Towards an Architecture for Pseudonymous E-Commerce

Applying Privacy by Design to Online Shopping

Sebastian Pape, Daniel Tasche, Iulia Bastys,
Akos Grosz, Jörg Lässig, Kai Rannenberg

Apr 25th, 2018 Sicherheit 2018 Konstanz, Germany

- Aim: Allow pseudonymous shopping in the internet
  - for physical goods
  - including shipping

SPONSORED BY THE
Federal Ministry of Education and Research

Cleopa GmbH

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

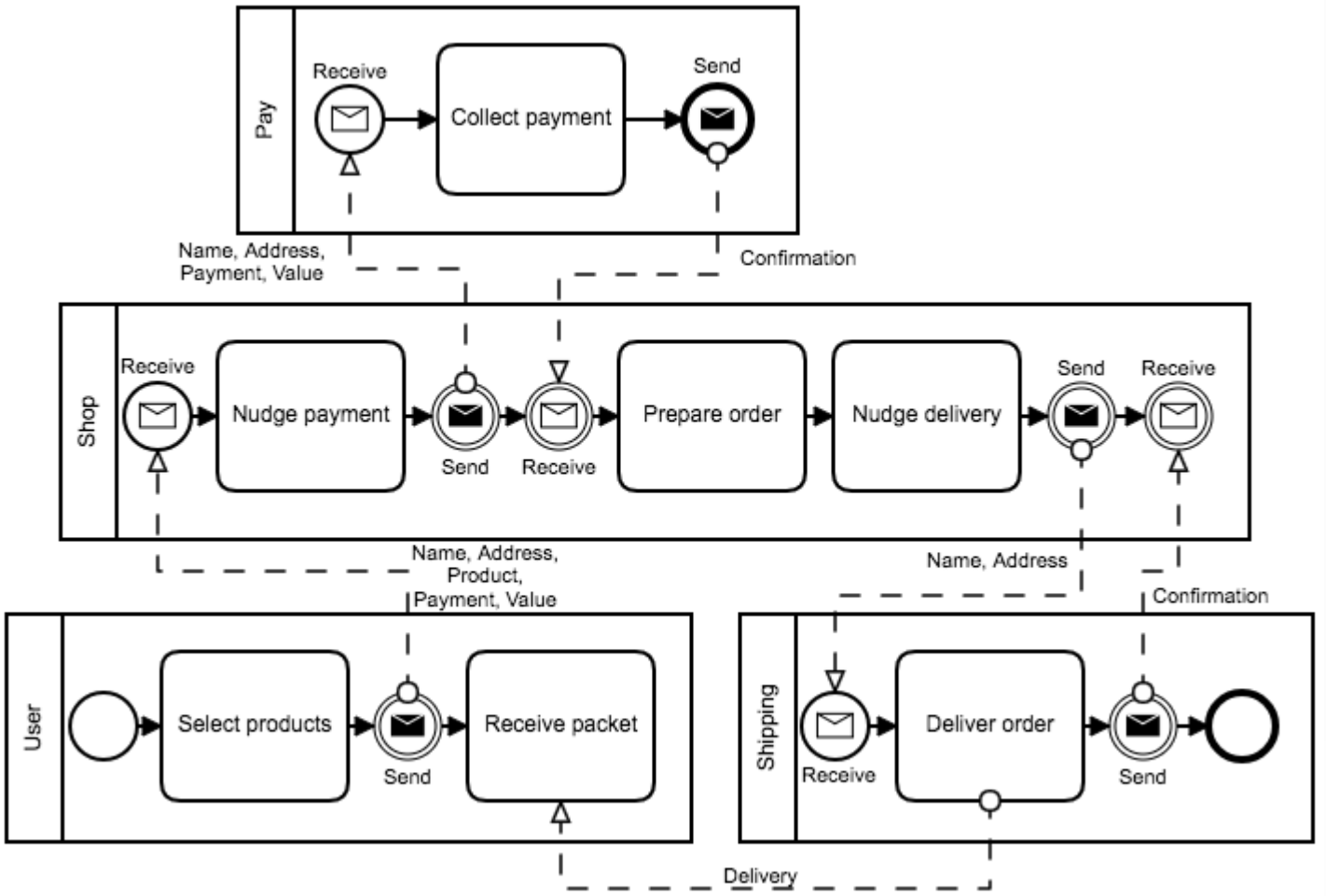
Hochschule Zittau/Görlitz UNIVERSITY OF APPLIED SCIENCES

payever

pin MAIL

OXID esales

Current Practice



Comp. Criteria / Requirem.

