

Lecture 1:

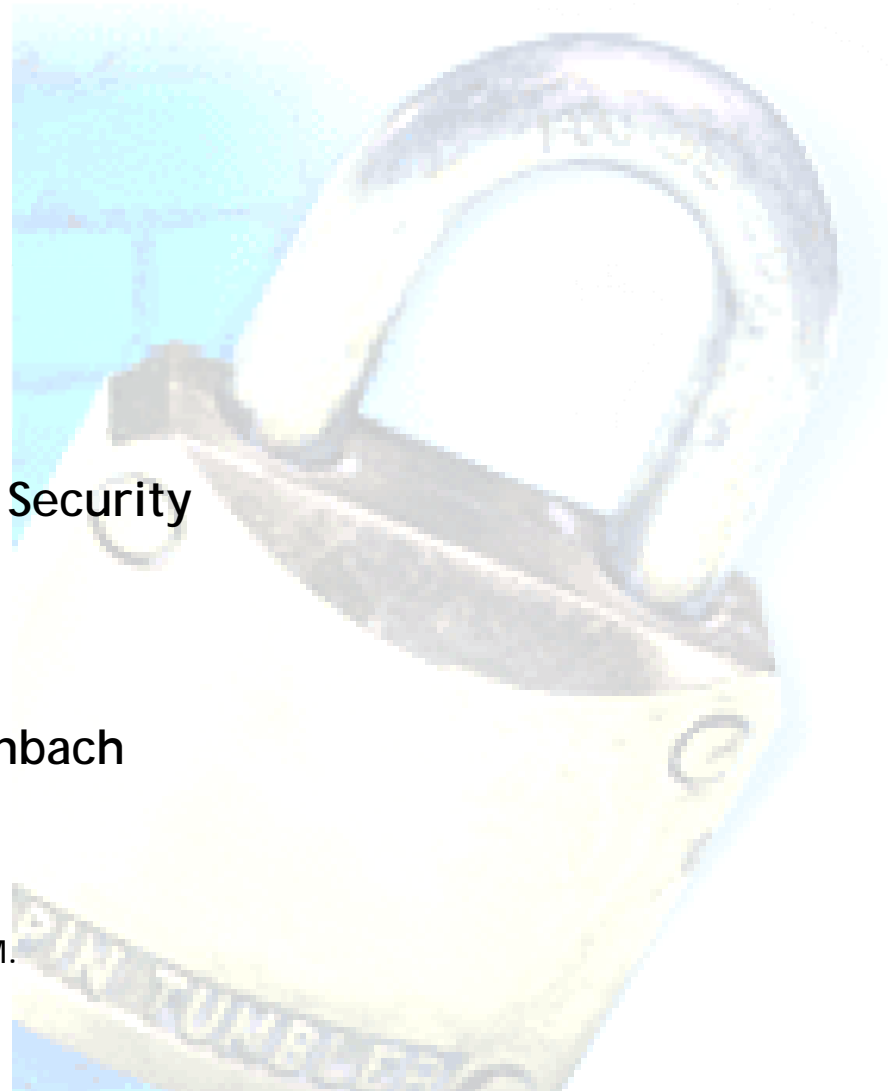
Introduction

Information and Communications Security
(WS2008)

Prof. Dr. Kai Rannenberg

Guest Lecturer Dr. Martin Reichenbach

T-Mobile Chair for
Mobile Business & Multilateral Security
Johann Wolfgang Goethe University Frankfurt a. M.
www.whatismobile.de



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

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

T-Mobile Chair of M-Business and Multilateral Security

Grüneburgplatz 1

60629 Frankfurt am Main

Phone: +49 69 798 25301

eMail: info@m-chair.net

The Chair moved to the new Campus!
Please watch for latest news at:
www.m-chair.net



Kai Rannenberg



Andreas Albers



Mike Radmacher



Denis Royer



Tobias Scherner



Jan Zibuschka



André Deuker



Christian Kahl



Katja Liesebach



Stefan Weiss



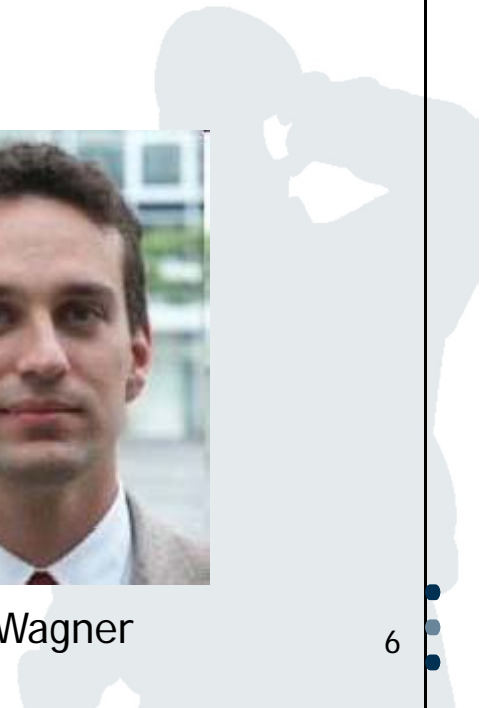
Evgenia Pisko



Thomas Leiber



Falk Wagner



Office:

Elvira Koch
elvira.koch@m-lehrstuhl.de

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

www.m-chair.net





Vita I

Freiburg, Furtwangen, Dresden, Cambridge, ...
Uni Freiburg (Dr. rer. pol.)

