An Introduction to Digital Identity

Andreas Pfitzmann
Dresden University of Technology, Department 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/

Keynote presentation at
OECD Workshop on Digital Identity Management
Trondheim, Norway, May 8, 2007

An Introduction to Digital Identity

Digital identity *of what?*

is set of attributes

Partial Identities (pIDs) *for privacy*

how to use?

Attributes: *Important kinds of*

Possible classifications

Example: How to (not) use biometrics

How to represent identity online?

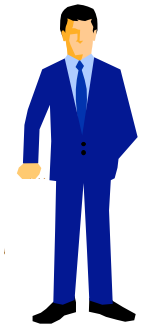
How to manage your identity online?

Identity management framework needed

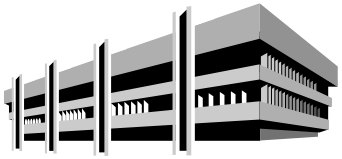
Digital identity of what?

Digital identity *of*

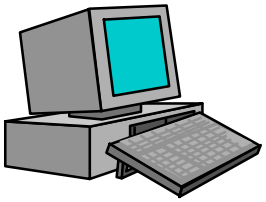
- Natural person,



- Legal person, or



- Computer



Digital identity is ?

Digital identity is much *more than*

- Names (easy to remember),
- Identifiers (unique), and
- Means of authentication (secure).

Digital identity is ...

Digital identity *primarily* is a

- **set of attributes**,

where some 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 digital data, a digital identity is

- **only growing** – never shrinking.

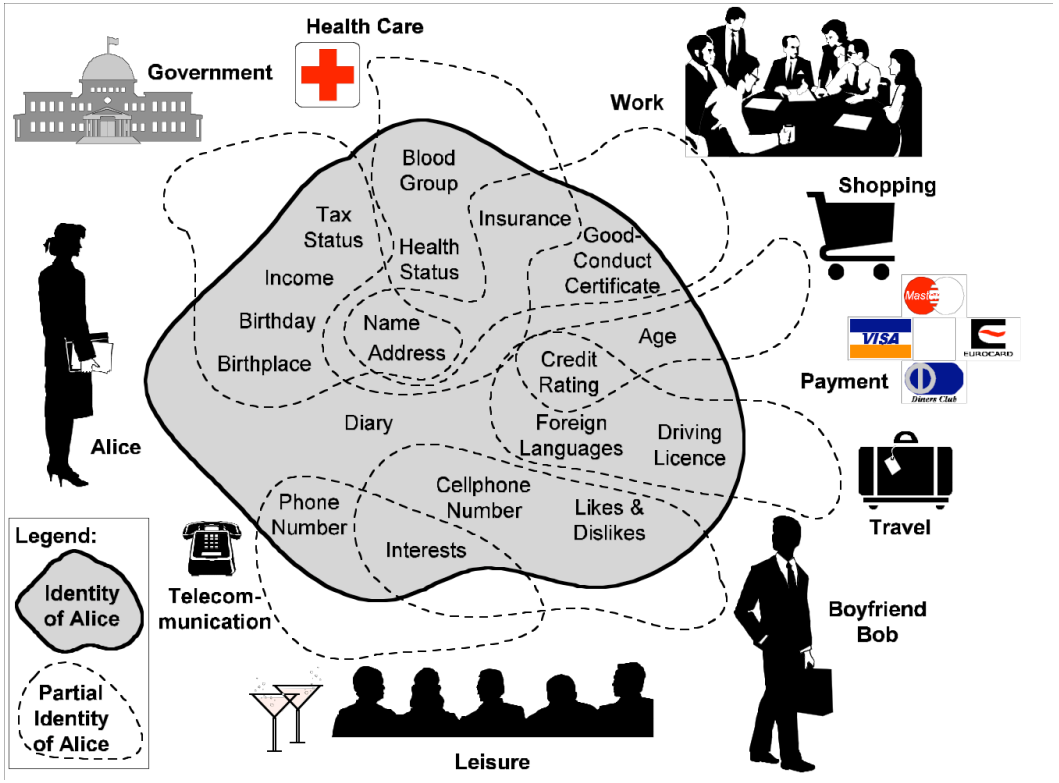
This is true both for a global observer as well as for each party (or set of parties pooling their information) interacting with a digital identity.

Partial Identities (pIDs)

Achieving security and privacy requires users to *subset* their *digital 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** administrating 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 attributes from one pID to another pID of the same digital identity (otherwise no transfer of certified attributes between pIDs, which drastically reduces their applicability).

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 attributes

- Authenticated by third parties or not?
  - If authenticated by third parties, third parties trusted by whom wrt what?
- Easy to change or not?
- Varying over time or not?
- Given attributes vs. chosen attributes
- Pure attributes vs. attributes containing side information
- Characterizing a single entity per se or an entity only in its relationship to other entities?

How much protection for which attributes?

Some attributes need much *more protection* than others, e.g. those which

- are not easy to change,
- do not vary over time,
- are given attributes, or
- contain side information.

These attributes 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

- Biometrics is an important example of an eternal core-identity attribute
- "How to (not) use biometrics" therefore is an interesting case study http://dud.inf.tu-dresden.de/literatur/Duesseldorf2005.10.27Biometrics.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 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.

