

# Information & Communication Security (SS 2022)

## Introduction

**Prof. Dr. Kai Rannenberg,**

Chair of Mobile Business & Multilateral Security  
Goethe University Frankfurt

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

## Business Informatics @ Goethe University Frankfurt

<b>E-Finance</b>  Prof. Dr. Peter Gomber	<b>Business Informatics (Informatics)</b>  Prof. Dr. Mirjam Minor	<b>Information Systems Engineering</b>  Prof. Dr. Roland Holten
<b>Business Education (associated)</b>  Prof. Dr. Gerhard Minnameier	<b>Mobile Business &amp; Multilateral Security</b>  Prof. Dr. Kai Rannenberg	<b>Business Education (associated)</b>  Prof. Dr. Eveline Wuttke
<b>Information Systems &amp; Information Management</b>  Prof. Dr. Wolfgang König	<b>Business Informatics &amp; Microeconomics</b>  Prof. Dr. Lukas Wiewiorra	<b>Business Informatics &amp; Information Management</b>  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, 2<sup>nd</sup> Floor

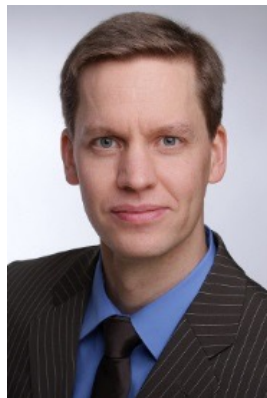
Phone: +49 69 798 34701  
Fax: +49 69 798 35004  
e-mail: [info@m-chair.de](mailto:info@m-chair.de)

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





Kai Rannenberg



Sebastian  
Pape



Narges  
Arastouei



Welderufael  
Tesfay



David  
Harborth



Frédéric  
Tronnier



Ahad  
Niknia



Sascha  
Löbner



Ann-Kristin  
Lieberknecht



Peter  
Hamm

# 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



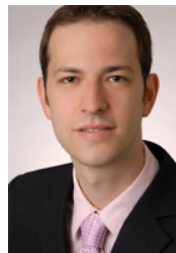
Tim  
Schiller



Niels  
Johannsen



Stephan  
Heim



Marvin  
Hegen



Fatbardh  
Veseli



Majid  
Hatamian



Michael  
Schmid



Christopher  
Schmitz



## Office:

Diana Weiß

Office Hours: Mo.-Fr. 09:00-15:00

RuW Building, Office 2.257

Email: [diana.weiss@m-chair.de](mailto:diana.weiss@m-chair.de)



## 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 at Goethe University Frankfurt at the Faculty of Business and Economics (FB02)
- Since 2012-04 Visiting Professor at the National Institute for Informatics (Tokyo, Japan)
- Since 2020-07 Professor, by courtesy, Goethe University Frankfurt at the Faculty of Computer Science and Mathematics (FB12)

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

	SS 2022	WS2022/2023
Bachelor		<i>Course</i> <b>Business Informatics 2 (PWIN)</b>
Master	<i>Course</i> <b>Information &amp; Communication Security:            Infrastructures, Technologies and            Business Models</b> <i>Course</i> <b>Mobile Business II:            Application Design, Applications,            Infrastructures and Security</b> <i>Course</i> <b>Privacy vs. Data:            Business Models in the digital, mobile            Economy</b> <i>Seminar</i> <b>Privacy Analysis in Cloud Services</b>	<i>Seminar</i> <b>Tba</b> <i>Course</i> <b>Mobile Business I:            Technology, Markets, Platforms, and            Business Models</b>

