

Lifelong Privacy

≈ 100 years: The world will change a lot and, in particular, ICT will change –
and each individual's appreciation of privacy will change several times

Andreas Pfitzmann

Dresden University of Technology, Faculty of Computer Science, D-01062 Dresden
Nöthnitzer Str. 46, Room 3071

Phone: +49 351 463-38277, e-mail: pfitza@inf.tu-dresden.de, <http://dud.inf.tu-dresden.de/>

September 8, 2009

Lifelong Privacy

1. Minimization of Personal Data

2. Long-term security

- information-theoretically secure crypto instead of complexity-theoretically secure crypto
- migration to stronger security platforms when they become available

Lifelong Privacy

Intro

Identity Management

Basics

Emphasizing lifelong aspects

Identity Management throughout the whole life

Identity management framework needed

Identity of which (data) subjects?

Identity of

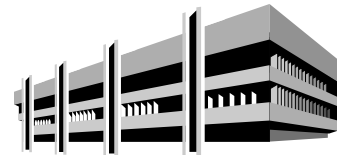
2009 → 2059

- Natural person,



$\approx 10^{10}$

- Legal person, or



$10^8 \rightarrow 10^{11}$

- Computer



$10^{10} \rightarrow 10^{14}$

Identity is ?

Identity is much *more than*

- Names (easy to remember),

- Identifiers (unique), and

Much change to be expected during our lifetime

- Means of authentication (secure).

Identity is ...

Identity *primarily* is a

- **set of attribute values,**

where **some attribute values might change** over time and **some may be certified by third parties**

Given that it is very hard – if not impossible – to erase widely used data, a digital identity as a set of attribute values valid at a particular time is

- **only growing** – never shrinking.

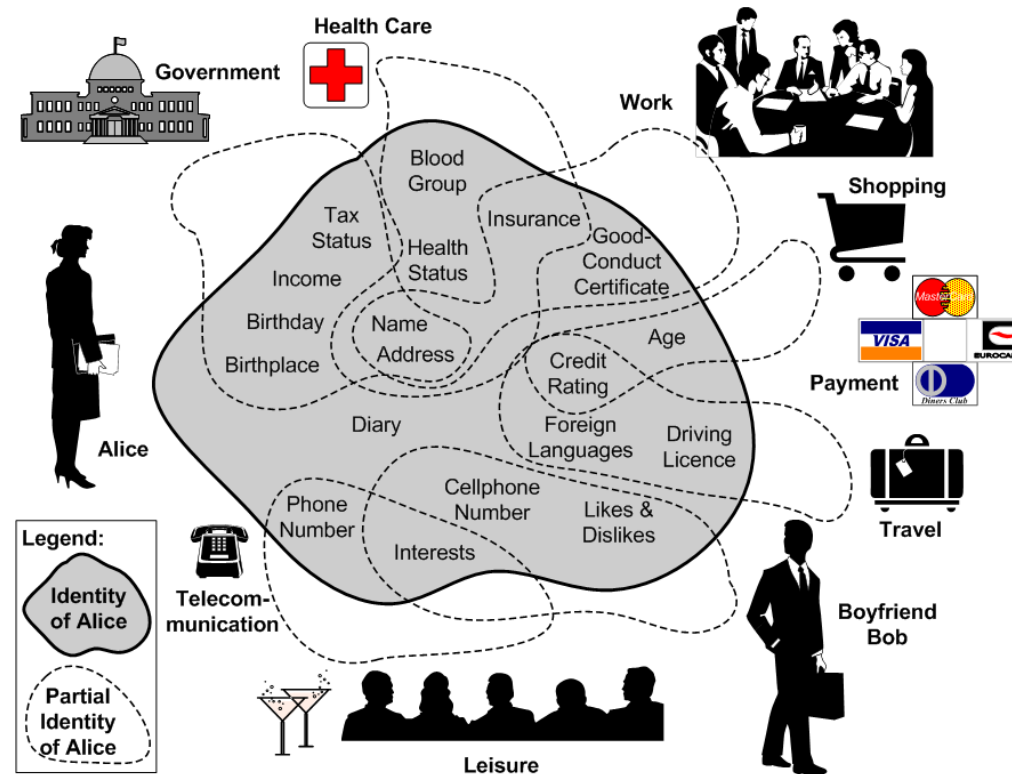
This is true both for a global observer as well as for each party (or set of parties pooling their information) interacting with an identity.

Partial Identities (pIDs)

Achieving security and privacy requires users to *subset* their *identity* in so-called

Partial Identities (pIDs),

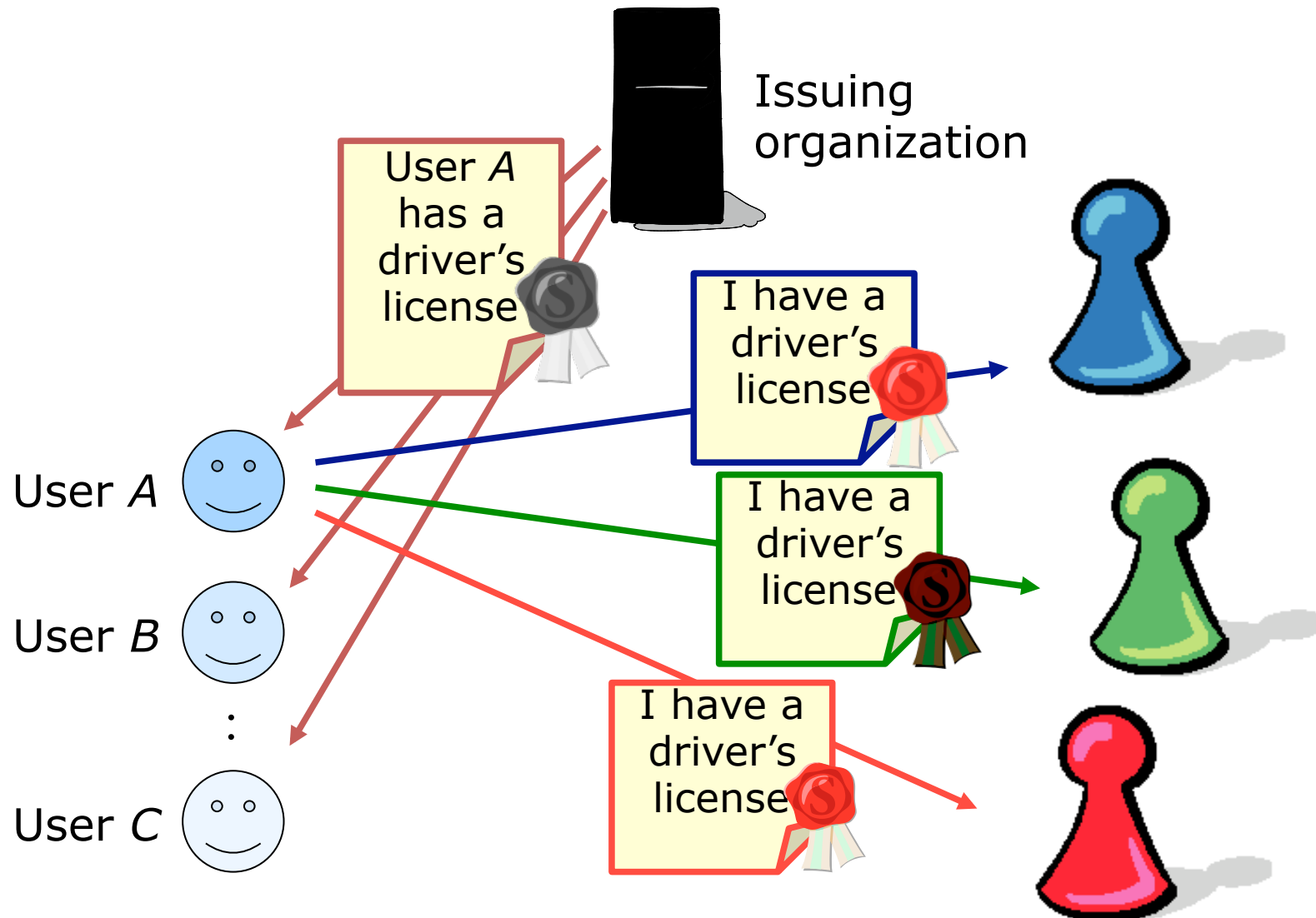
where each pID might have its own name, own identifier, and own means of authentication.



Using pIDs requires ...

- **Basic understanding by users** (and by government and businesses),
- At least one **personal computer** administering personal data and executing cryptographic protocols **fully controlled by the user** (otherwise no way to validate privacy properties, i.e., unlinkable pIDs),
- **Digital pseudonyms** for secure authentication (otherwise no way to achieve accountability),
- **Anonymous credentials** to transfer certified attribute values from one pID to another pID of the same digital identity (without anonymous credentials, no transfer of certified attribute values between pIDs, which drastically reduces applicability of pIDs).

Anonymous credentials



Important kinds of attributes

- Names (easy to remember),
- Identifiers (unique),
- Means of authentication (secure)
 - **Digital pseudonyms** are unique identifiers suited to test authentication (e.g., public keys of PGP)
- Biometrics (binding to natural person)
- Addresses (useful for communication)
- Bank account (payment)
- Credit card number (payment and creditworthiness)

Possible classifications of attribute values

- Authenticated at all? If so, by
 - First party (= data subject)?
 - Third parties? If so, third parties trusted by whom wrt what?
- Known to first party or to 2nd party (= communication partner) only?
- Easy to change or not?
- Varying over time or not? Changes predictable?
- Given attribute values vs. chosen attribute values
- Pure attribute values vs. attribute values containing significant side information
- Characterizing a single entity per se or an entity only in its relationship to other entities?
- Sensitive in at least one context or not?

How much protection for which attributes?

Some attribute values need much *more privacy protection* than others, e.g., those which

- are not easy to change,
- do not vary over time or can be predicted,
- are given attribute values,
- contain significant side information, or
- are sensitive in least one context.

