Today‘s Privacy Technologies: Possibilities and Limits

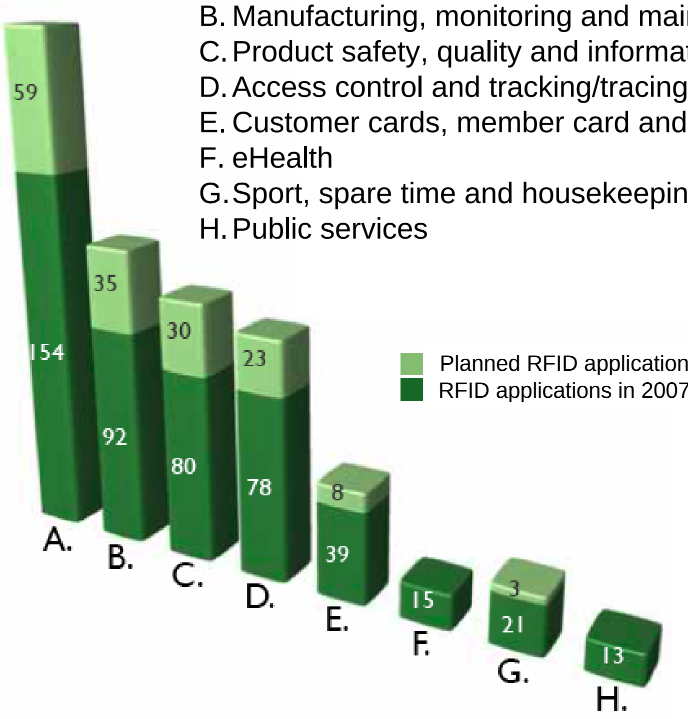
June 11th, 2008

Sven Wohlgemuth

Albert-Ludwig University Freiburg, Germany
Institute of Computer Science and Social Studies
Department of Telematics

RFID influences Privacy

A. Logistics (Tracking & Tracing)
B. Manufacturing, monitoring and maintenance
C. Product safety, quality and information
D. Access control and tracking/tracing of individuals
E. Customer cards, member card and payment
F. eHealth
G. Sport, spare time and housekeeping
H. Public services



Collection and usage of personal data

Privacy?

(e.g. Big BrotherAward 2003 for RFID in supermarket)

Strüker et al, 2008:
RFID Report 2008

Agenda

I. Privacy in Business Processes as in CRM

II. Delegation of Rights as in CRM

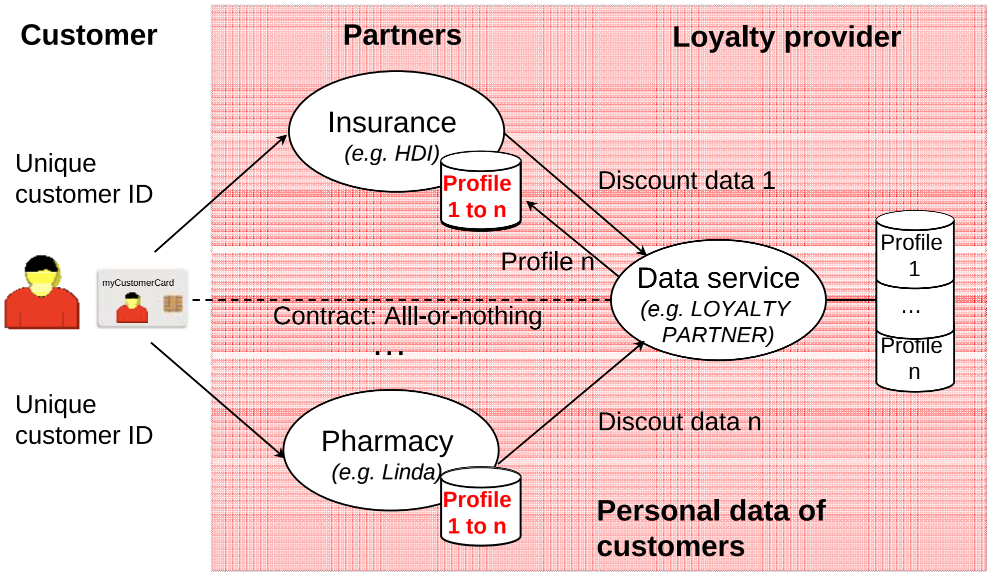
III. DREISAM: Protocols for Delegation of Rights

