

## *Lecture 1*

# Introduction

Information & Communication Security  
(WS 2010/11)

Prof. Dr. Kai Rannenber

T-Mobile Chair of Mobile Business & Multilateral Security  
Johann Wolfgang Goethe-Universität Frankfurt a. M.



- The Chair of M-Business and Multilateral Security
- Teaching & Research Agenda
- Organizational Issues
- Introduction into information and communication security
- Outline of this course

## Department “Business Informatics” @ Goethe-University

<p><b>e-Finance</b></p> <p>Prof. Dr. Peter Gomber</p>	<p><b>Media Services</b></p> <p>PD Dr. Hans-Dieter Groffmann</p>	<p><b>Information Systems Engineering</b></p> <p>Prof. Dr. Roland Holten</p>
<p><b>Business Education (associated)</b></p> <p>Prof. Dr. Manfred Horlebein</p>	<p><b>Business Education (associated)</b></p> <p>Prof. Dr. Eveline Wuttke</p>	<p><b>Financial Services</b></p> <p>Prof. Dr. Clemens Jochum</p>
<p><b>Information Systems &amp; Information Management</b></p> <p>Prof. Dr. Wolfgang König</p>	<p><b>Mobile Business &amp; Multilateral Security</b></p> <p>Prof. Dr. Kai Rannenber</p>	<p><b>Wirtschaftsinformatik und Simulation (Informatics)</b></p> <p>Dr. Andreas Lattner</p>

Chair of Business Administration, especially  
Business Informatics, Mobile Business and  
Multilateral Security

T-Mobile Chair of M-Business and Multilateral Security

Grüneburgplatz 1  
Campus Westend, RuW  
2<sup>nd</sup> Floor

Phone: +49 69 798 34701

Fax: +49 69 798 35004

eMail: info@m-chair.net

[www.m-chair.net](http://www.m-chair.net)





Kai Rannenberg



Andreas Albers



Ioannis Krontiris



André Deuker



Christian Kahl



Katja Liesebach



Markus Tschersich



Gökhan Bal



Sascha Koschinat



Christian Weber



Stephan Heim



Marvin Hegen



Lars Wolos



Stefan Weiss



Denis Royer



Stefan Figge



Mike Radmacher



Evgenia Pisko



Lars Janssen



Thomas Leiber



Falk Wagner

**Office:**

Elvira Koch

elvira.koch@m-chair.net

**Office Hours:**

Mo.-Fr. 10:00-14:00



[www.m-chair.net](http://www.m-chair.net)

## Vita of Kai Rannenberg

Einbeck, Göttingen, Eystrup, Wolfsburg, ...

TU Berlin (Dipl.-Inform.)

Uni Freiburg (Dr. rer. pol.)

Dissertation **“Kriterien und Zertifizierung mehrseitiger IT-Sicherheit“**

Standardization at ISO/IEC JTC 1/SC 27 and DIN NI-27

Kolleg **“Sicherheit in der Kommunikationstechnik“**

Gottlieb Daimler- and Karl Benz-Foundation

**Multilateral Security:**

**“Empowering Users, Enabling Applications“, 1993 - 1999**

## Recent history of Kai Rannenberg

1999-09 till 2002-08

Microsoft Research Cambridge UK

[www.research.microsoft.com](http://www.research.microsoft.com)

Responsible for “Personal Security Devices and Privacy Technologies“

2001-10 Call for this chair

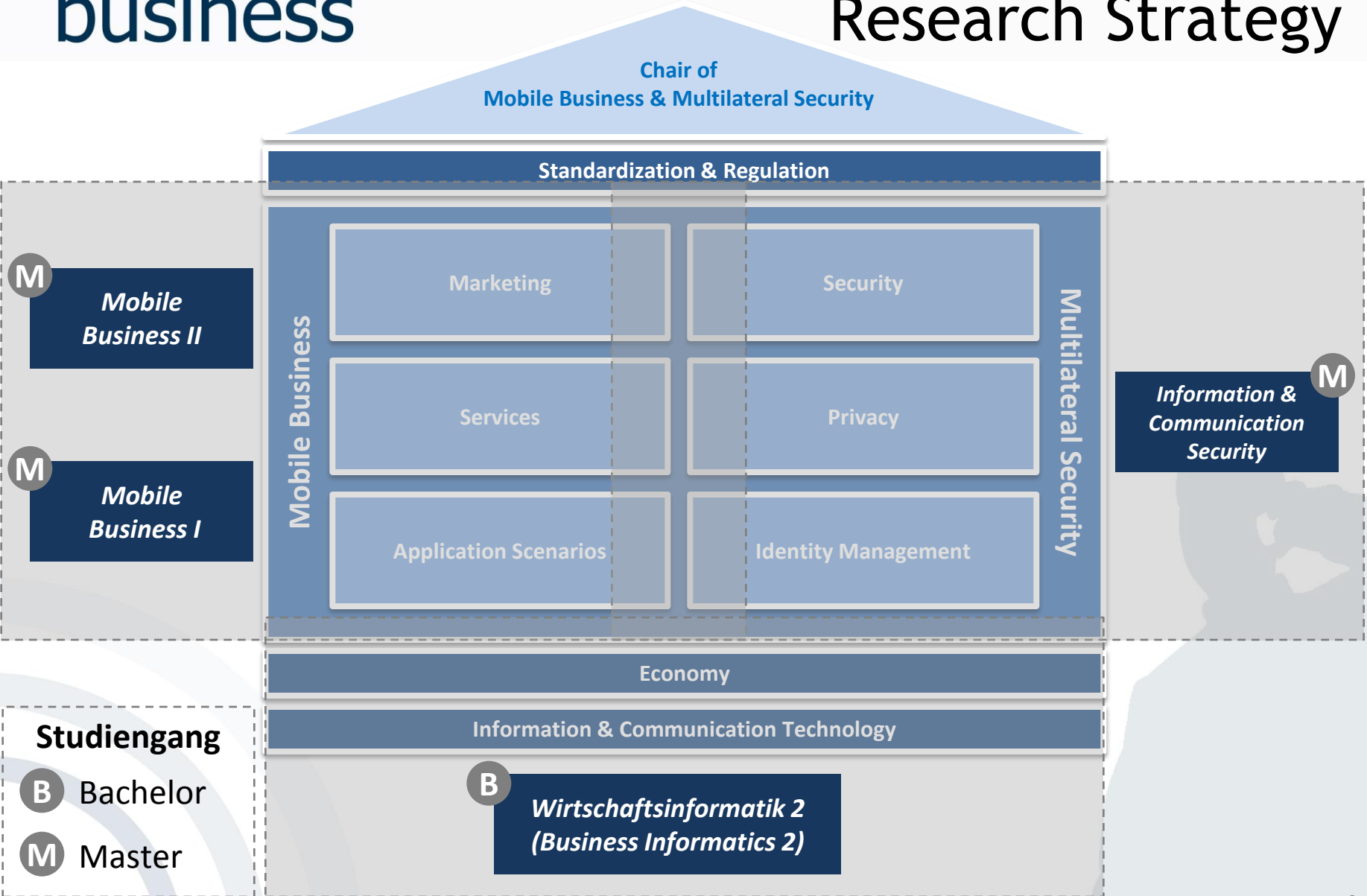
2001-12 till 2002-07 Stand-in for the chair

Since 2002-07 Professor

- The Chair of M-Business and Multilateral Security
- Teaching & Research Agenda
- Organizational Issues
- Introduction into information and communication security
- Outline of this course