These attribute values are part of the **“core identity”**

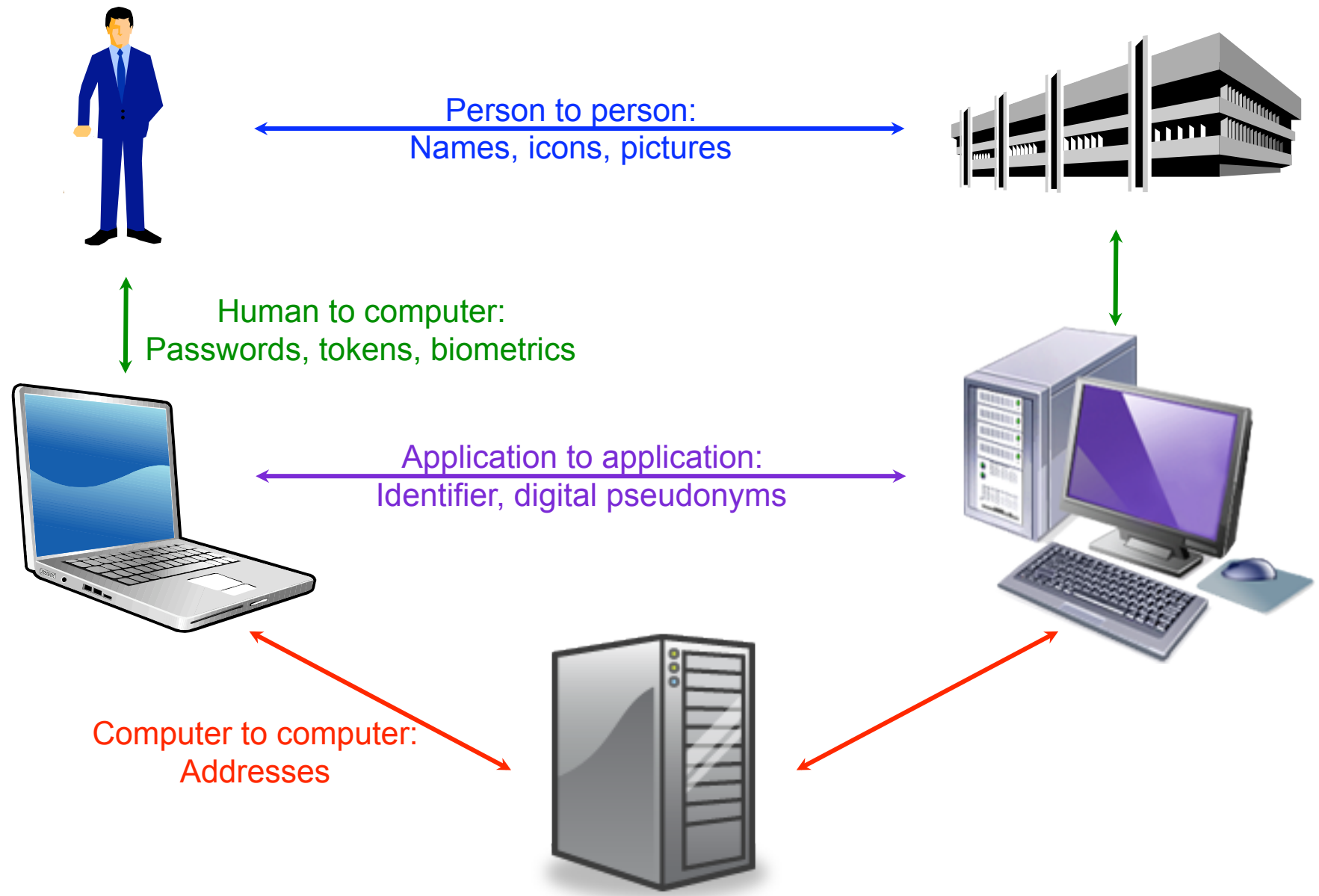
Advancements and use of technology may shift some attributes from “core identity” to “non-core identity”.

E.g., the address of your house or flat is core, the current address of your laptop maybe not.

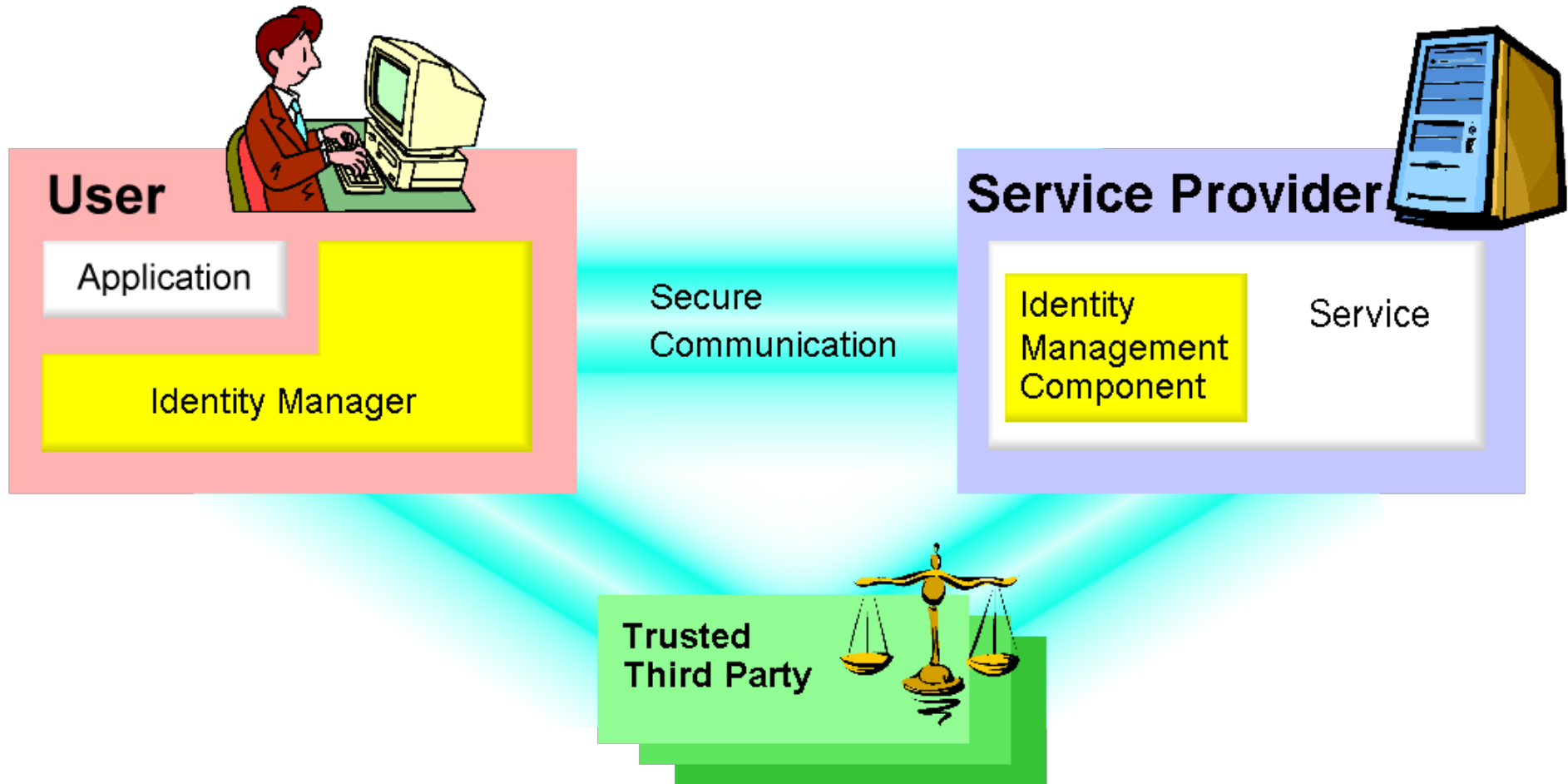
An eternal core-identity attribute: Biometrics

- Some biometrics
 - Contain very significant side information (still to be fully understood)
 - Are an eternal core-identity attribute
- “How to (not) use biometrics” therefore is an interesting case study <http://dud.inf.tu-dresden.de/literatur/BiometricsTrustBus2008-09-04.pdf>
- Main result:
Biometrics between **data subject** and **his/her devices** only
 - Authentication by possession and/or knowledge *and* biometrics
 - No devaluation of classic forensic techniques (e.g., by foreign devices reading fingerprints, digital copies will make it into databases of foreign secret services and organized crime, enabling them to leave dedicated false fingerprints at the scenes of crime)
 - No privacy problems caused by biometrics (measurements may contain medical or psychological side information)
 - But: Safety problem remains unchanged
 - ⇒ Provide possibility to switch off biometrics after successful biometric authentication.

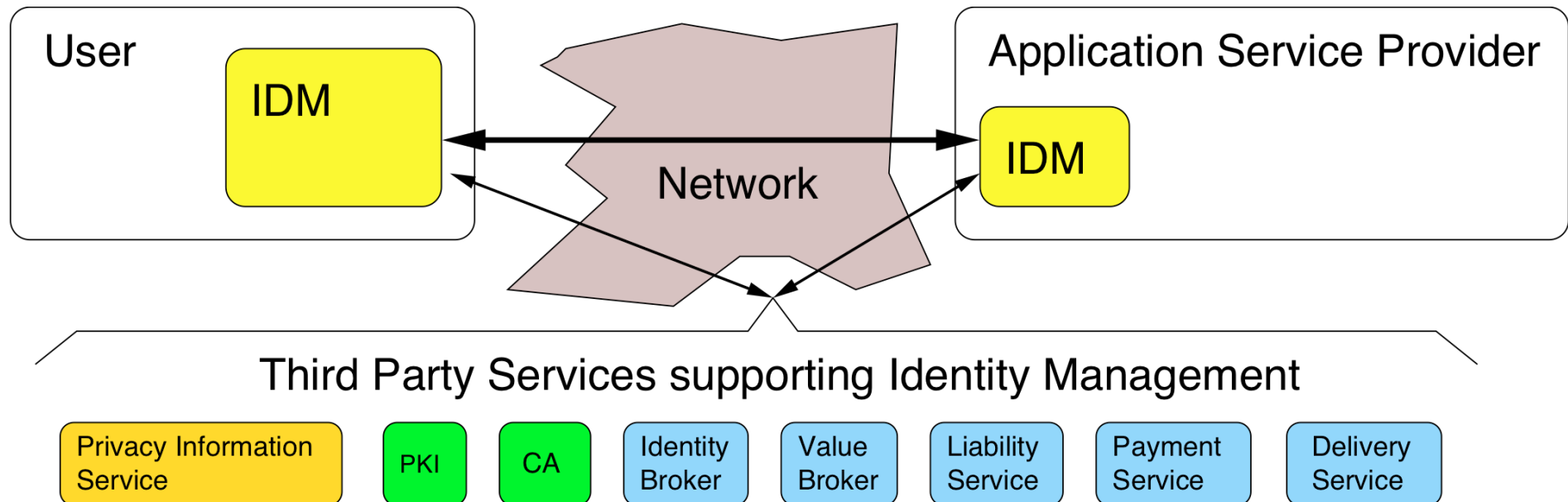
How it works together



Architecture for identity management



Third party services supporting identity management



How to represent identity online?