IV. Evaluation of DREISAM

V. Summary

Today: Privacy in CRM

Service: Personalized advertisement and offers

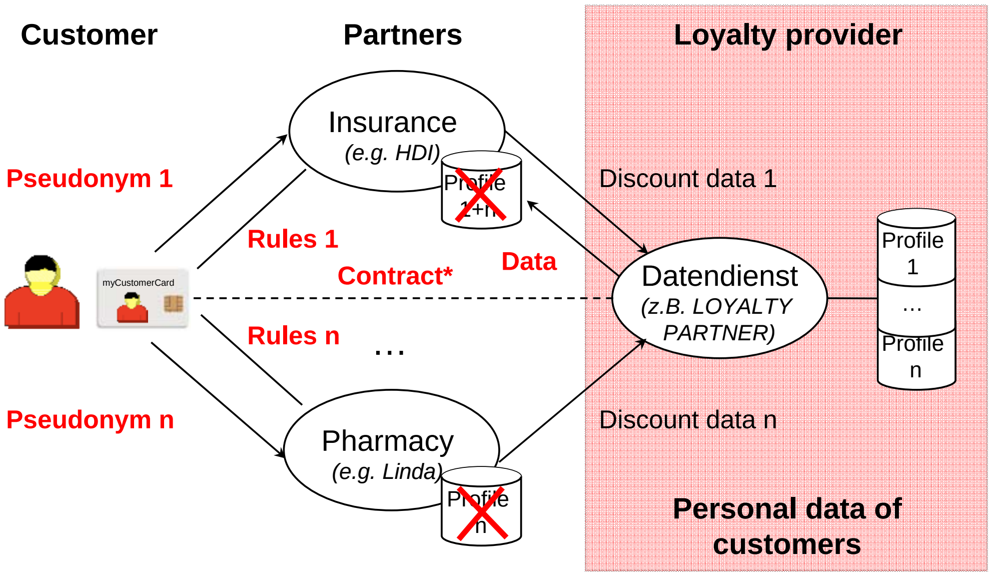


Privacy: Trust domain embraces loyalty provider and partners

Future: Privacy in Multilateral CRM

Objective: Minimizing trust domain

- Accountability of transactions
- Confidentiality of personal data
- Delegation: Case-by-case agreement of access rules



Multilateral CRM: Requirements

a) Data protection acts:

- Purpose-based
- Case-by-case consent
- Revocation of consent

b) CRM:

- Accountability of transactions

c) Threat analysis:

- Non-linkability of transactions excl. for loyalty provider

Agenda

I. Privacy in Business Processes as in CRM

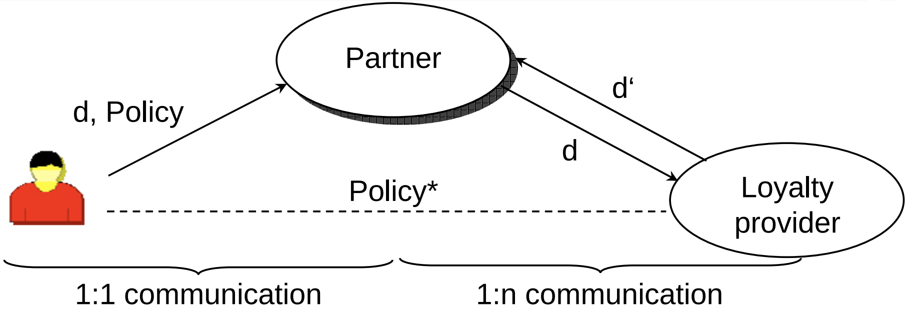
II. Delegation of Rights as in CRM

III. DREISAM: Protocols for Delegation of Rights

IV. Evaluation of DREISAM

V. Summary

Today's Solutions



Partner

d, Policy

d'

