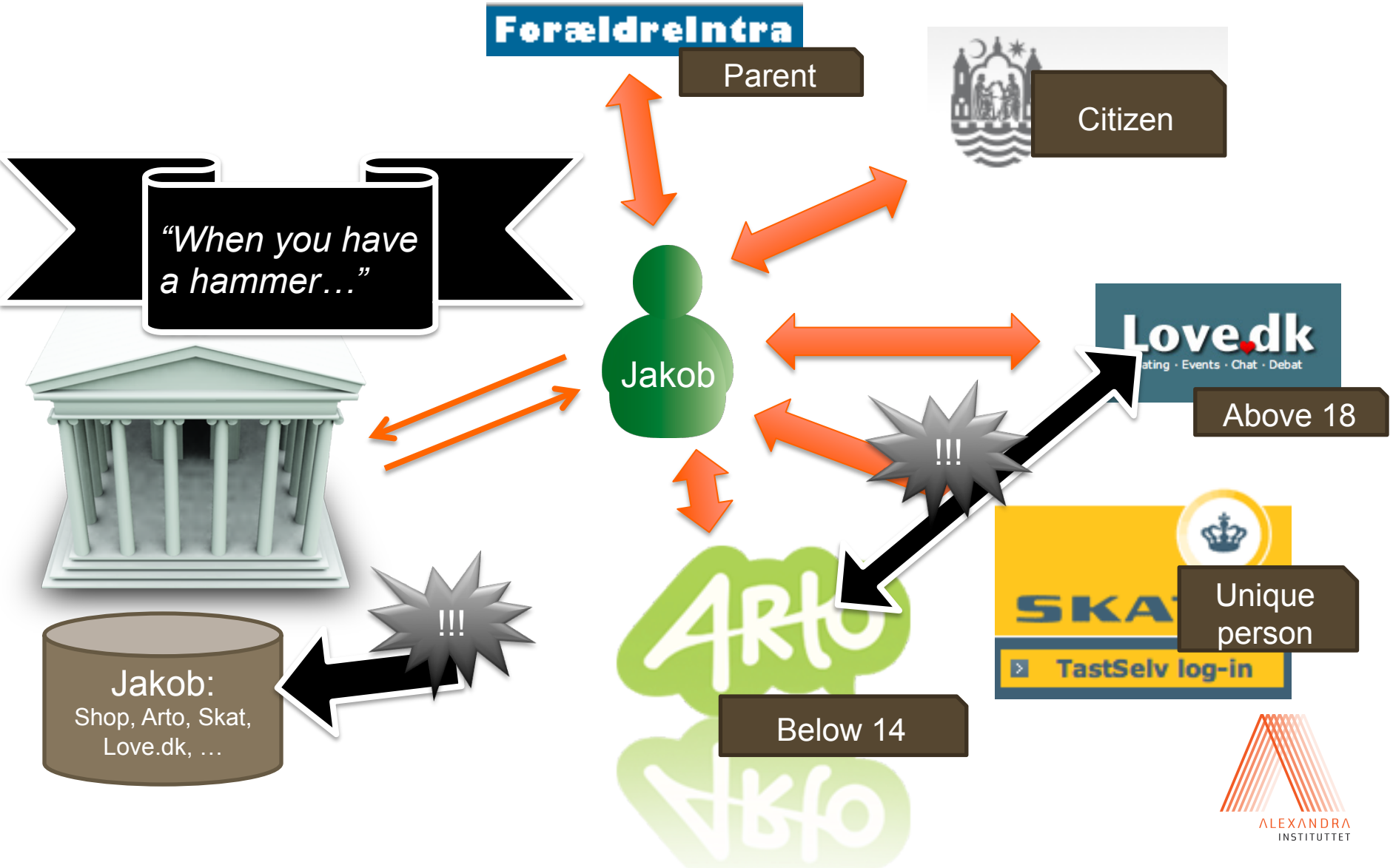
Submit bids

Elasticity => confidentiality!

4. Make the deal

ALEXANDRA INSTITUTTET

ABC: Identity in the cloud (simplified)



ABC: properties

Existing properties (digital signatures/IdP)

- Identification
- Accountability

Can we have it all?

Yes we can!