- Privacy
- Usability
- Transparency
- Compatibility

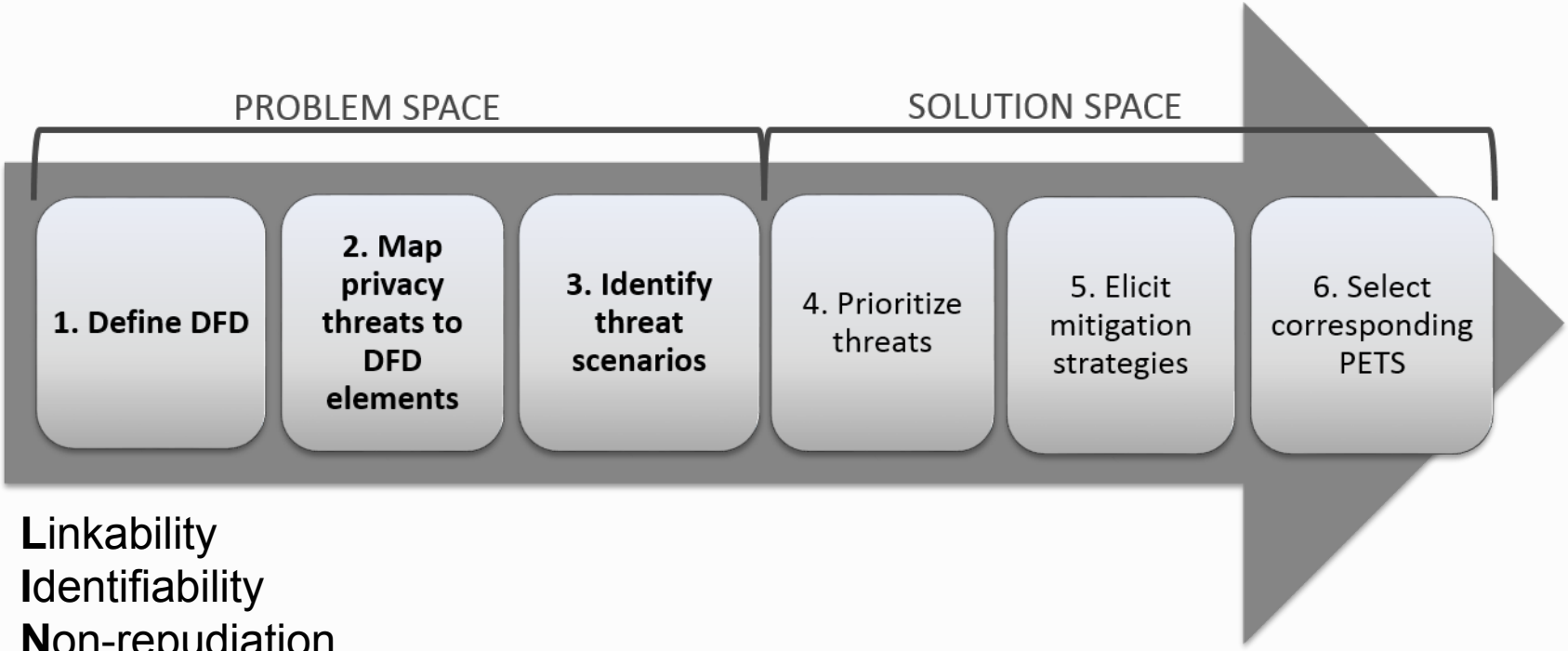
- Shop should learn only user's activity on platform
  - i.e. purchased products
  - total value
- Shop does not learn payment or shipping data.