- **Only partial identities** – otherwise Big Brother (or Little Sisters) will be quite happy
- **(Digital) Pseudonyms as identifiers** for partial identities
- How to **establish** and **use** (digital) pseudonyms
 - Initial linking between the pseudonym and its holder
 - Linkability due to the use of the pseudonym in different contexts

Pseudonyms: Initial linking to holder

Public pseudonym:

The linking between pseudonym and its holder may be publicly known from the very beginning.

Phone number with its owner listed in public directories

Initially non-public pseudonym:

The linking between pseudonym and its holder may be known by certain parties (**trustees for identity**), but is not public at least initially.

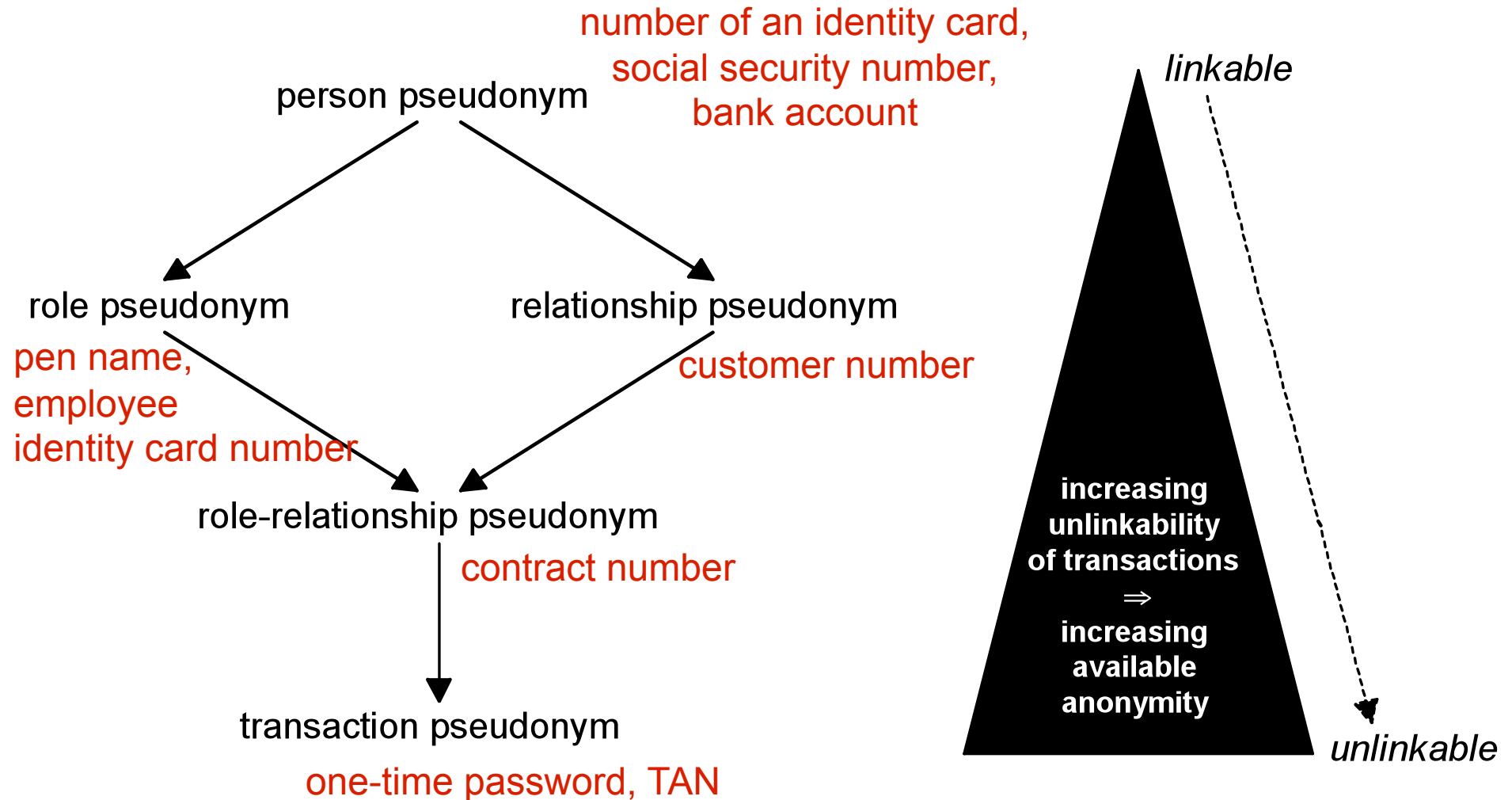
Bank account with bank as trustee for identity,
Credit card number ...

Initially unlinked pseudonym:

The linking between pseudonym and its holder is – at least initially – not known to anybody (except the holder).

Biometric characteristics; DNA (as long as no registers)

Pseudonyms: Use in different contexts → partial order



A → B stands for “B enables stronger anonymity than A”

Trustee for values vs. Trustee for identities

- **Accountability of digital pseudonyms**
(by depositing money to cover claims against damage caused under that pseudonym)

vs.

- **Accountability of holders** of digital pseudonyms
(by identifying holders in case of uncovered damage)

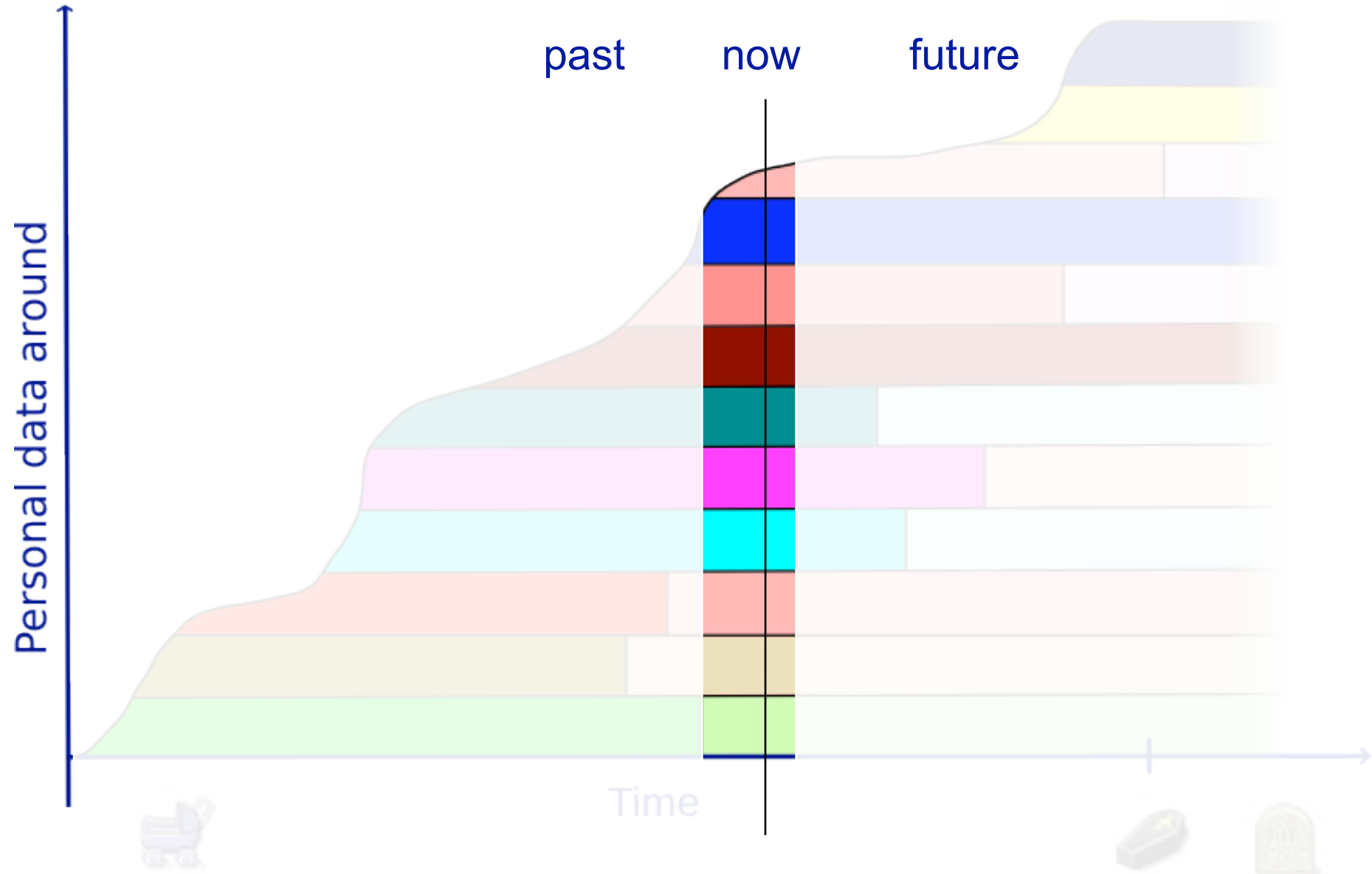
Cf. Holger Bürk, Andreas Pfitzmann: Value Exchange Systems Enabling Security and Unobservability; Computers & Security 9/8 (1990) 715-721.
<http://dud.inf.tu-dresden.de/sireneLit.shtml#pay.fair>

