mobile business

Lecture 01

GOETHE UNIVERSITÄT FRANKFURT AM MAIN

Information & Communication Security (WS 2018/19)

Introduction

Prof. Dr. Kai Rannenberg

Chair of Mobile Business & Multilateral Security
Johann Wolfgang Goethe University Frankfurt a. M.

Agenda

- The Chair of M-Business and Multilateral Security
- Teaching & Research Agenda
- Organizational Issues
- Introduction into information and communication security
- 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	**Mobile Business & Multilateral Security** Prof. Dr. Kai Rannenberg	**Business Education** (associated) Prof. Dr. Eveline Wuttke
Information Systems & Information Management Prof. Dr. Wolfgang König	**Business Informatics & Microeconomics** Prof. Dr. Lukas Wiewiorra	**Business Informatics & Information Management** Prof. Dr. Oliver Hinz

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

Chair of Mobile Business & Multilateral Security

Theodor-W.-Adorno-Platz 4
Campus Westend
RuW, 2nd Floor

Phone: +49 69 798 34701
Fax: +49 69 798 35004
e-mail: info@m-chair.de

www.m-chair.de

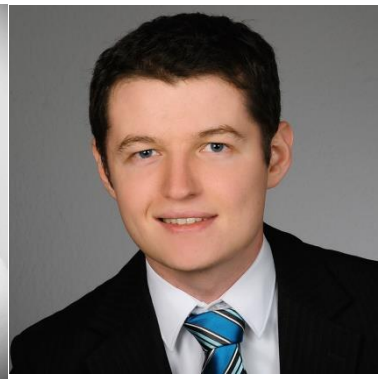
Team

Kai Rannenberg

Sebastian Pape

David Harborth

Majid Hatamian



Peter Hamm

Christopher Schmitz

Welderufael Tesfay

Ahmed Yesuf

Research Fellows & External PhD Students


Markus Tschersich


Jetzabel Serna-Olvera


Mike Radmacher


Andreas Albers


Stefan Weiss


Shuzhe Yang


André Deuker


Christian Kahl


Gökhan Bal


Ahmad Sabouri


Fatbardh Veseli


Tim Schiller


Niels Johannsen


Stephan Heim


Marvin Hegen


Michael Schmid

Team

Office:

Elvira Koch

Email: elvira.koch@m-chair.de

Office Hours: Mo.-Mi. 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 2018/19	SS 2019
Bachelor	*Seminar* **Innovations in Information Systems, Augmented Reality and the Role of Digital Platforms**	*Course* **Business Informatics 2 (PWIN)**
Master	*Course* **Mobile Business I: Technology, Markets, Platforms and Business Models** *Course* **Information & Communication Security: Infrastructures, Technologies and Business Models**	*Course* **Mobile Business II: Application Design, Applications, Infrastructures and Security** *Seminar* **Applications of Blockchain Technology**

Teaching in Frankfurt

Teaching Topics

- Identity Management
- Privacy
- ICT Security
- Mobile Business
- Business Informatics

Master Courses

Lectures

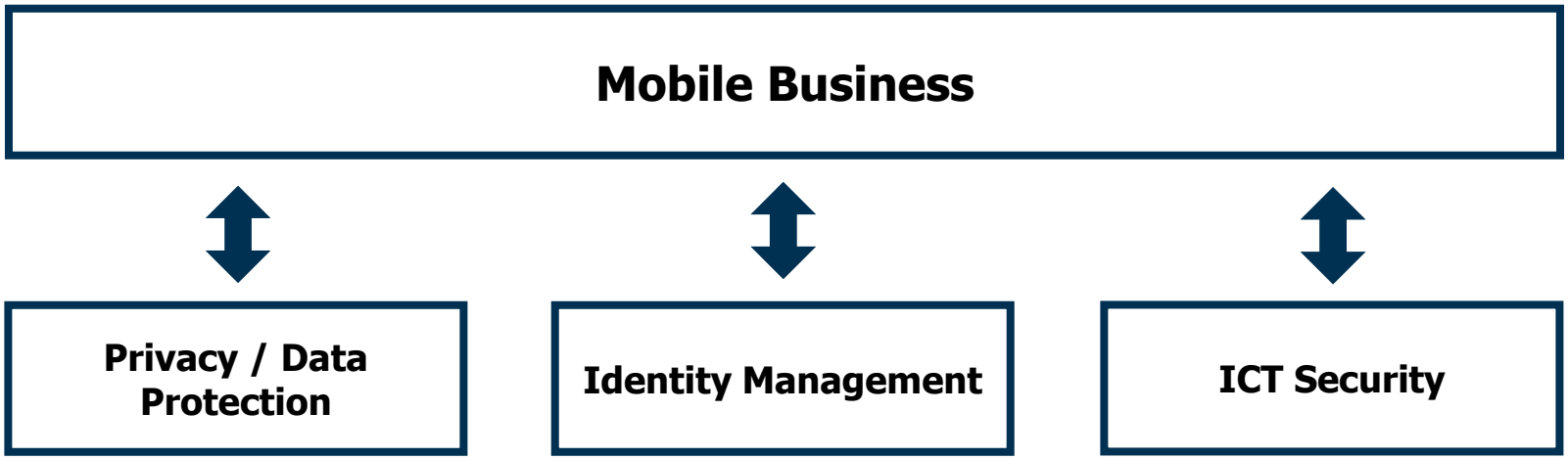
- Mobile Business 1
- Mobile Business 2
- I & C Security
- Privacy vs. Data
- Seminars
- Master Thesis