## Teaching Topics

Identity Management

Privacy

ICT Security

Mobile Business

Business Informatics

## Master Courses

### Lectures

Mobile Business 1

Privacy vs. Data

Seminars

Mobile Business 2

Master Thesis

I & C Security

## Bachelor Courses

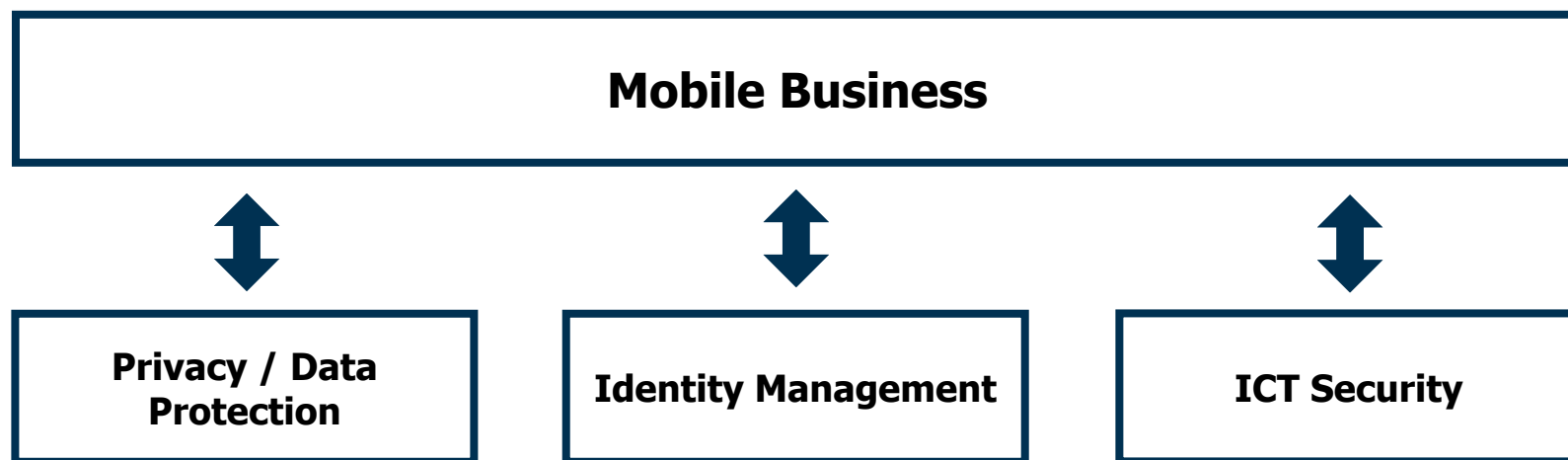
### Lectures

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

Chair of  
Mobile Business & Multilateral Security

Standardization & Regulation

M

*Mobile  
Business II*

Business Models

ICT Security

Mobile Business

Social Media/Marketing

Privacy/Data Protection

Multilateral Security

M

*Mobile  
Business I*

Applications & Services

Identity Management

*Information &  
Communication  
Security*

M

Online/Mobile Economy

Information & Communication Technology

B

**Bachelor**

M

**Master**

B

*Wirtschaftsinformatik 2  
(Business Informatics 2)*

- **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



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



**Dr. David Harborth**

RuW Building, Office 2.233

Email: [david.harborth@m-chair.de](mailto:david.harborth@m-chair.de)



