mobile business

Lecture 1

Introduction

Information & Communication Security
(WS 2014/15)

Prof. Dr. Kai Rannenberg

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

Agenda

- The Chair of M-Business and Multilateral Security
- Teaching and Research Agenda
- Introduction into Mobile Business – History of Mobile Business & Mobile Telecommunication Systems
- Outline of this Course

Who we are

Business Informatics @ Goethe University Frankfurt

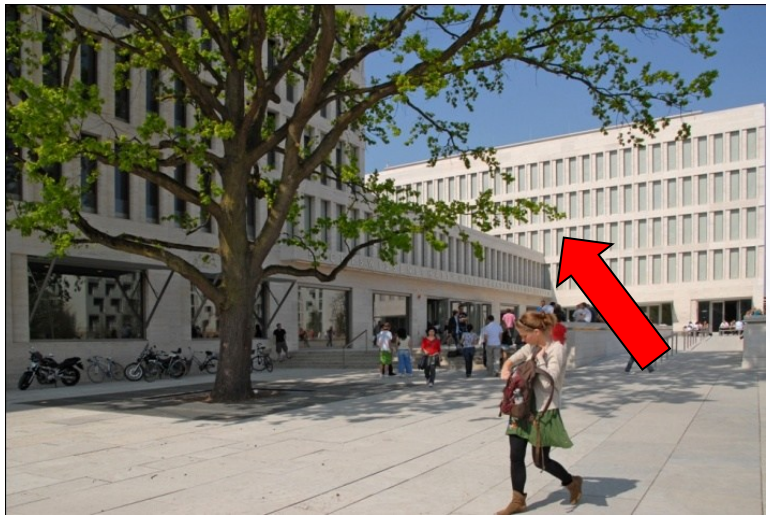
E-Finance Prof. Dr. Peter Gomber	**Business Informatics (Informatics)** Prof. Dr. Mirjam Minor	**Information Systems Engineering** Prof. Dr. Roland Holten
Business Education (associated) Prof. Dr. Gerhard Minnameier	**Business Informatics**	**Business Education** (associated) Prof. Dr. Eveline Wuttke
Information Systems & Information Management Prof. Dr. Wolfgang König	**Business Informatics & Microeconomics** Prof. Dr. Lukas Wiewiorra	**Mobile Business & Multilateral Security** Prof. Dr. Kai Rannenberg

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

Deutsche Telekom Chair of Mobile Business & Multilateral Security

Grüneburgplatz 1
Campus Westend
RuW Building, 2nd Floor

Phone: +49 69 798 34701
Fax: +49 69 798 35004
Email: info@m-chair.de
URL: www.m-chair.de



mobile business

Team

Kai Rannenberg

Jetzabel Serna-Olvera

Markus Tschersich

Stephan Heim

Gökhan Bal

Lars Wolos

Marvin Hegen

Team

Shuzhe Yang

Ahmad Sabouri

Fatbardh Veseli

Christopher Schmitz

Welderufael Tesfay

Ahmed Yesuf

Research Fellows & External PhD Students

Mike Radmacher

Andreas Albers

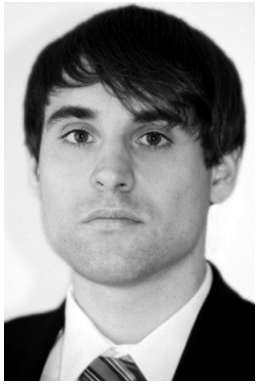
Stefan Weiss

Christian Kahl

André Deuker

Sascha Koschinat

Christian Weber



Andreas Leicher

Tim Schiller

Niels Johannsen

Thomas Leiber

Team

Office:

Elvira Koch

Email: elvira.koch@m-chair.de

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

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

Kai Rannenberg

Recent history of Kai Rannenberg

1999-09 till 2002-08
- Microsoft Research Cambridge UK
- 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