Identity Management (IDM)

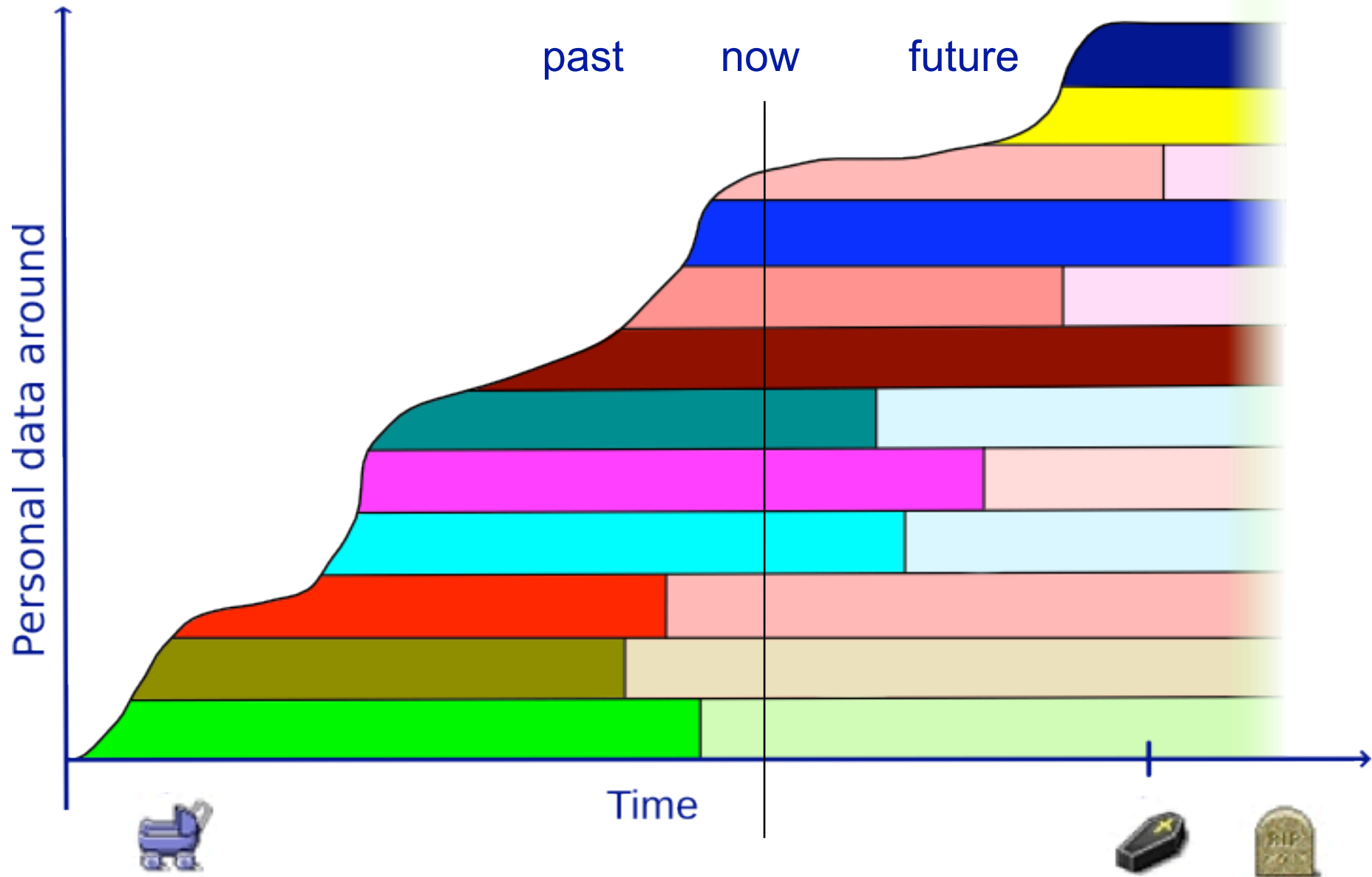
IDM as the communicational gateway
to the outside world
throughout the whole life

HW and SW interfaces to legacy and emerging systems

Identity management today



Identity management during an individual's lifetime



Privacy throughout life

- short-term vs. long-term effects covering the full lifespan
- context-specific vs. context-spanning covering all areas of life
- constant vs. changing abilities/behaviour of individuals covering different stages of life

IDM covering all areas of life

- Formal areas (I have to participate in)
 - government
 - education
 - work
 - health care
 - ...

- Informal areas (I might choose to participate in – or others decide for me)
 - family
 - friends
 - shopping
 - church
 - ...

IDM covering all stages of life

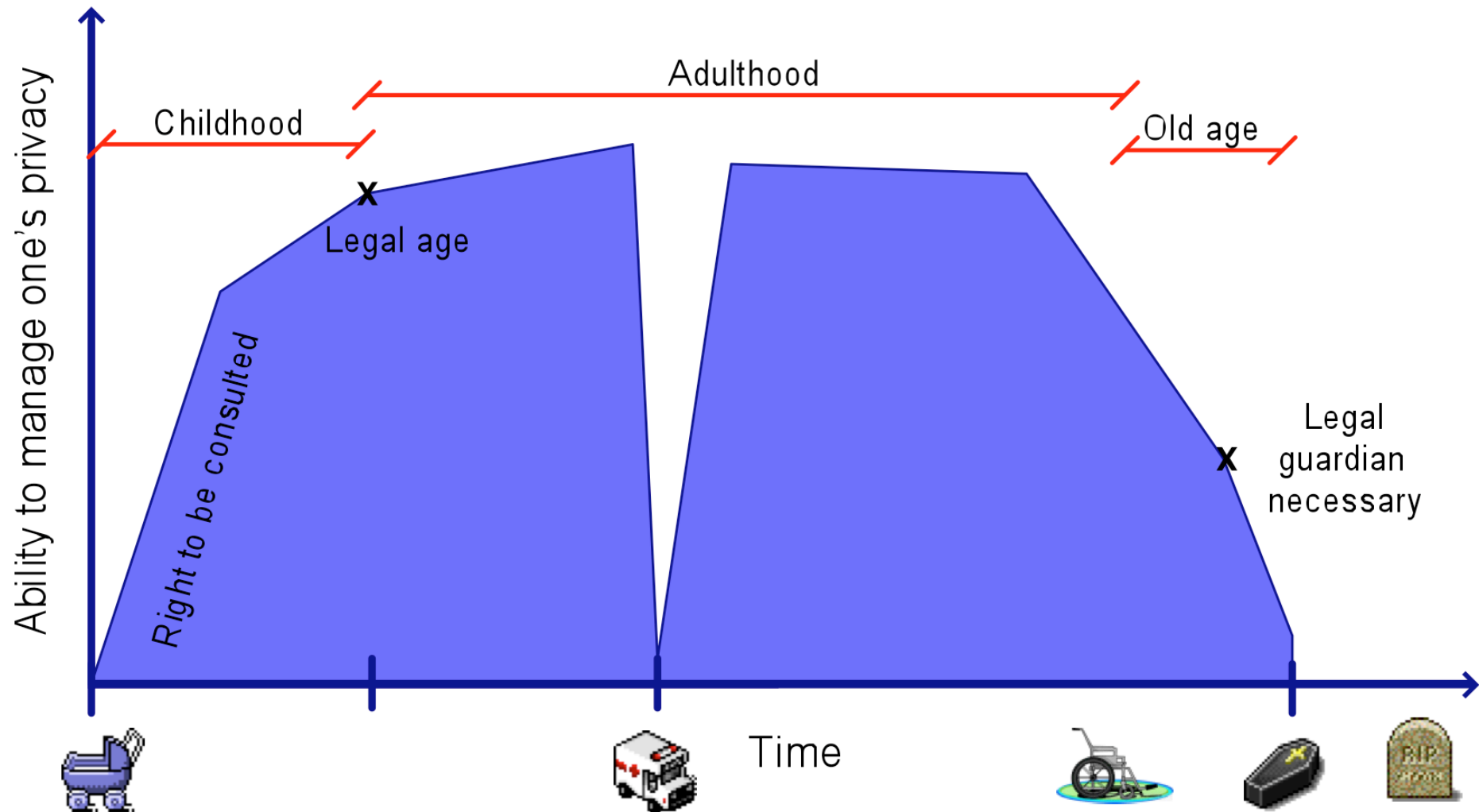
- A stage of life of an individual wrt managing his privacy is a period of life in which his ability to do so remains between defined boundaries characterizing this stage of life.

- A concrete stage might be defined in different areas of life differently:
 - in Christian churches, a young man becomes adult after his confirmation
 - for a national government, a young man becomes adult when reaching a certain age (usually 18).