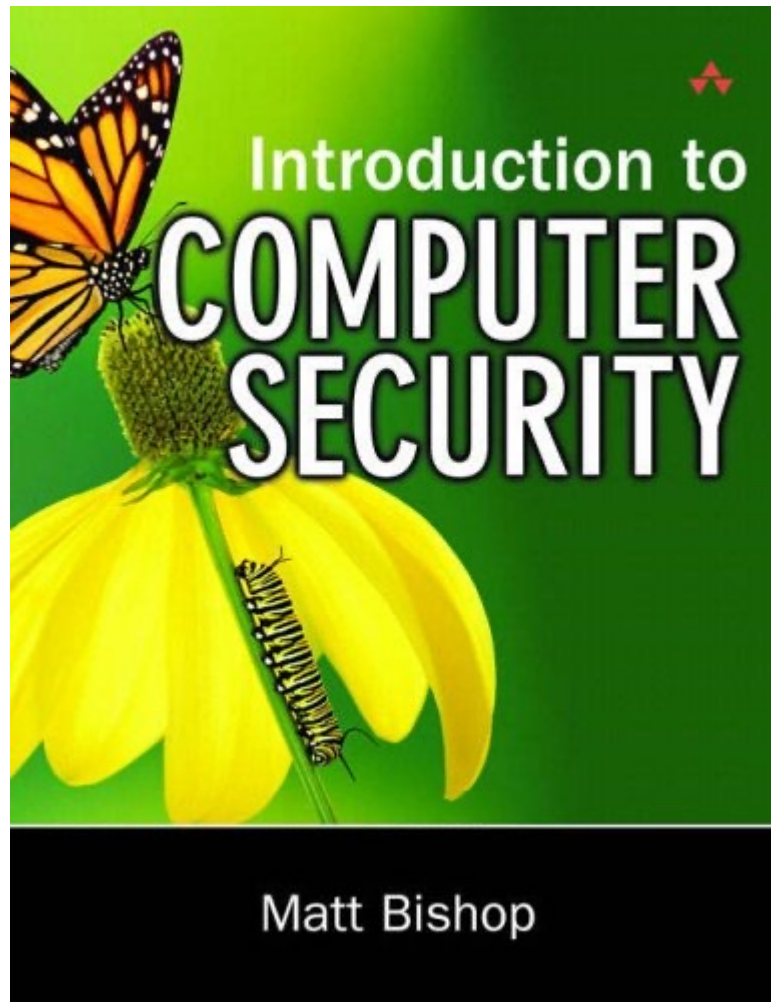
**Sascha Löbner, M.Sc.**

RuW Building, Office 2.236

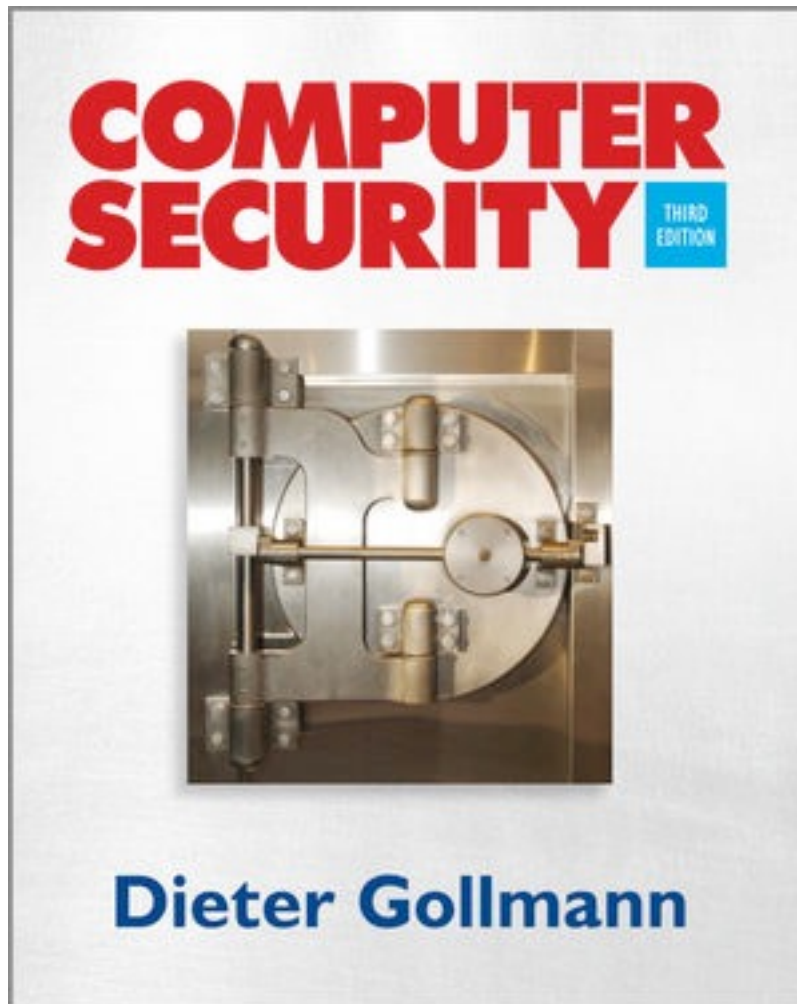
Email: [sascha.loebner@m-chair.de](mailto:sascha.loebner@m-chair.de)



**[security@m-chair.de](mailto:security@m-chair.de)**



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



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



In German:

Claudia Eckert:

IT-Sicherheit

Oldenbourg

ISBN: 978-3-11-055158-7

## 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](http://www.ub.uni-frankfurt.de/login.html)



[search.epnet.com/login.asp](http://search.epnet.com/login.asp)  
[www.jstor.org](http://www.jstor.org)



Internet search engines:

[academic.live.com](http://academic.live.com)  
[scholar.google.com](http://scholar.google.com)



# On the dates and the agenda

- **Exam date and regulations not fixed yet.**
  - Please keep yourself updated!
  - Check the website of the examination office:  
<https://www.wiwi.uni-frankfurt.de/en/study/services/examination-office/service-and-contact.html>
- **Course agenda is online.**
  - Please keep yourself updated!
  - Check the website of the course:  
[https://www.m-chair.de/index.php?option=com\\_teaching&view=lecture&id=67](https://www.m-chair.de/index.php?option=com_teaching&view=lecture&id=67)