- Payment Provider should only learn
  - amount to be payed
  - Payment data

- Shipping Provider should learn only
  - the shipping data

	Shipping	Payment	Products	Value
Shop			✓	✓
Payment		✓		✓
Shipping	✓			

LINDDUN: Overview

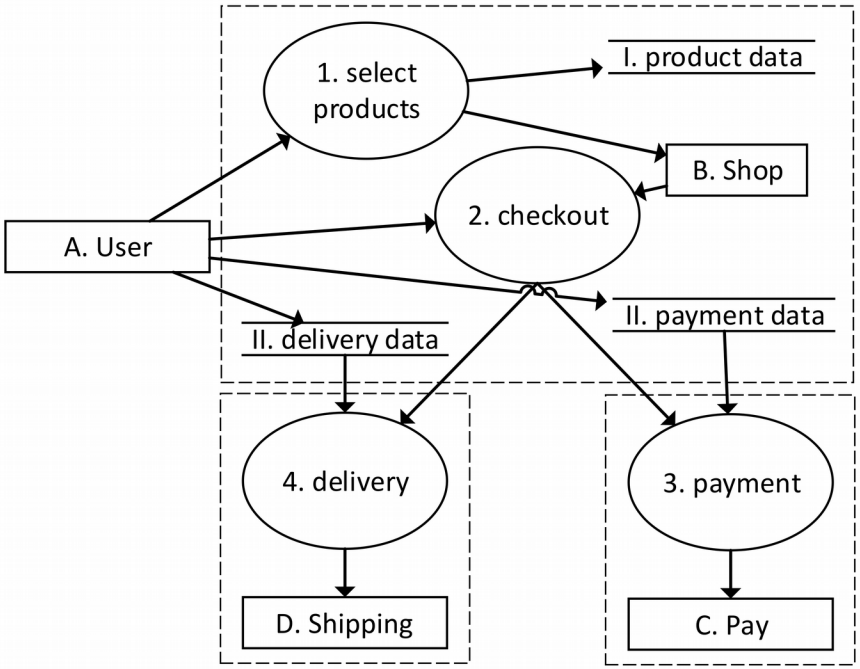


Linkability
Identifiability
Non-repudiation
Detectability
Disclosure of information
Unawareness
Non-compliance

LINDDUN: Regarded Threats

Abbreviation	Threat
Link	Linkability purchase
Iden	Identifiability
DeLo	Detectablility login
DePu	Detectablility purchase
DePa	Detectablility payment
DeDe	Detectablility delivery
DiSC	Disclosure shopping cart
DiTV	Disclosure total value
DiPd	Disclosure payment data
DiDd	Disclosure delivery data

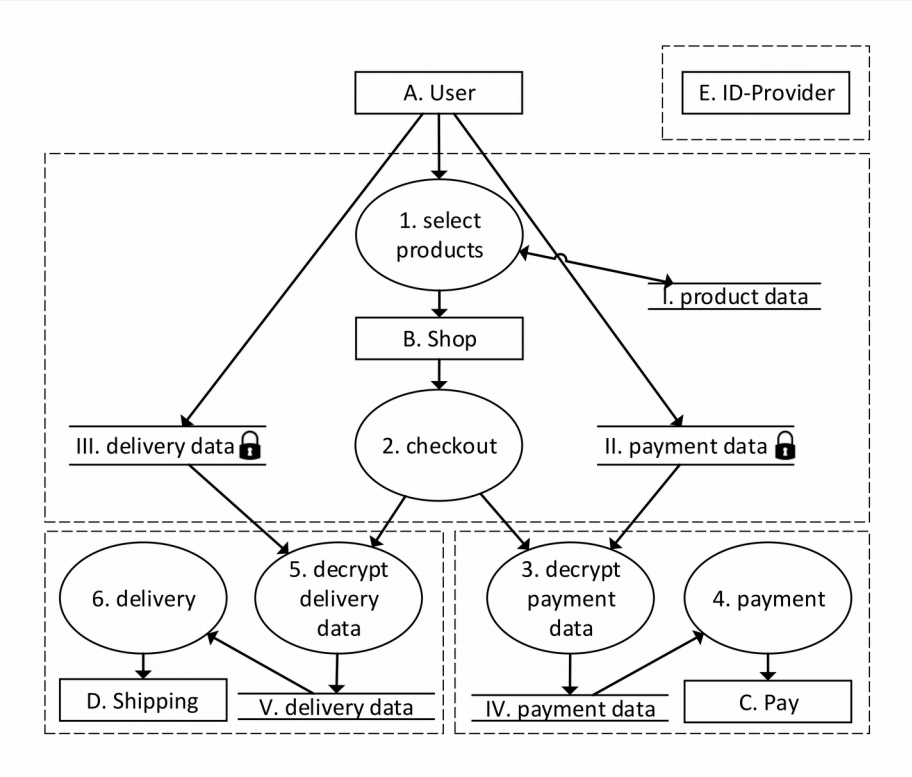
Standard Scenario



A

	Link	Iden	DeLo	DePu	DePa	DeDe	DiSC	DiTV	DiPd	DiDd
A. User	X	X	X	X	X	X	X	X	X	X
B. Shop	X	X	X	X	X	X	X	X	X	X
C. Pay	(X)	(X)		X	X			X	X	
D. Shipping	(X)	(X)		X		X				X