	WiSe 2010/2011	SoSe 2011
Bachelor	<p><i>Vorlesung</i> Einführung in Mobile Business (EMB)</p>	<p><i>Vorlesung</i> Wirtschaftsinformatik 2 (PWIN)</p>
Master/Diplom*)	<p><i>Vorlesung</i> Mobile Business I - Technology, Markets, Platforms, and Business Models (MB1)</p> <p>Informations- und Kommunikationssicherheit: Infrastrukturen, Technologien und Geschäftsmodelle (SEC)</p> <p><i>Seminar</i> Managing Privacy and Trust in Social Media Applications</p>	<p><i>Vorlesung</i> Mobile Business II: Platforms, Infrastructures, and Business Models (MB2)</p> <p>Informations- und Kommunikationssicherheit: Infrastrukturen, Technologien und Geschäftsmodelle (SEC)</p> <p>Seminar In Planung</p>

\*) Der Diplomstudiengang läuft aus - nach dem Wintersemester 2010/2011 wird es keine Möglichkeit mehr geben, entsprechende Veranstaltungen zu besuchen und es werden auch keine Klausuren mehr gestellt.



- Usage and trial of “Mobile Services & Devices”
- Experience “M-Business” life
- Experience security issues
- Compare with state of the discussion in research
- Feedback to designer and developers
- Influence future work environments



Experimental Seminar

- **Multilateral Security**
  - Security, Trust and Privacy
  - Mobile Signatures
  - Personal Security Devices
- **Mobile Life, Work, and Business**
  - Location Based Services
  - Mobile Communities
- **M-Infrastructures**
  - Combination, Integration, Innovation
  - Standardisation, Regulation

- The Chair of M-Business and Multilateral Security
- Teaching & Research Agenda
- Organizational Issues
- Introduction into information and communication security
- Outline of this course

## Dr. Ioannis Krontiris

- Grüneburgplatz 1, room 2.220
- Phone: 069 - 798 34668
- ioannis.krontiris@m-chair.net

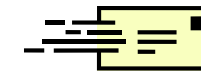


## Dipl.-Inf. Gökhan Bal

- Grüneburgplatz 1, room 2.235
- Phone: 069 - 798 34702
- goekhan.bal@m-chair.net



[twitter.com/mchair](https://twitter.com/mchair)



[sec@m-chair.net](mailto:sec@m-chair.net)

## Dipl.-Ing. (FH) Christian Weber MBA

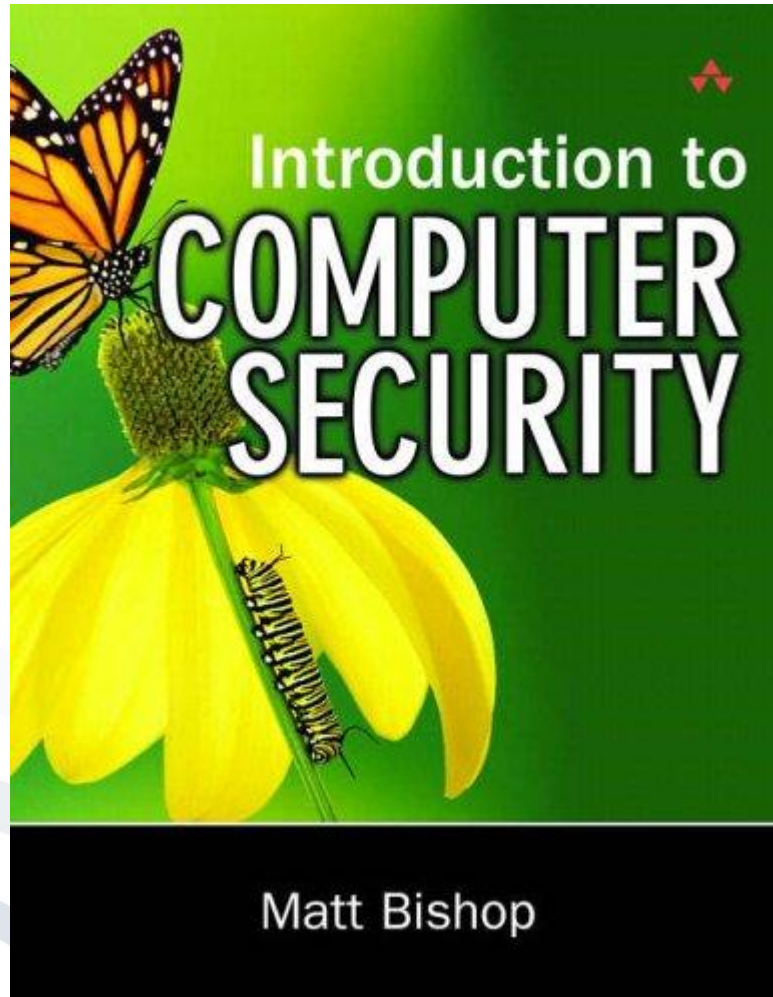
- Grüneburgplatz 1, room 2.233
- Phone: 069 - 798 34704
- christian.weber@m-chair.net



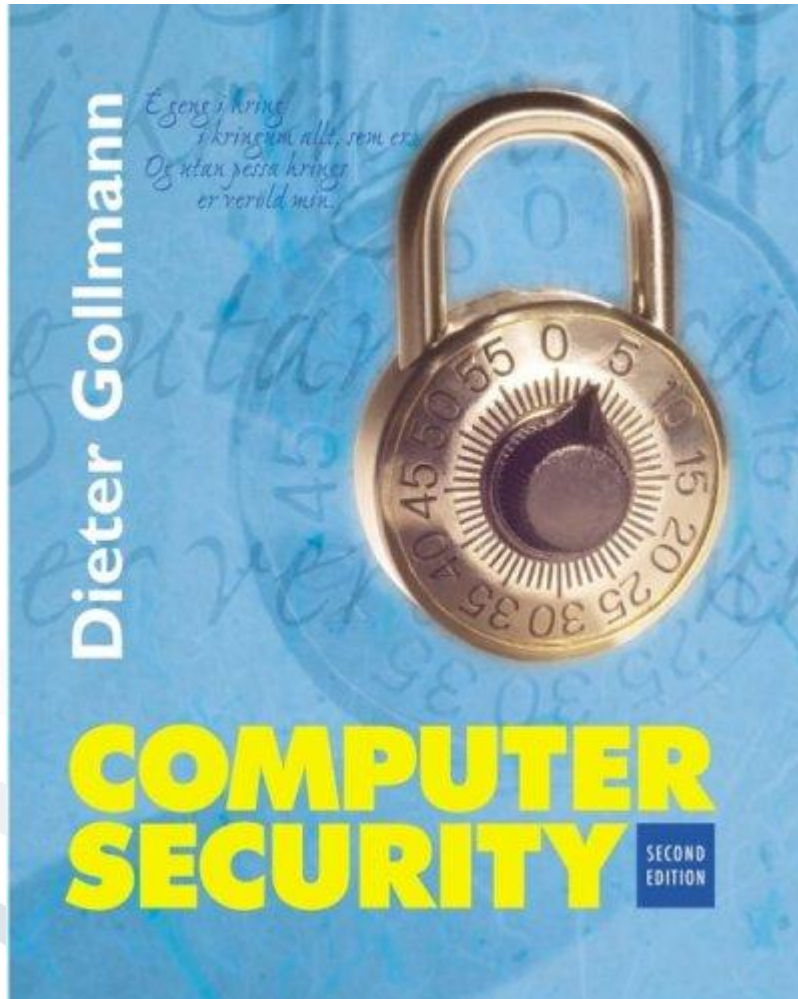
Date not yet fixed but in the  
period between 21.02.2011 and  
11.03.2011

Please keep yourself updated!