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

The New York Times

## Facebook Security Breach Exposes Accounts of 50 Million Users

Sept. 28, 2018

February 15, 2012, 2:14PM

## Anonymous-Linked Attacks Hit US Stock Exchanges

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

bitkom

German businesses under attack: losses of more than 220 billion euros per year

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

The New York Times

## Security Gap Leaves 885 Million Mortgage Documents Exposed

May 24, 2019

BBC

Sign in

News

Sport

Reel

Worklife

Travel

Future

More

NEWS

## Facebook's Twitter and Instagram accounts hacked

8 February 2020

# Risks of Unprotected Market Activities

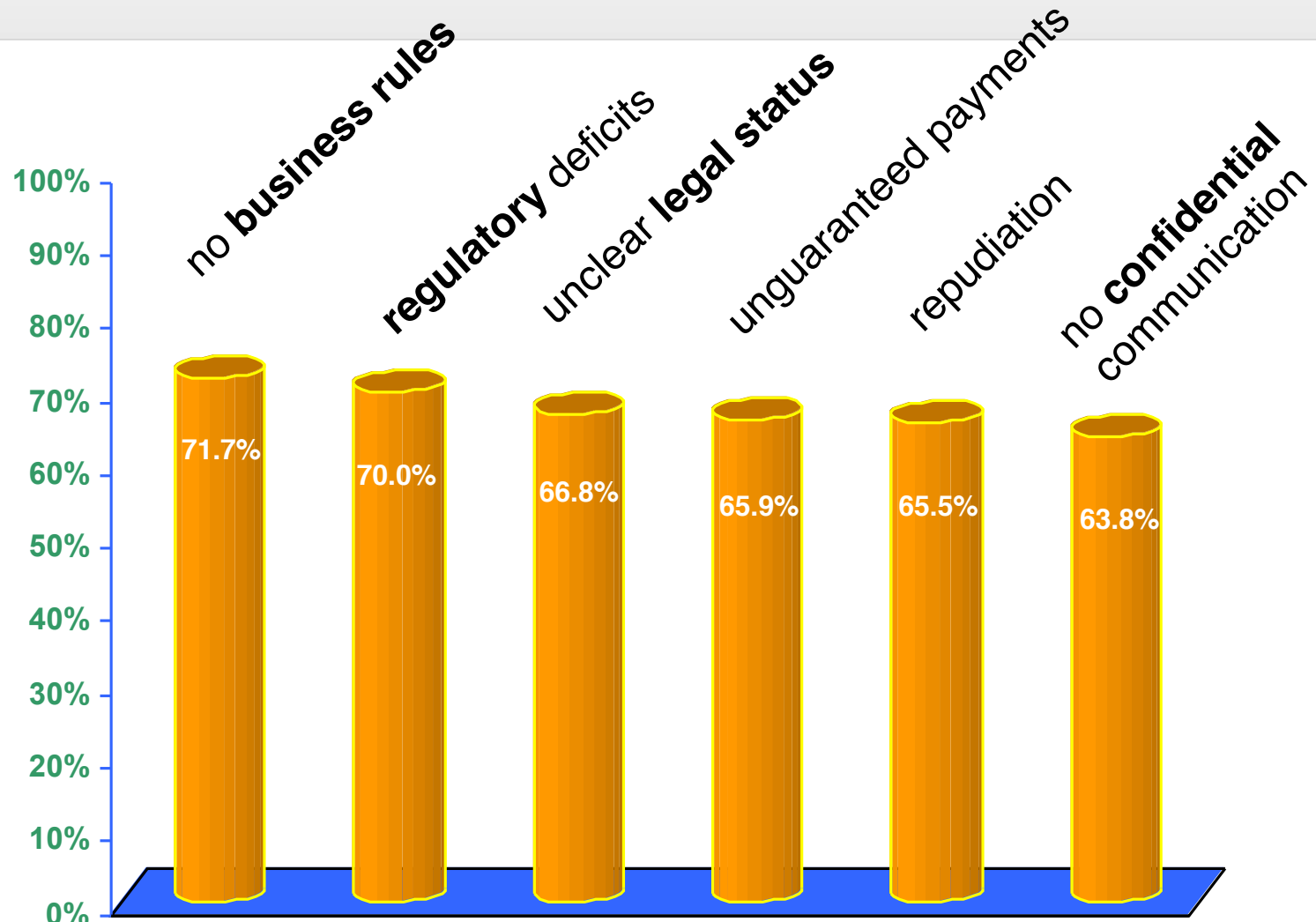
## Provider

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

## Consumer

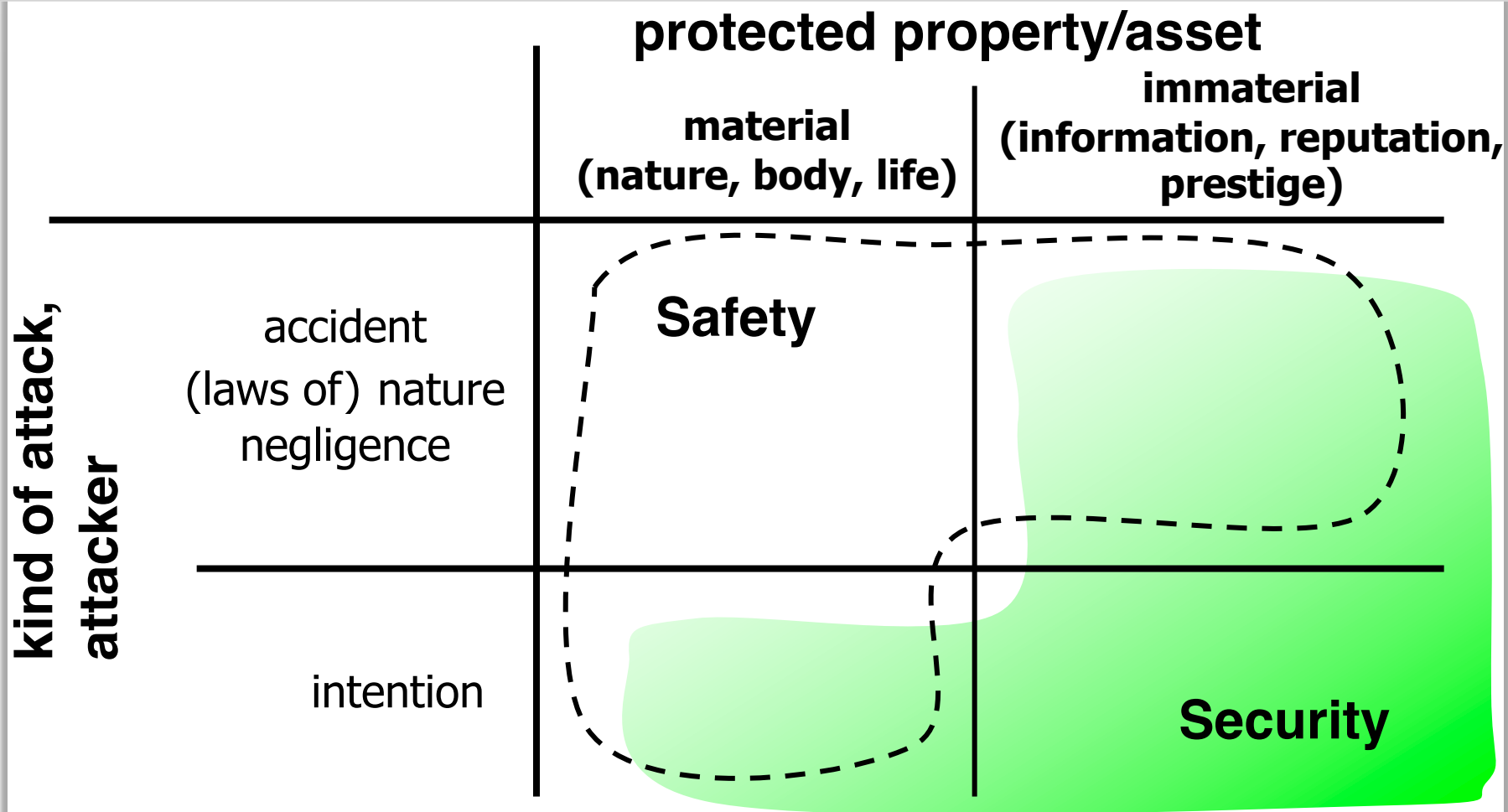
- Unwanted deliveries (false, not ordered, ...)