Dissertation "Individuelle Risikohandhabung Elektronischer
Zahlungssysteme"

Seit 2002:

Informationssicherheitsbeauftragter der Commerzbank AG

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

	SS 08	WS 08/09	SS 09
Advanced phase			<i>Lecture</i> "Business Informatics II"
Specialisation phase	<i>Lecture</i> "M-Business II" & "Information and Communications Security"	<i>Lecture</i> "M-Business I" & "Information and Communications Security"	<i>Lectures</i> "M-Business II"
	<i>Seminar</i> "Social Communities als Marketingplattform - Merkmale, Transparenz und Potentiale"	<i>Seminar</i> Mobilkommunikation und Identitätsmanagement in Communities(Diplom)	<i>Seminar</i> Topic not yet defined

- 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



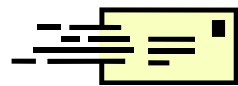
Experimental Seminar

- **Multilateral Security**
 - Security and Privacy
 - Mobile Signatures
 - Personal Security Devices
- **Mobile Life, Work, and Business**
 - Portals for Mobile Communication
 - Location Based Services
 - M-Banking/M-Brokerage
- **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

Dipl.-Kfm. André Deuker

- Gräfstr. 78, Room 401
- Phone: 069 - 798 25315
- andre.deuker@m-chair.net



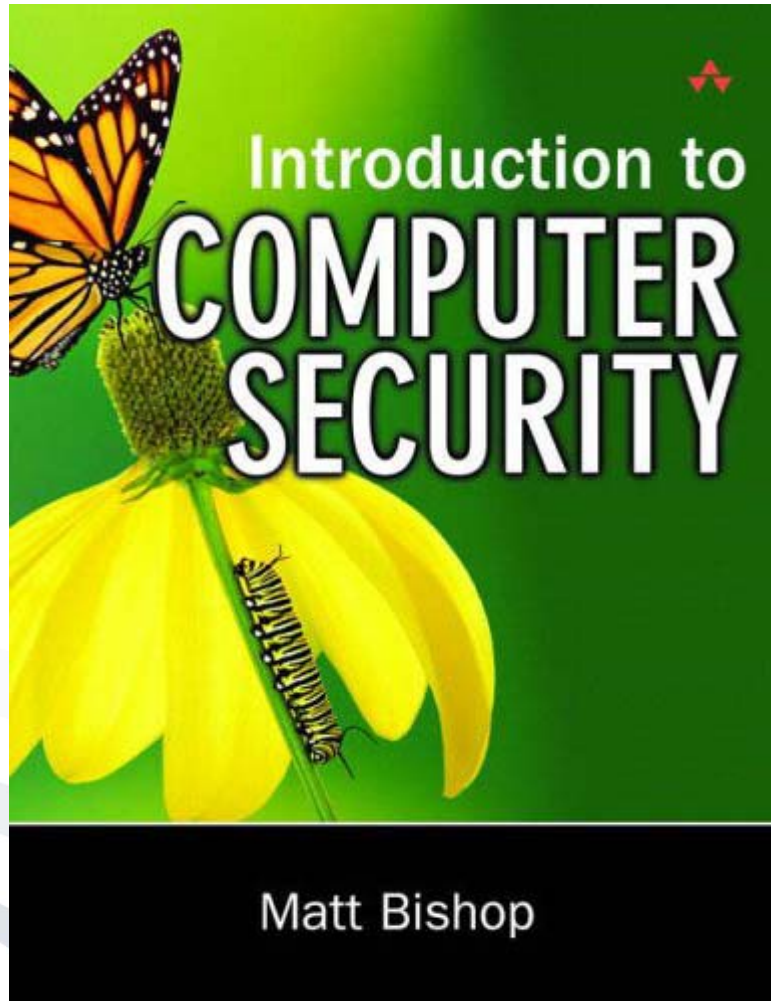
sec@m-chair.net

Date not yet fixed, somewhere after
Feb 10, 2009.

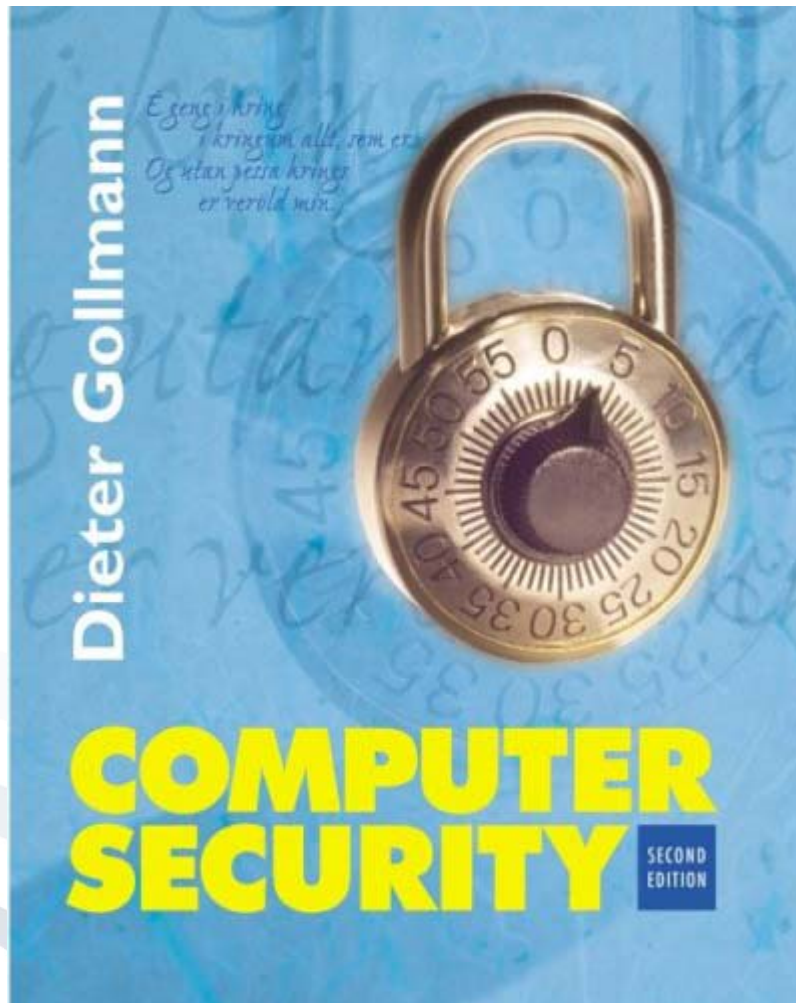
So stay tuned ...