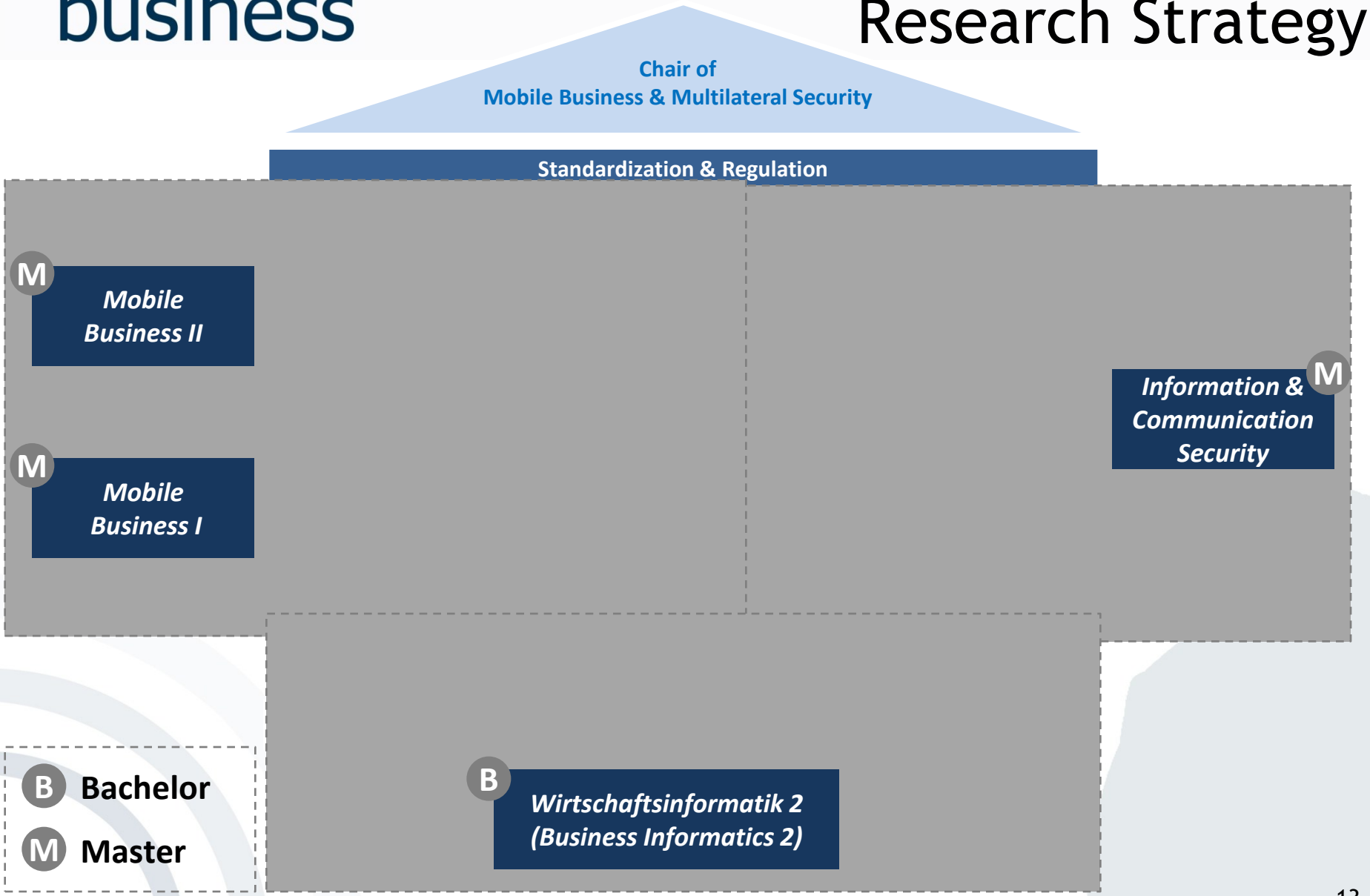
Agenda

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

Teaching

	WS 2014/15	SS 2015
Bachelor		*Course* **Business Informatics 2**
Master	*Course* **Informations- und Kommunikationssicherheit: Infrastrukturen, Technologien und Geschäftsmodelle** *Course* **Mobile Business I: Technology, Markets, Platforms, and Business Models** *Seminar* **User-centric Privacy Enhancing Technologies and Mobile Services for Consumer Goods**	*Course* **Mobile Business II - Application Design, Applications, Infrastructures, and Security** *Seminar* **TBA** *Course* **Information and Communication Security: Infrastructures, Technologies, and Business Models** *Course* **Privacy vs. Data: Business Models in the digital, mobile Economy**

Teaching & Research Strategy



M-Research in Frankfurt

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

Agenda

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

Contact Persons

M.Sc. Fatbardh Veseli

RuW Building, Office 2.232

Phone: 069 / 798 – 34704

Email: fatbardh.veseli@m-chair.de

M.Sc. Ahmed Yesuf

RuW Building, Office 2.236

Phone: 069 / 798 – 34699

Email: ahmed.yesuf@m-chair.de

M.Sc. Christopher Schmitz

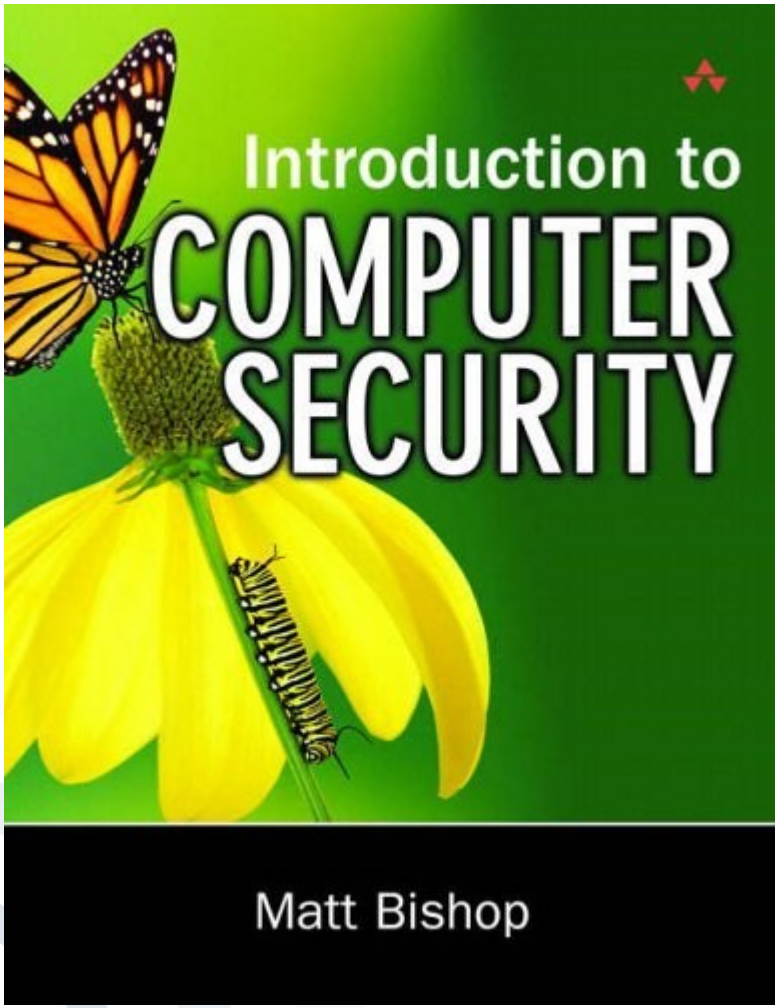
RuW Building, Office 2.236

Phone: 069 / 798 - 34703

Email: christopher.schmitz@m-chair.de

Please use the email address **sec@m-chair.de**

Literature



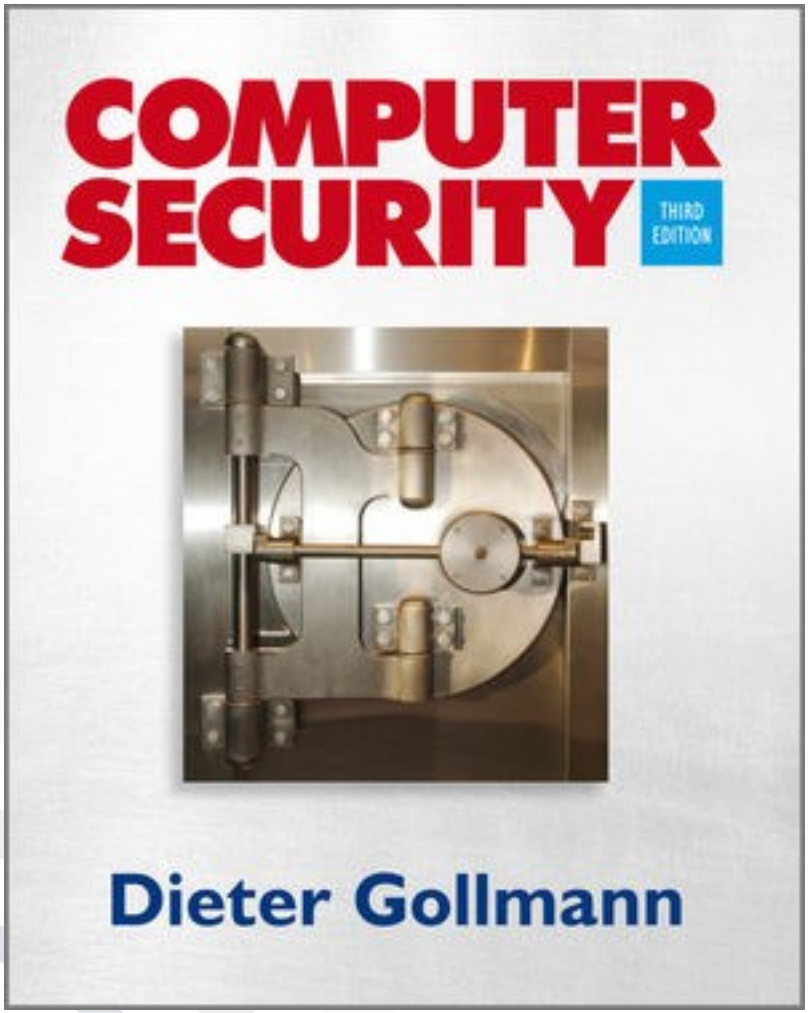
Matt Bishop:

Introduction to Computer Security

Addison Wesley

ISBN: 0-321-24744-2

Literature



Dieter Gollmann:
Computer Security
John Wiley & Sons
ISBN: 0-470-74115-5

Literature

In German:

Claudia Eckert:
IT-Sicherheit
Oldenbourg
ISBN: 978-3-486-70687-1

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)

EBSCO HOST Research Databases

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

Online search engines:

http://citeseer.ist.psu.edu/

http://scholar.google.com

On the dates and the agenda

- **Exam date not fixed yet.**
  - Please keep yourself updated!
  - Check the website of the Prüfungsamt: http://www.wiwi.uni-frankfurt.de/mein-wiwi-studium/pruefungsamt.html
- **Course agenda is online.**
  - Please keep yourself updated!
  - Check the website of the course: http://www.m-chair.de/wps/wse/lv/det/rannenberg/175/

Agenda

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

Electronic Business and Security

February 15, 2012, 2:14PM

Anonymous-Linked Attacks Hit US Stock Exchanges

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

March 5, 2012, 3:40PM

Hacker Group Breaches Library of Congress Site, Publishes Passwords

Risks of Unprotected Market Activities

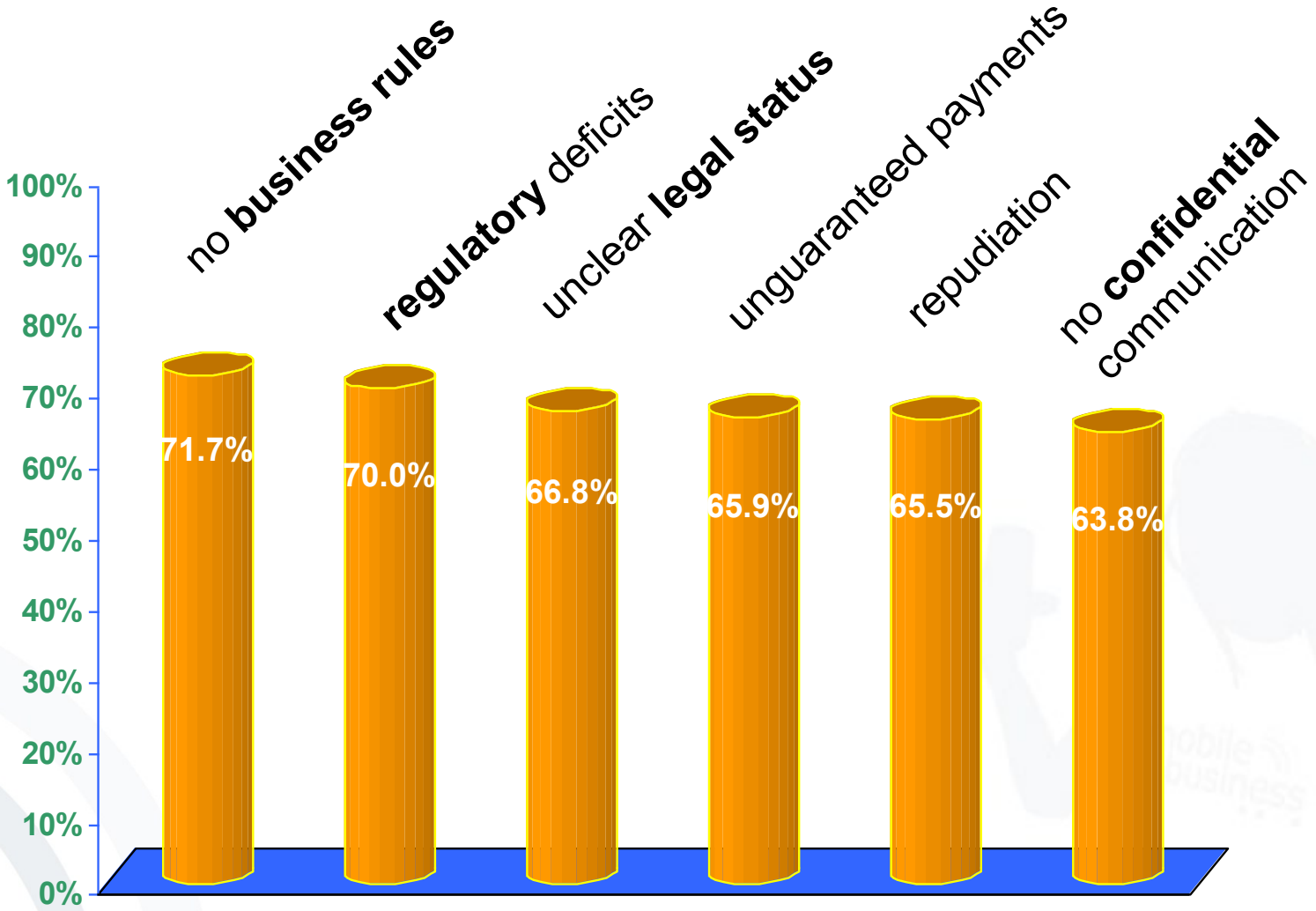
Provider

- 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

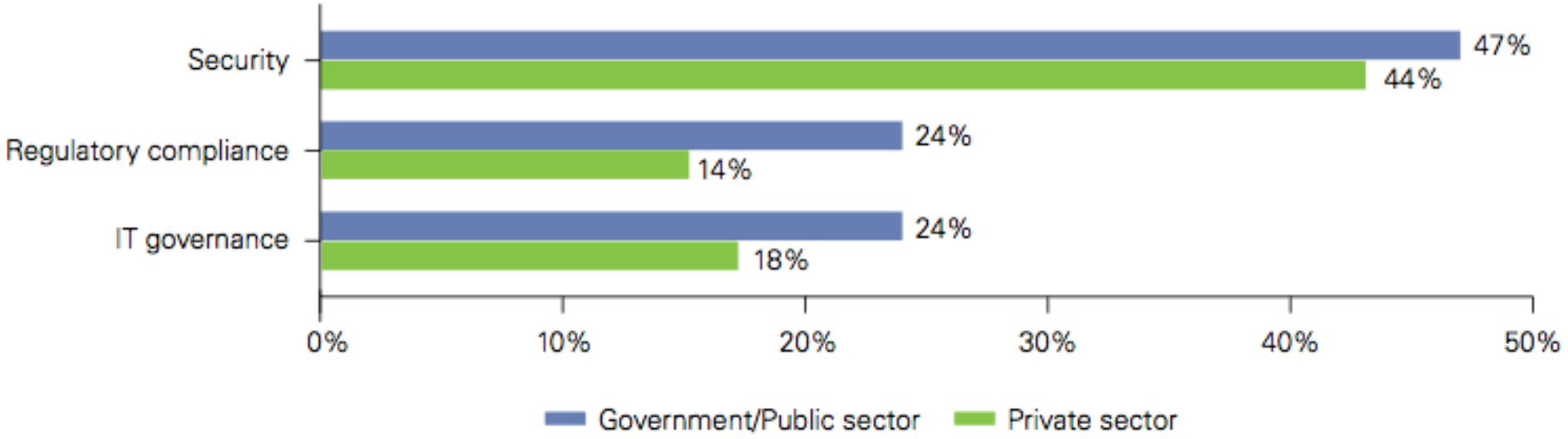


Source: Electronic Commerce Enquête, Universität Freiburg, 1998
(32 options + free text for choice, 6 options with highest agreement listed)