(<http://www.wiwi.uni-frankfurt.de/mein-wiwi-studium/pruefungsamt/>)



Matt Bishop:  
Introduction to  
Computer Security  
Addison Wesley  
ISBN: 0-321-24744-2



Dieter Gollmann:  
Computer Security  
John Wiley & Sons  
ISBN: 0-470-86293-9



In German:

Claudia Eckert:

IT-Sicherheit

Oldenbourg

ISBN: 3-486-5827-04

## Please Note:

Electronic library of magazines, access to more than 2000 magazines

<http://www.ub.uni-frankfurt.de/banken.html>

(available only for University members via HRZ account (141.2.XXX.XXX IP-adresses; PC Pool or dial-in via HRZ; see [www.rz.uni-frankfurt.de/campusnetz/vpn/index.html](http://www.rz.uni-frankfurt.de/campusnetz/vpn/index.html))



<http://search.epnet.com/login.asp>

## Online search engines:

<http://citeseer.nj.nec.com/cs>

<http://scholar.google.com>



- The Chair of M-Business and Multilateral Security
- Teaching & Research Agenda
- Organizational Issues
- Introduction into information and communication security
- Outline of this course

c't 14/2004, S. 48: Distributed Denial of Service

Patrick Brauch

## Geld oder Netz!

Kriminelle erpressen Online-Wettbüros mit DDoS-Attacken

Es sieht ganz so aus, als habe das organisierte Verbrechen ein neues Gesicht. Motto: „Zahlt oder wir machen den Laden dicht“.

Hi! Wir werden bald einen Angriff gegen Eure Seite starten. Unser Team braucht 15 000 US-Dollar ein angemessener Betrag für Euch wäre. Wenn Ihr nicht Böses tun, es ist nur unsere Arbeit. Viel Glück!

(Distributed) „Denial of Service“-Attacks on e-auctioneers/broker/betting office

### Denial of Service-Attacke legt Bluewin lahm

Bluewin-Portal heute morgen teilweise unerreikbaar.

Beim Bluewin-Portal [www.bluewin.ch](http://www.bluewin.ch) sowie einigen andere Bluewin-Sites gab es anscheinend heute zumindest zeitweise Probleme. Einer unserer Leser informierte uns, dass er schon heute morgen um halb zwei Uhr Bluewin.ch nicht erreichen konnte. Bei einem ersten Test kurz vor 10 Uhr kamen auch wir noch nicht auf die Site, kurz darauf war Bluewin wieder problemlos erreichbar.

Swisscom-Sprecher Christian Neuhaus bestätigte gegenüber inside-it.ch, dass, wie wir gerüchteweise erfahren hatten, eine Denial-of-Service-Attacke der Grund für die Ausfälle war. (Bei einer DoS-Attacke versuchen Angreifer eine Website mit automatisierten Zugriffen zu überfluten, so dass die Server die Last nicht mehr bewältigen können und blockiert werden.) Für Bluewin-ADSL-Kunden gemäss Neuhaus nur eine Stunde lang nicht erreichbar. Ich weiss allerdings nicht, wie lange nicht-Bluewin-Zugriff hatten.

APBnews.com  
YOU HAVE THE RIGHT TO KNOW

Crime, Justice, Safety:  
 ▶ NEWSCENTER  
 ▶ SAFETY CENTER  
 ▶ CRIME SOLVERS  
 ▶ VIDEO CENTER  
 ▶ CRIM  
 ▶ CRIM  
 ▶ RESO  
 ▶ MEDI

Breaking News | Missing | Internet Crime | Can You Believe Th

> E-MAIL THIS STORY TO A FRIEND | E-MAIL THE EDITOR | TALK ABOUT IT

U.S. | WORLD

**FOX NEWS.COM**

## Hack Attack Shuts Down Online Auction Site

BidBay Offers Reward as FBI Investigates Denial of Service

NATIONAL FRONT

## Report: Blackmailer Reveals Stolen Internet Credit Card Data

Update

CNET | News | Hardware | Downloads | Builder | Games | Jobs | Auctions | Price

„Sale of customer data“

cnet NEWS.COM TECH NEWS FIRST

## Failed dot-coms may be selling your private information

By [Greg Sandoval](#)  
Staff Writer, CNET News.com

FOR SALE  
**Toysmart.com**  
 Toysmart.com, an Internet retailer of toys, is selling its core of the art. Customers who register may purchase all or part of the tangible or intangible assets located in Hardware, Revenue and Bank Account. (including:  
 - By inventory  
 - Database Center  
 - Office and local facility  
 - Store fixtures, office and warehouse furniture and equipment  
 - Internet advertisement  
 - Intangibles, i.e. URL name, database, customer lists, customer plans, website content, software intellectual property

For additional information regarding the purchase of any or all of the assets, visit the website at: [www.toysmart.com/buy](http://www.toysmart.com/buy) or contact Stephen Gray, Recovery Group (67) 482-4342; Fax: (67) 482-9904.

**Intangibles, i.e. URL name, databases, customer lists,**

cnet NEWS.COM NEWS OF CHANGE

News.com Mobile for PDA or phone

Login:  E-mail address  Password

My News | Readers' Choice

Front Door | Business Tech | Cutting Edge | Access | Threats | Media 2.0 | Markets | Digital Life