Shop Stores Encrypted Data

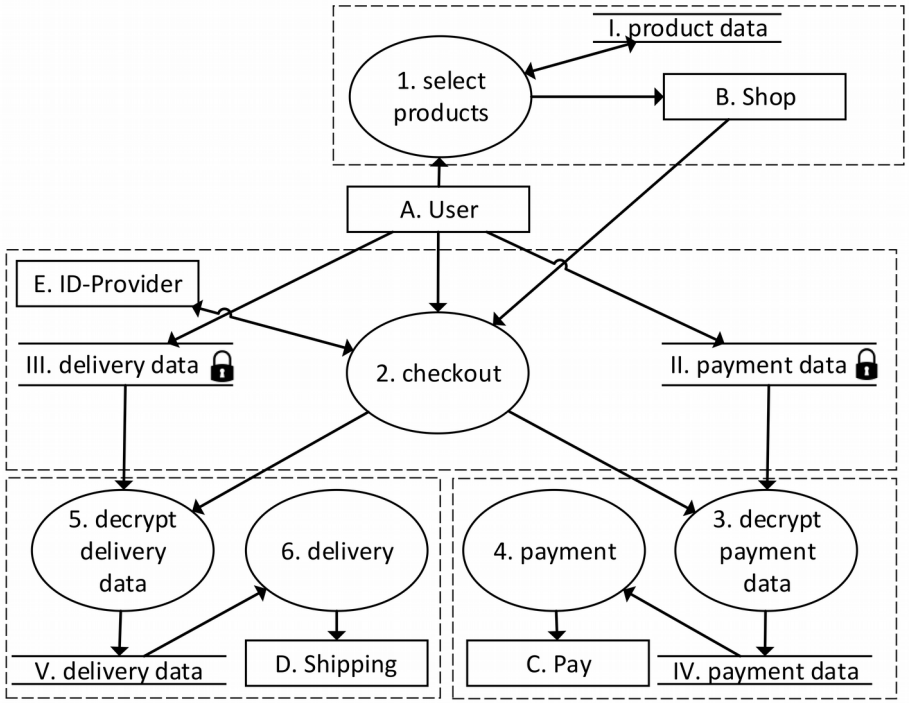


B

	Link	Iden	DeLo	DePu	DePa	DeDe	DiSC	DiTV	DiPd	DiDd
B. Shop	(X)		X	X	X	X	X	X		
C. Pay	(X)	(X)		X	X			X	X	
D. Shipping	(X)	(X)		X		X				X
E. ID-P		X	X							