Cloud adoption and security

Figure 13: Top challenges of adopting a cloud environment

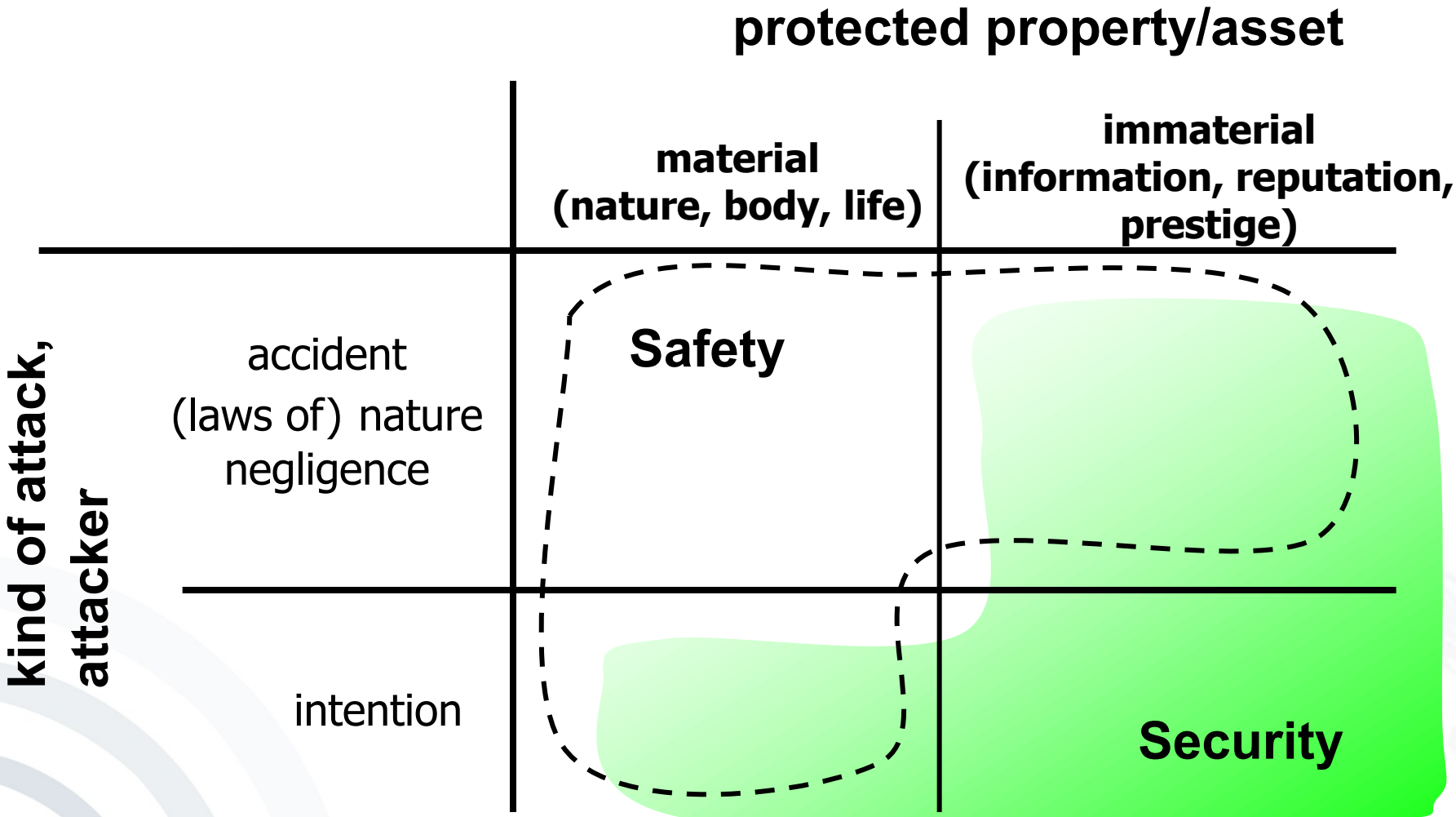
What do you believe are the top challenges or concerns your organization faces in adopting a cloud environment?



Source: KPMG International 2012, Government Cloud Survey
KPMG International 2011, Clarity in the Cloud

Source: Exploring the Cloud, KPMG, 2012: A Global Study of Governments' Adoption of Cloud

Security vs. Safety



Security

A very human discrepancy

- **Privacy**
  Protect the own sphere and the own values/assets
- **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.

Concepts and their Motivation (1)

- ***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 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.

Concepts and their Motivation(2)

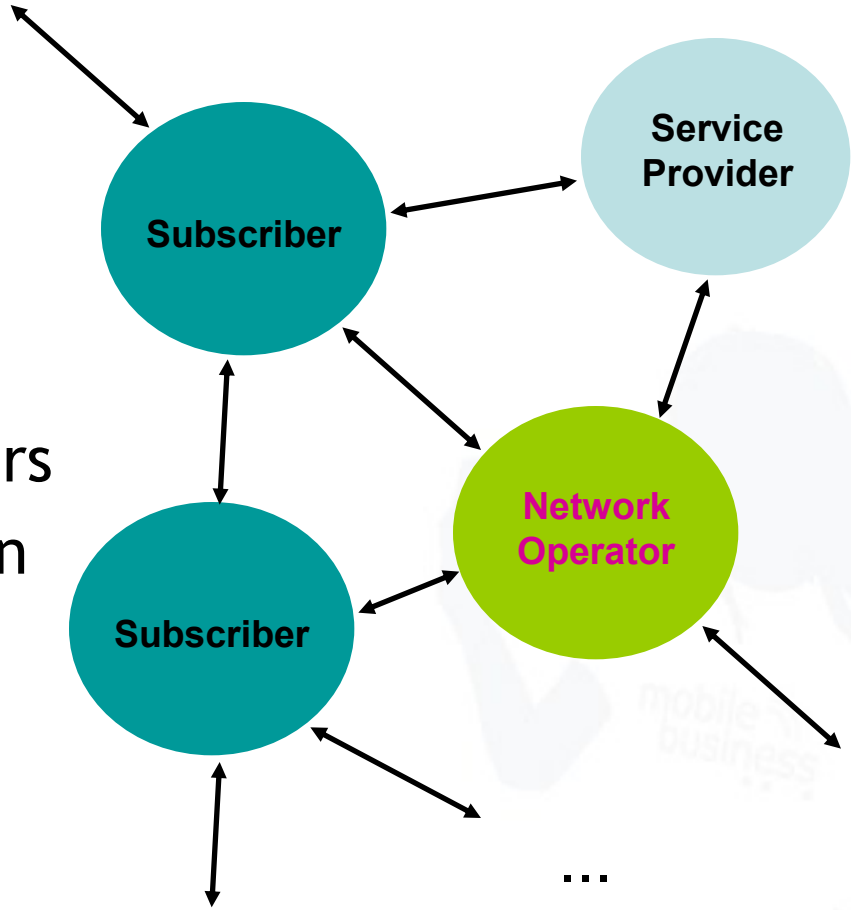
- ***Unauthorized impair of functionality***, that means loss of **availability**: If the medical history is accessible solely via one network and this network has a breakdown when patient data has to be queried it may be life-threatening for the patient.