## Credit card breach exposes 40 million accounts

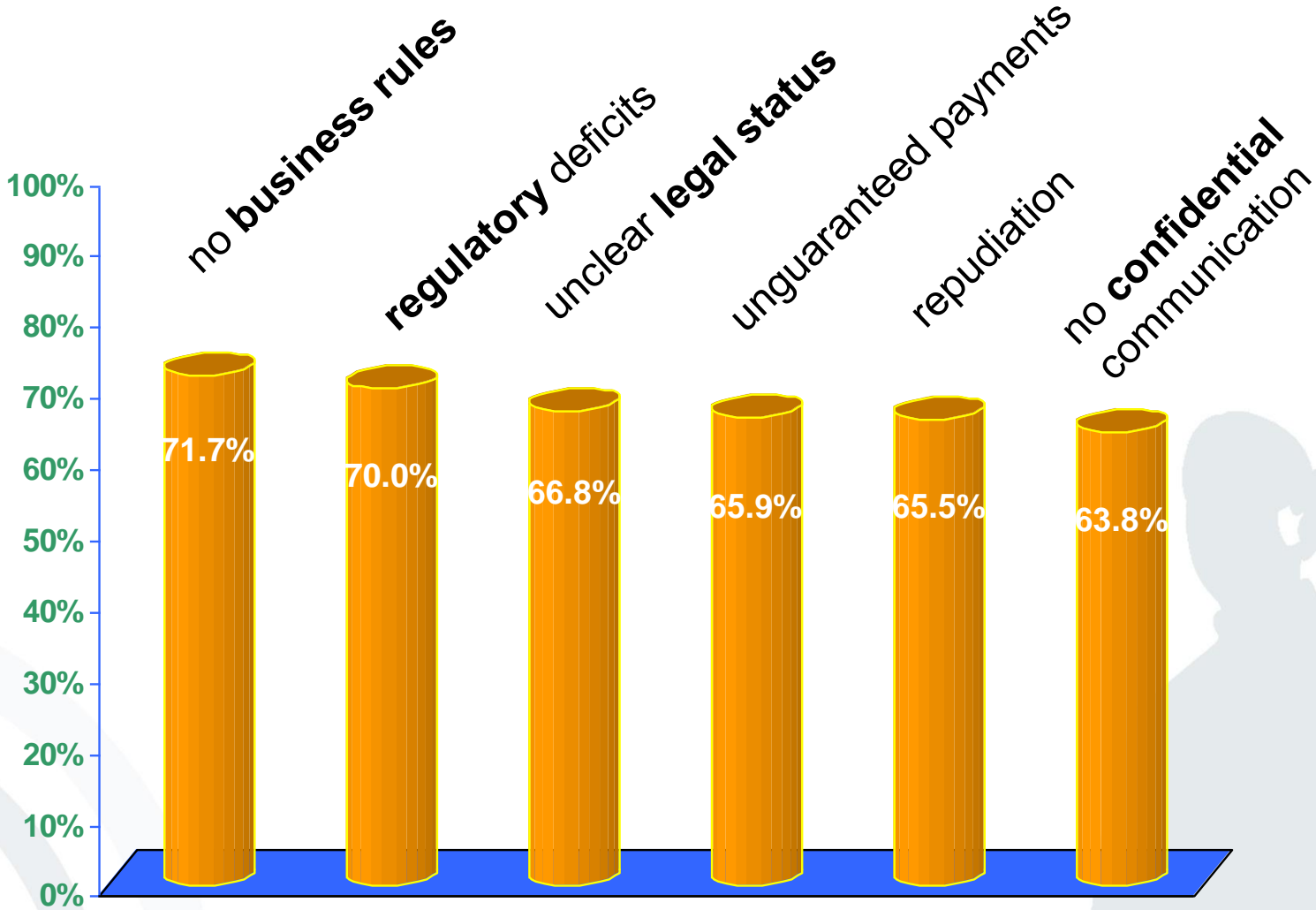
## Provider

- no payment - debtor cannot be captured
- wrong or fake orders
- copyright violations
- www attacks
- internal server intrusion
- ...

## Consumer

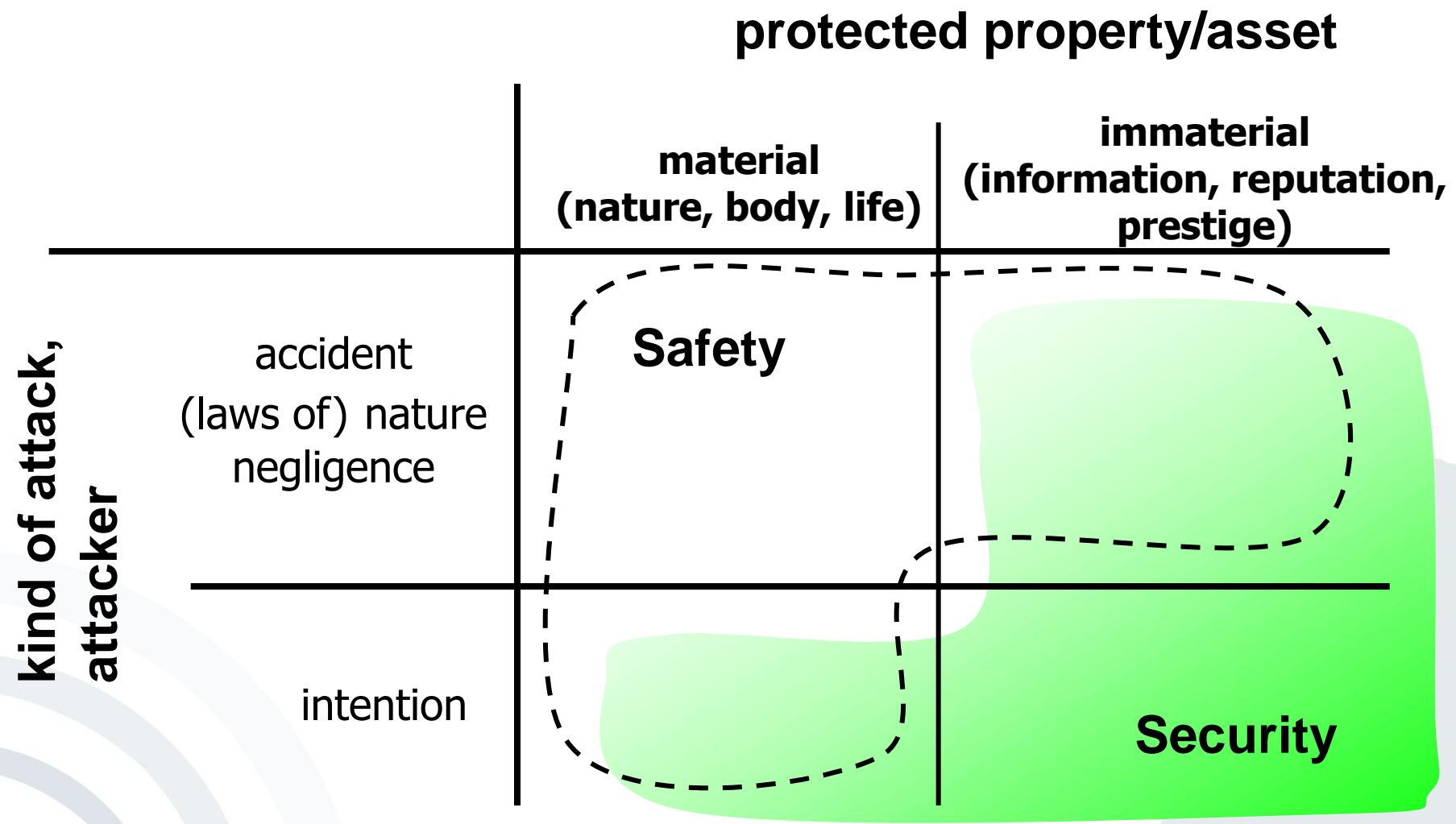
- unwanted deliveries (false, not ordered, ...)
- unauthorized / unexpected direct debt of money, e.g. from a credit card account
- unwanted advertising mail (“spamming”)
- transparent consumers
- ...

# E-Commerce Requires Security



Source: Electronic Commerce Enquête, Universität Freiburg, 1998  
(32 options + free text for choice, 6 options with highest agreement listed)

# Security vs. Safety



## A very human discrepancy

- **Privacy**  
Protect the own sphere and the own values
- **Binding**  
Gain trust (of partners), transfer values

## Kind of technical arrangement

- **Confidentiality**  
Information delivery just to whom it is intended
- **Integrity**  
no faking of information
- **Availability**  
no system failures / no loss of data
- **Accountability**  
actions are always accountable to responsible parties