d

Policy*

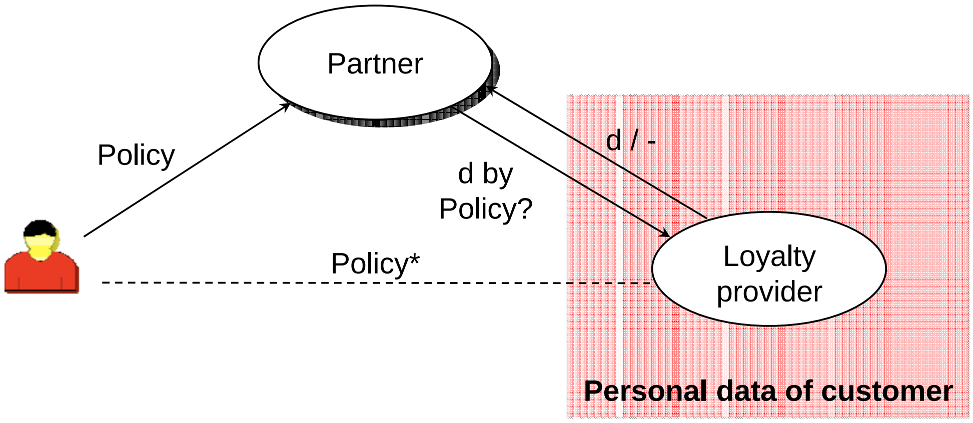
Loyalty provider

1:1 communication

1:n communication

	Principle	Mechanism	Examples	Pers.	Suitable for CRM
1:1	Controlled disclosure of personal data	Anonymity	Anonymizer, JAP	No	No
		Pseudonymity, Identity	Liberty Alliance, iManager, IBM idemix	Yes	Limit (Premise for 1:n)
	Agreed rules for collection	Seals, Languages for conditions	TRUSTe, P3P	Yes	No
1:n	Agreed rules for delegation	Languages for obligations	EPAL, NAPS	Yes	No
	Enforcement of agreed rules	Sticky policy, ***Delegation of rights***	HP Adaptive PMS, ***DREISAM***	Yes	Yes

Delegation von Rights and CRM



Partner

Policy

d by Policy?

d / -

Policy*

Loyalty provider

Personal data of customer

Properties:

- Case-by-case consent / revocation for data d by delegation of policy (rights)
- Purpose-based by case-by-case policy

To be solved:

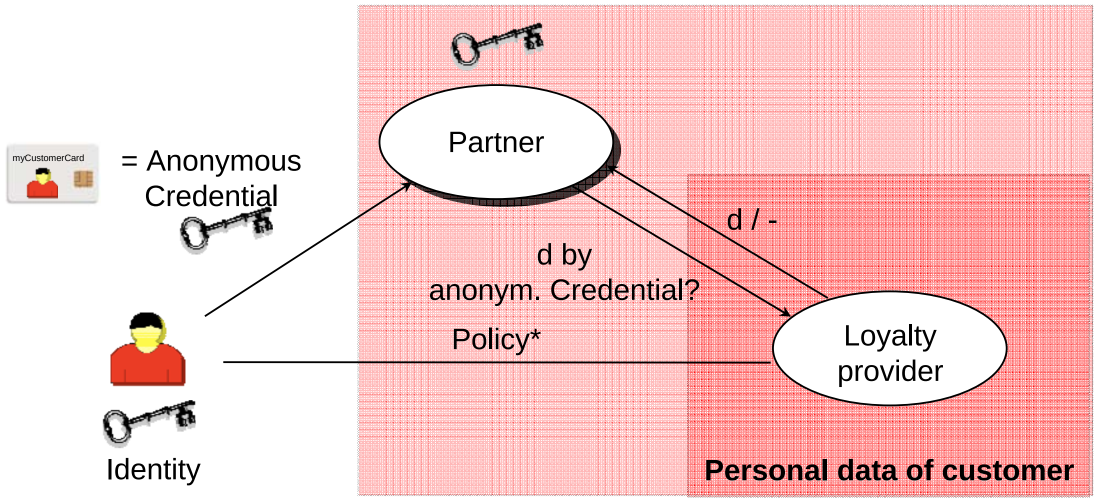
- Accountability of transactions
- Non-linkability regarding partners and third parties