Please keep yourself updated!

(<http://www.wiwi.uni.frankfurt.de/612.0.html>)



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: 3-486-20000-3

Please Note:

Electronic library of magazines, access to more than 2000 magazines

www.seb.uni-frankfurt.de/torezs.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://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

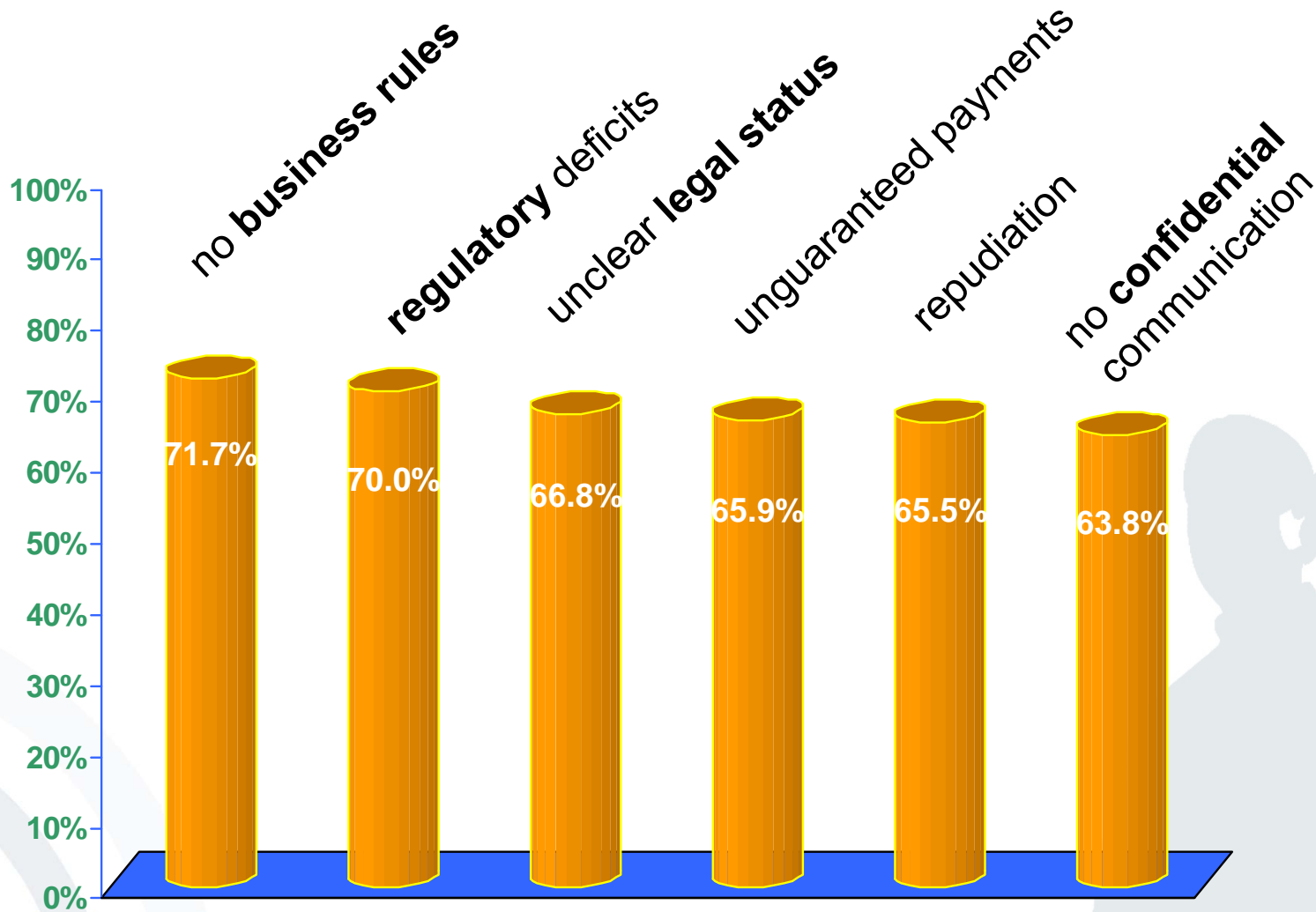
Provider