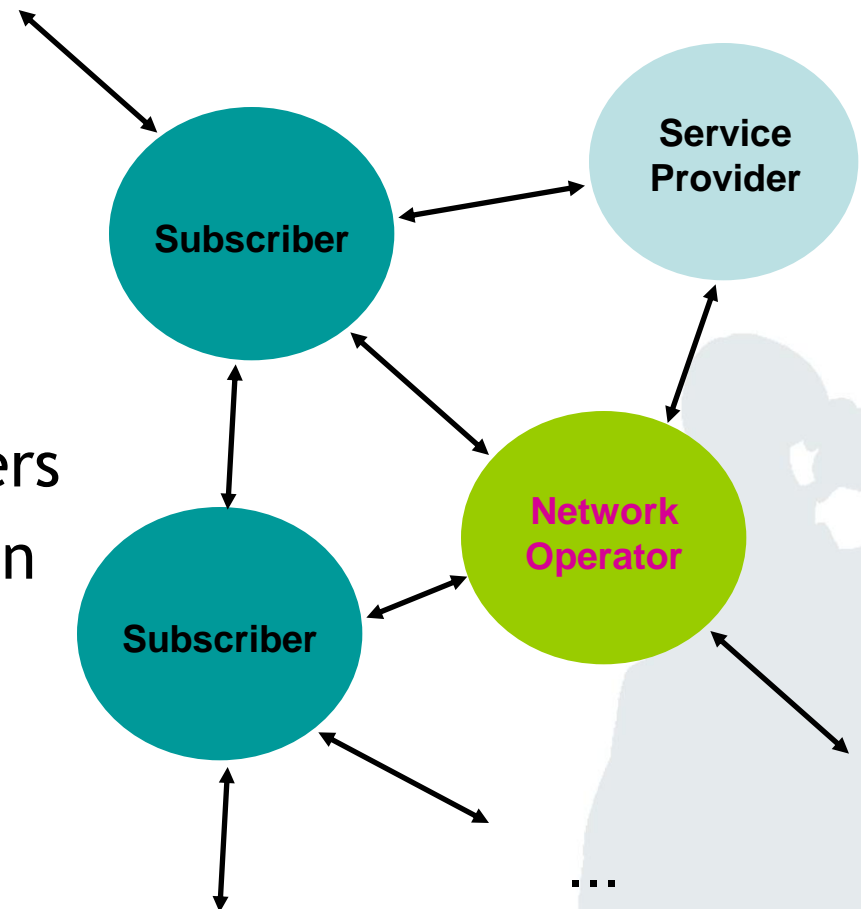
A **combination** of technical, organizational and legal methods is necessary.

- *Unauthorized earning of information*, that means loss of **confidentiality**: patient data (for example information of physical examinations, diagnoses or therapy attempts, but also content of meetings on patient cases which is stored in databases) shall not be accessible to unauthorized persons (e.g. other patients, hospital employees or employees of the network operator whose (mobile) network is used to transfer the data from hospital to hospital).
- *Unauthorized modification* of information, that means loss of **integrity**: Unauthorized and unobserved data modifications (e.g. a prescription, a medicament ordering or a dosage instruction) may lead to life-threatening consequences.

- ***Unauthorized impair of functionality***, that means loss of **availability**: If the medical history is accessible solely via one network and this network has a breakdown when patient data has to be queried it may be life-threatening for the patient.
- ***Incorrect non-committalness***, that means loss of **accountability**: If the persons liable for procedures in IT-systems (e.g. for the delivery of diagnoses, therapy instructions or billings) cannot be identified unwarrantable actions may occur. Moreover, the consequences of a mistake may be worse for the injured party since there is no information on whom to ask for compensation.

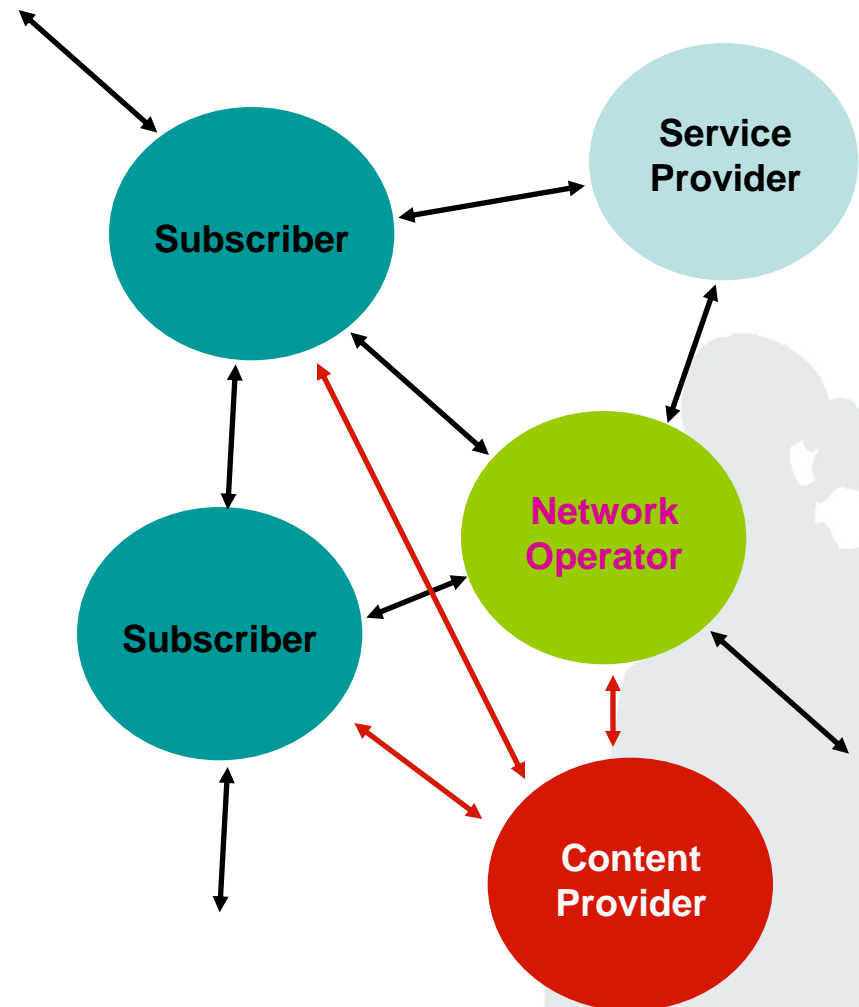
Different Parties  
with  
different Interests