Bachelor Courses

Lectures

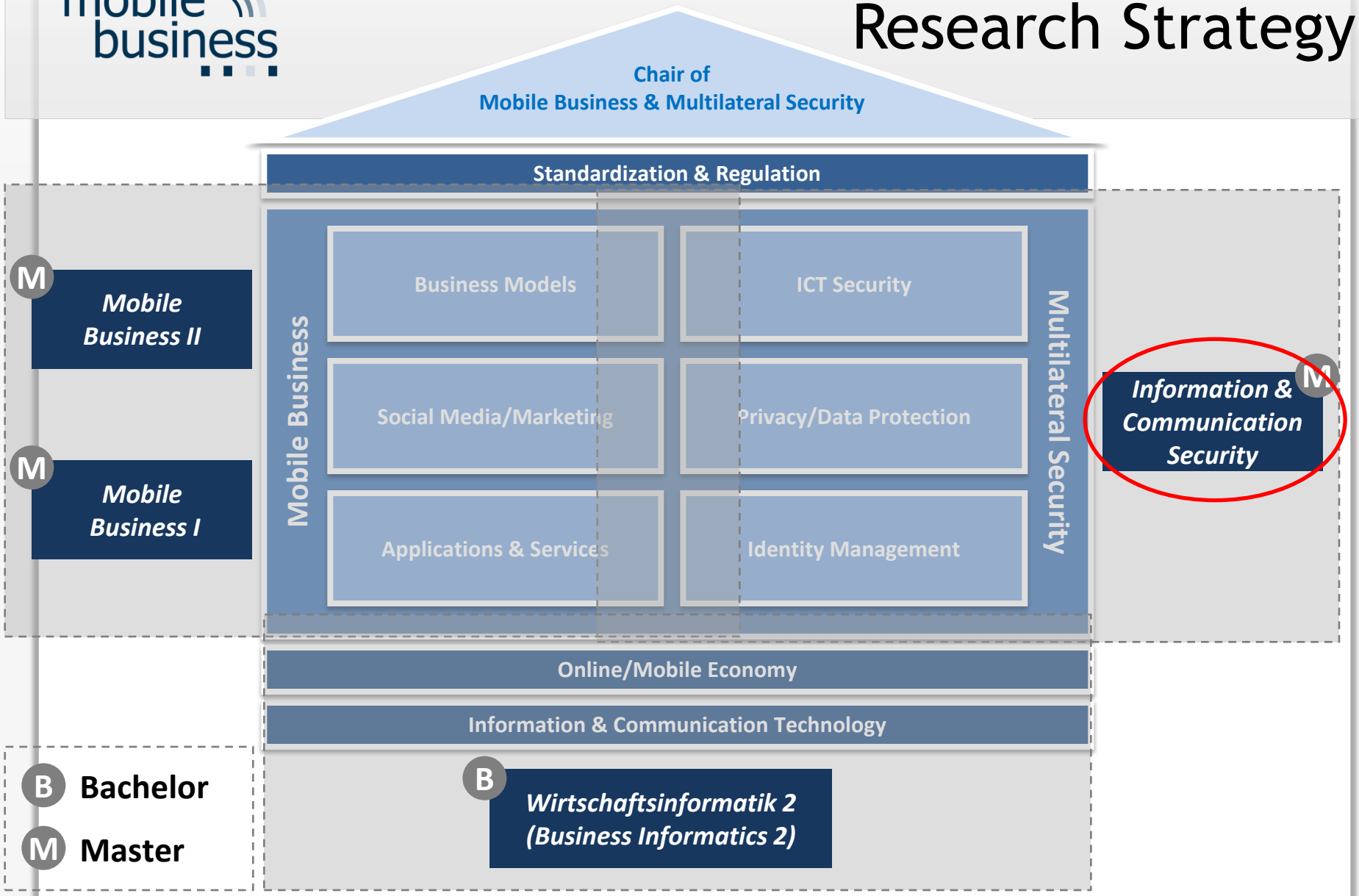
- Business Informatics 2
- Seminars
- Bachelor Thesis

M-Chair Research Statement



Advancing ***Mobile Business*** while enabling individuals to be in control of their personal data by providing ***Identity Management***, ***Privacy Protection***, and ***ICT Security*** within the Digital Economy

Teaching & Research Strategy



M-Research in Frankfurt

- **Multilateral Security**
  - Security, Trust, Identity Management, and Privacy
  - Security and Privacy Management
  - 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

Teaching Assistance

Christopher Schmitz, M.Sc.

RuW Building, Office 2.234

Phone: 069 / 798 – 34703

Email: christopher.schmitz@m-chair.de

Majid Hatamian, M.Sc.