Cryptographic Protocols and Delegation of Rights

	Liberty Alliance	Shibboleth	iManager	IBM idemix	SPKI	Kerberos
Accountability	+	+	+	+	+	+
Purpose-based	+	+	+	+	+	+
Case-by-case consent	+	+	+	+	+	+
Revocation of consent	-	-	-	+	+	-
Non-linkability	-	-	-	+	-	-
Communicat-ion supported	1:1 & 1:n	1:1	1:1	1:1	1:n	1:1 & 1:n

Crypto modules available, but no protocol.

Delegation of Rights and Anonymous Credentials



- All-or-nothing delegation → Loss of control
- **Privacy:** Trust domain embraces partner and loyalty provider

Agenda

IIG Telematics

I. Privacy in Business Processes as in CRM

II. Delegation of Rights as in CRM

III. DREISAM: Protocols for Delegation of Rights

IV. Evaluation of DREISAM

V. Summary

DREISAM

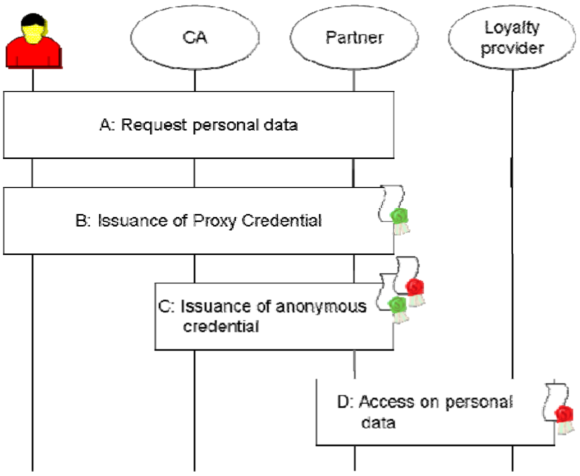
- Enhancing identity management for 1:n by 2 protocols
- DREISAM protocols combines crypto modules

	IBM idemix	SPKI	DREISAM
Accountability	Pseudonym & ZKP	Digitale signature	Pseudonym, ZKP & digitale signature
Purpose-based	Commitment	Proxy Credential	Commitment & Proxy Credential
Case-by-case consent	Anonymous Credential	Proxy Credential	Anonymous & Proxy Credential
Revocation of consent	Dynamic accumulator	Revocation list	Dyn. accumulator & revocation list
Non-linkability	ZKP	-	ZKP
Communcation supported	1:1	1:n	1:1 & 1:n

DREISAM: Protocols

- Delegation by Proxy Credential instead of cryptographic key
- PKI for certification of ownership of rights