- Unauthorized / unexpected direct debt of money, e.g. from a credit card account
- Unwanted advertising mail ("spamming")
- Transparent consumers
- ...

# E-Commerce Requires Security



Source: Electronic Commerce Enquête, Universität Freiburg, 1998 [Schoder, Müller 1999]  
(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/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. [Rannenbergh 2000a]

- *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.



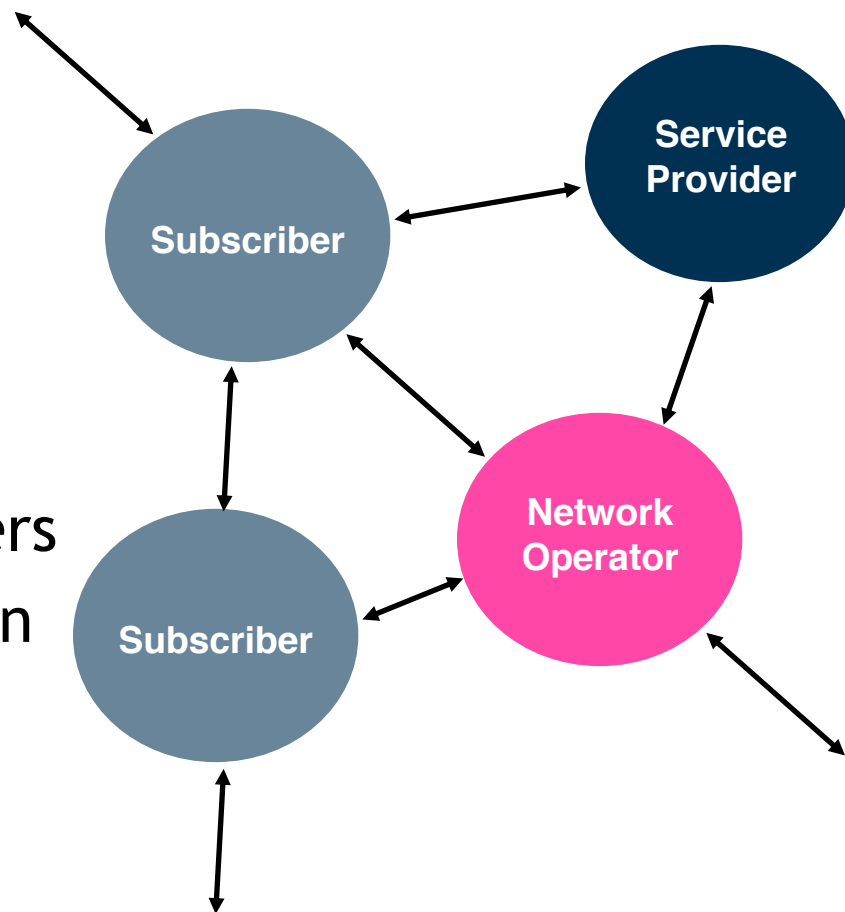
- *Unauthorized modification* of information = loss of **integrity**:
- Unauthorized and unobserved data modifications (e.g. a prescription, a medicament ordering or a dosage instruction) may lead to life-threatening consequences.
- Forging of electronic records can create chaos in society - often discussed as informational warfare.
- Manipulation of traffic regulation and control in (smart) cities is a nuisance and can even be life-threatening.