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

Consumer

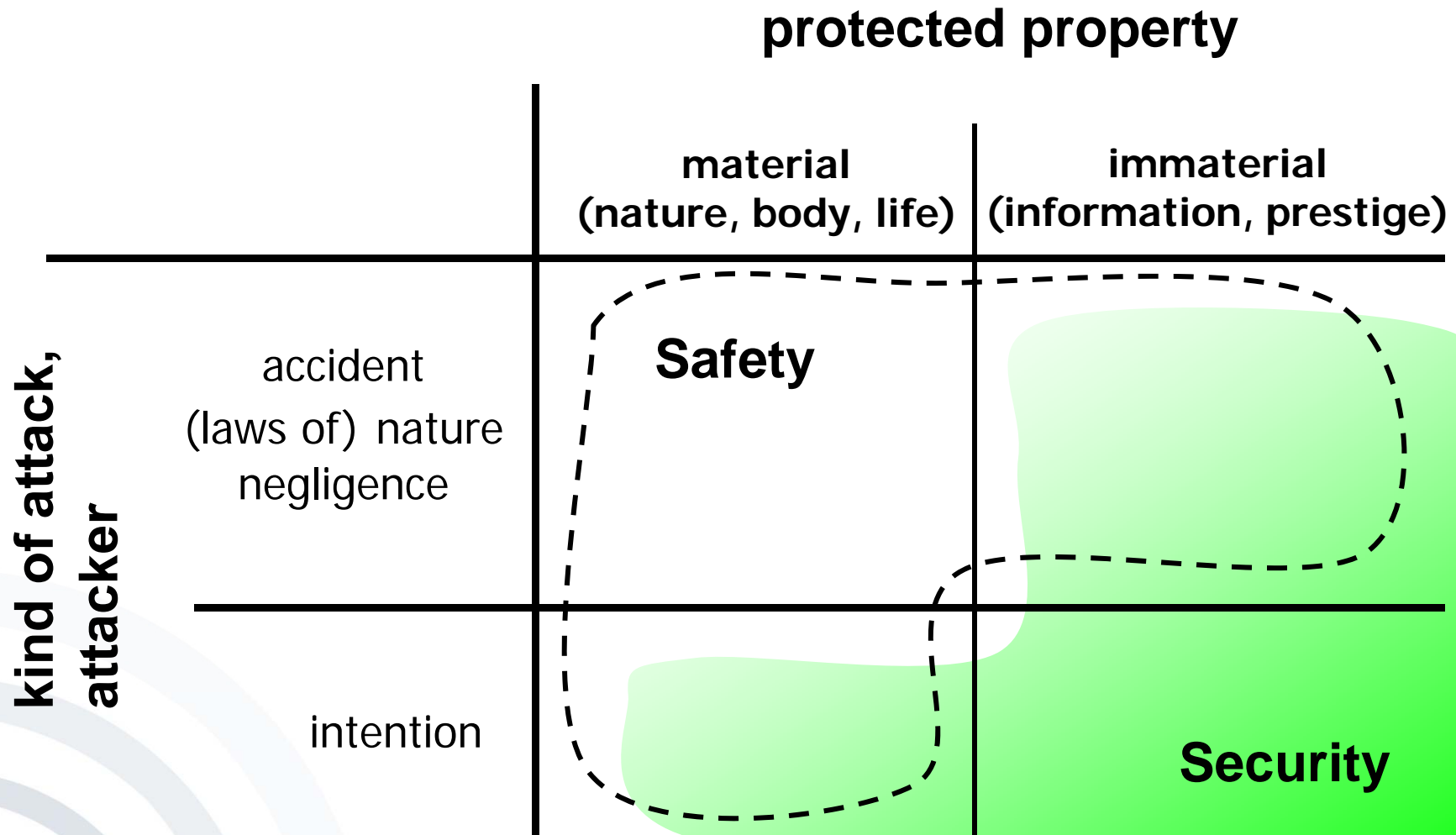
- unwanted deliveries (false, not ordered, ...)
- unauthorized / unexpected direct debt of money, e.g. from a credit card account
- unwanted advertising mail ("spamming")
- transparent consumers
- ...

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

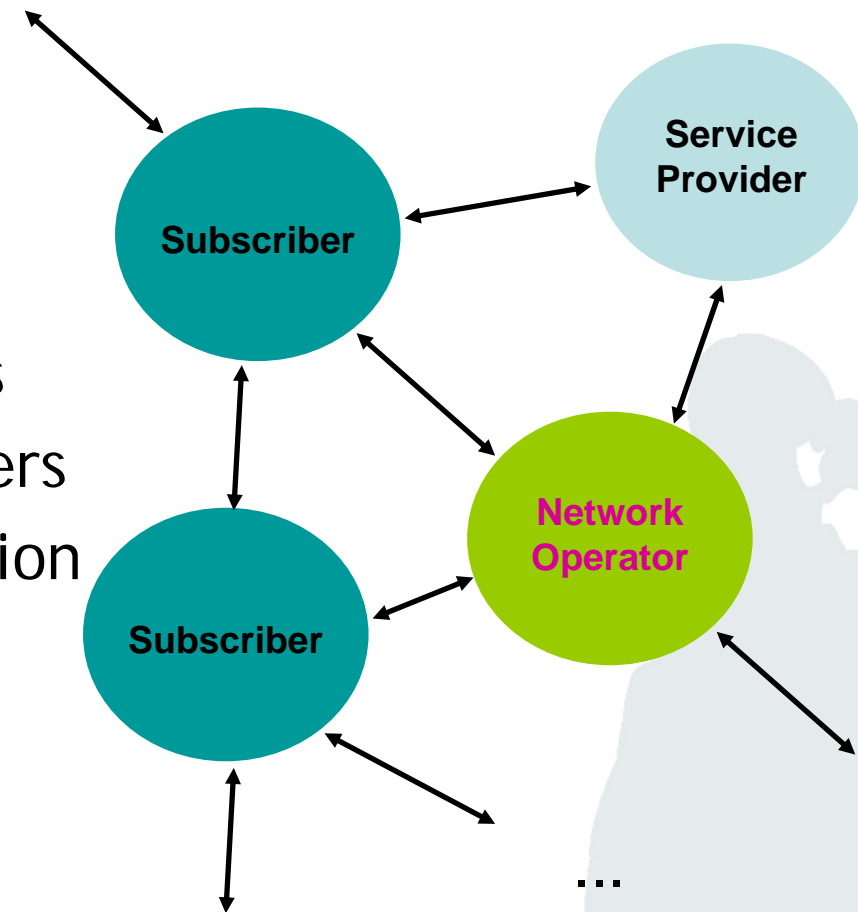
A **combination** of technical, organizational and legal methods is necessary.