- Typical formal stages:
 - minors
 - adults
 - senior citizens

Ability to manage one's private sphere during an individual's lifetime

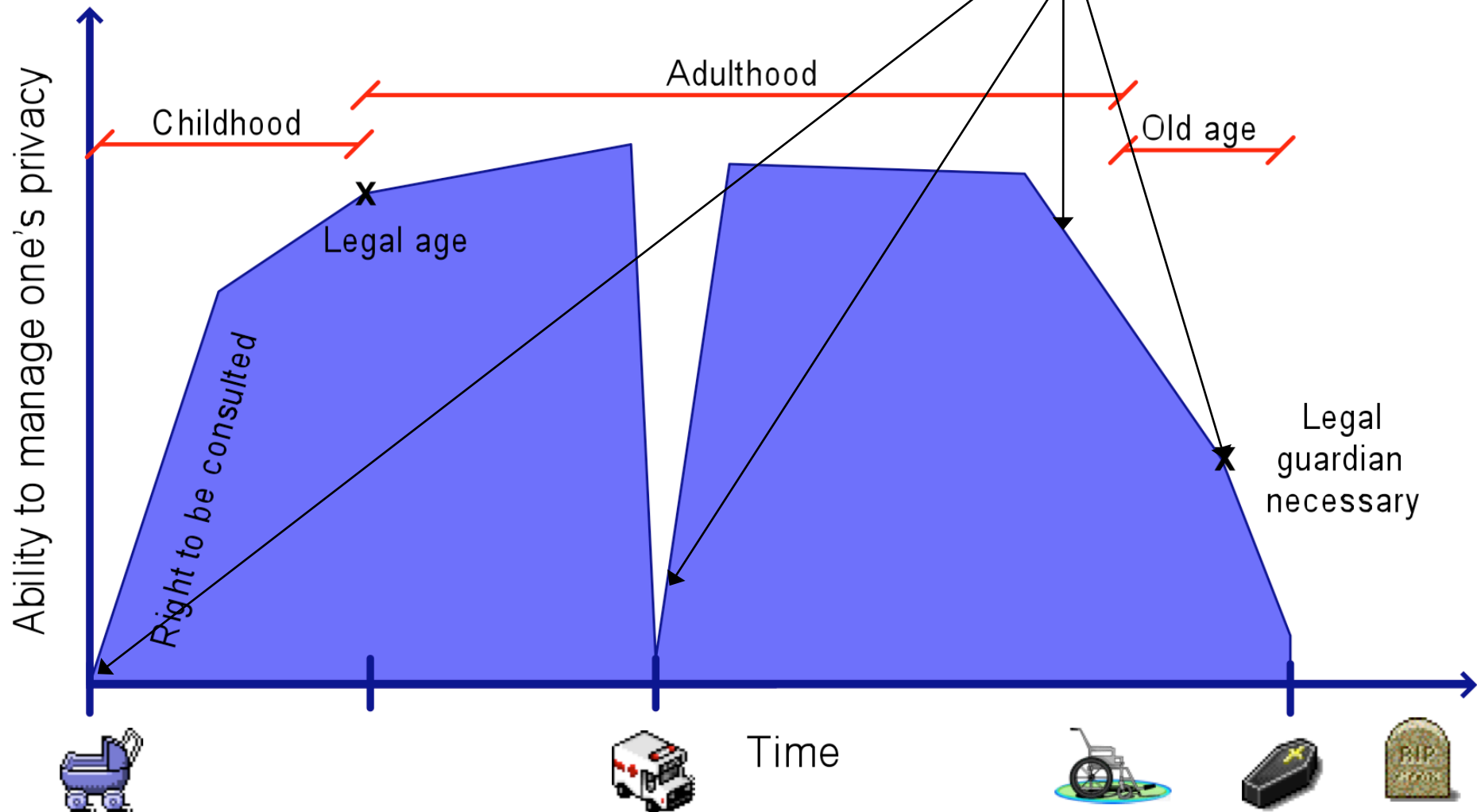
Understand
Act accordingly
Use required (technical) means



Ability to manage one's private sphere during an individual's lifetime

Understand
Act accordingly
Use required (technical) means

Delegation
• mandatory
• discretionary



Technological, social, legal, ... mechanisms

What we have:

- technological mechanisms for user-controlled privacy
 - handling of partial identities
 - data minimisation
 - enforceable rules for data processing
 - transparency functionality

What we need:

- to develop/adapt mechanisms for covering
 - as many areas of life as possible and sensible
 - many stages of life
 - the full lifespan

Mechanisms, tools, and services

- Post-mortem notary service
- Encrypted file system with secret sharing
- Passing SNS sub-profiles onto kids
- Show (and remove?) my Digital Footprint
- Central data handling policy repository
- Assisted Living for old people
- Lifelong Data Track

How to manage your identity online?

- Get **attentive** to managing your identity, i.e., your pIDs (otherwise others will manage you)
- Consider both, **reputation** and **privacy**, make a **compromise**

- Get the right **tools**



- **Privacy-enhancing identity management tools**,
cf. PRIME prime-project.eu and PrimeLife primelife.eu



- **Communication infrastructure** which does **not define permanent identifiers attached to you** (your network address) making privacy-enhancing identity management at the application layer void

- **Choose** the right communication **partners** (including: avoid those which are unnecessarily privacy-invasive)

Identity management framework needed

- Now, we have an identity management *patchwork*.
- As security is only as good as the weakest link of the chain, privacy is at most as good as the most privacy-invasive “layer” you are using.
- Therefore, an identity management patchwork will not lead to secure and privacy-enhancing identity management.
- An **identity management framework** is needed addressing both, *security* and *privacy*.

Further reading

Marit Hansen, Andreas Pfitzmann, Sandra Steinbrecher:
Identity management throughout one's whole life;
Information Security Technical Report 13/2 (2008) 83-94.

Sebastian Clauß, Marit Hansen, Andreas Pfitzmann, Maren Raguse, Sandra
Steinbrecher: Tackling the challenge of lifelong privacy;
eChallenges e-2009, Istanbul, Oct. 21-23, 2009. <http://www.echallenges.org/e2009/>