- ***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.

Multilateral Security

Different Parties
with
different Interests

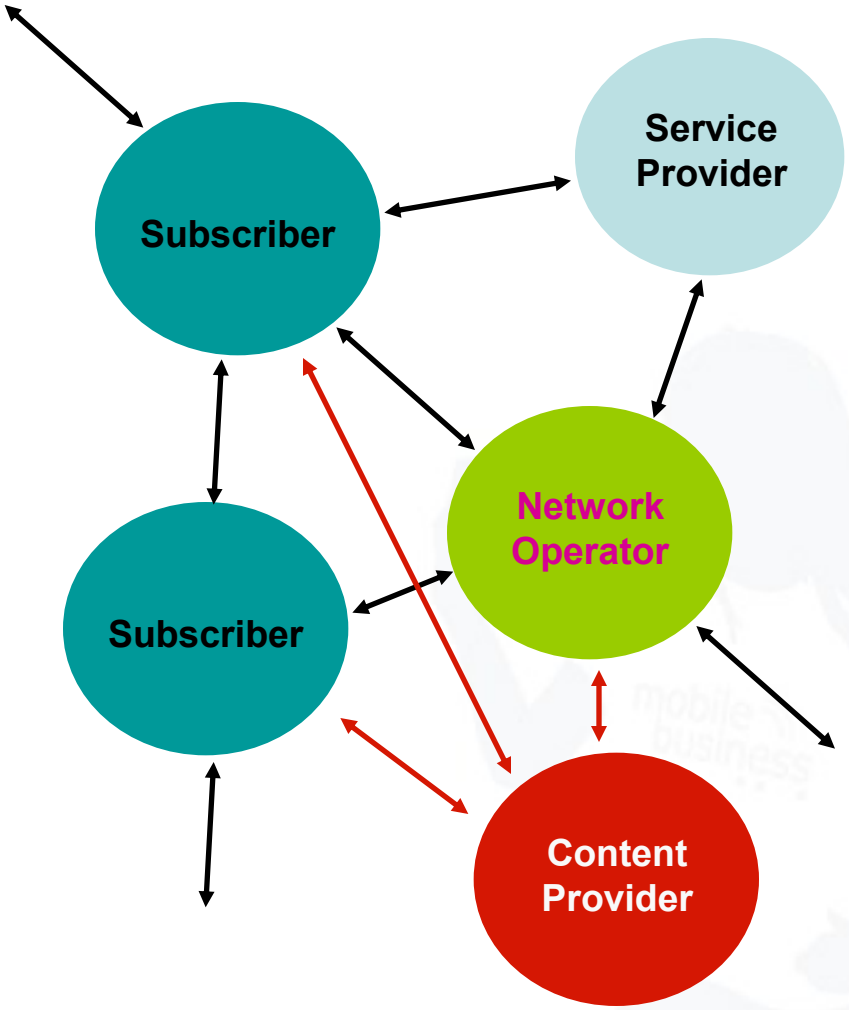
- Customers/Merchants
- Communication partners
- Citizens/Administration