- *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.

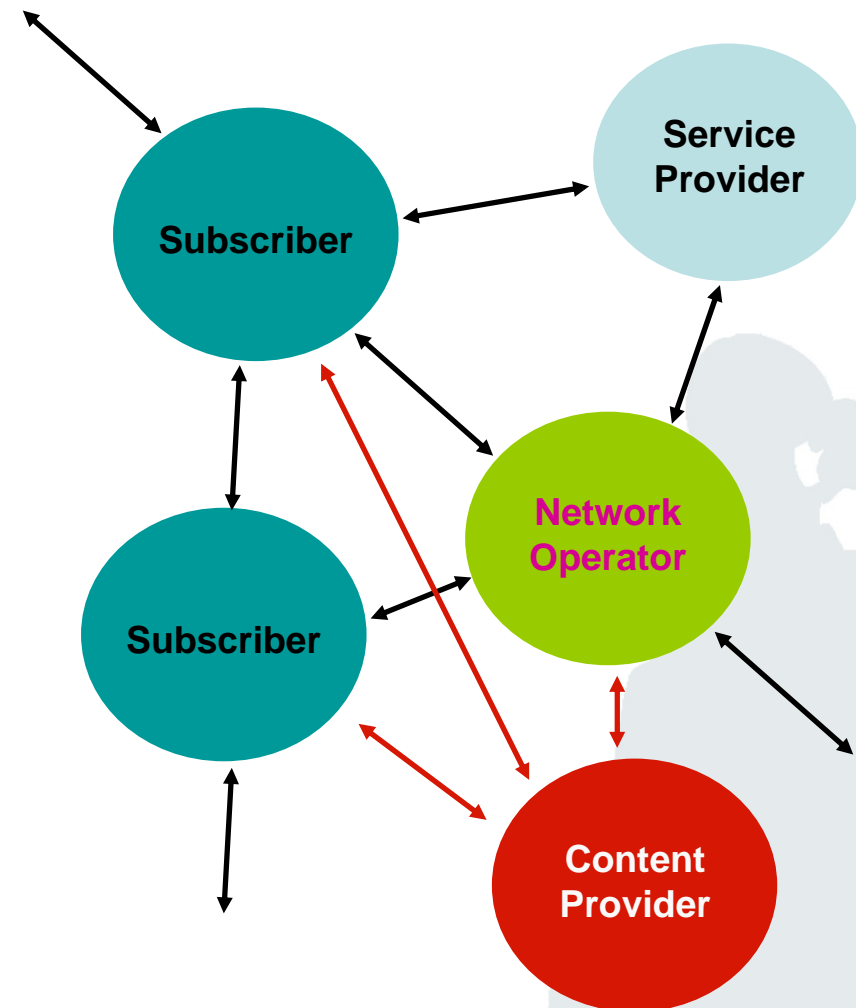
Different Parties
with
different Interests

- Customers/ Merchants
- Communication partners
- Citizens/ Administration



... in a world of consortia

- more partners
- more complex relations



Respecting
Interests

Supporting
Sovereignty

**Protection
of different
parties and their
interests**

Considering Conflicts

Respecting Interests

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

Supporting Sovereignty

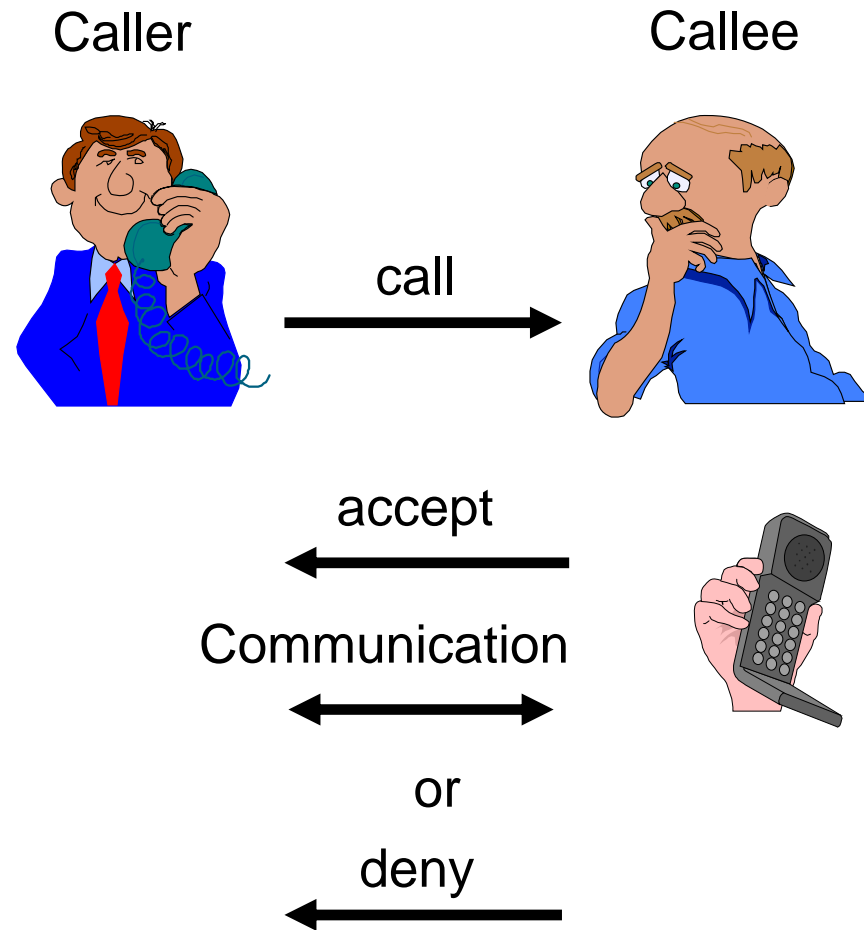
- Requiring each party to **only minimally** trust in the honesty of others
- Requiring **only minimal** or **no** trust in technology of others