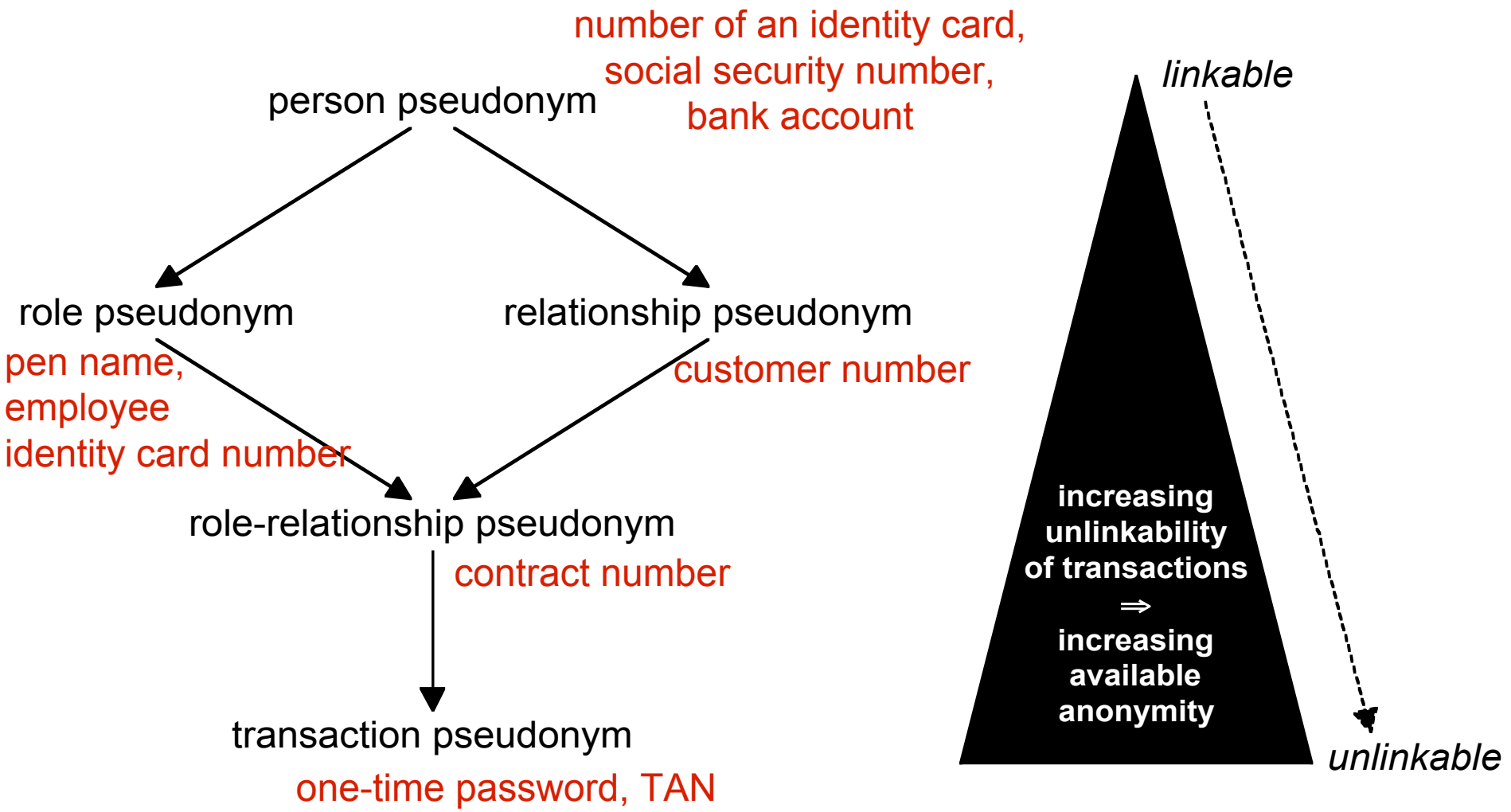
Bank account with bank as trustee for identity,
Credit card number ...

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

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. FP6 EU-Project PRIME https://prime-project.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*.