1. Delegation



CA

Partner

Loyalty provider

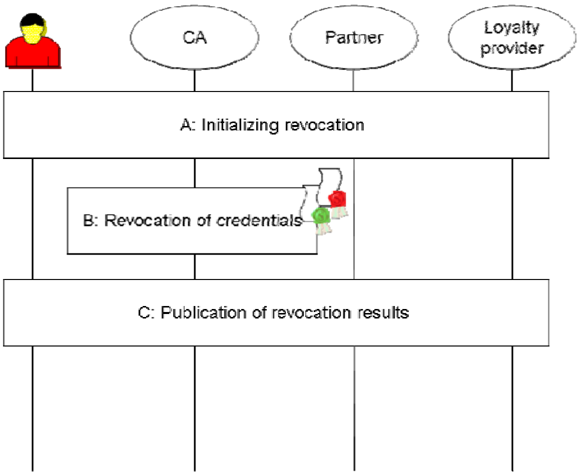
A: Request personal data

B: Issuance of Proxy Credential

C: Issuance of anonymous credential

D: Access on personal data

2. Revocation



CA

Partner

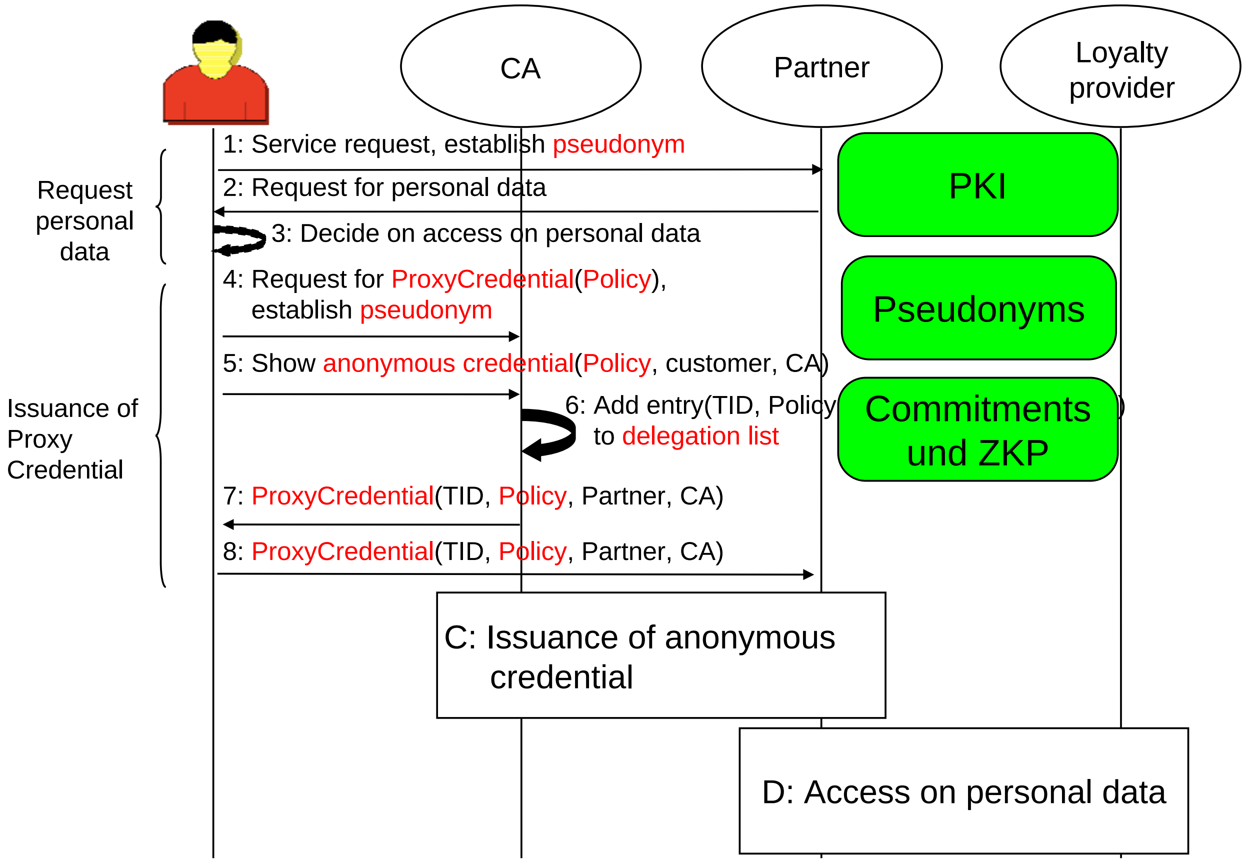
Loyalty provider

A: Initializing revocation

B: Revocation of credentials

C: Publication of revocation results

Delegation: Phases A & B



CA

Partner

Loyalty provider

Request personal data

1: Service request, establish pseudonym

2: Request for personal data

3: Decide on access on personal data

Issuance of Proxy Credential

4: Request for ProxyCredential(Policy), establish pseudonym

5: Show anonymous credential(Policy, customer, CA)