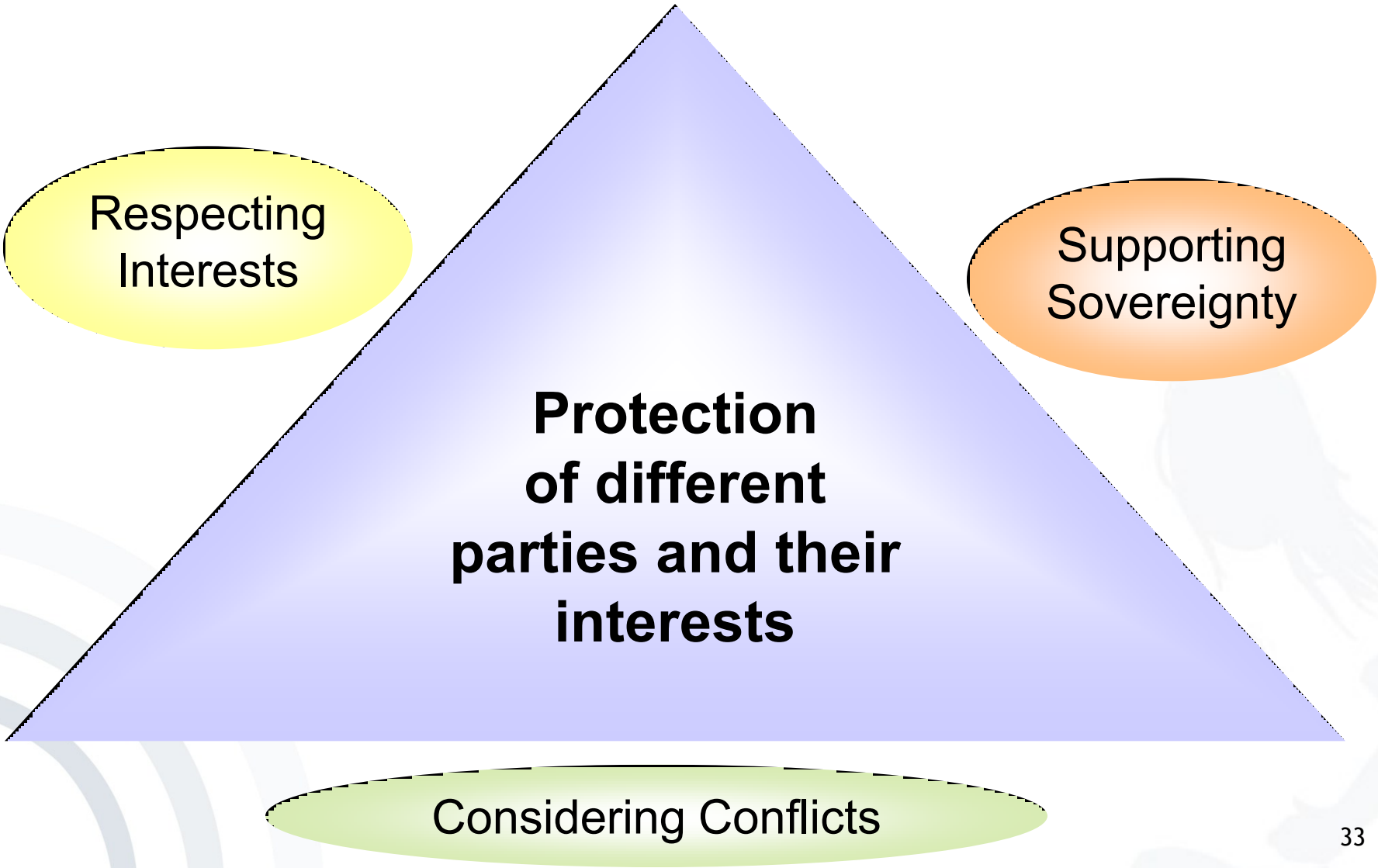
Multilateral Security

… in a world of consortia

- more partners
- more complex relations



Multilateral Security



Multilateral Security considers conflicts

Respecting Interests

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

Supporting Sovereignty

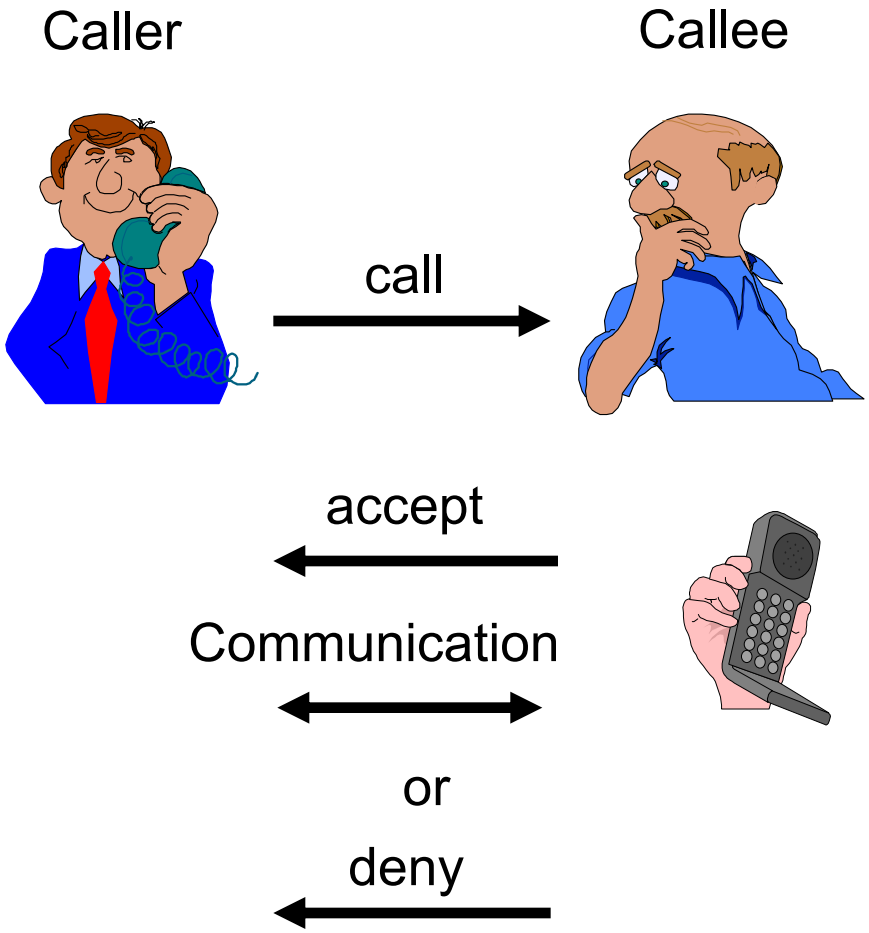
- Requiring each party to **only minimally trust** in the honesty of **others**
- Requiring **only minimal or no trust in technology** of others

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

Multilateral Security in daily communication

The Challenge

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



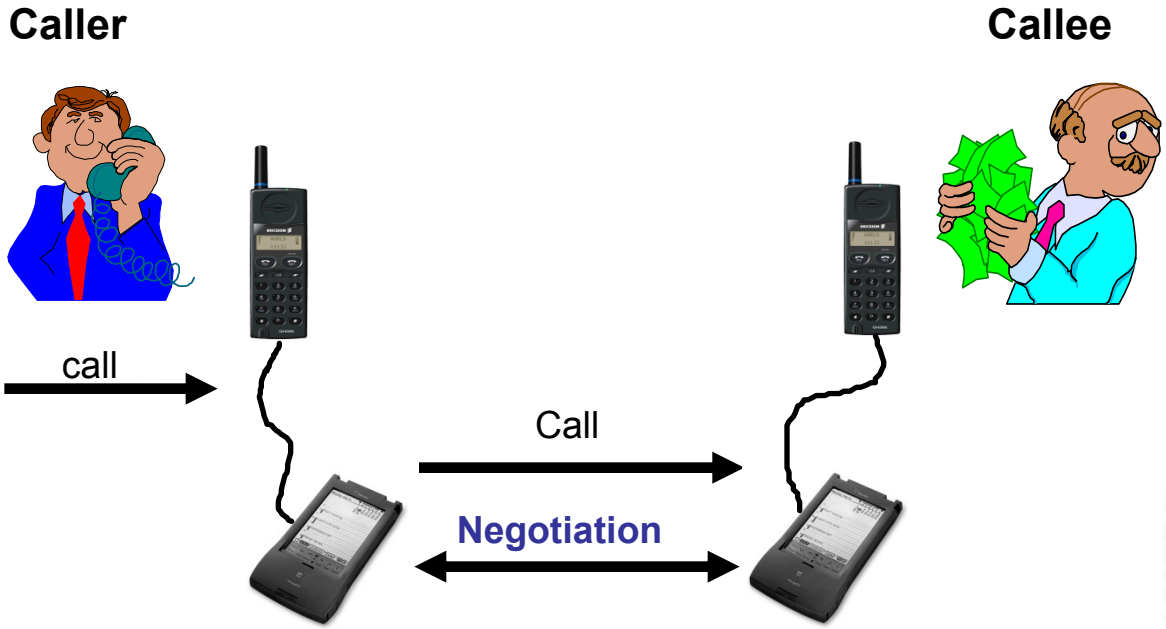
→ Reachability Management (RM)