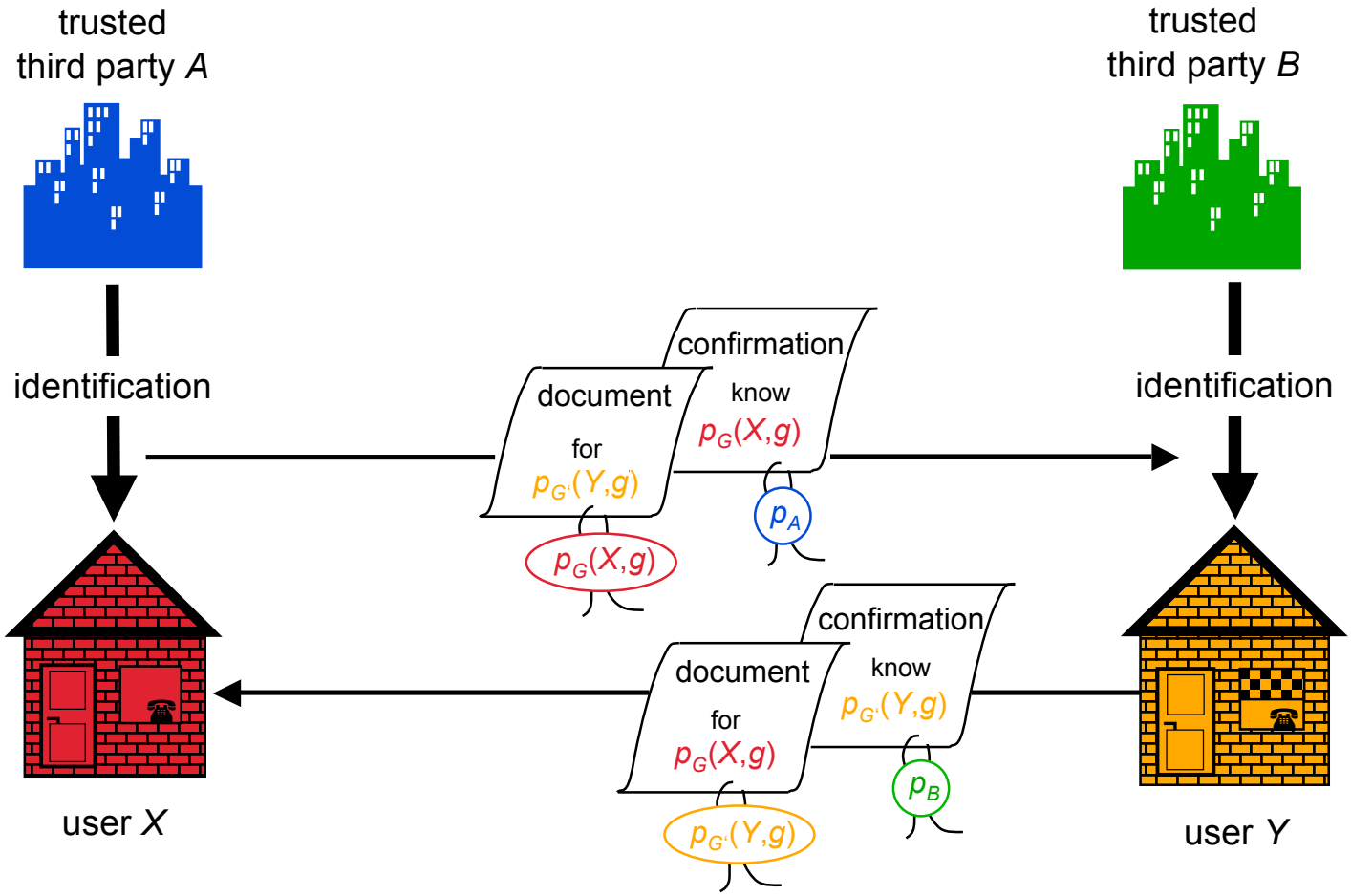
Further reading

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

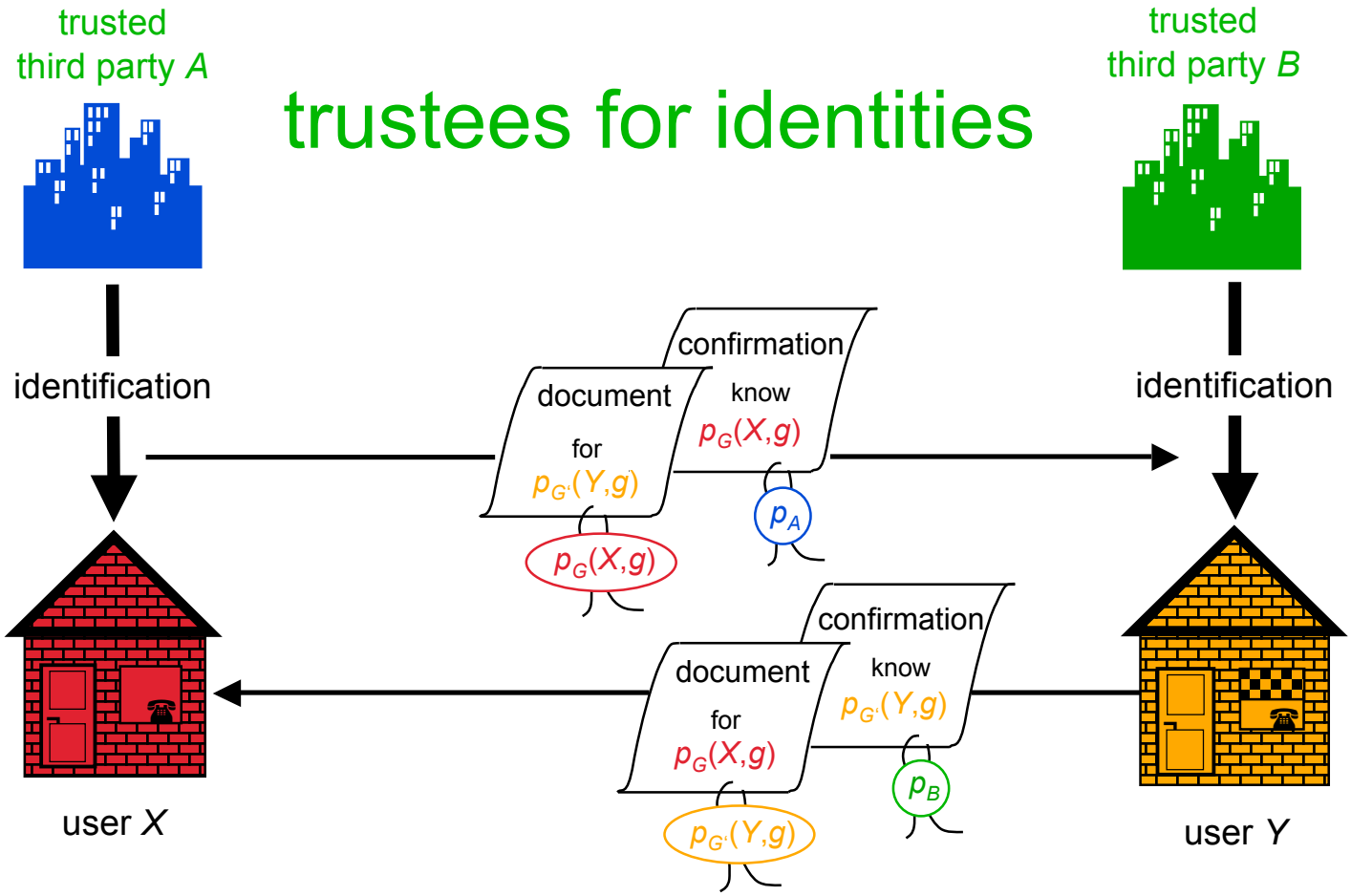
The following backup slides are taken from:

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

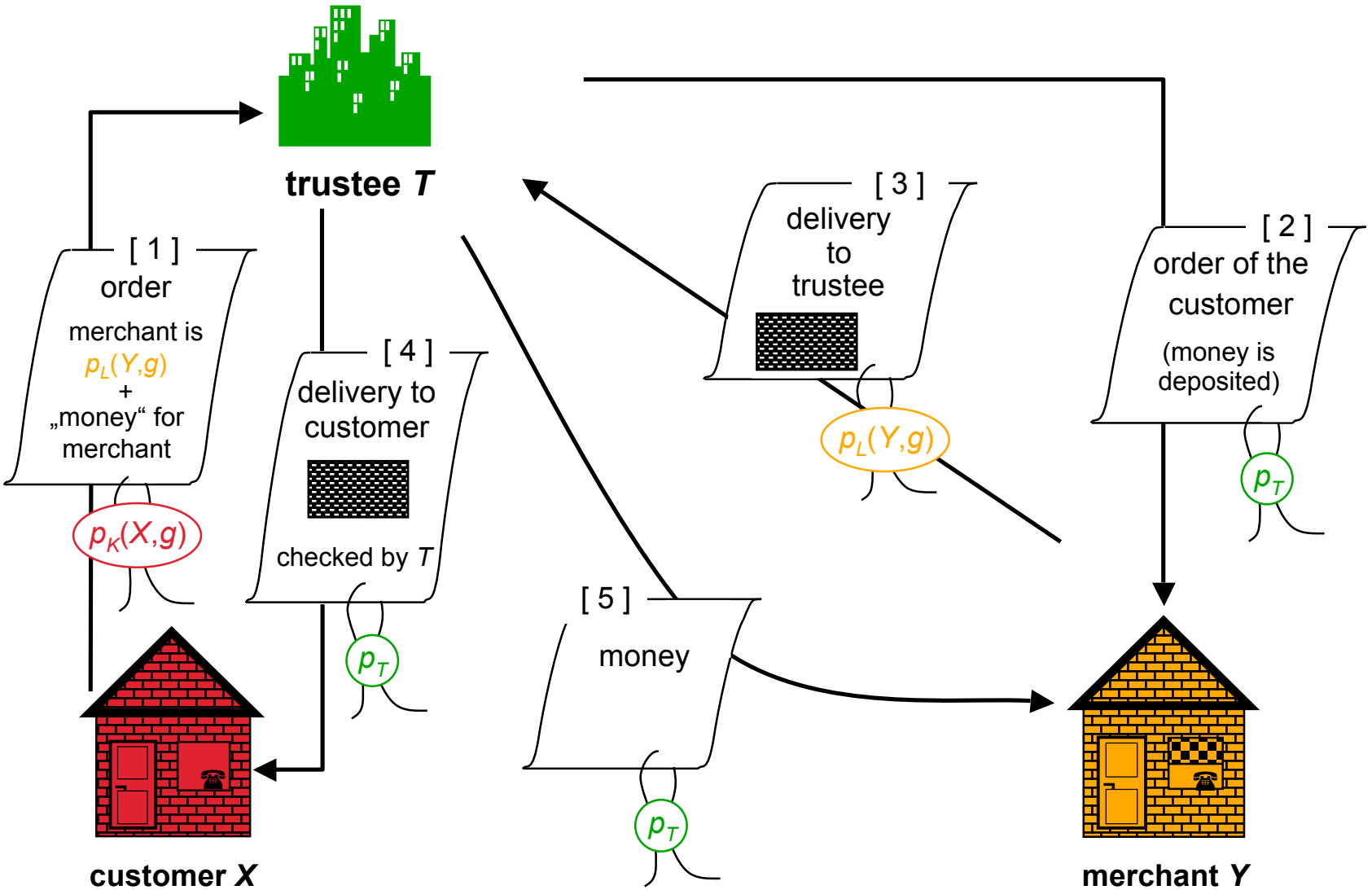
Authenticated anonymous declarations between business partners that can be de-anonymized