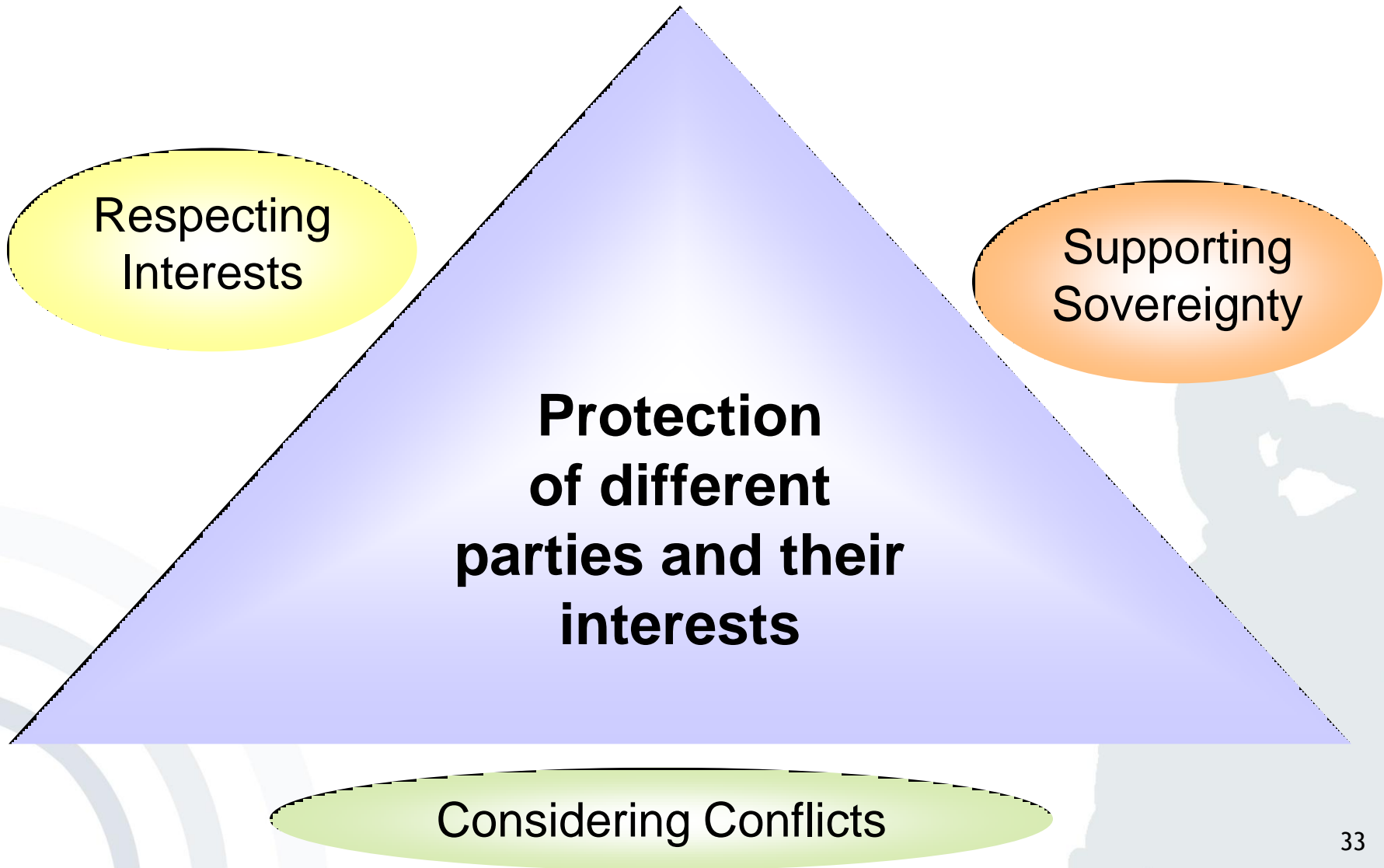
- Customers/Merchants
- Communication partners
- Citizens/Administration



... in a world of consortia

- more partners
- more complex relations





## Respecting Interests

- Parties can define their own **interests**.
- Conflicts can be **recognized** and **negotiated**.
- Negotiated **results** can be **reliably enforced**.

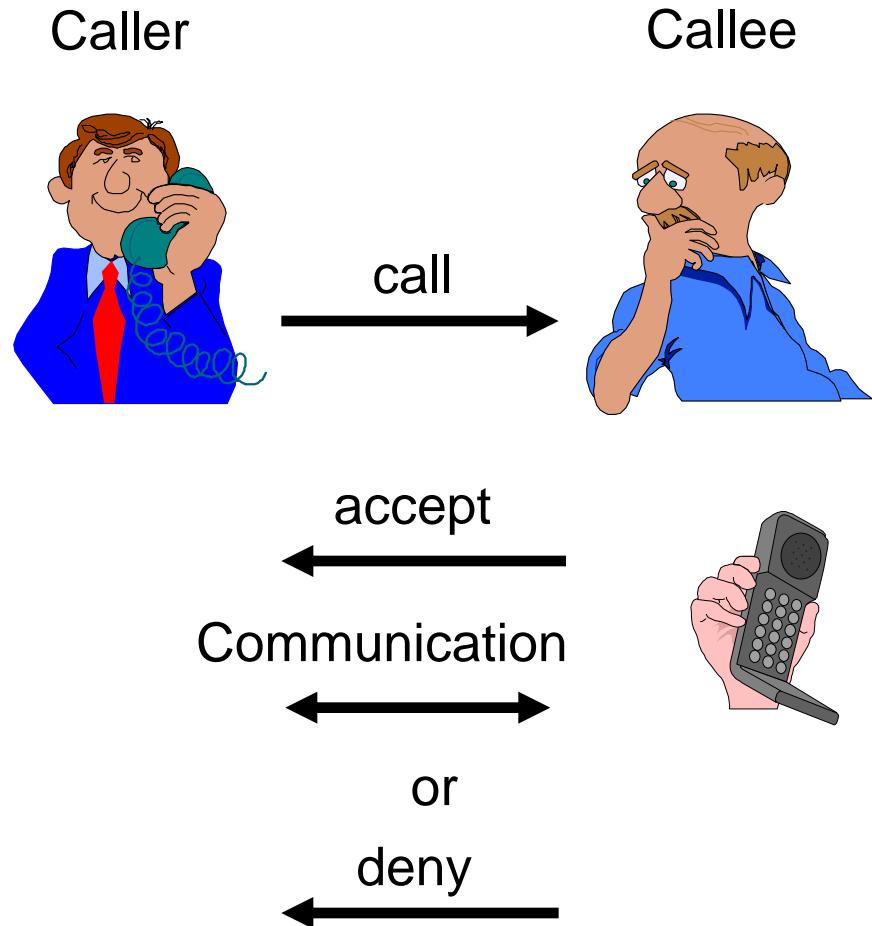
## Supporting Sovereignty

- Requiring each party to **only minimally trust** in the honesty of others
- Requiring **only minimal or no trust** in technology of others

Protection of **different parties** and their **interests**

## The Challenge

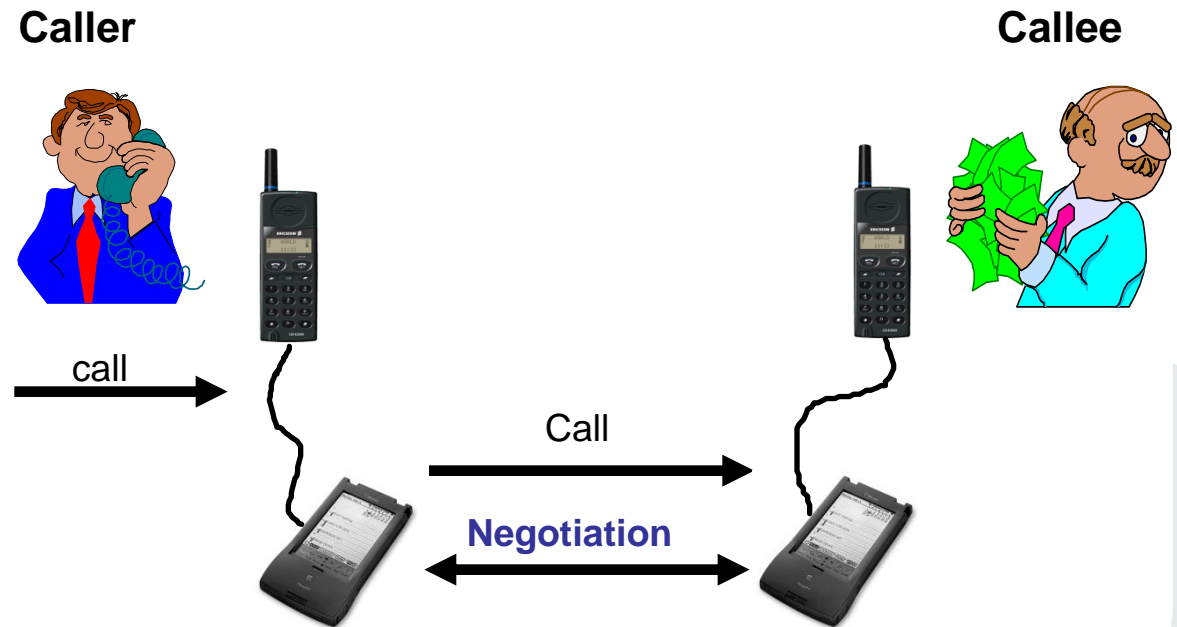
- Increased reachability due to new communication services
- Annoying calls
- Shortage of time
- Caller-ID conflict



→ Reachability Management (RM)

## The Features

- Automatic call filtering under user control
- Privacy protection for both caller and callee
- Choice of different ways to express urgency
- Choice of different reactions for different situations



# Topics of Negotiation


- Urgency of the call
- Extent of identification
- Security requirements
  - authentication
  - confidentiality
  - non-repudiation

**RMS Call**

**Who** Rannenberg, Katrin

◆ **My ID:** none

◆ **Subject:** Meeting?