mobile business

Communication supported by an RM System

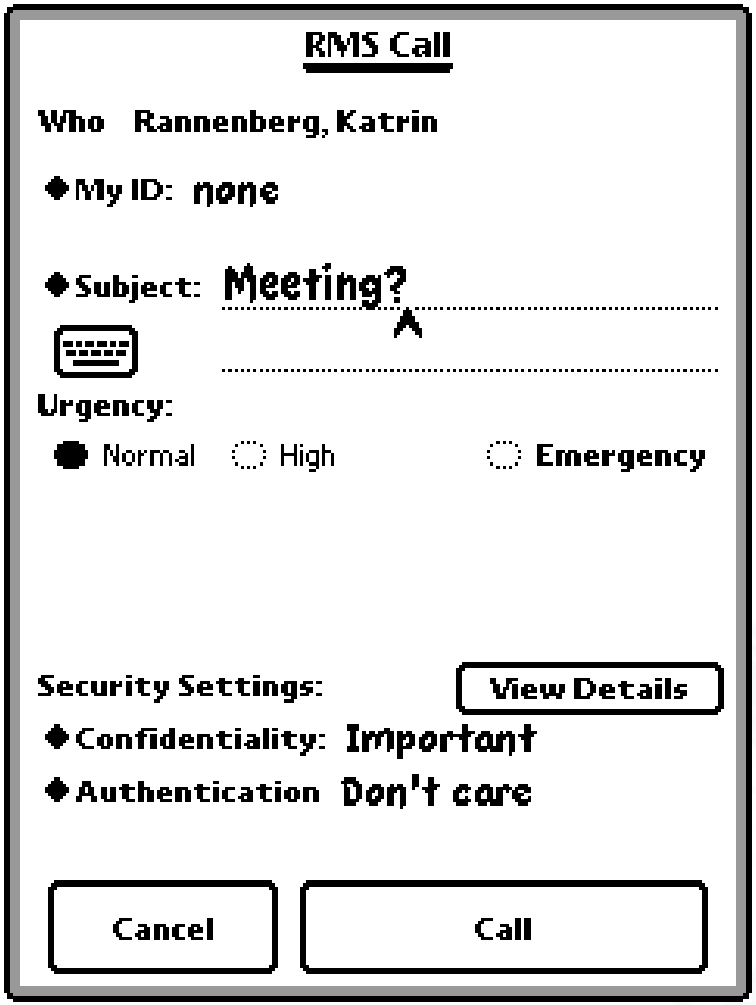
The Features

- 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



mobile business

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

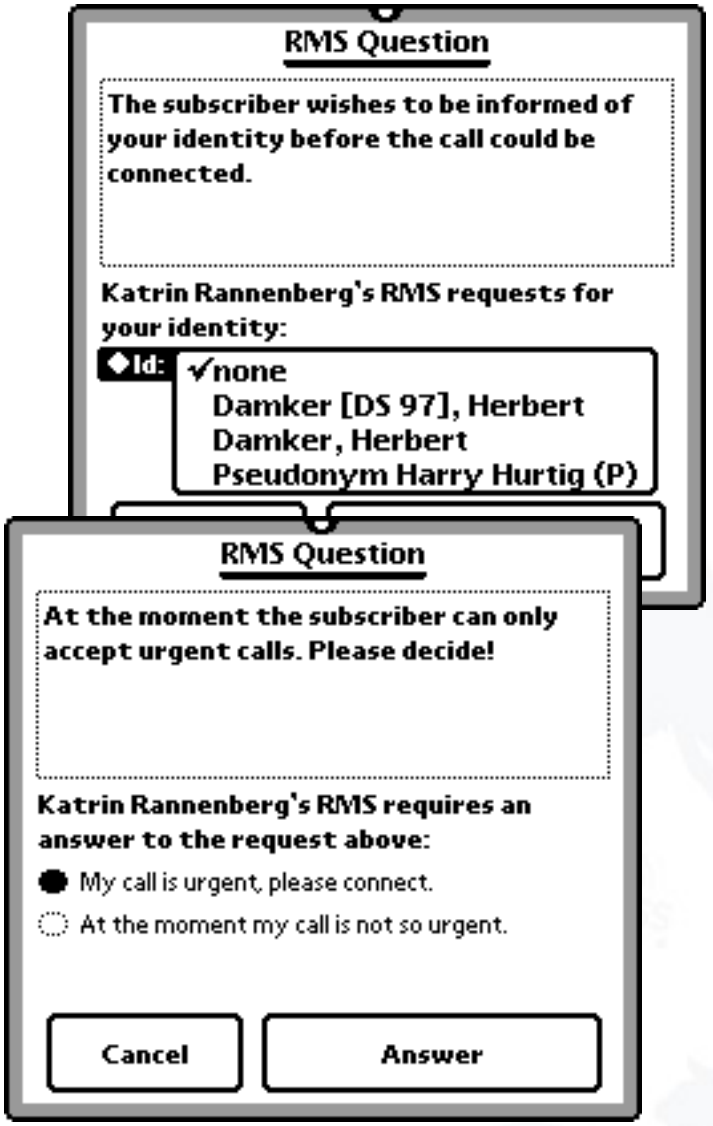
"I welcome you calling back."

Provision of a reference

"My friends are your friends!"

Offering a surety

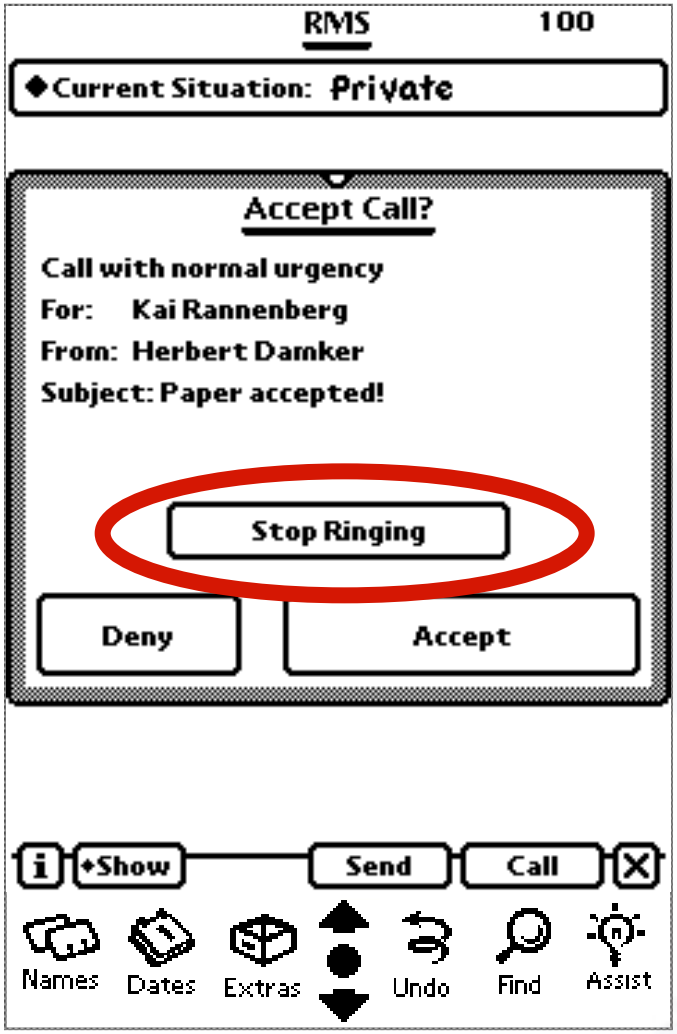
"Satisfaction guaranteed or this money is yours!"



mobile business

RMS accepted call (Callee display)