ID-Provider stores Encrypted Data

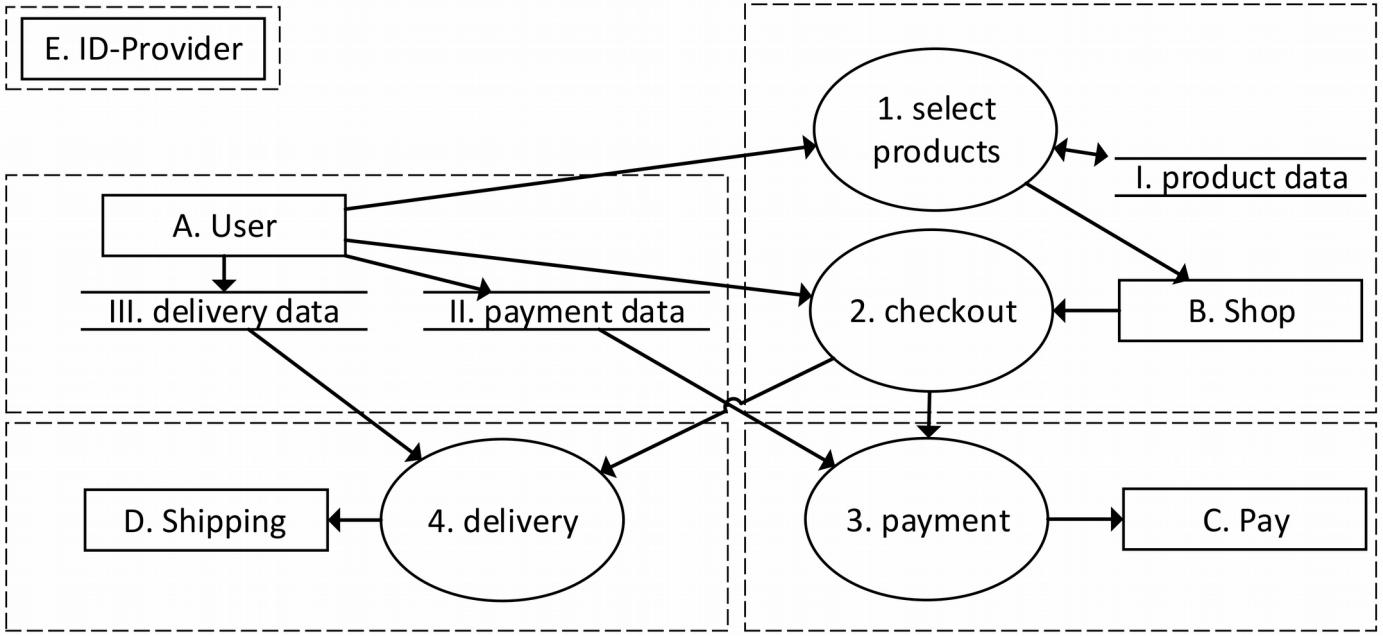
C



	Link	Iden	DeLo	DePu	DePa	DeDe	DiSC	DiTV	DiPd	DiDd
B. Shop	(X)		X	X	X	X	X	X		
C. Pay	(X)	(X)		X	X			X	X	
D. Shipping	(X)	(X)		X		X				X
E. ID-P	X	X	X	X	X	X				

Redirection to 3rd Party

D



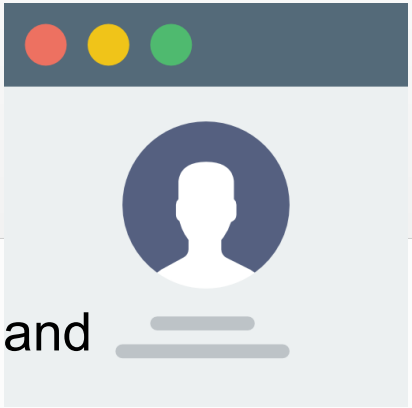
	Link	Iden	DeLo	DePu	DePa	DeDe	DiSC	DiTV	DiPd	DiDd
B. Shop	(X)		X	X	X	X	X	X		
C. Pay	(X)	(X)		X	X			X	X	
D. Shipping	(X)	(X)		X		X				X
E. ID-P		X	(X)							

Comparison Privacy

Threat \ Entity	Shop	Pay	Ship	Identity Provider
Identifiability	A	(ABCD)[2]	(ABCD)[3]	B C D
Disclosure shopping cart	A B C D			
Disclosure total value	A B C D	A B C D		
Disclosure payment data	A	A B C D		
Disclosure delivery data	A		A B C D	
Linkability purchase	A(BCD)[1]	(ABCD)[2]	(ABCD)[3]	C
Detectablility login	A B C D			B C D
Detectablility purchase	A B C D	A B C D	A B C D	C
Detectablility payment	A B C D	A B C D		C
Detectablility delivery	A B C D		A B C D	C

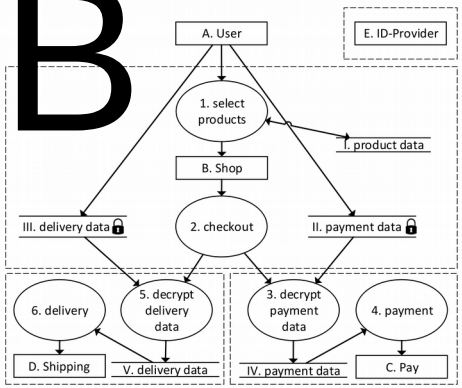
[1] Depends on the user's choice. [2] Depends on user's payment [3] Depends on user's shipping