http://dud.inf.tu-dresden.de/Anon_Terminology.shtml

<https://www.prime-project.eu/>

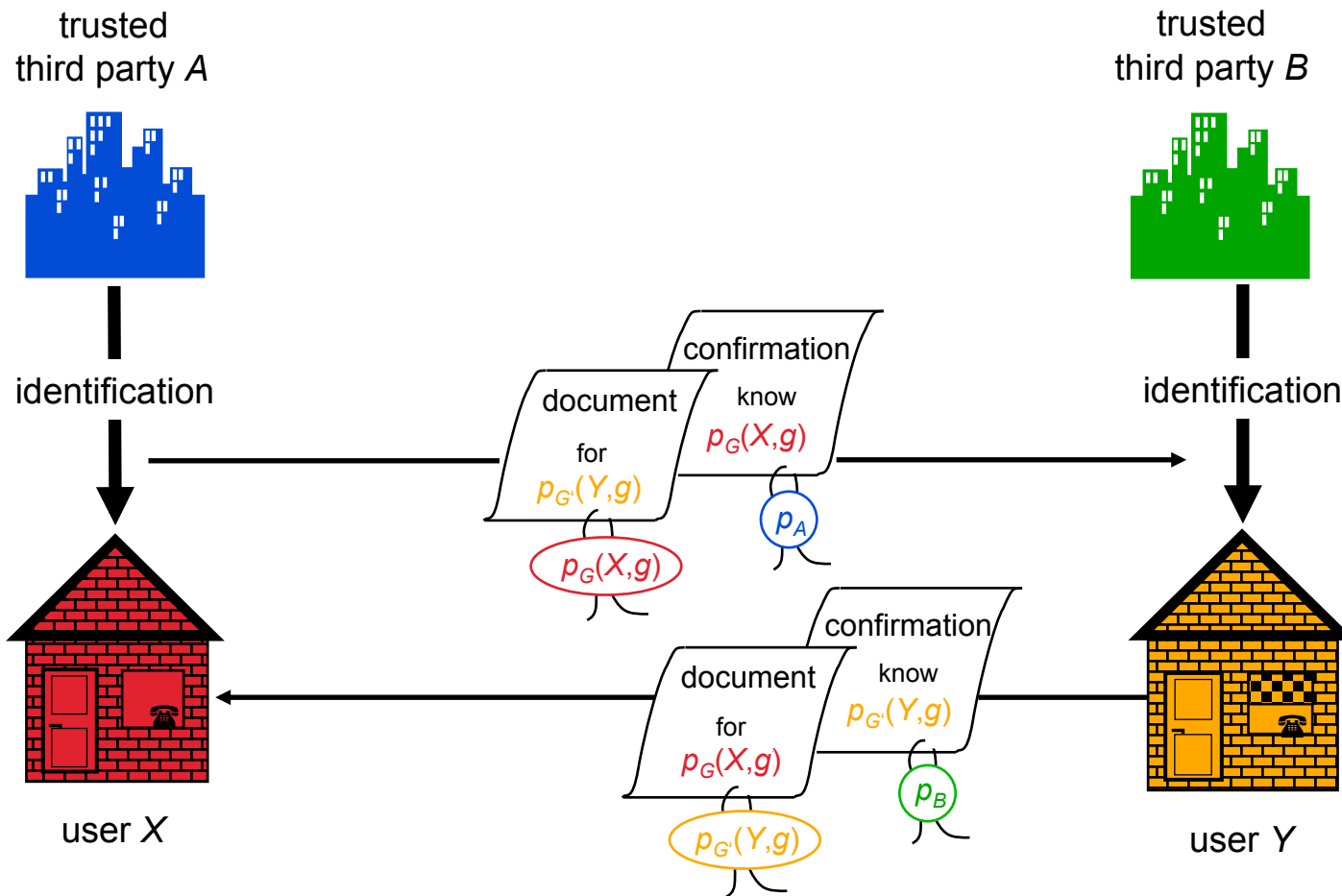
<http://www.primelife.eu/>

<http://www.fidis.net/>

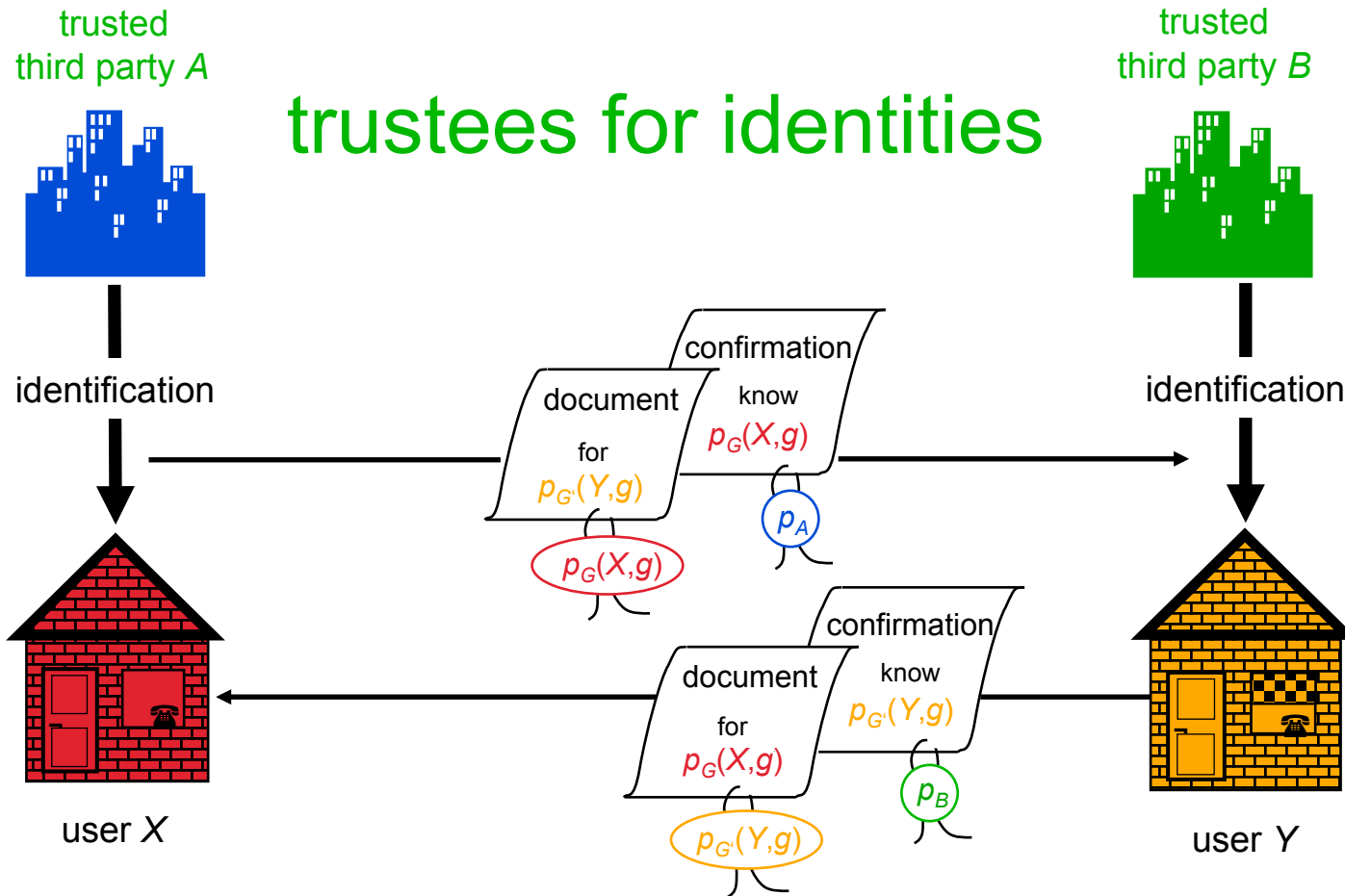
The following backup slides are taken from:

http://www.inf.tu-dresden.de/index.php?node_id=510&ln=en

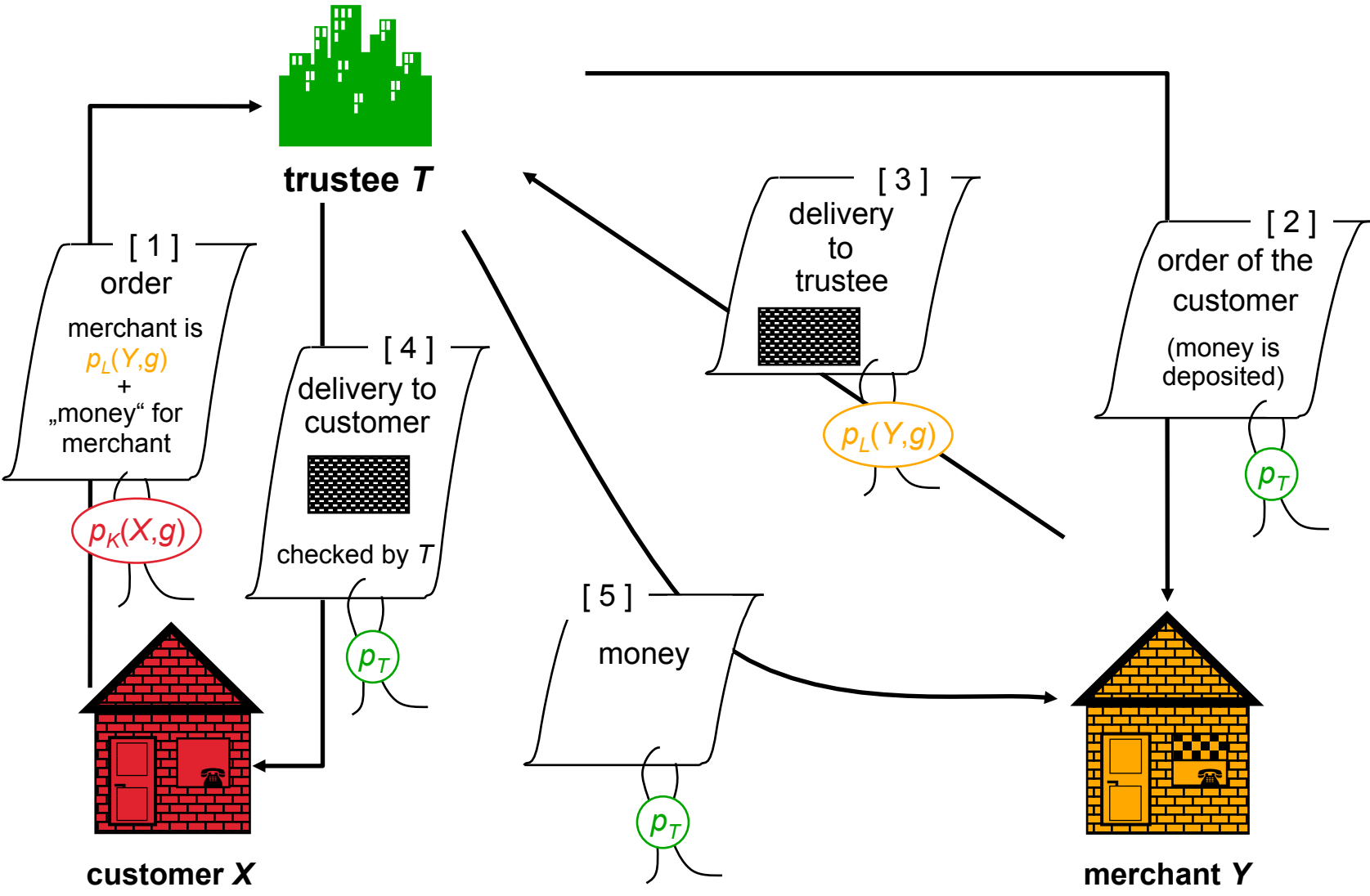
Authenticated anonymous declarations between business partners that can be de-anonymized



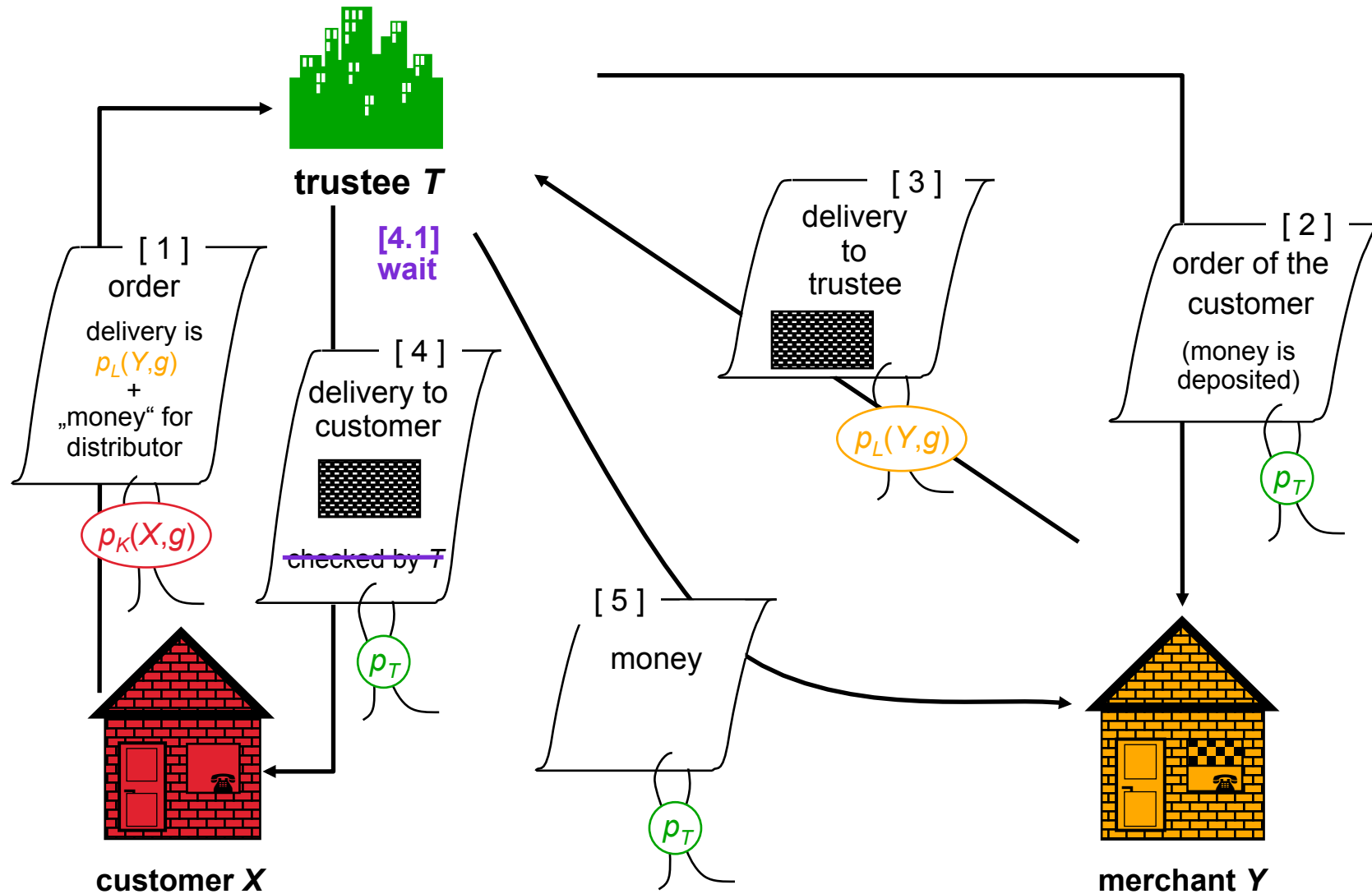
Authenticated anonymous declarations between business partners that can be de-anonymized