- *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.

- *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, irresponsible 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.

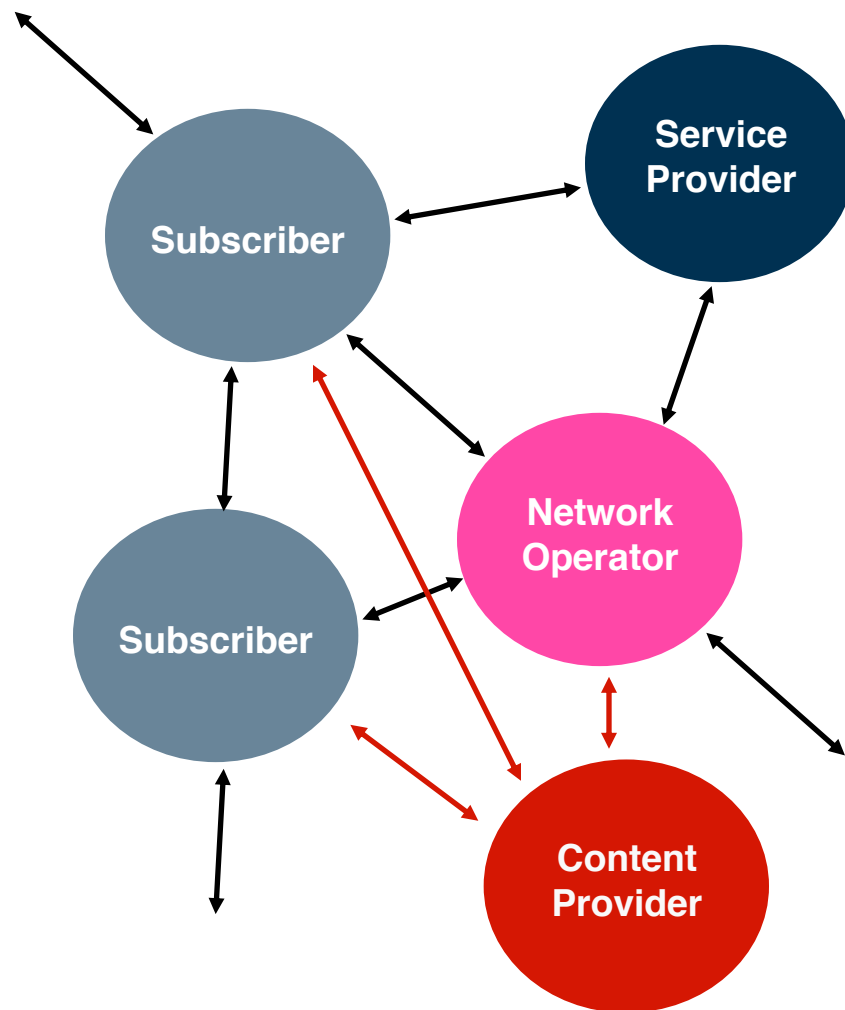
## Different Parties with different Interests