RuW Building, Office 2.237

Phone: 069 / 798 – 34662

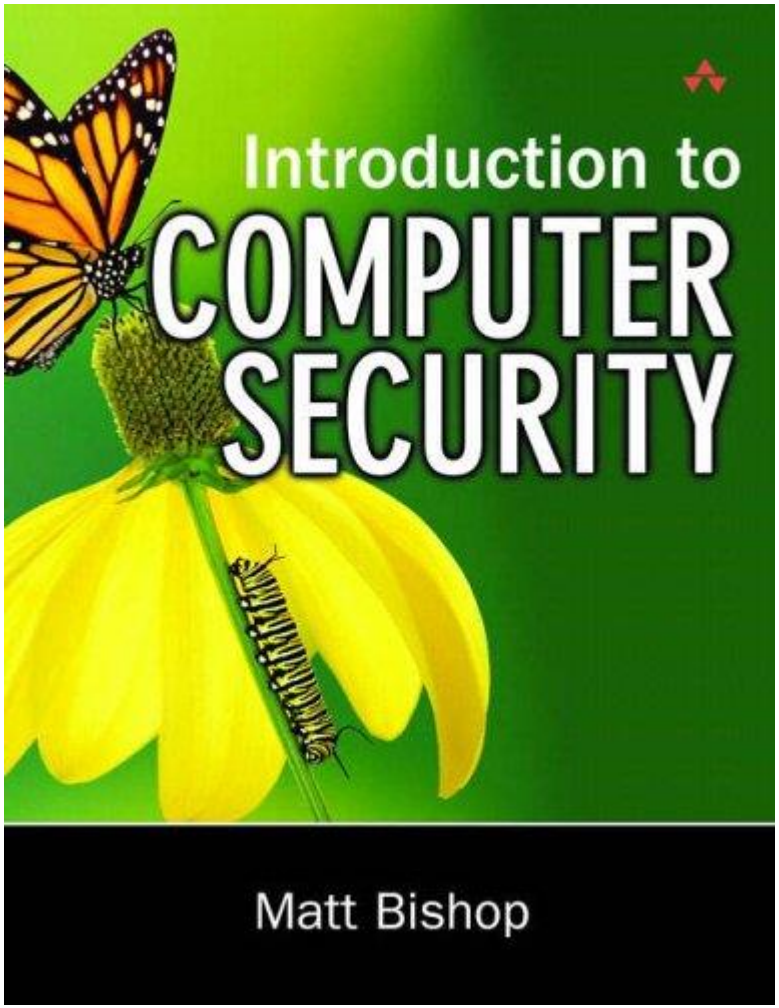
Email: majid.hatamian@m-chair.de

twitter.com/mchair

security@m-chair.de

mobile business

Literature



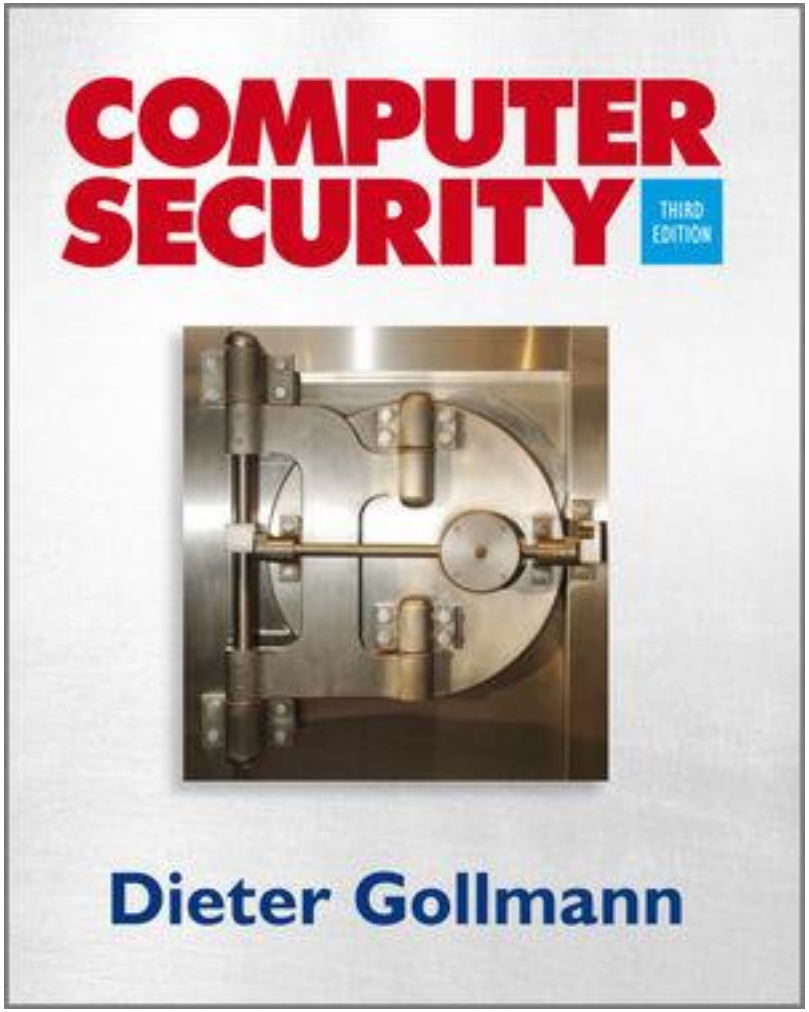
Matt Bishop:

Introduction to Computer Security

Addison Wesley

ISBN: 0-321-24744-2

Literature



Dieter Gollmann:

Computer Security

John Wiley & Sons

ISBN: 0-470-74115-5

19

Literature

In German:

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

Literature

Please Note:

Electronic library of journals, access to more than 2000 journals

http://www.ub.uni-frankfurt.de/online/emedien.html

Available only for university members via HRZ account (141.2.XXX.XXX IP-addresses; PC Pool) or via university library login:
www.ub.uni-frankfurt.de/login.html

search.epnet.com/login.asp
www.jstor.org

Research Databases

Internet search engines:

scholar.google.com
academic.live.com

21

On the dates and the agenda

- **Exam date not fixed yet.**
  - Please keep yourself updated!
  - Check the website of the examination office:

  https://www.wiwi.uni-frankfurt.de/studium/service-beratung/pruefungsamt/service-und-kontakt.html
- **Course agenda is online.**
  - Please keep yourself updated!
  - Check the website of the course: https://m-chair.de/index.php?option=com_teaching&view=lecture&id=40

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

Electronic Business and Security

The New York Times

Facebook Security Breach Exposes Accounts of 50 Million Users

February 15, 2012, 2:14PM

Anonymous-Linked Attacks Hit US Stock Exchanges

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

theguardian

News | Sport | Comment | Culture | Business | Money | Life & style

News › World news › Edward Snowden

Everyone is under surveillance now, says whistleblower Edward Snowden

People's privacy is violated without any suspicion of wrongdoing, former National Security Agency contractor claims