Usability

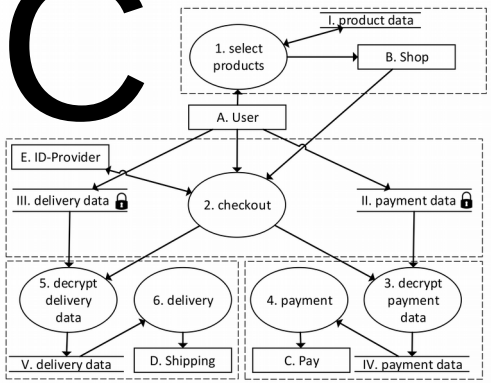


- B (+): User needs to take care of key management and encryption
- C (++): User may delegate crypto to ID-Provider
- D (o) : transactional load is put on the User
  - check information is sent to the correct party
  - Re-enter of data or 3 logins needed

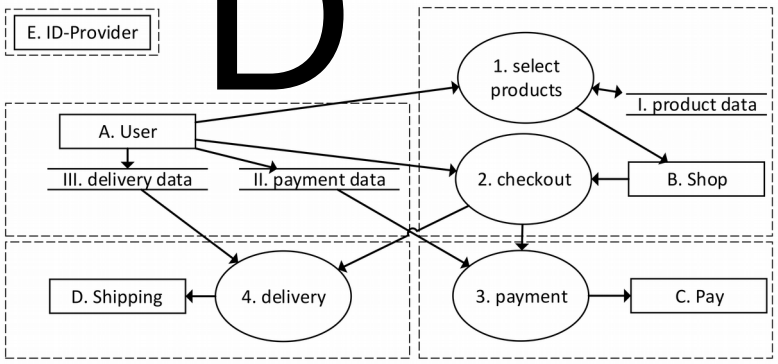
B



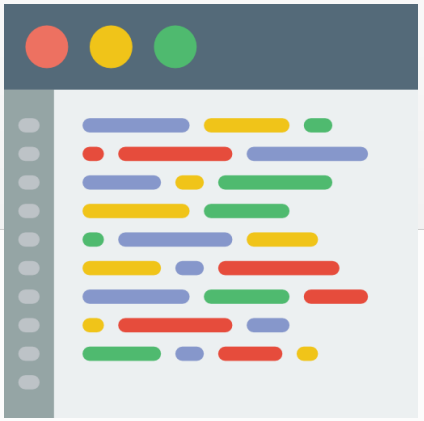
C



D

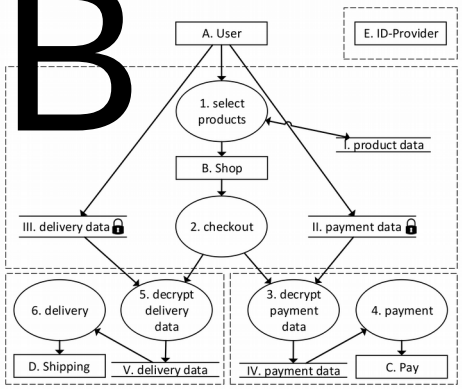


Transparency

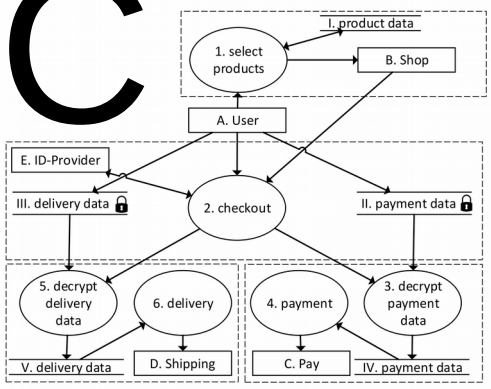


- D (+): The user can see the data providers.
- B (o): Data is sent encrypted via a third party.
- C (o): Data is sent encrypted via a third party.