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

The Challenge

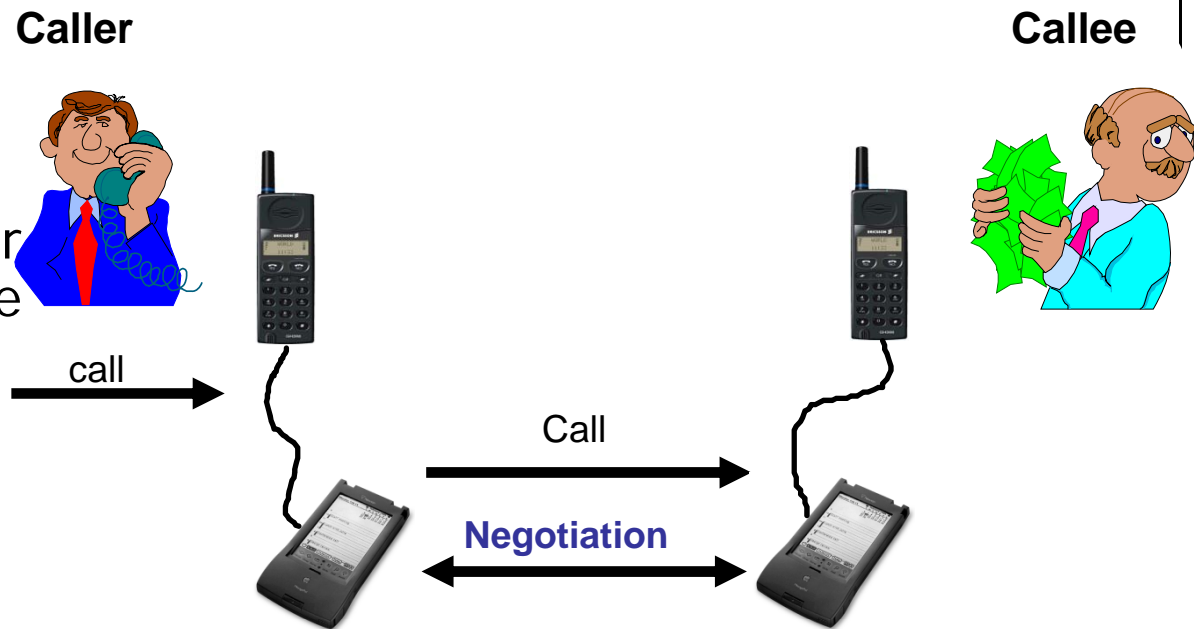
- Increased reachability due to new communication services
- Annoying calls
- Shortage of time
- Caller-ID conflict

→ 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



The Challenge

Increased reachability due to
new communication services

Annoying calls

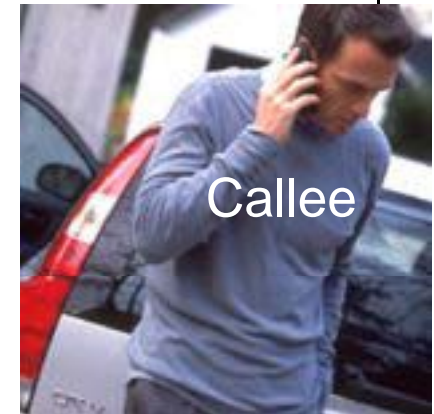
Shortage of time

Caller-ID conflict

-> Reachability Management (RM)