 .....

**Urgency:**

Normal     High     Emergency

**Security Settings:** [View Details](#)

◆ **Confidentiality:** Important

◆ **Authentication:** Don't care

[Cancel](#)    [Call](#)

# Why should your call go through?

Statement of urgency

“It is really urgent!”

Specification of a function

“I am your boss!”

Specification of a subject

“Let’s have a party tonight.”

Presentation of a voucher

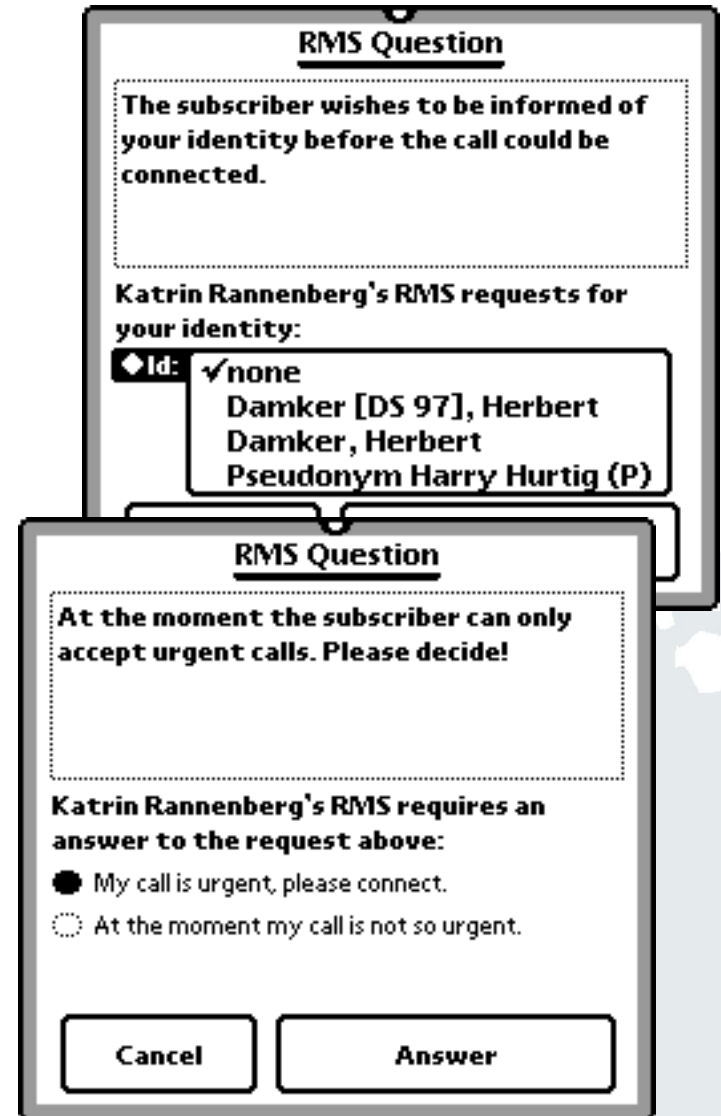
“I welcome you calling back.”

Provision of a reference

“My friends are your friends!”

Offering a surety

“Satisfaction guaranteed  
or this money is yours!”



**RMS Question**

The subscriber wishes to be informed of your identity before the call could be connected.

Katrin Rannenberg's RMS requests for your identity:

◆ Id:  none  
Damker [DS 97], Herbert  
Damker, Herbert  
Pseudonym Harry Hurtig (P)

**RMS Question**

At the moment the subscriber can only accept urgent calls. Please decide!

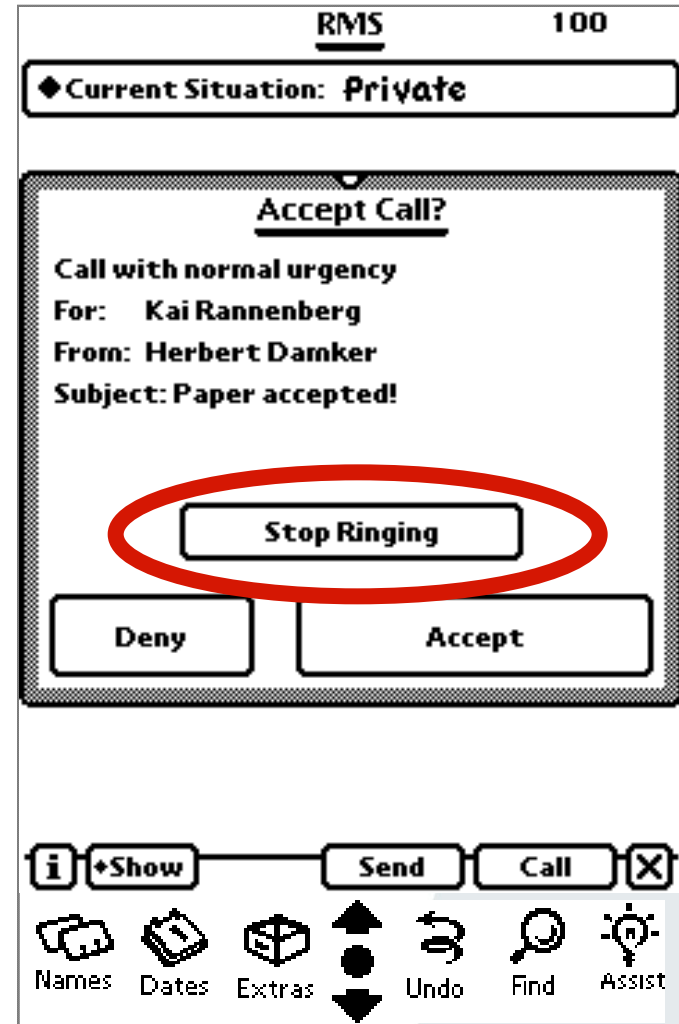
Katrin Rannenberg's RMS requires an answer to the request above:

My call is urgent, please connect.  
 At the moment my call is not so urgent.

Cancel Answer

# RMS accepted call (Callee display)

- Bell is ringing!
- Callee notified
- Callee can still decide to accept or deny the call



# RMS denied call (Caller display)

- Call not connected
- Caller gets information (configured by callee)
- Caller can leave a message or request a call back

**RMS: Call denied**

Unfortunately the subscriber can not accept the call at the moment.

**Leave with Katrin Rannenber:**

Text message  
 Request for callback (with voucher)  
 No message

## Situations

Set of rules how to deal with an incoming call

## Rules

Combination of features

Users can reconfigure initial rules and situations as they like.

The image shows two overlapping screenshots of a configuration interface. The top screenshot is titled "Define Situation 'Meeting'" and contains a list of actions with checkboxes and arrows. The bottom screenshot is titled "Define Rule" and contains a list of conditions and actions with radio buttons and checkboxes.