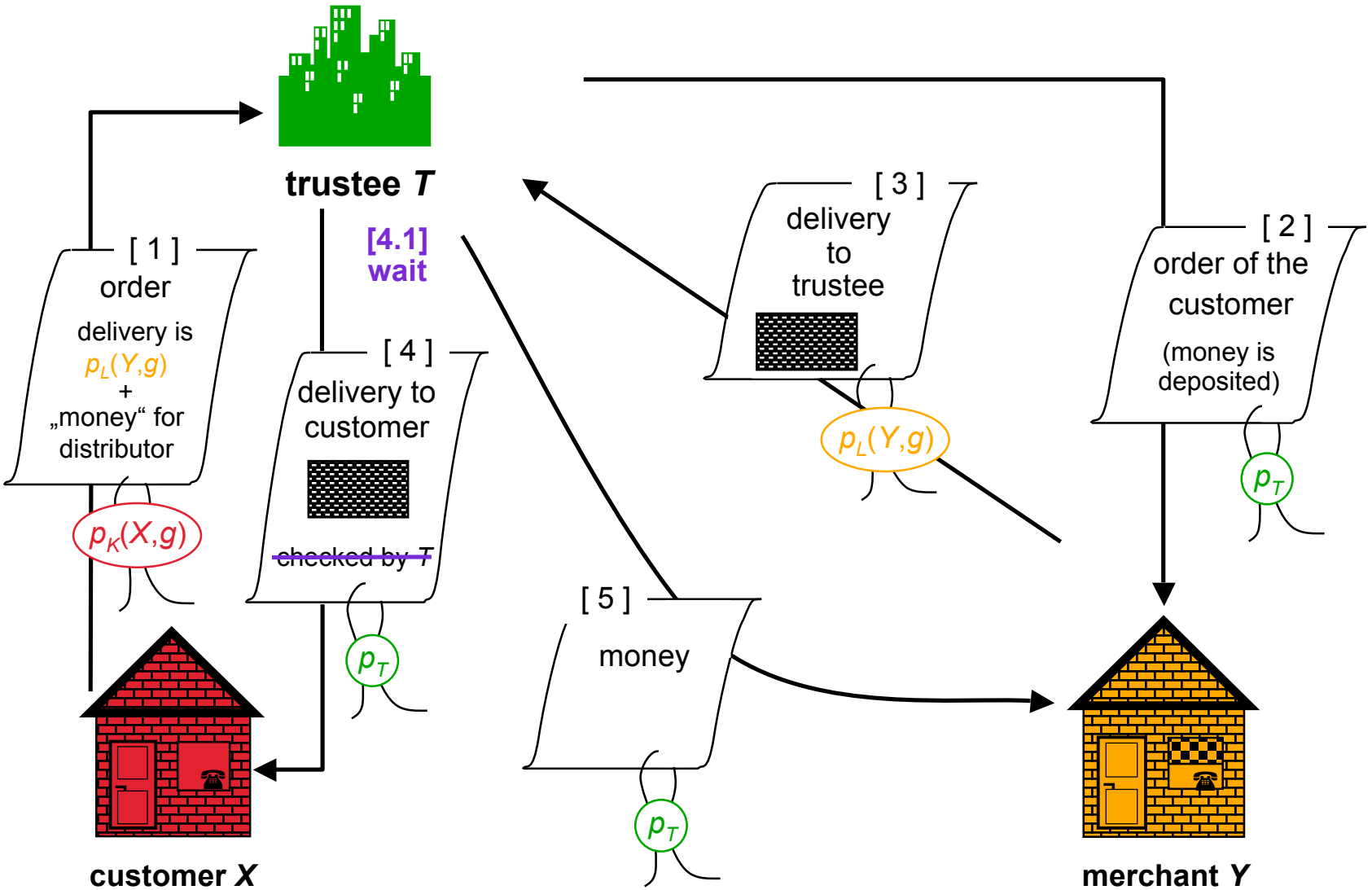
Authenticated anonymous declarations between business partners that can be de-anonymized



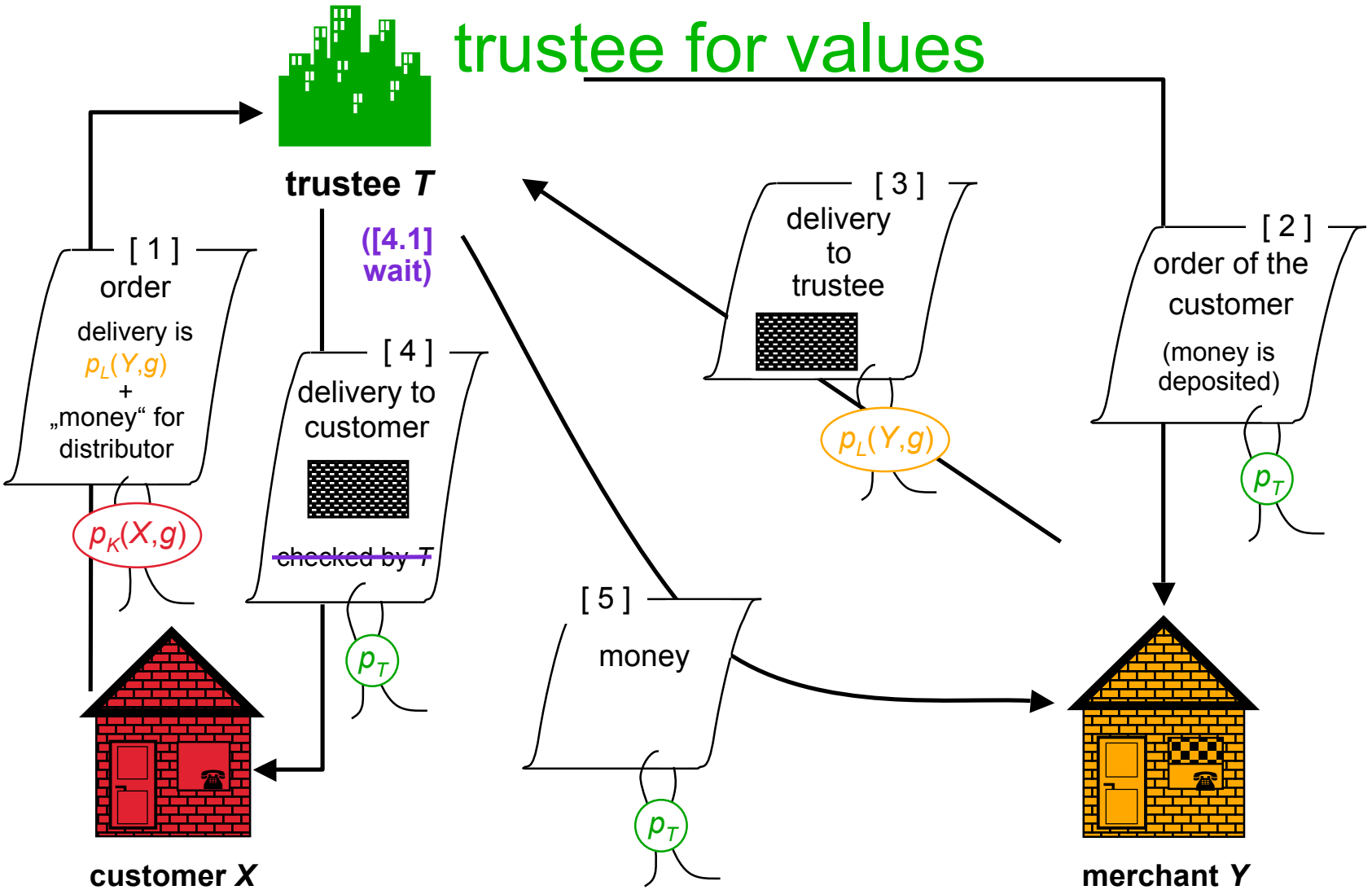
Security for completely anonymous business partners using active trustee who can check the goods