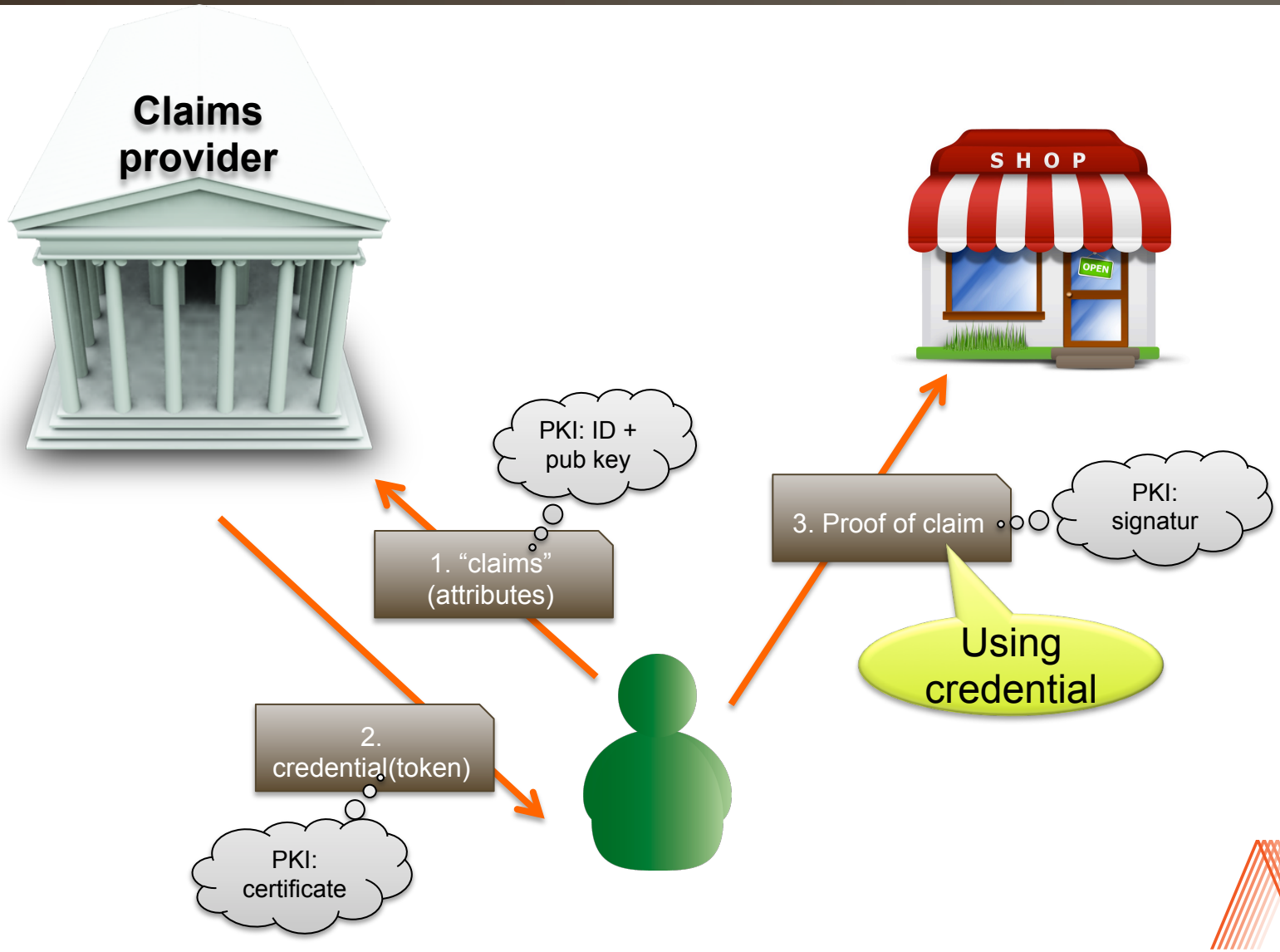
New desirable properties

- Non-traceable/anonymitet
  - *IdP can't trace your transactions*
- Unlinkable/pseudonymitet
  - *Eg. a provider can't link your profile in a merger with another provider*
- Verified claims
  - *Eg. age og zipcode*