March 5, 2012, 3:40PM

Hacker Group Breaches Library of Congress Site, Publishes Passwords

Bloomberg Our Company | Professional | Anywhere | QUEUE Microsoft

HOME | QUICK | NEWS | OPINION | MARKETS | PERSONAL FINANCE | TECH (NEW) | SUSTAINABILITY

Related News: Law · Asia · Japan · U.S. · Retail · Technology · Media

Sony Data Breach Exposes Users to Years of Identity-Theft Risk

theguardian

News | Sport | Comment | Culture | Business | Money | Lond

News › Technology › PlayStation

PlayStation Network hackers access data of 77 million users

Risks of Unprotected Market Activities

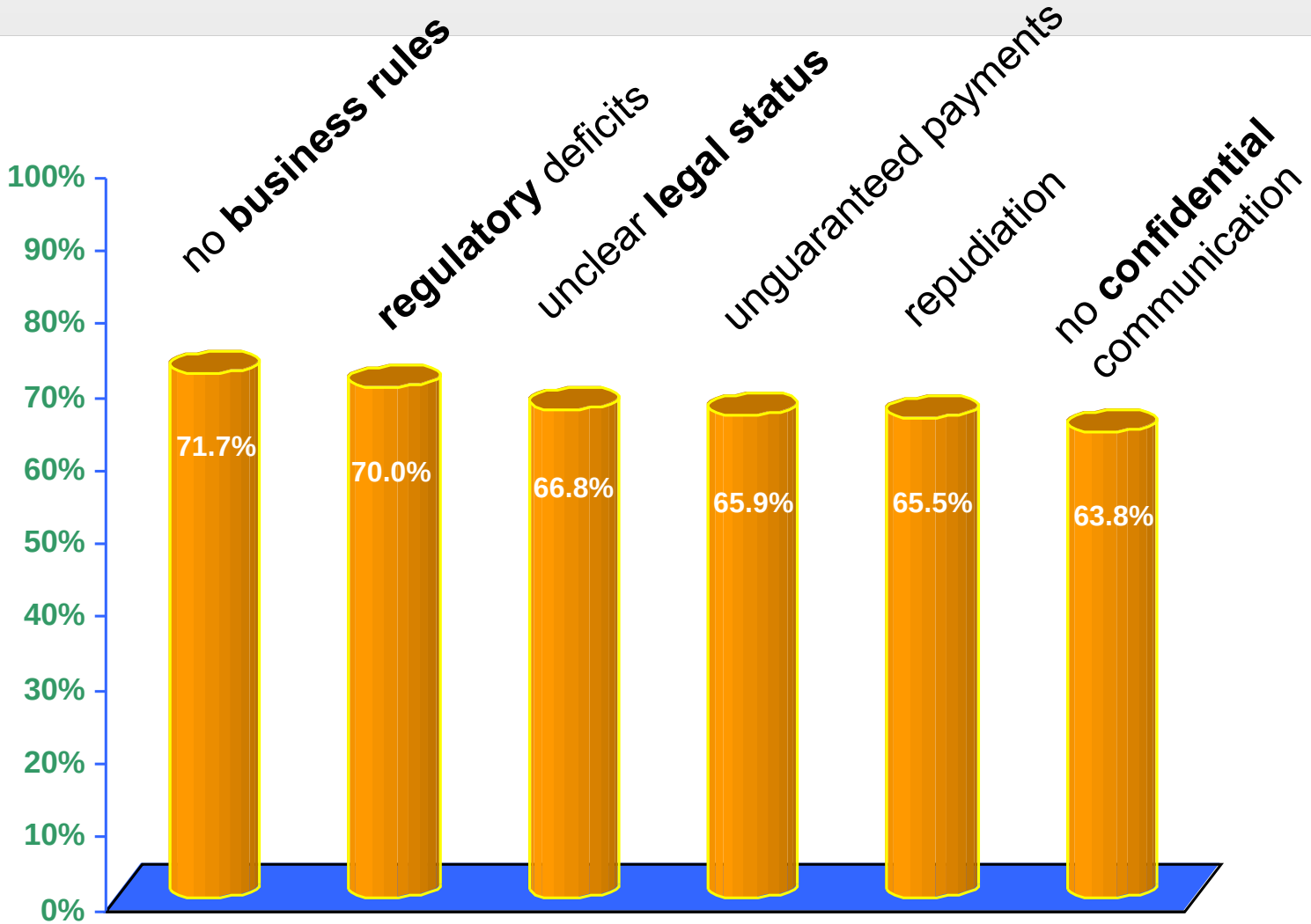
Provider

- No payment – debtor cannot be captured
- Wrong or fake orders
- Copyright violations
- www attacks
- Internal server intrusion
- …

Consumer

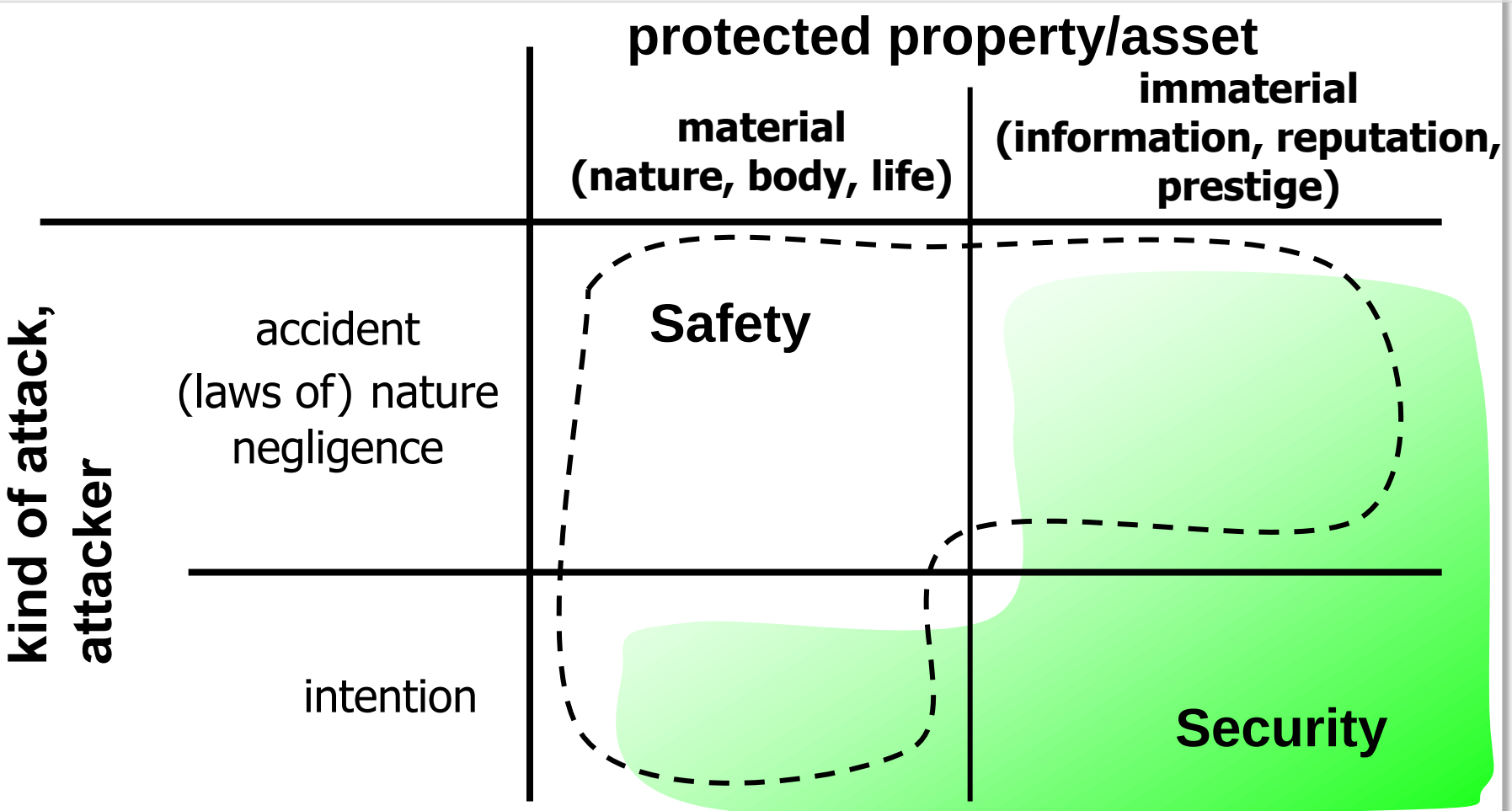
- Unwanted deliveries (false, not ordered, …)
- Unauthorized / unexpected direct debt of money, e.g. from a credit card account
- Unwanted advertising mail (“spamming”)
- Transparent consumers
- …