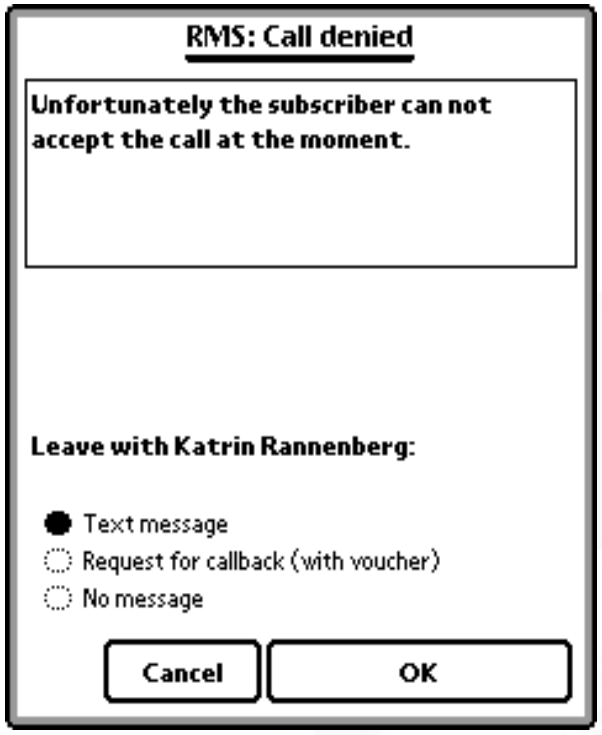
- Bell is ringing!
- Callee notified
- Callee can still decide to accept or deny the call



mobile business

RMS denied call (Caller display)

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



Configuring your RMS

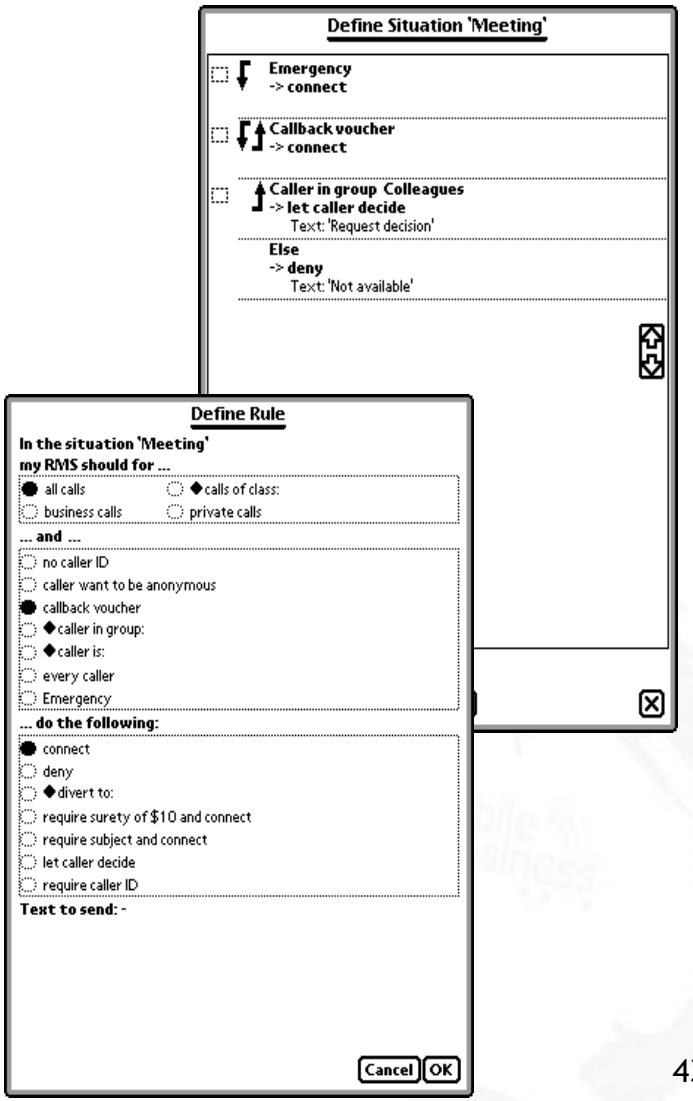
Situations

Set of rules how to deal with an incoming call

Rules

Combination of features

Users can reconfigure initial rules and situations as they like.



Reachability Management and Multilateral Security

???????

Multilateral Security considers 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**

Reachability Management and Multilateral Security

- 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

mobile business

Some lessons learned

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

Challenge
Security introduces extra complexity

- Complexity was **accepted** as **benefit** was **seen**, e.g. **Situations** in Reachability Management vs. **pagers**.
- 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 situations**,
  - 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”.

So what ...

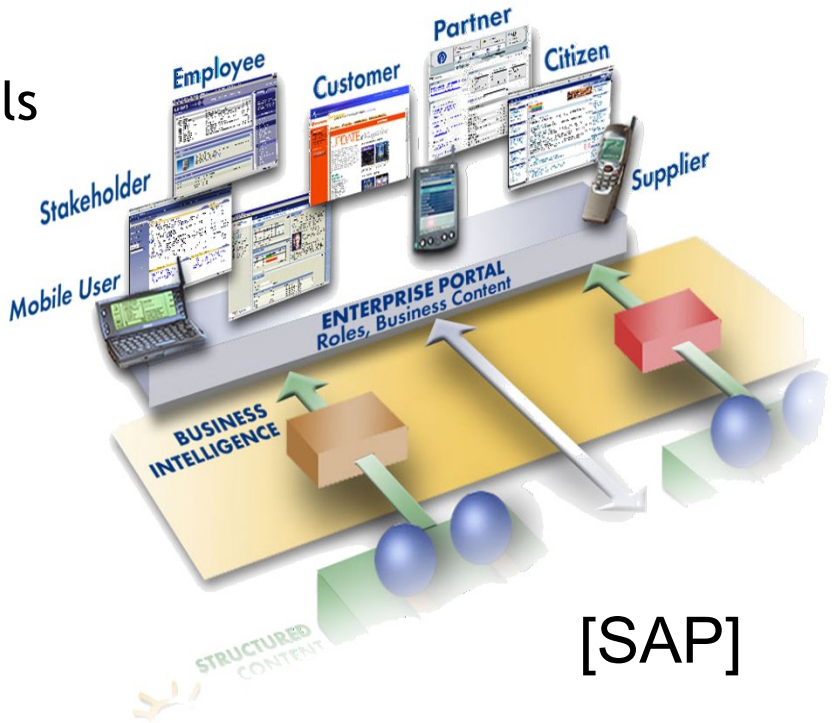
Just a small example, **but**

- Integration of voice and data services

Think this within

- Enterprise communication portals
- Mobile access
- Shared calendars

New dimensions for negotiation



[SAP]

Agenda

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

mobile business

Outline of this course

Lectures and Exercises

No.	Day	Title
VL02	15-Oct-14	Authentication
VL03	28-Oct-14	Access Control
UE02	05-Nov-14	Access Control
UE03	12-Nov-14	Guest Lecture 1 - Jürgen Kühn - Biometrics
VL07	25-Nov-14	Identity Management

Outline of this course

Lectures and Exercises

No.	Day	Title
VL09	09-Dec-14	Computer System Security
VL11	17-Dec-14	Network Security II
UE05	20-Jan-15	Guest Lecture 2 - Jens Eichler - Social engineering
UE07	28-Jan-15	Guest Lecture 4 - Dr. Daniel Hamburg - Pentests - more than just using the proper tools
VL14	04-Feb-15	Evaluation Criteria