- **Minimal disclosure**

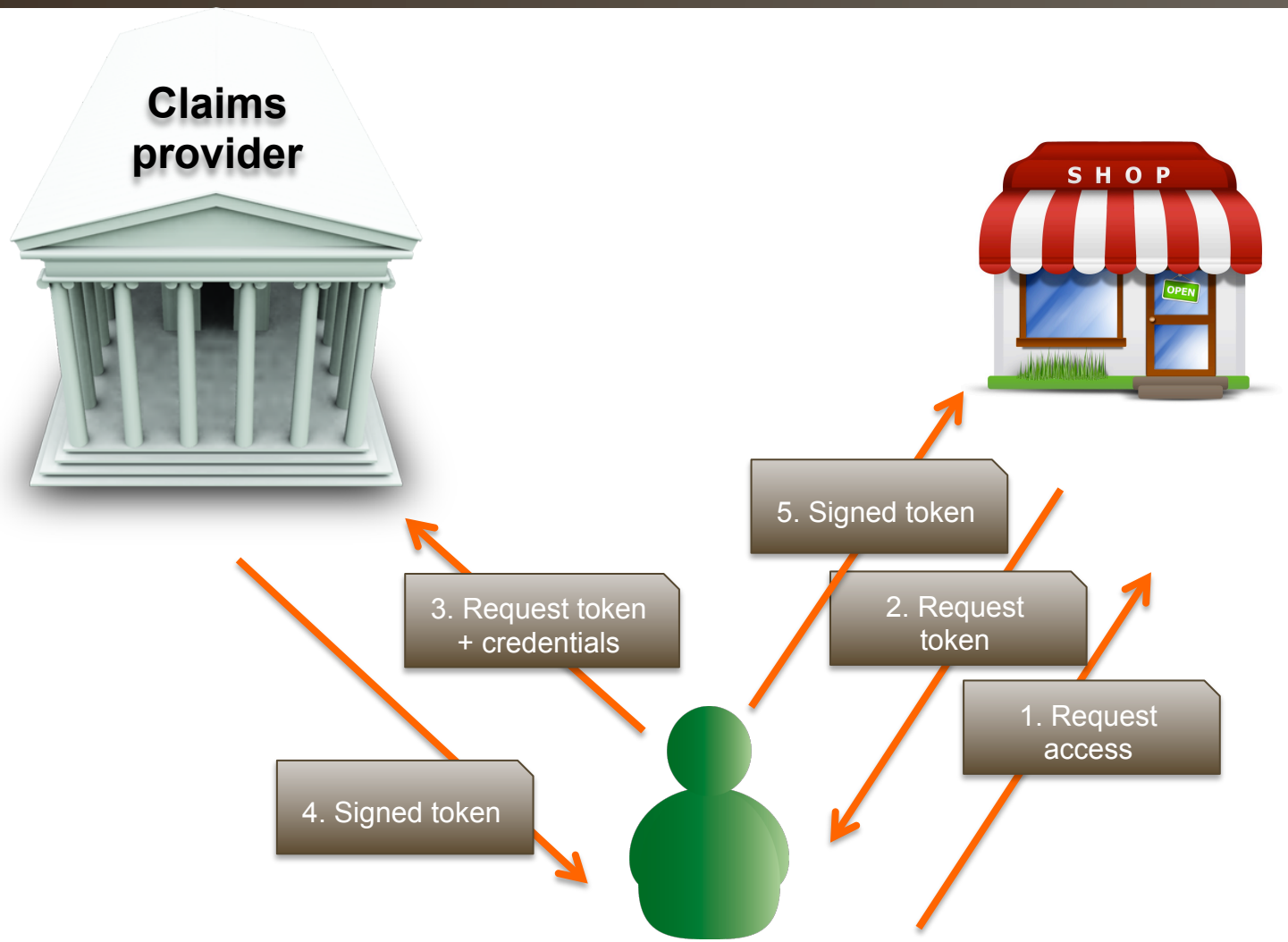
ALEXANDRA INSTITUTTET

ABC: Credentials