E-Commerce Requires Security



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

Security vs. Safety



mobile business

Security

A very human discrepancy

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

A 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 always accountable to responsible parties

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

Confidentiality

- ***Unauthorized acquisition of information*** = 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).
- Citizens (in smart cities) should not be monitored or tracked by default.

mobile business

Integrity

- ***Unauthorized modification*** of information = 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.
- Forging of electronic records can creates chaos in society – often discussed as informational warfare.
- Manipulation of traffic regulation and control in (smart) cities is a nuisance and can even be life-threatening.

mobile business

Availability

- ***Unauthorized impair of functionality*** = loss of **availability**:
- If a patient's medical record is accessible solely via one network and this network fails, when patient data is needed, this may be life-threatening for the patient.
- (Smart) cities have a major problem, if critical infrastructures for e.g. electricity distribution are not available anymore.

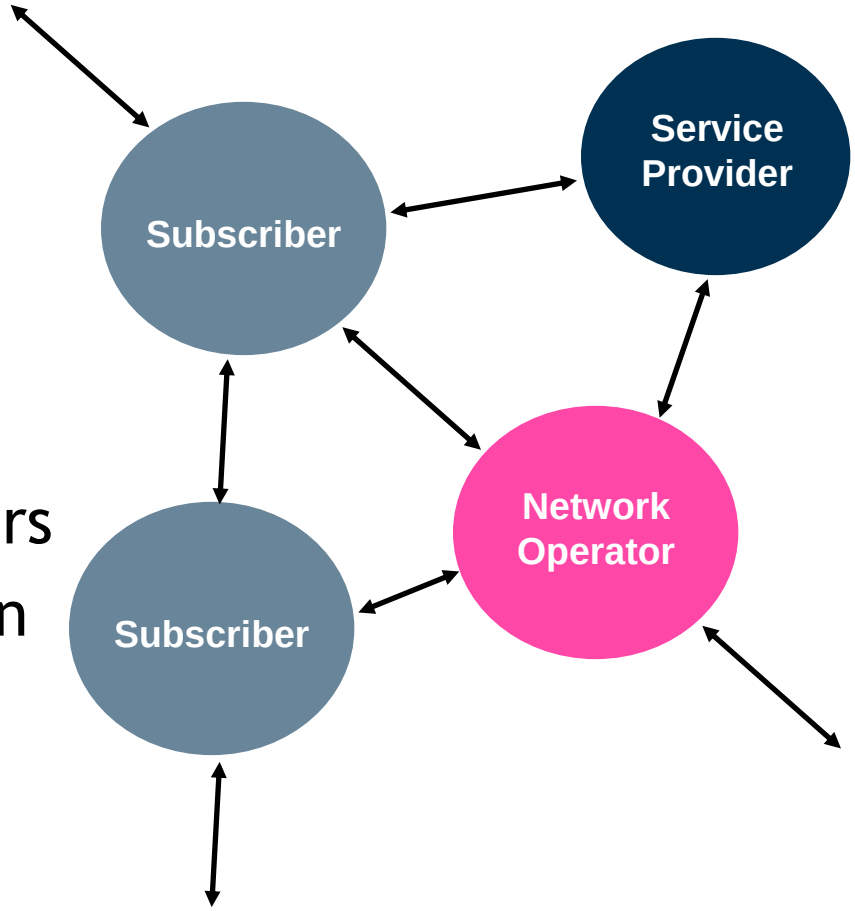
Accountability

- ***No responsible parties for actions*** = loss of accountability:
- If the persons liable for procedures in medical ICT systems (e.g. for the delivery of diagnoses, therapy instructions or billings) cannot be identified, unresponsible actions may occur.
- The consequences of a mistake may be worse for the injured party since it is unclear whom to ask for compensation.
- If (restrictive) measures (e.g. traffic suspension) taken in smart cities cannot be attributed to responsible parties ("the computer has decided") citizens lose trust.

Multilateral Security

Different Parties
with
different Interests

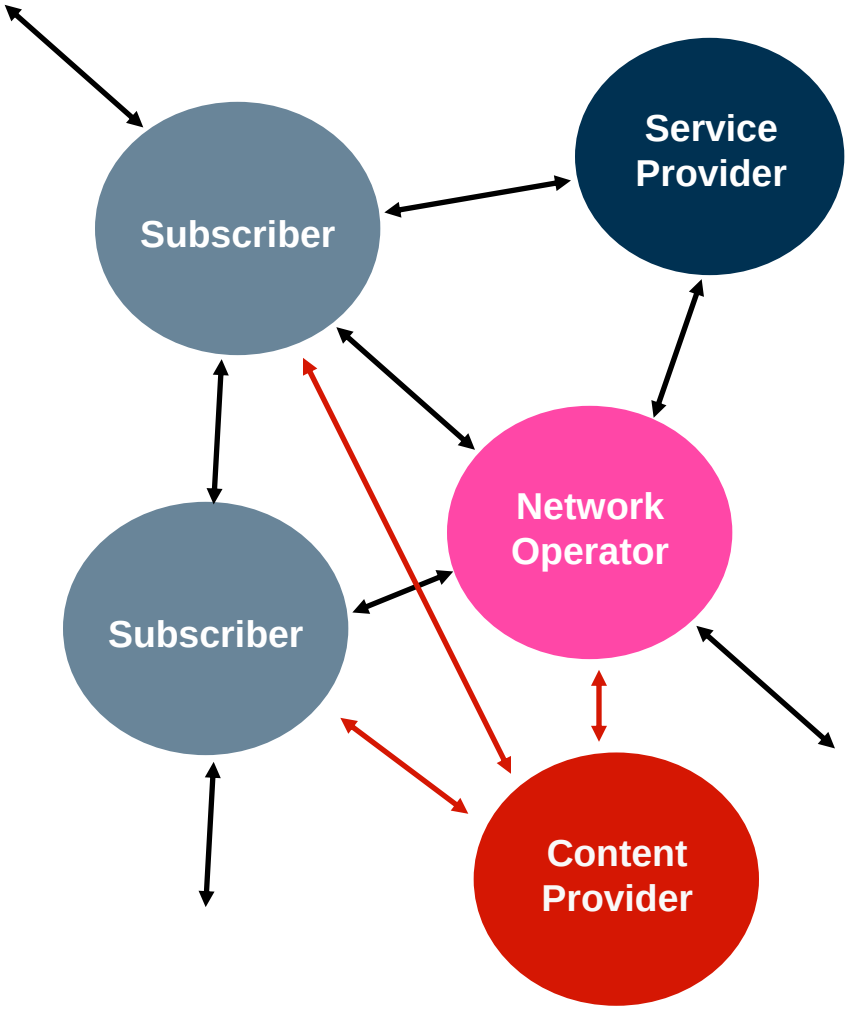
- Customers/Merchants
- Communication partners
- Citizens/Administration