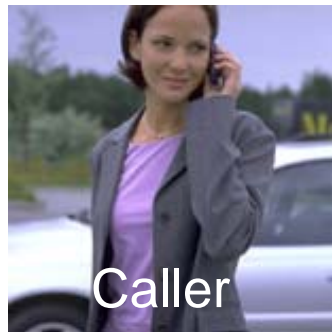
accept



or

deny





Call →



Call →



Negotiation ↔

↕



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


- 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

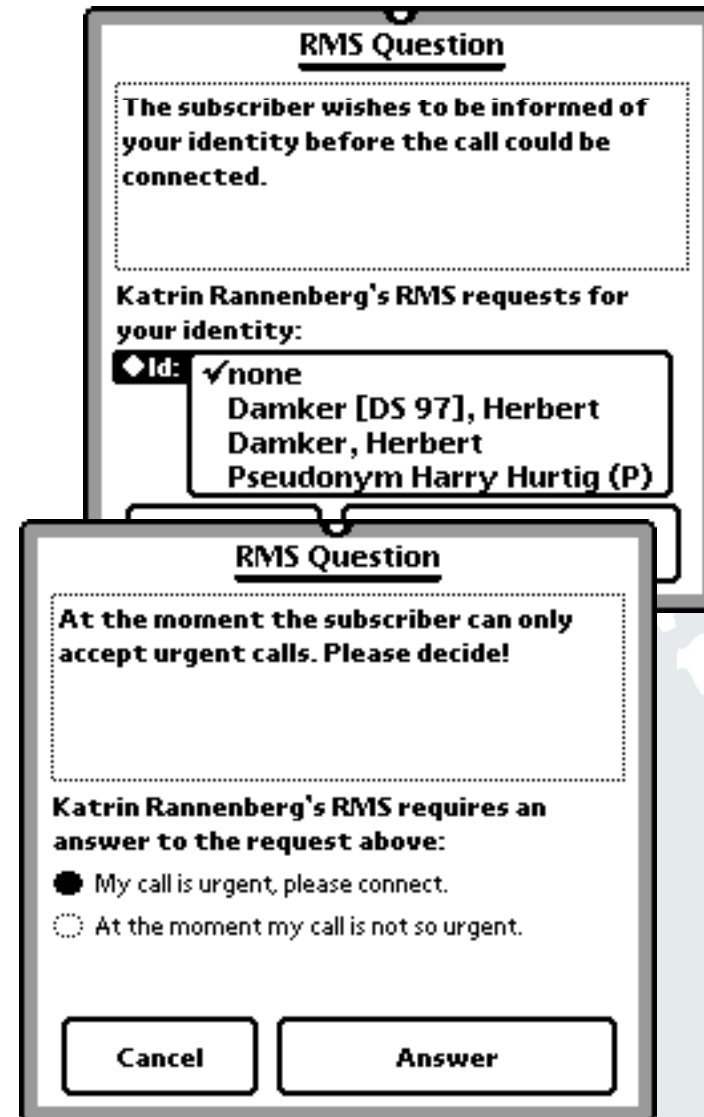
“I welcome you calling back.”

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!

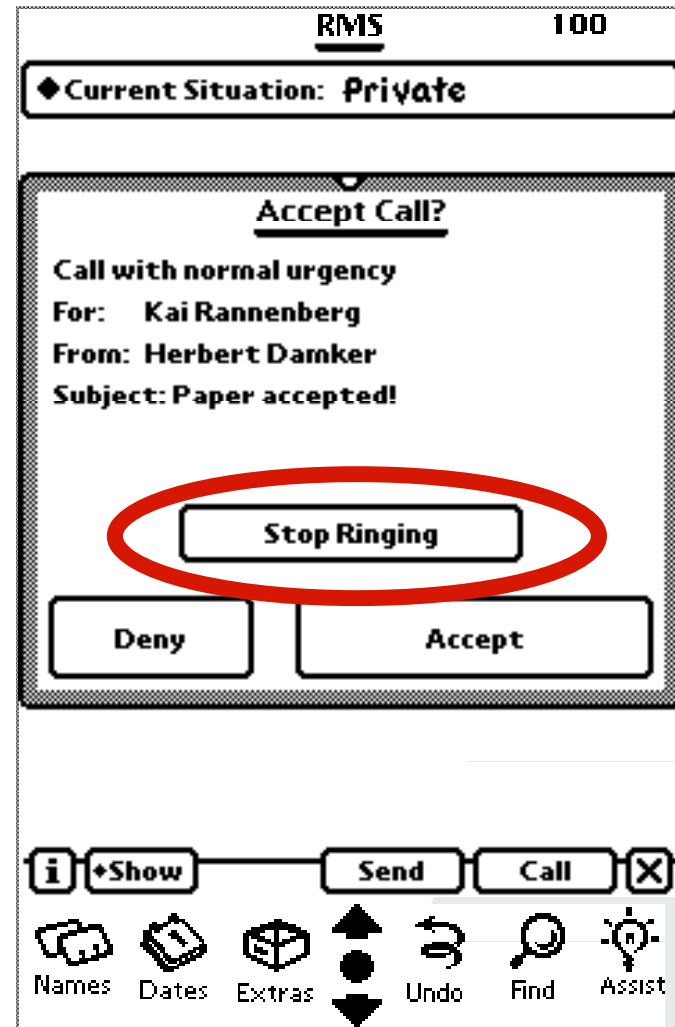
Katrin Rannenberg's RMS requires an answer to the request above:

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

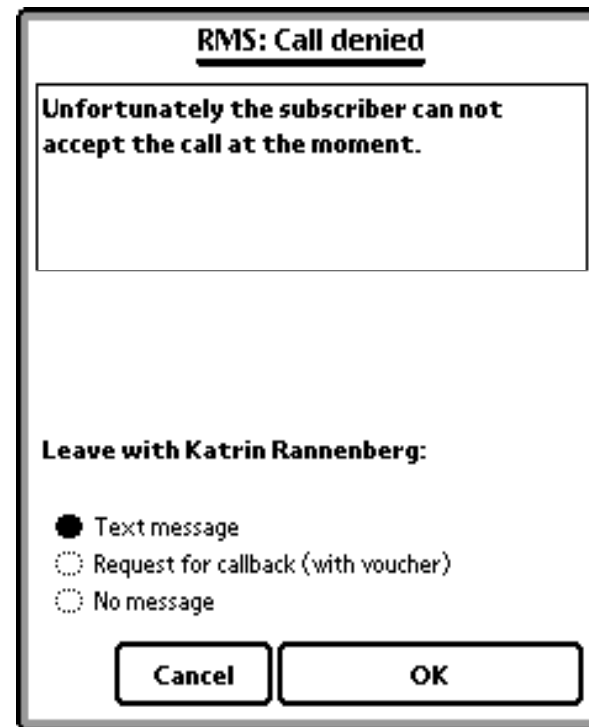
Cancel Answer

RMS accepted call (Callee display)

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



- 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 Rannenbergl:

Text message
 Request for callback (with voucher)
 No message

Cancel **OK**

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.