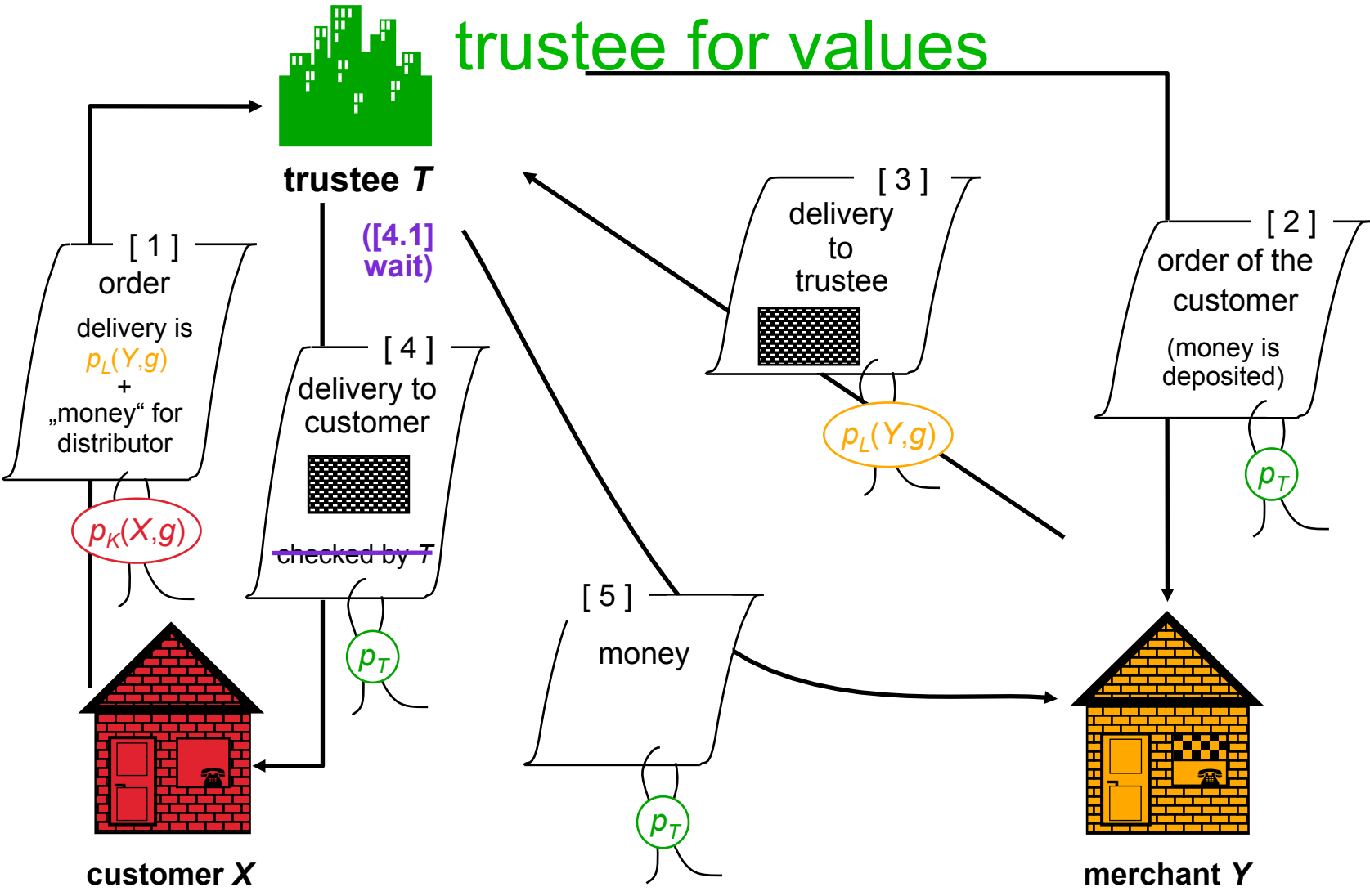
Security for completely anonymous business partners using active trustee who can check the goods



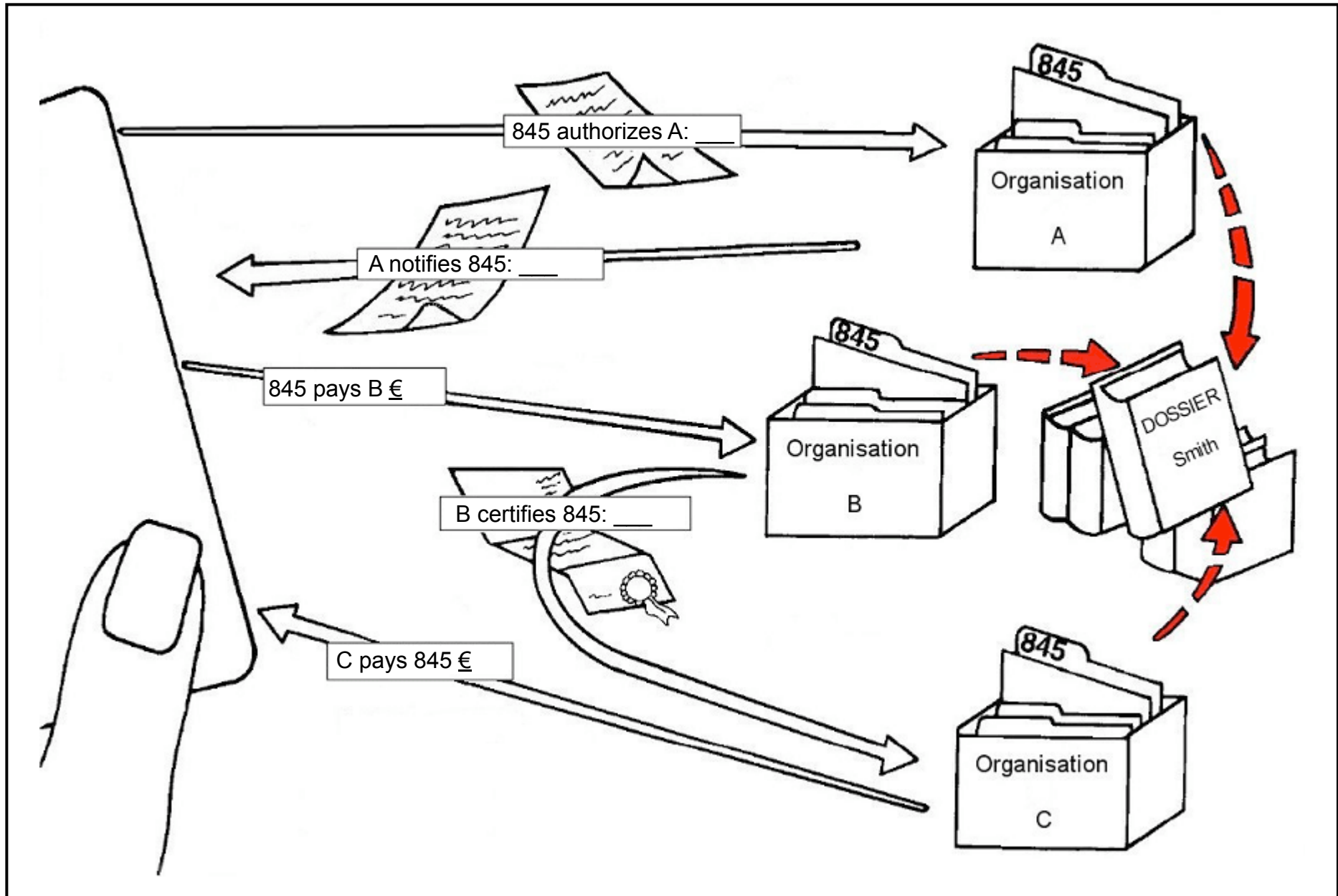
Security for completely anonymous business partners using active trustee who can **not** check the goods