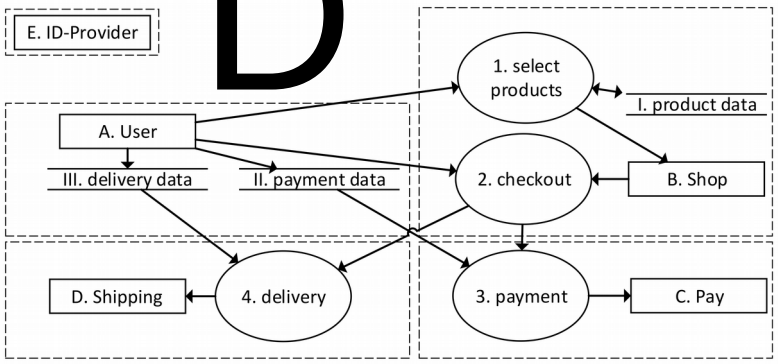
B



C



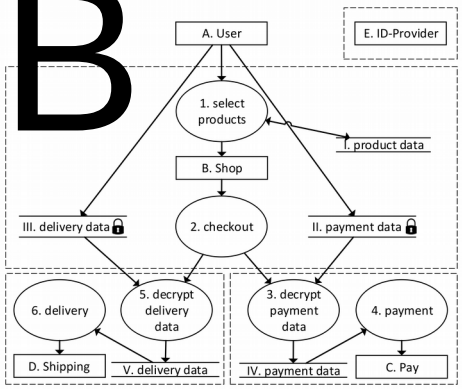
D



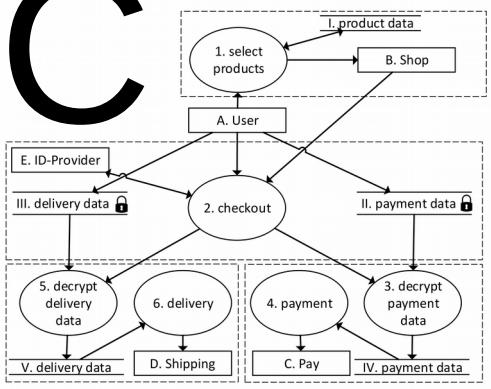
Compatibility

- B (+): All three versions hide the identity of the user
- C (+): as required, but besides that respect the
- D (+): business model

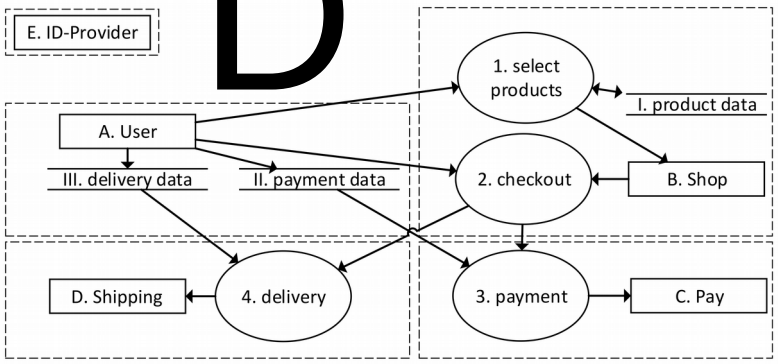
B



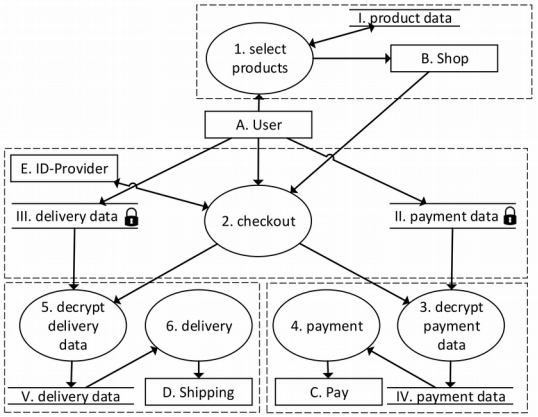
C



D



Comparison



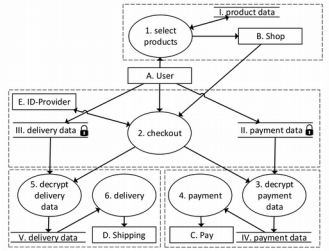
	Privacy	Usablity	Transpa-rency	Compati-bility
A	-	o	+	++
B	++	+	o	+
C	+	++	o	+
D	++	o	+	+

Summary and Future Work

Comparison of 4 architectures

- Privacy
- Usability
- Transparency
- Compatibility

ID-Provider stores encrypted data.



Next step: Implementation

Open Questions:

- Willingness to Pay
- Impact on Business Models

Deutsche Telekom Chair of Mobile Business & Multilateral Security

Dr. Sebastian Pape
Goethe University Frankfurt
Theodor-W.-Adorno-Platz 4
60629 Frankfurt, Germany

Phone +49 (0)69 798 34668
Fax +49 (0)69 798 35004

E-Mail: sebastian.pape@m-chair.de
WWW: www.m-chair.de