**Define Situation 'Meeting'**

- Emergency -> connect
- Callback voucher -> connect
- Caller in group Colleagues -> let caller decide  
Text: 'Request decision'
- Else -> deny  
Text: 'Not available'

**Define Rule**

In the situation 'Meeting'  
my RMS should for ...

- all calls
- business calls
- calls of class:
- private calls

... and ...

- no caller ID
- caller want to be anonymous
- callback voucher
- caller in group:
- caller is:
- every caller
- Emergency

... do the following:

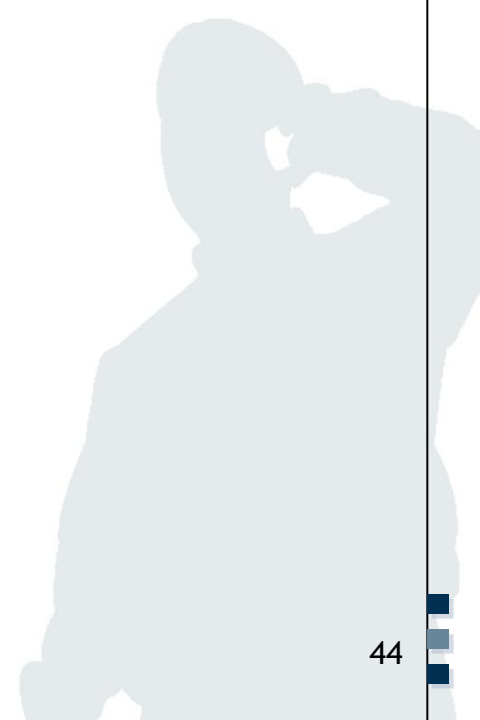
- connect
- deny
- divert to:
- require surety of \$10 and connect
- require subject and connect
- let caller decide
- require caller ID

Text to send: -

Cancel OK

# Reachability Management and Multilateral Security

????????



## Respecting Interests

- Parties can define their own **interests**.
- Conflicts can be **recognized and negotiated**.
- Negotiated **results** can be **reliably enforced**.

## Supporting Sovereignty

- Requiring each party to **only minimally trust** in the honesty of others
- Requiring **only minimal or no trust in technology** of others

Protection of **different parties** and their **interests**

- Protection of **callers and callees**
- **Balance** of security requirements
- Processing and storage of **sensitive data** in a **personal environment**
- Assessment of the concept in a simulation study in the Heidelberg health service

## Simulation study in Heidelberg health service

- **Fictitious**, but **realistic** cases
- **Real users**: ca 40 doctors, nurses, admin people, etc.
- 1 week “**Playtime**”
- 18 months **preparation and analysis**: workflow analysis usability tests, script writing, attack planning



- Reachability manager
- Negotiating security
- Identities and pseudonyms
- Signing device
- Medical information (patient records and knowledge base)
- Hospital communication

## Overall results

- High benefit for everyday tasks
- Increasing awareness of security
- Integration of asynchronous messages very useful
- Manual filtering of calls often used

## User demands

- Smaller device - RMS functionality in mobile phone
- Integration of full-flavour email
- Authentication also during a call

## Many more design hints



- Complexity was **accepted** as **benefit** was **seen**, e.g. **Situations** in Reachability Management vs. **paggers**.
- Users **coped** with complexity in **different** ways:
  - **Conservatives**: Never changed the given rule sets
  - **Reformers**: Added the odd situation or rule
  - **Power Users**: Designed large sets of situations and rules, even if they never used all of them later.
- **Most** ended up with **3-5 levels**,
  - but with **different** ones, and
  - they came by **different routes**.
- **Experimenting** was **encouraged** by the nature of the control: “It’s just a call, not a top secret data base”.

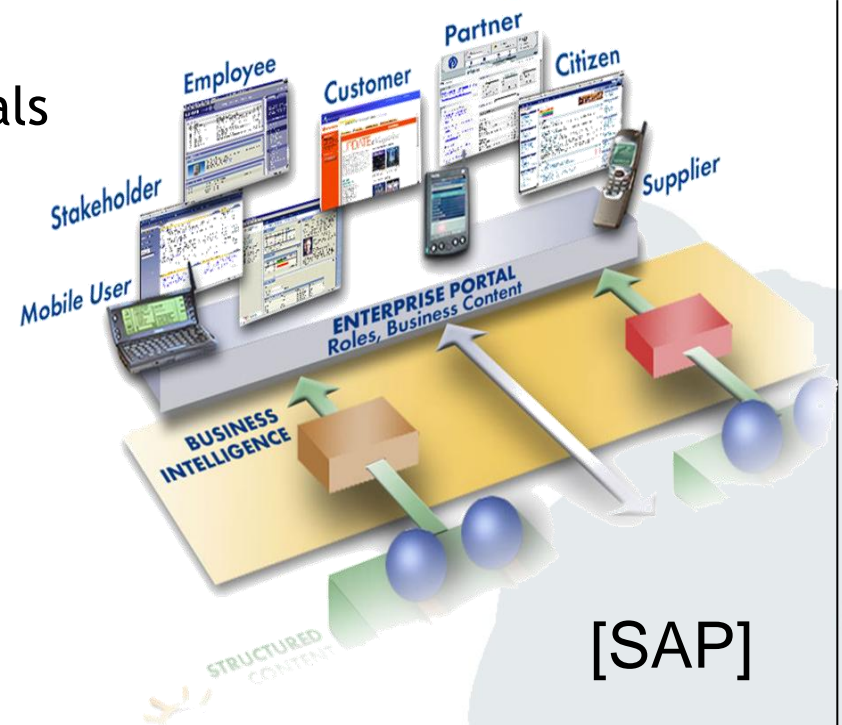
Just a small example, **but**

- Integration of voice and data services

Think this within

- Enterprise communication portals
- Mobile access
- Shared calendars

New dimensions for negotiation



- The Chair of M-Business and Multilateral Security
- Teaching & Research Agenda
- Organizational Issues
- Introduction into information and communication security
- Outline of this course

## *Lectures and Exercises (2010)*

20.10.2010	Lecture	Introduction
26.10.2010	Lecture	Authentication
27.10.2010	Lecture	Access Control
03.11.2010	Guest Lecture	Jens Eichler (Dimension Data)
09.11.2010	Lecture	Cryptography I
10.11.2010	Lecture	Cryptography II
17.11.2010	Exercise	Authentication
23.11.2010	Lecture	Electronic Signatures
24.11.2010	Lecture	Identity Management I
01.12.2010	Exercise	Access Control
07.12.2010	Exercise	Cryptography
08.12.2010	Lecture	Identity Management II
15.12.2010	Lecture	Computer System Security
21.12.2010	Guest Lecture	Udo Helmbrecht (ENISA)
22.12.2010	Lecture	Network Security I

## *Lectures and Exercises (2011)*

12.01.2011	Lecture	Network Security II
18.01.2011	Guest Lecture	Stefan Weiss (KPMG)
19.01.2011	Lecture	Security Management
26.01.2011	Lecture	Security Engineering
01.02.2011	Lecture	Evaluation Criteria
02.02.2011	Guest Lecture	Jürgen Kühn (Trivadis GmbH)
09.02.2011	Guest Lecture	Martin Reichenbach (Commerzbank AG)
15.02.2011	Lecture	Aktuelle Forschungsthemen
16.02.2011	Lecture	Vertiefung ausgesuchter Inhalte