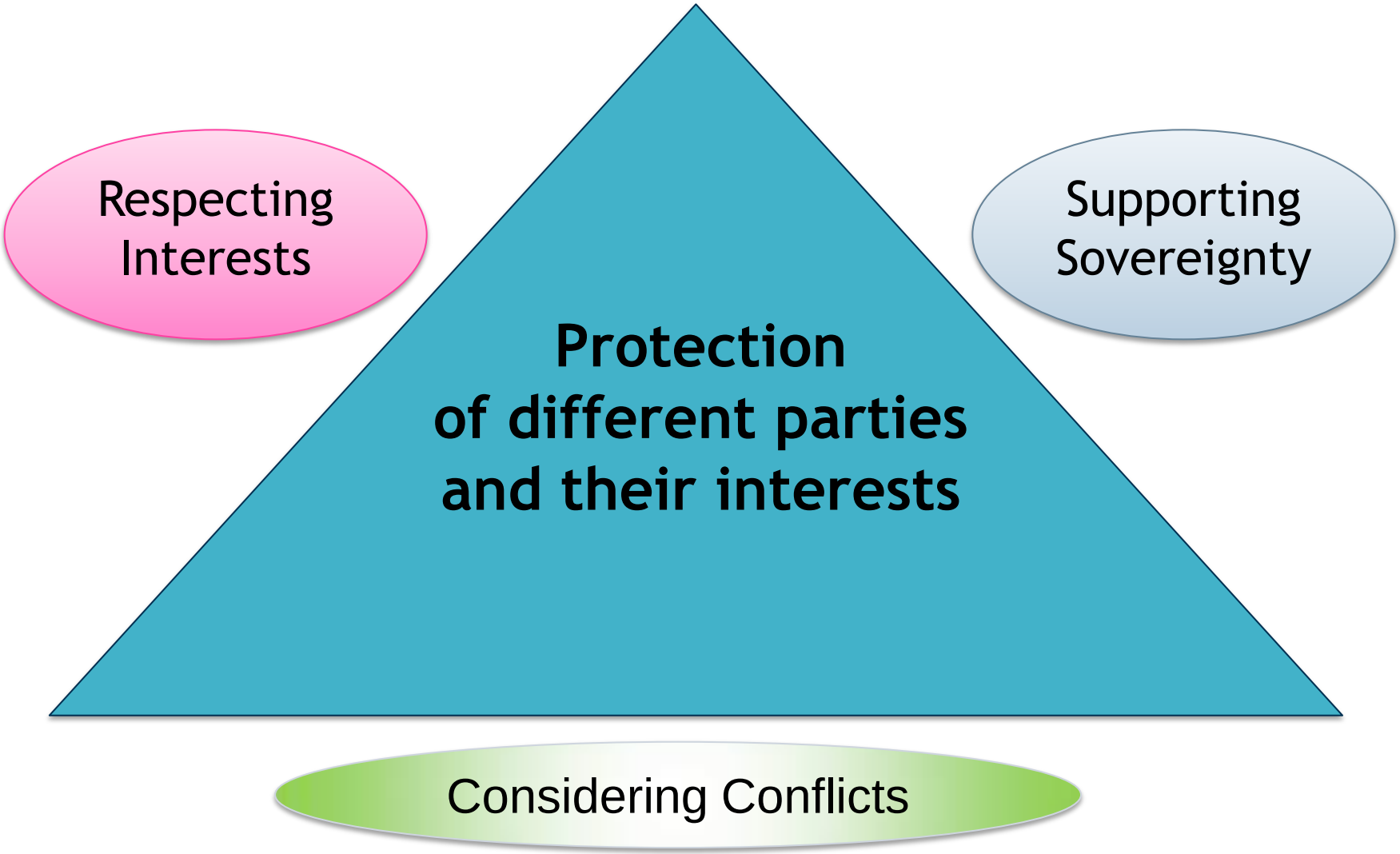
Multilateral Security

… 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

accept

or

deny

→ Reachability Management (RM)