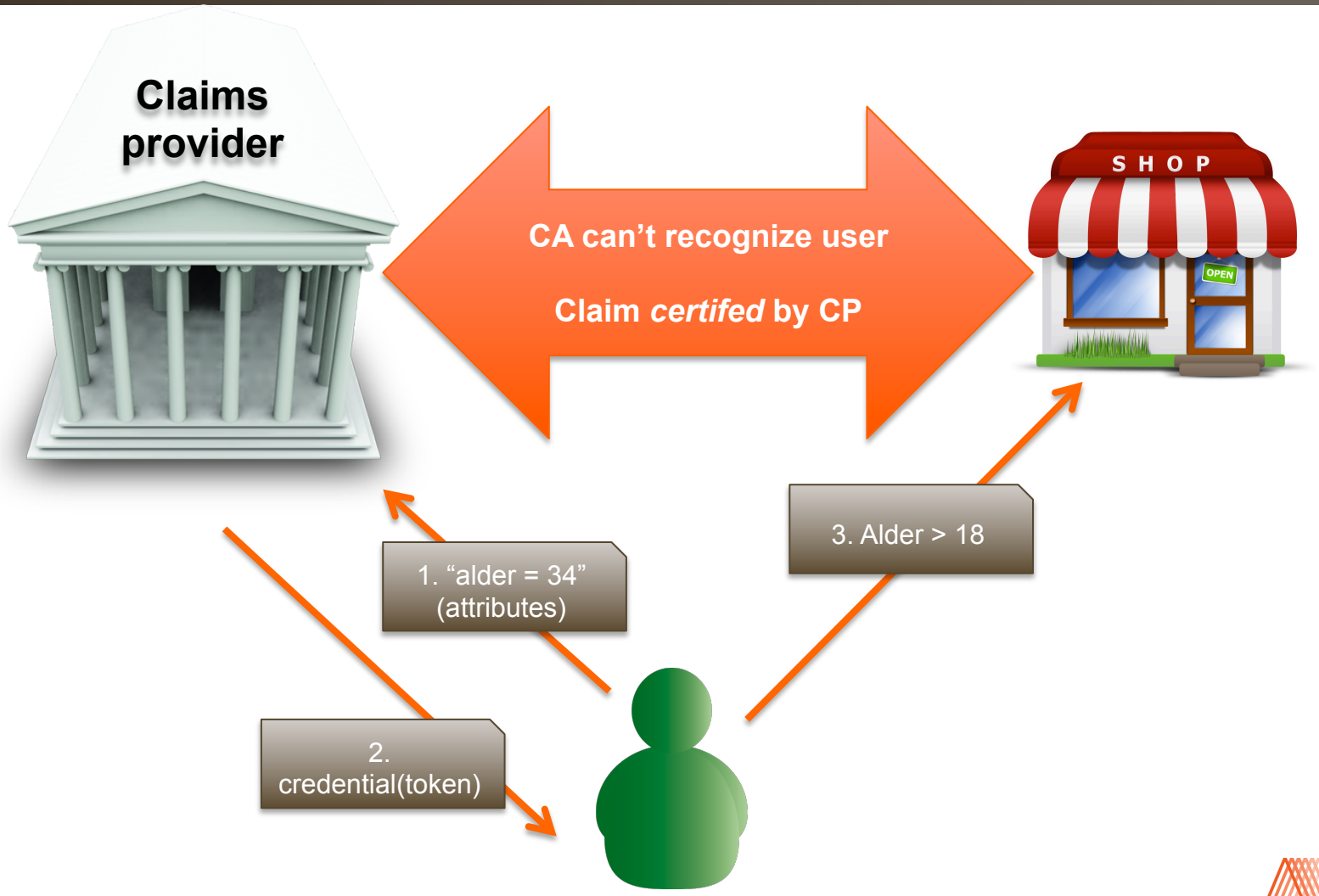
ALEXANDRA INSTITUTTET

ABC: IdP vha. credentials (“on-demand”)