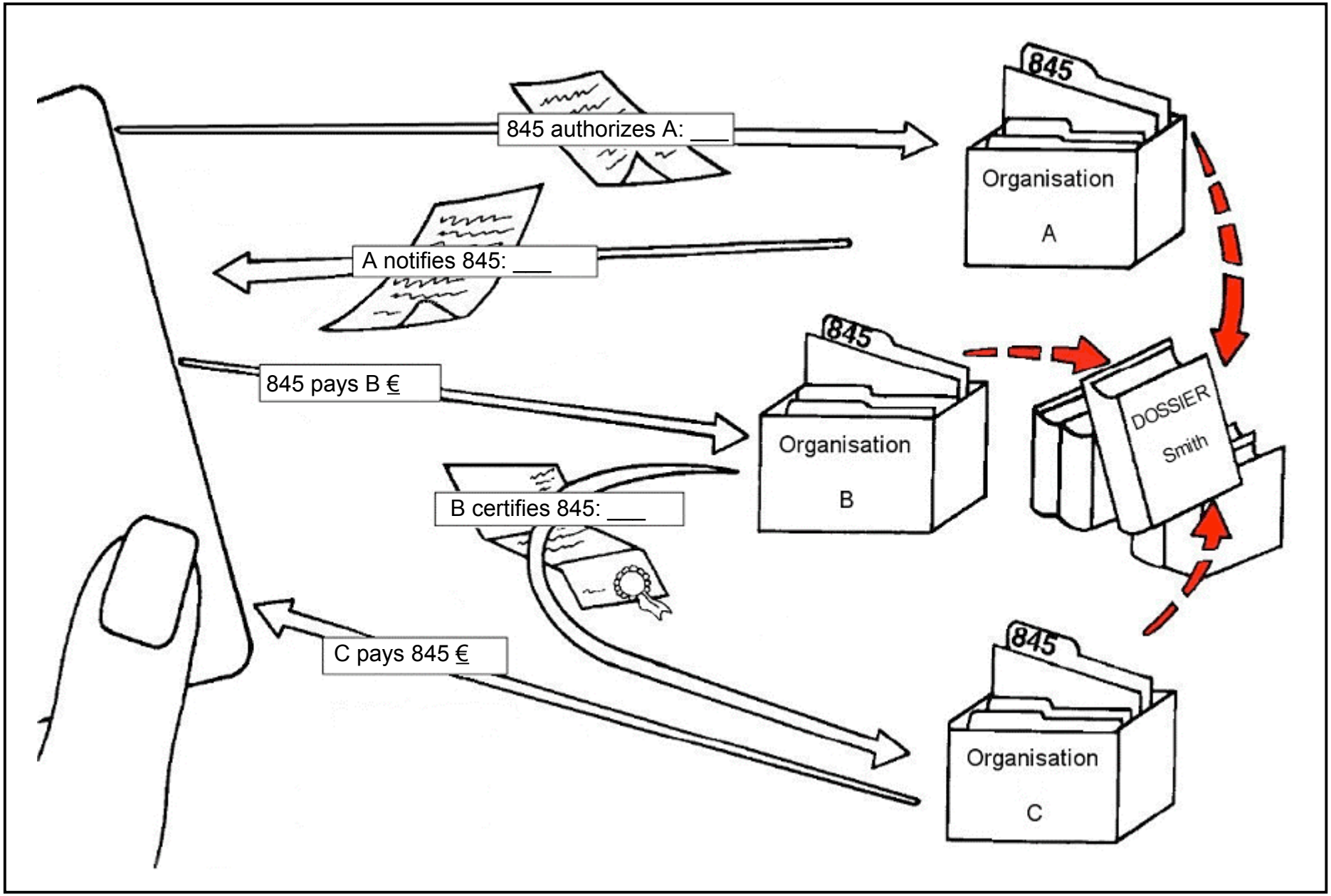
Security for completely anonymous business partners using active trustee who can not check the goods