Reachability Management

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

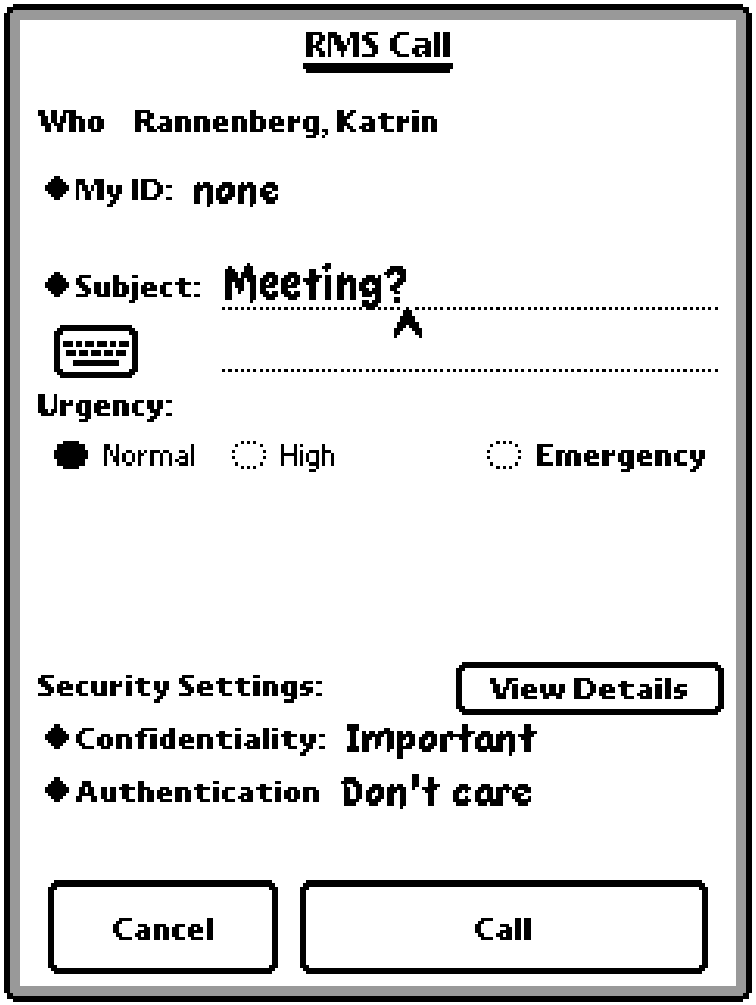
Call

Call

Negotiation

Topics of Negotiation

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



Why should your call go through?

Statement of urgency
- "It is really urgent!"

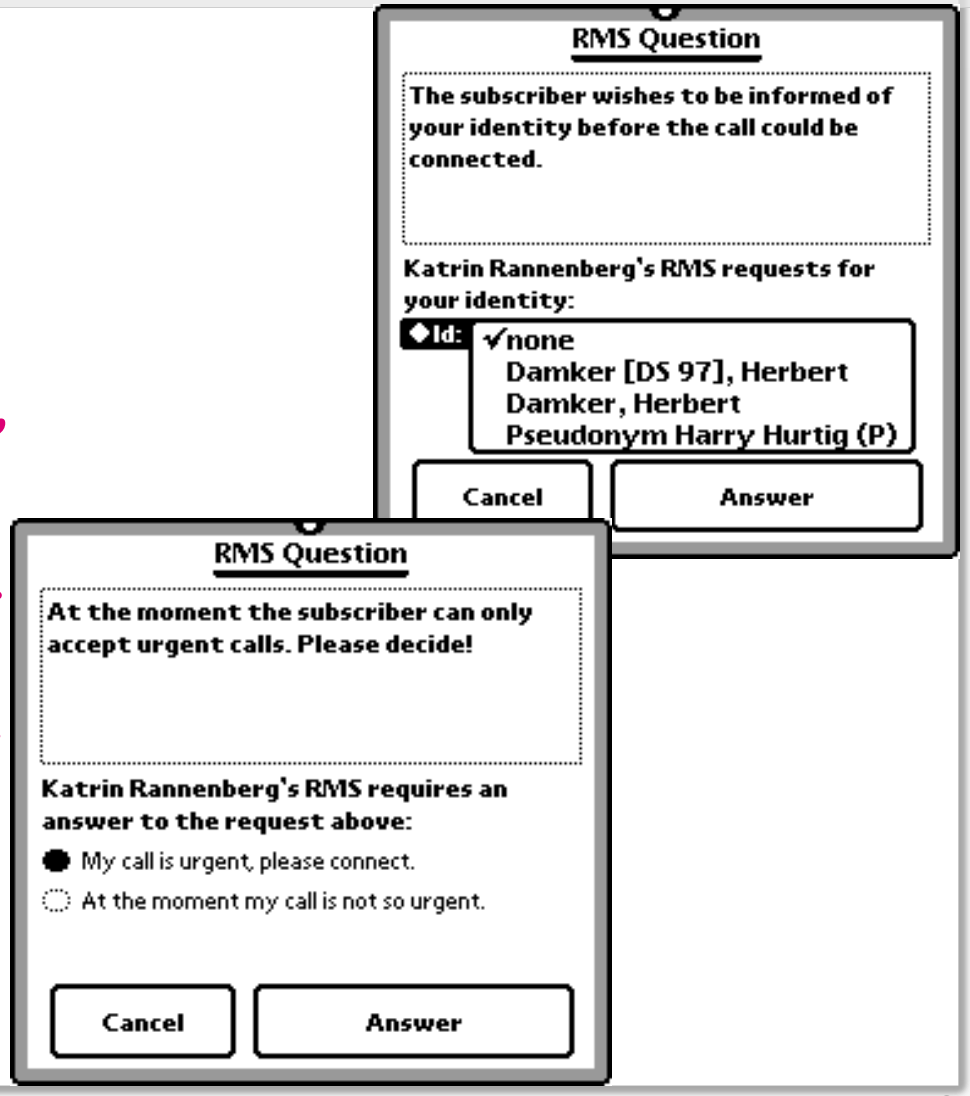
Specification of a function
- "I am your boss!"

Specification of a subject
- "Let's have a party tonight."

Presentation of a voucher
- "I welcome you calling back.

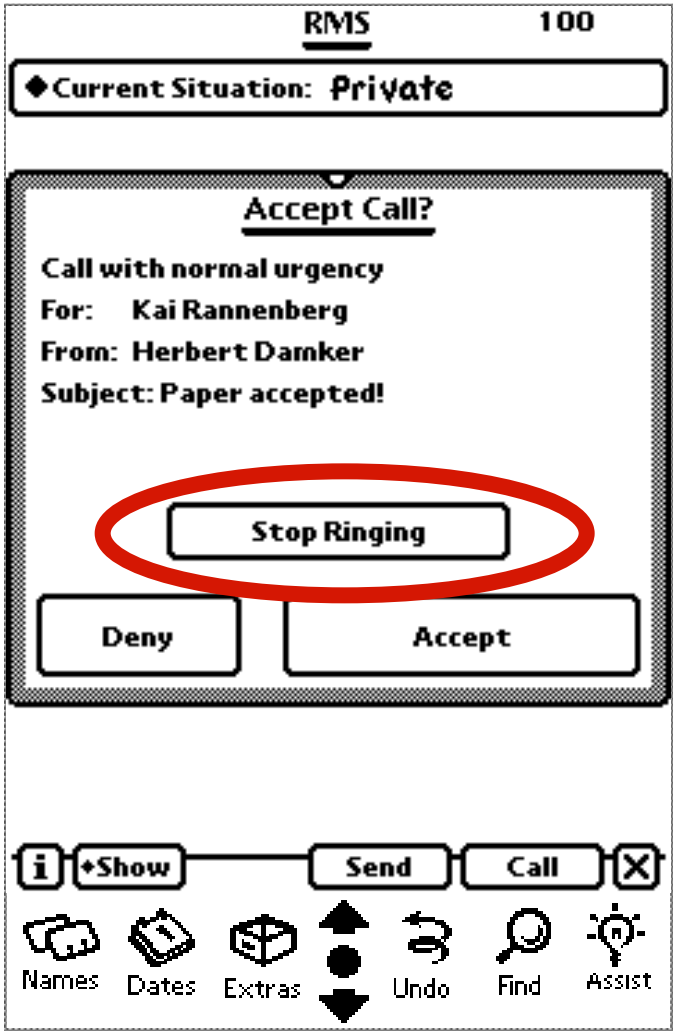
Provision of a reference
- "My friends are your friends!