6: Add entry(TID, Policy)
to delegation list

7: ProxyCredential(TID, Policy, Partner, CA)

8: ProxyCredential(TID, Policy, Partner, CA)

PKI

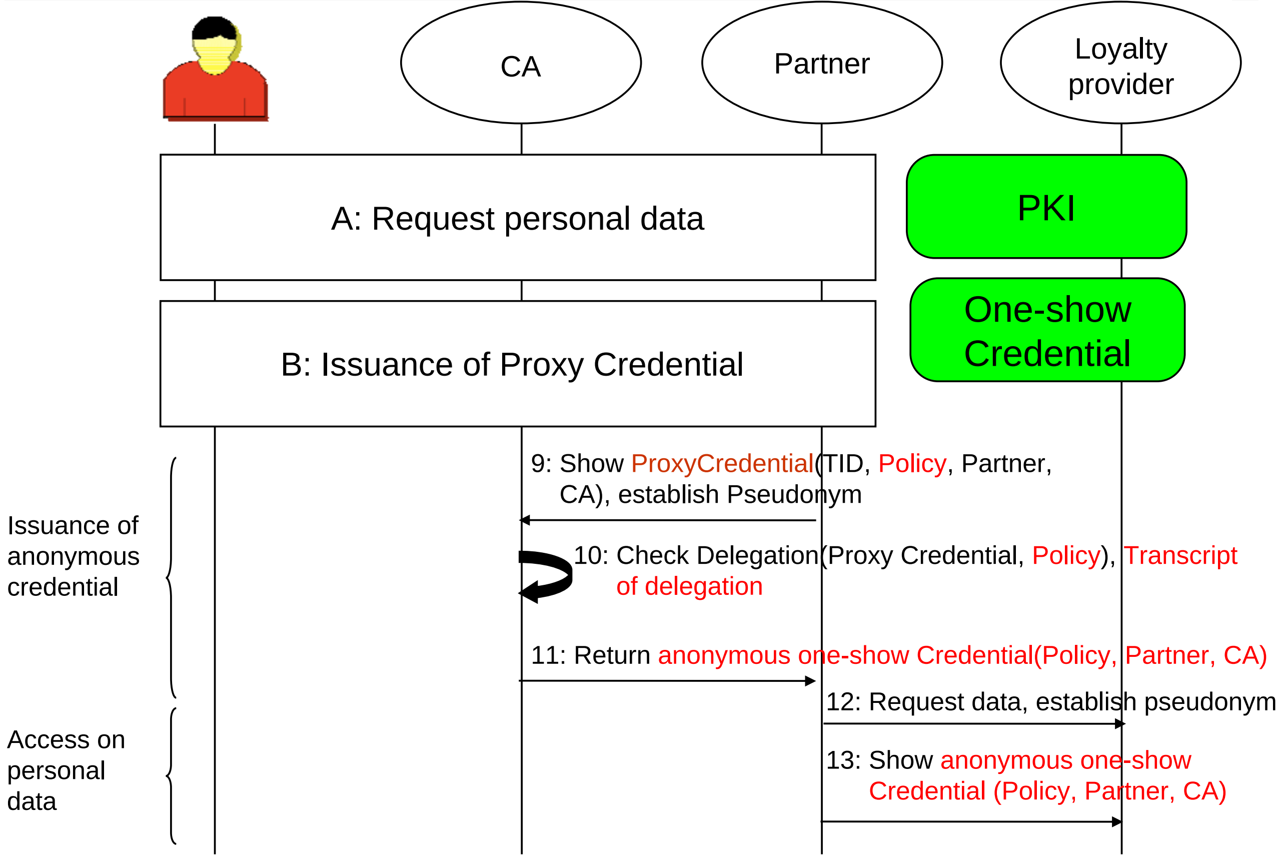
Pseudonyms

Commitments und ZKP

C: Issuance of anonymous credential

D: Access on personal data

Delegation: Phasen C & D



CA

Partner

Loyalty provider

A: Request personal data

B: Issuance of Proxy Credential

PKI

One-show Credential

Issuance of anonymous credential

9: Show ProxyCredential(TID, Policy, Partner, CA), establish Pseudonym

10: Check Delegation(Proxy Credential, Policy), Transcript of delegation

11: Return anonymous one-show Credential(Policy, Partner, CA)

Access on personal data

12: Request data, establish pseudonym

13: Show anonymous one-show Credential (Policy, Partner, CA)

Agenda

I. Privacy in Business Processes as in CRM

II. Delegation of Rights as in CRM

III. DREISAM: Protocols for Delegation of Rights

IV. Evaluation of DREISAM