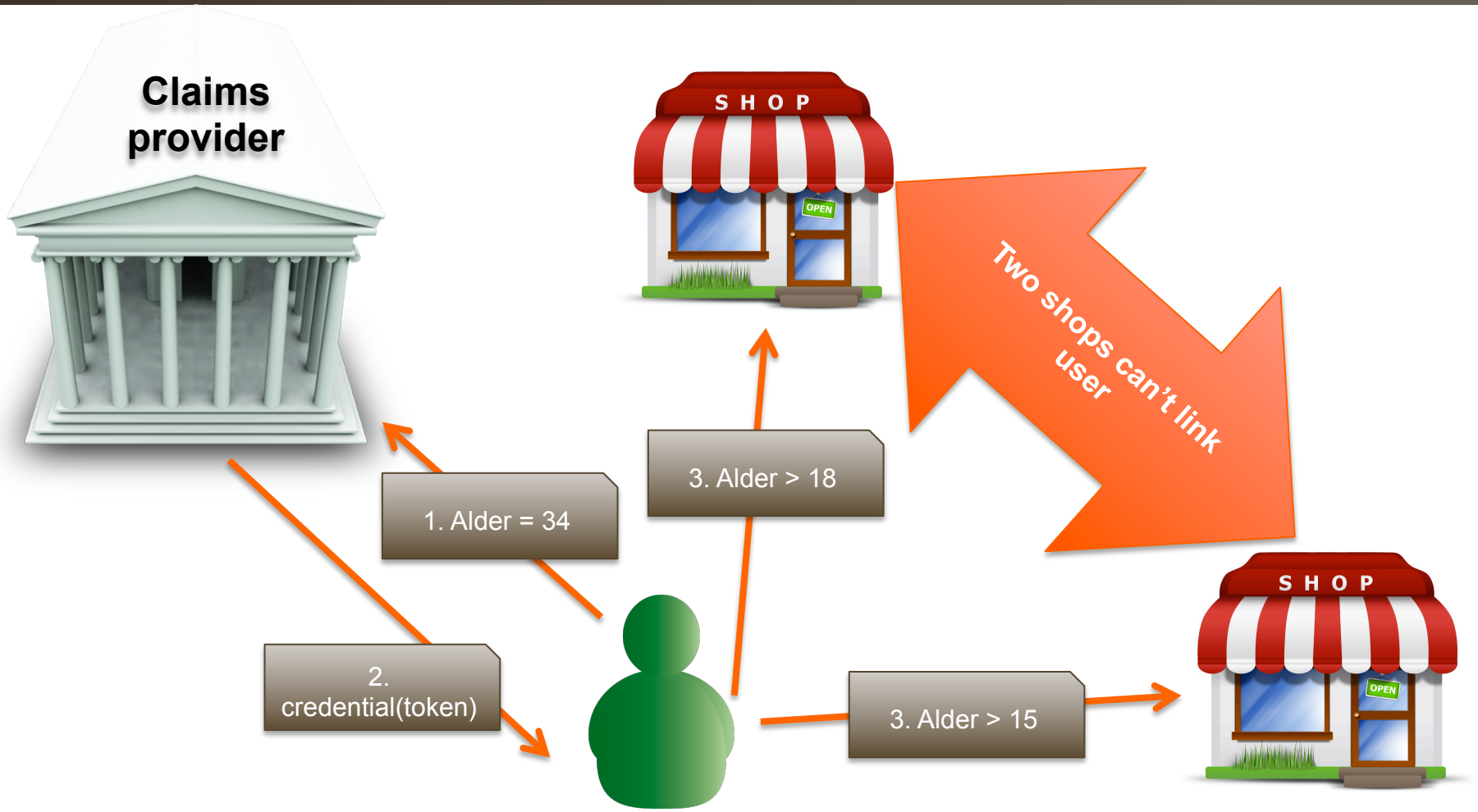
ALEXANDRA INSTITUTTET

ABC: Anonymity



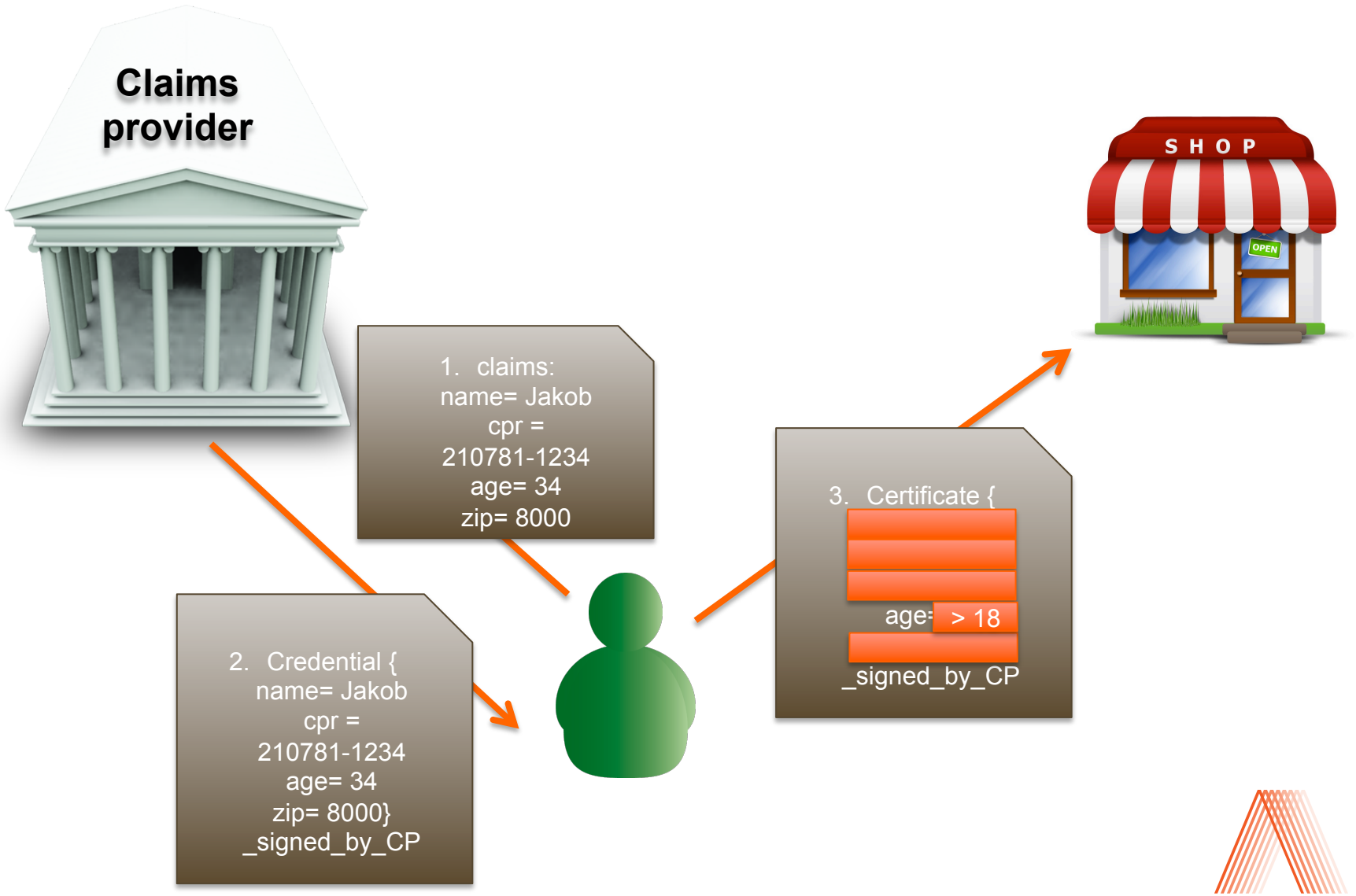
ALEXANDRA INSTITUTTET

ABC: Pseudonymity



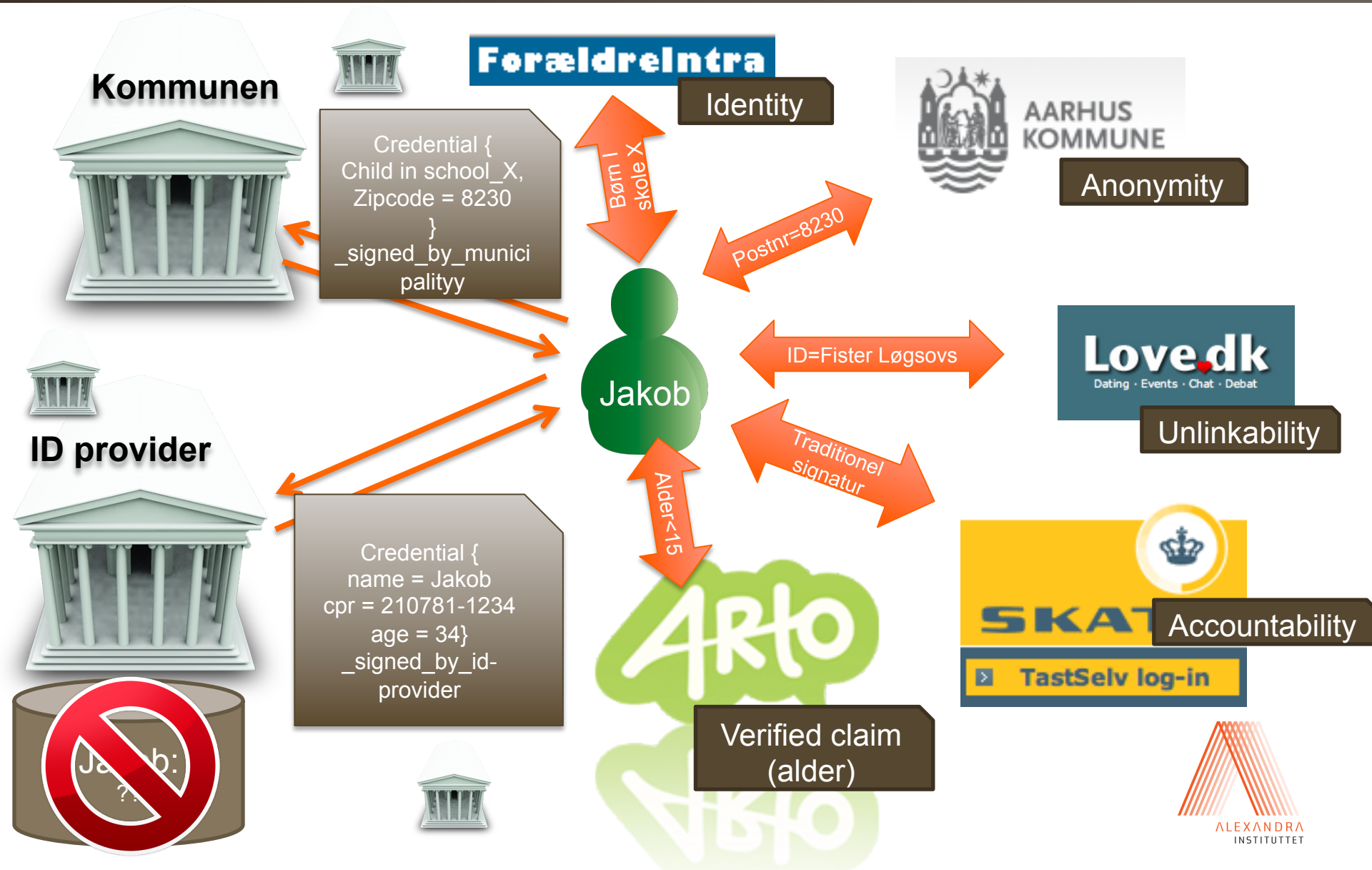
ALEXANDRA INSTITUTTET

ABC: Selective disclosure



ALEXANDRA INSTITUTTET

ABC: Id-brug vha. credentials