Offering a surety
- "Satisfaction guaranteed or this money is yours!"



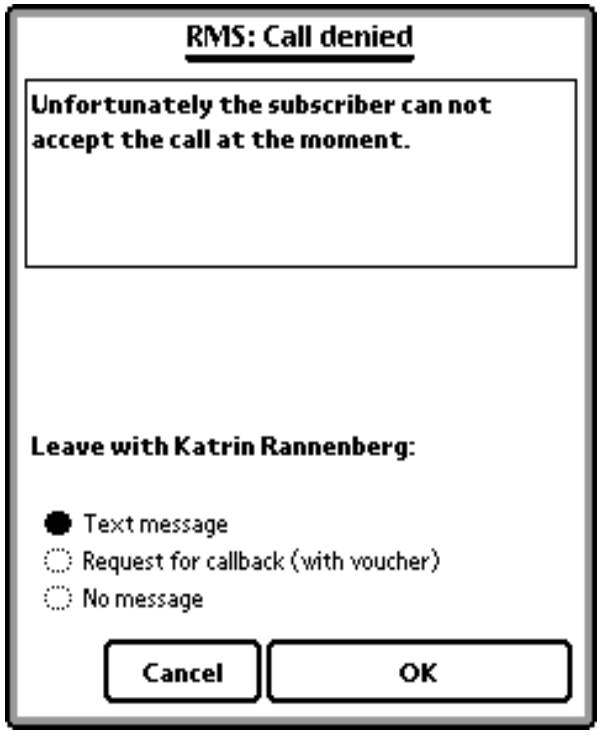
RMS accepted call (Callee display)

- 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



Configuring your RMS

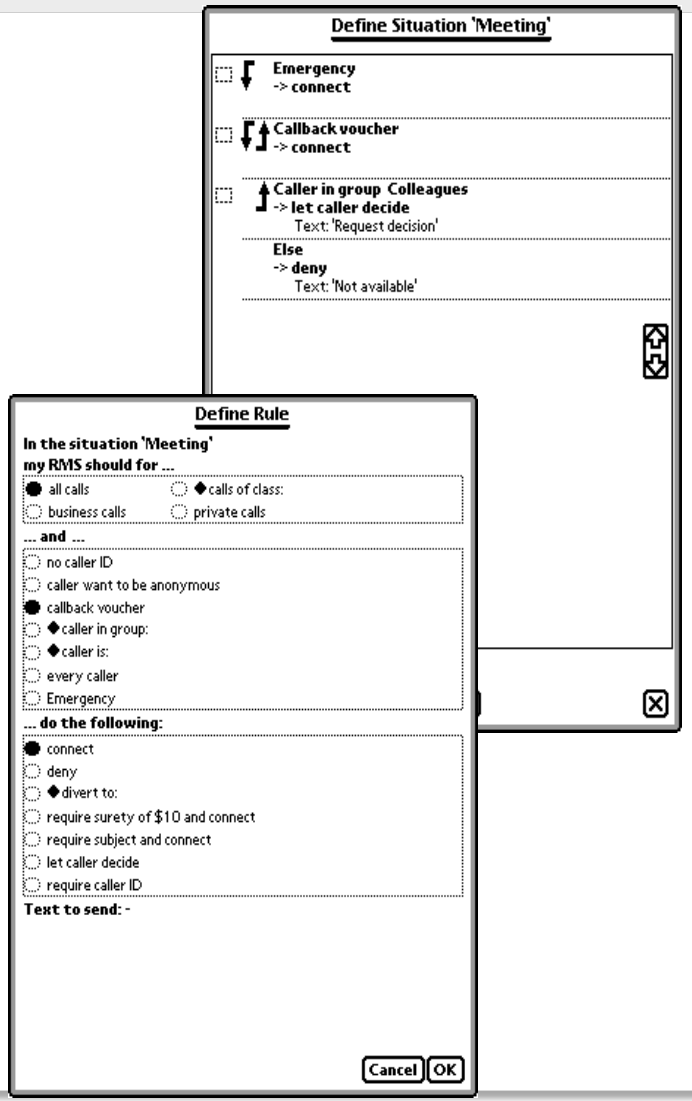
Situations

Set of rules how to deal with an incoming call

Rules

Combination of features

Users can reconfigure initial rules and situations as they like.



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**

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

Lectures and Exercises

Outline of this course

16. Okt 18	Lecture	Introduction
17. Okt 18	Lecture	Authentication
24. Okt 18	Exercise	Authentication
30. Okt 18	Lecture	Access Control
31. Okt 18	Lecture	Cryptography I
07. Nov 18	Lecture	Guest Lecture
13. Nov 18	Lecture	Electronic Signatures
14. Nov 18	Lecture	Guest Lecture by Jürgen Kühn (SVA System Vertrieb Alexander)
21. Nov 18	Exercise	Access Control
27. Nov 18	Lecture	Cryptography II
28. Nov 18	Lecture	Identity Management
05. Dez 18	Lecture	Guest Lecture by Amir Neziri (Deutsche Bank)
11. Dez 18	Lecture	Privacy Protection I
12. Dez 18	Exercise	Cryptography I
17. Dez 18	Lecture	Privacy Protection II
19. Dez 18	Exercise	Cryptography II
16. Jan 19	Lecture	Computer System Security
28. Jan 19	Lecture	Network Security I
30. Jan 19	Lecture	Network Security II
05. Feb 19	Lecture	Security Engineering
06. Feb 19	Lecture	Evaluation Criteria
13. Feb 19	Exercise	Exam prep and wrap up