V. Summary

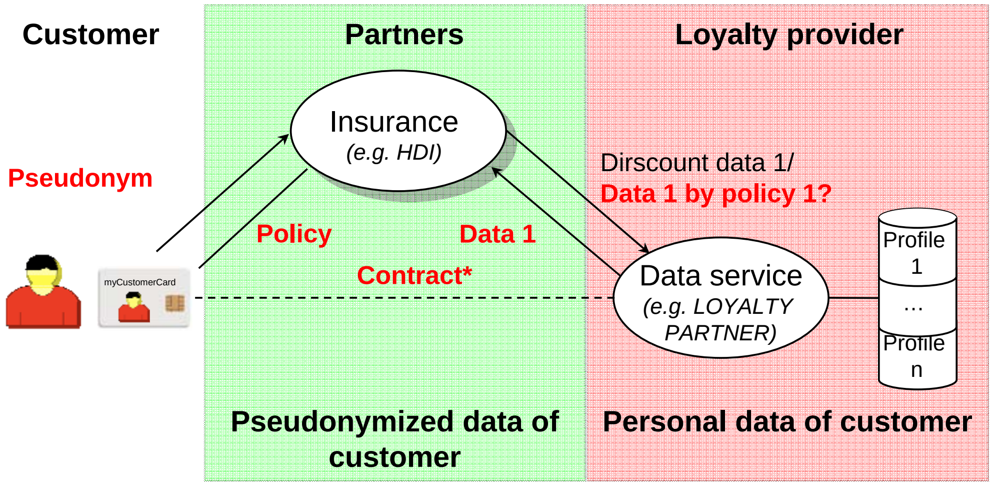
Evaluation: Attacks

Technical threats according to BSI IT-Grundschutz		**Attacks on DREISAM**
• Non-compliance to purpose (G6.2) • Lack of or insufficient data economy (G6.4)	→	Linkability of customer’s transactions
• Exceeding of principle of necessity (G6.4) • Forbidden automated case-by-case decision or access (G6.12)	→	Access for non-agreed purpose
• Violation of data confidentiality (G6.5)	→	Forbidden delegation of credential

Summary

Trust domain has been reduced to loyalty provider

- Protocols for non-linkable delegation of rights and their revocation
- Enhancement of identity management for 1:n communications


Customer
Partners
Loyalty provider
Insurance
(e.g. HDI)
Pseudonym
Dirscount data 1/
Data 1 by policy 1?
Policy
Data 1
Contract*
myCustomerCard
Data service
(e.g. LOYALTY PARTNER)
Profile 1
…
Profile n
Pseudonymized data of customer
Personal data of customer