- Customers/Merchants
- Communication partners
- Citizens/Administration

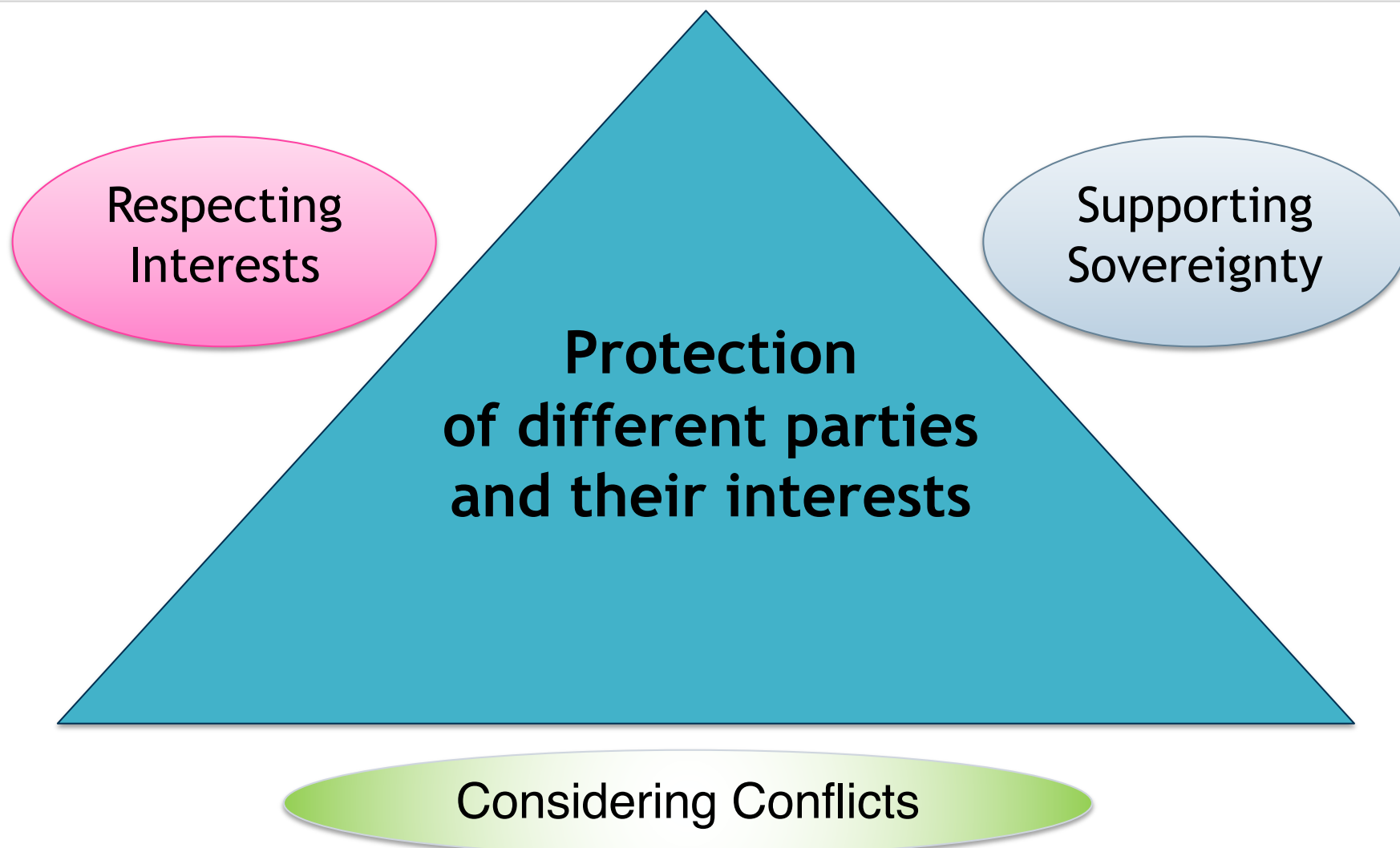


## ... in a world of consortia

- more partners
- more complex relations



# 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**



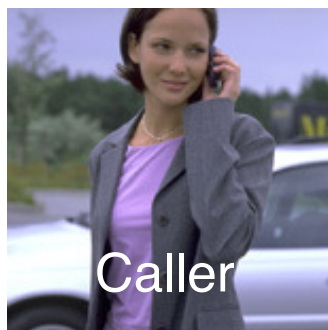
# Multilateral Security in daily communication

## The Challenge

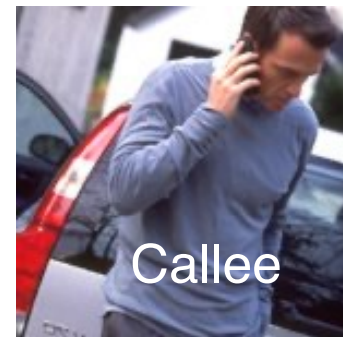
- Increased reachability due to new communication services
- Annoying calls
- Shortage of time
- Caller-ID conflict

→ Reachability Management (RM)

[Rannenbergh 2000b,c]