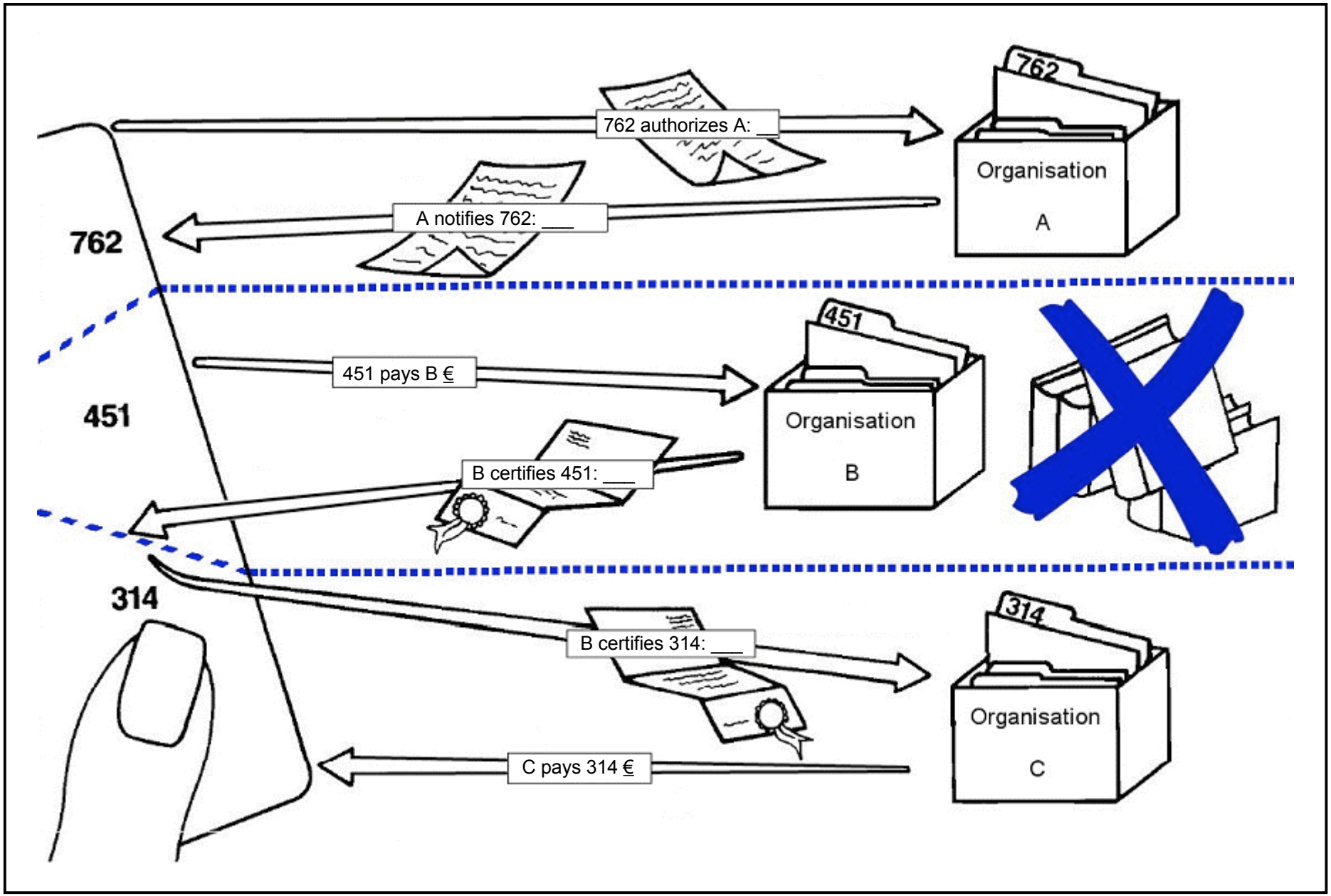
Security for completely anonymous business partners using active trustee who can (not) check the goods



Personal identifier



Role-relationship and transaction pseudonyms



Encryption in layer models

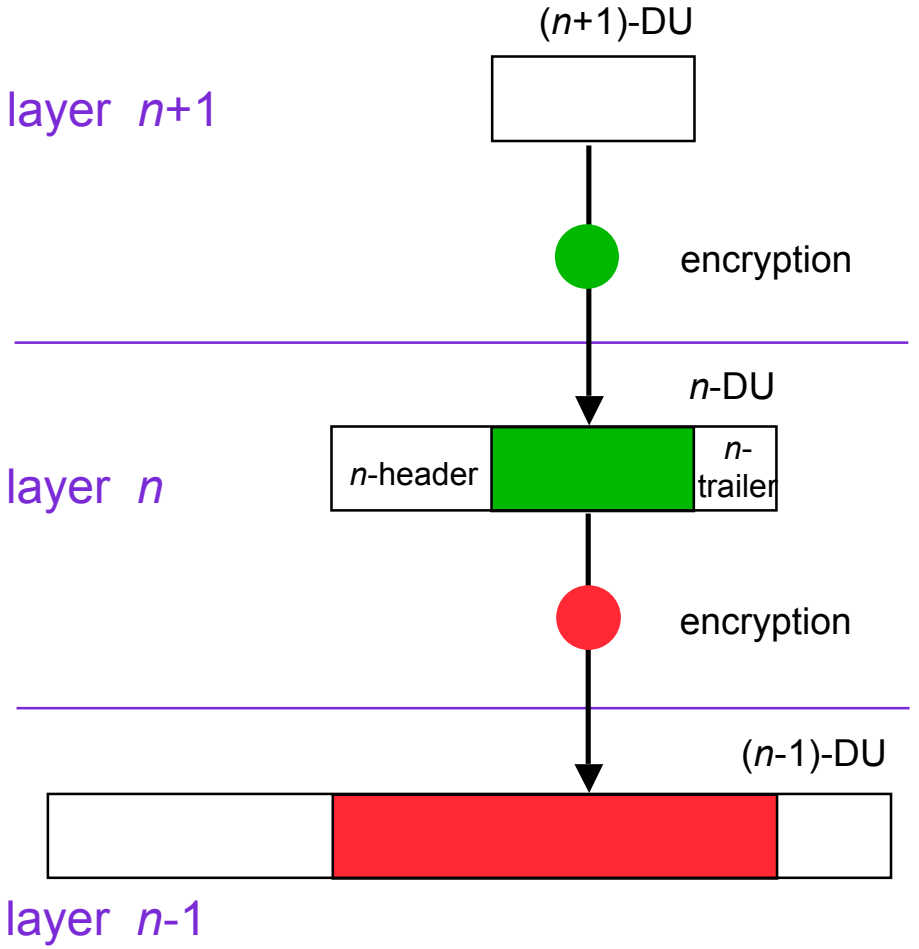
In the OSI model it holds:

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*.

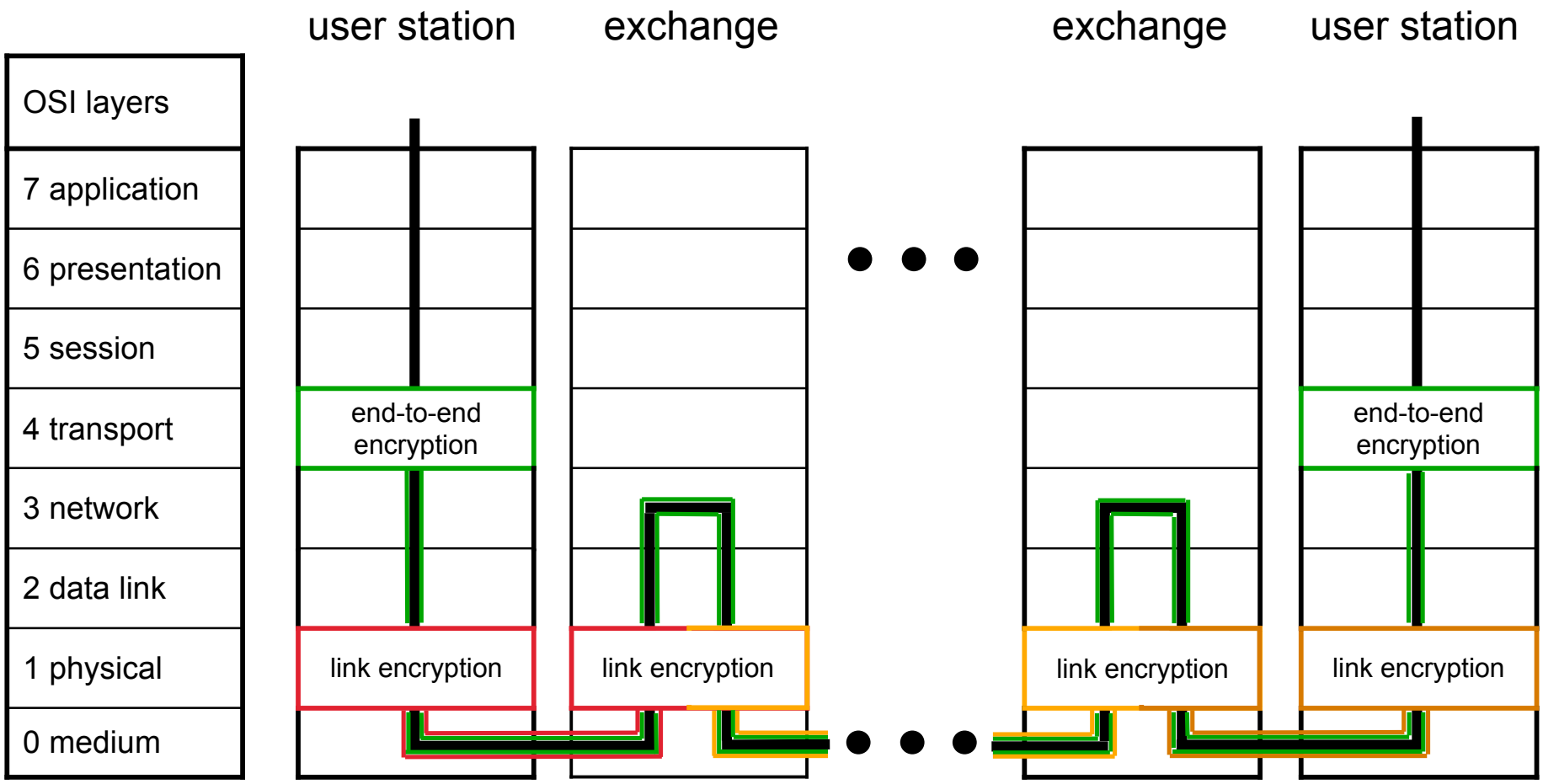
For packet-oriented services, the layer *n* typically furnishes the (*n*+1)-DUs with a *n*-header and possibly with an *n*-trailer, too, and delivers this as *n*-DU to layer *n*-1. This can also be done encrypted again.

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 addressing	implicit 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