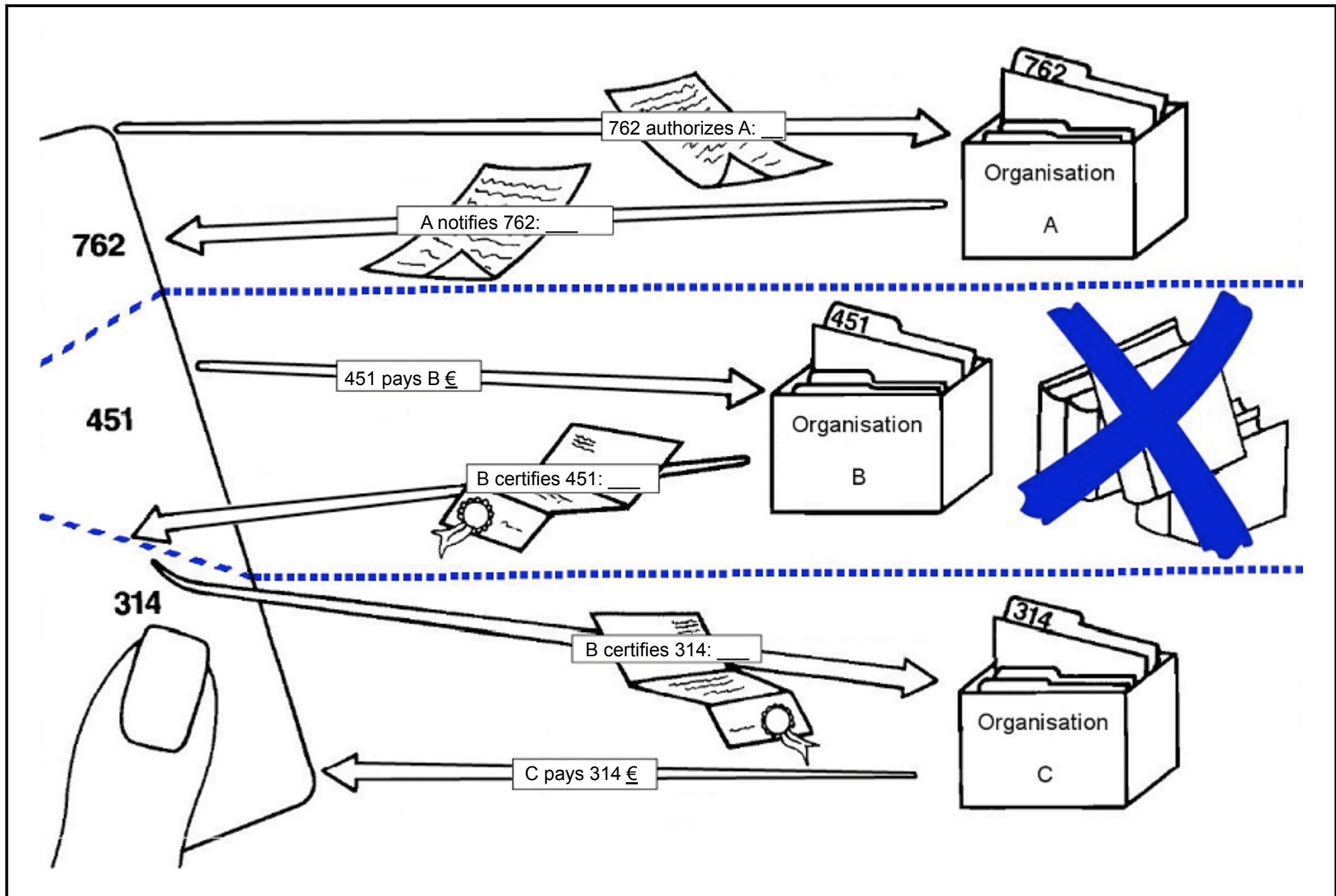
Security for completely anonymous business partners using active trustee who can (not) check the goods



Personal identifier



Role-relationship and transaction pseudonyms



Encryption in layer models

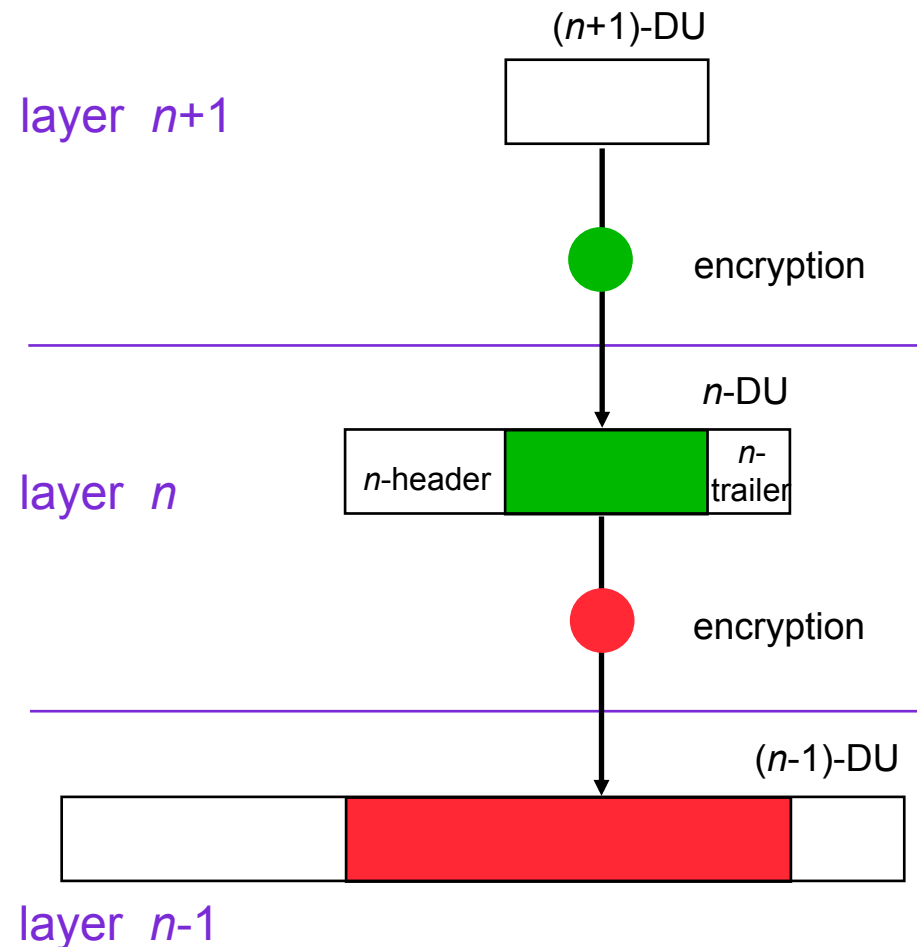
In the OSI model it holds:

Layer n doesn't have to look at Data Units (DUs) of layer $n+1$ to perform its service. So layer $n+1$ can deliver $(n+1)$ -DUs encrypted to layer n .

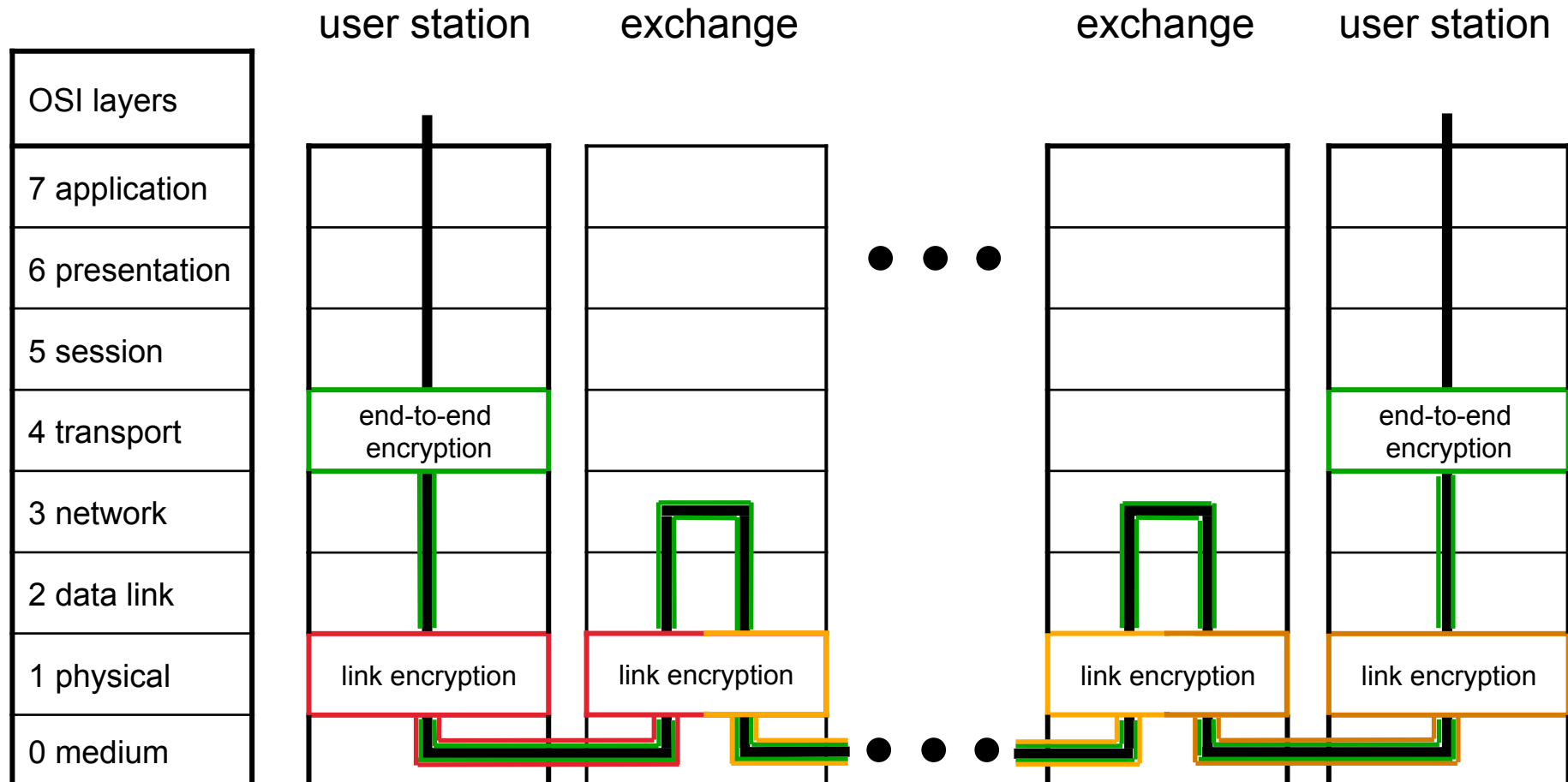
For packet-oriented services, the layer n typically furnishes the $(n+1)$ -DUs with a n -header and possibly with an n -trailer, too, and delivers this as n -DU to layer $n-1$. This can also be done encrypted again.

and so on.

All encryptions are independent with respect to both the encryption systems and the keys.



Arranging it into the OSI layers (1)



Arranging it into the OSI layers (2)

OSI layers	broadcast		query	MIX-network	DC-network	RING-network
7 application						
6 presentation						
5 session						
4 transport	implicit		implicit			
	addressing		addressing			
3 network	broad-cast		query and superpose	buffer and re-encrypt		
2 data link					anonymous access	anonymous access
1 physical		channel selection			superpose keys and messages	digital signal regeneration
0 medium						ring

has to preserve anonymity against the communication partner
 end-to-end encryption

has to preserve anonymity
 realizable without consideration of anonymity