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 calls of class:
 business calls private calls

... and ...

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

... do the following:

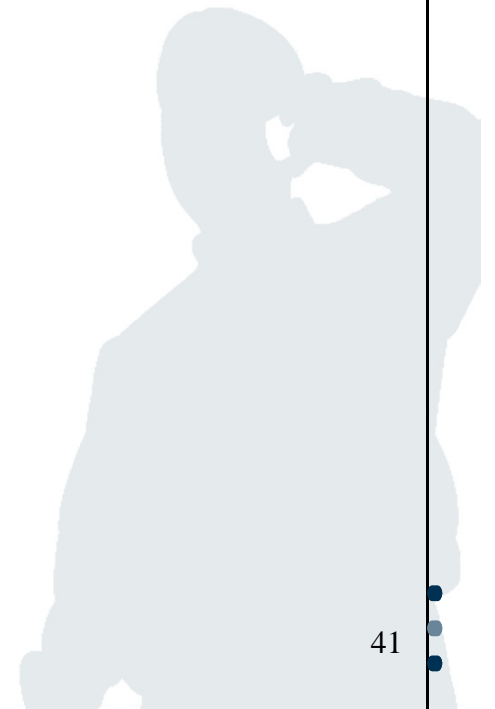
connect
 deny
 divert to:
 require surety of \$10 and connect
 require subject and connect
 let caller decide
 require caller ID

Text to send: -

Cancel OK

Reachability Management and Multilateral Security

????????



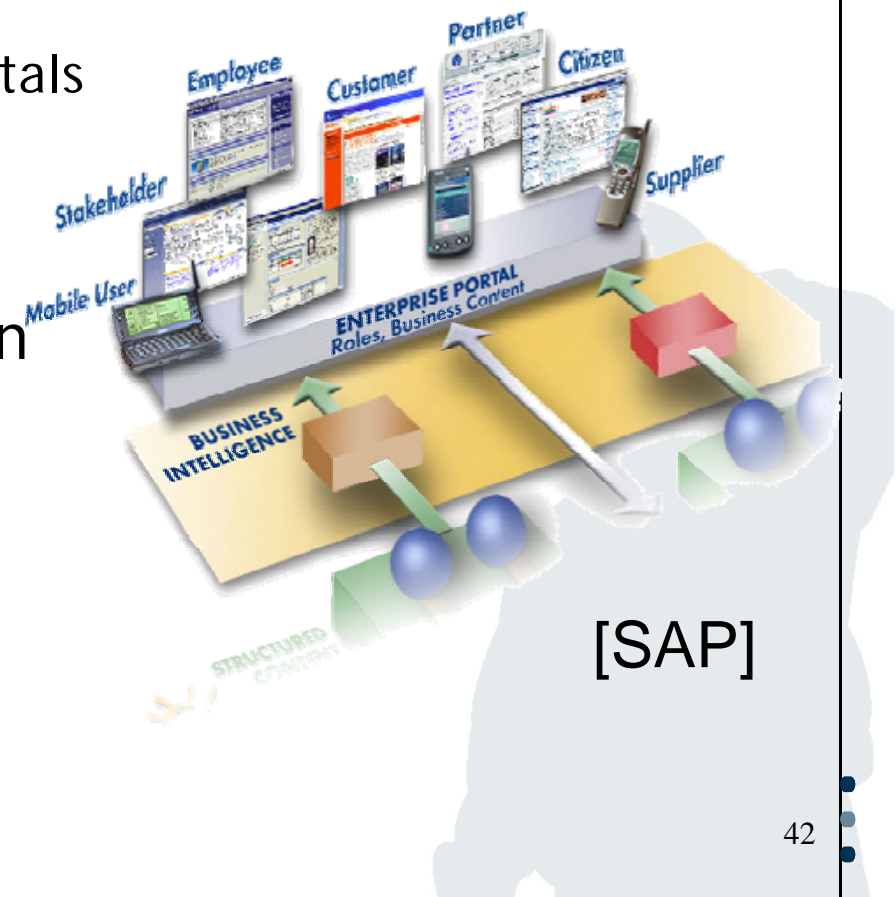
Just a small example, **but**

- Integration of voice and data services

Think this within

- Enterprise communication portals
- Mobile access
- Shared calendars

New dimensions for negotiation



\$

\$\$ \$ \$

\$

\$ \$ \$ \$

Lectures and Exercises

14.10.2008	Introduction	Lecture
	Multilateral Security, Design of Mobile Apps & Services: HCI Issues	Lecture
15.10.2008	Authentication	Lecture
28.10.2008	Authentication	Exercise
04.11.2008	Access Control	Lecture
05.11.2008	Access Control	Exercise
11.11.2008	Cryptography	Lecture
12.11.2008	Cryptography	Exercise

Lectures and Exercises

18.11.2008	Cryptography II	Lecture
25.11.2008	Cryptography III	Lecture
26.11.2008	Corporate Security	Guest Lecture
02.12.2008	Identity Management I	Lecture
09.12.2008	Identity Management II	Lecture
10.12.2008	Profiling Challenge	Exercise
16.12.2008	Computer System Security	Lecture
17.12.2008	Biometry	Guest Lecture
13.01.2009	Network Security I	Lecture
14.01.2009	Social Engineering	Guest Lecture
20.01.2009	Network Security II	Lecture
21.01.2009	Computer Forensics	Guest Lecture
27.01.2009	Security Engineering	Lecture
03.02.2009	Evaluation Criteria	Lecture
10.02.2009	Vertiefung ausgesuchter Vorlesungsinhalte	Lecture