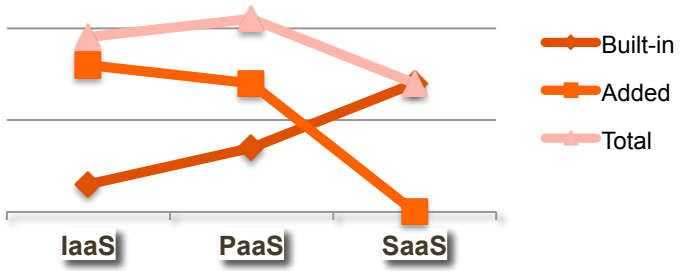


ABC vs. signatur etc.

Egenskab	Signatur	ABC
Identity	✔	✔
Accountability	✔	✔
Anonymity (non-traceability)	✗	✔
Pseudonymity (unlinkability)	✗	✔
Selective (minimal) disclosure	✗	✔

ALEXANDRA INSTITUTTET

ABC and SMC



Curious…?
- SMC: partisia.com
- ABC: www.abc4trust.eu

Solution	DYI	ABC	SMC
Service(s)	Some	Any	Any
Client-side encryption	yes	yes	yes
Trust in third parties	no	(yes)	Divide-and-conquer
Minimal user responsibility	no	(yes)	(yes)
Full functionality	no	(yes)	yes

ALEXANDRA INSTITUTTET

Thanks for you attention!

Jakob I. Pagter
jakob.i.pagter@alexandra.dk