accept



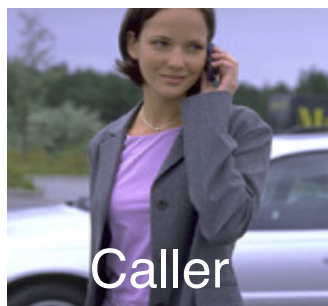
*or*

deny

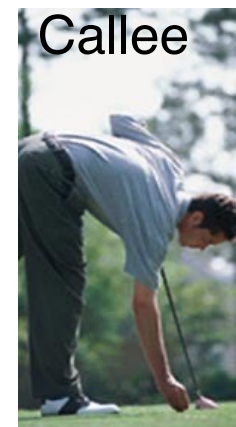


## The Features

- 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




Negotiation



# 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)

Cancel Answer

**RMS Question**

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

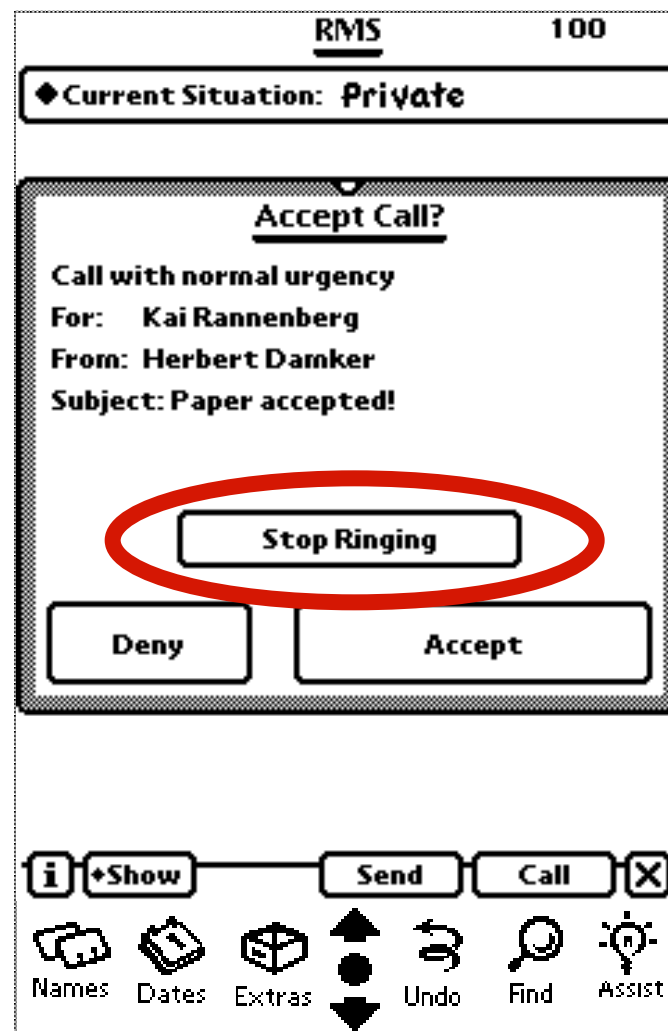
Katrin Rannenberg's RMS requires an answer to the request above:

☒ 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 Rannenberg:**

☒ Text message  
☐ Request for callback (with voucher)  
☐ No message

**Cancel** **OK**

# 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.

### Define Situation 'Meeting'

<input type="checkbox"/>	Emergency	-> connect
<input type="checkbox"/>	Callback voucher	-> connect
<input type="checkbox"/>	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 ...

<input checked="" type="radio"/> all calls	<input type="radio"/> calls of class:
<input type="radio"/> business calls	<input type="radio"/> private calls

... and ...

<input type="radio"/> no caller ID
<input type="radio"/> caller want to be anonymous
<input checked="" type="radio"/> callback voucher
<input checked="" type="radio"/> caller in group:
<input type="radio"/> caller is:
<input type="radio"/> every caller
<input type="radio"/> Emergency

do the following:

<input checked="" type="radio"/> connect
<input type="radio"/> deny
<input type="radio"/> divert to:
<input type="radio"/> require surety of \$10 and connect
<input type="radio"/> require subject and connect
<input type="radio"/> let caller decide
<input type="radio"/> require caller ID

Text to send: -

Cancel OK

## 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**

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

## Outline of this course

Date	Time	Session	Title
12.04.22	10:00-12:00	Lecture	Introduction
19.04.22	10:00-12:00	Lecture	Authentication
19.04.22	16:00-18:00	Lecture	Access Control
26.04.22	10:00-12:00	Lecture	Cryptography I
03.05.22	10:00-12:00	Lecture	Cryptography II
03.05.22	16:00-18:00	Exercise	Access Control
10.05.22	10:00-12:00	Lecture	Electronic Signatures
17.05.22	10:00-12:00	Lecture	Identity Management
17.05.22	16:00-18:00	Exercise	Authentication
24.05.22	10:00-12:00	Lecture	Privacy Protection I
31.05.22	10:00-12:00	Lecture	Privacy Protection II
31.05.22	16:00-18:00	GL1	TBA
07.06.22	10:00-12:00	Lecture	Computer System Security
14.06.22	10:00-12:00	GL2	Biometrics
14.06.22	16:00-18:00	Exercise	Cryptography
21.06.22	10:00-12:00	Lecture	Network Security I
28.06.22	10:00-12:00	GL3	Security Management
28.06.22	16:00-18:00	Exercise	Security Management
05.07.22	10:00-12:00	GL4	Security Management
12.07.22	10:00-12:00	Lecture	Network Security II
12.07.22	16:00-18:00	Lecture	Exam Prep and Wrap Up

- [FGGKMMRS 2014] Felix Freiling, Rüdiger Grimm, Karl-Erwin Großpietsch, Hubert B. Keller, Jürgen Mottok, Isabel Münch, Kai Rannenberg & Francesca Saglietti: Technische Sicherheit und Informationssicherheit, Unterschiede und Gemeinsamkeiten; Informatik-Spektrum, February 2014, Vol. 37, Issue 1, February 2014, pp. 14-24, DOI: 10.1007/s00287-013-0748-2; <https://fb-sicherheit.gi.de/fileadmin/FB/SICHERHEIT/AKBegriffsbildungIS-1-2014.pdf>
- [Rannenberg 2000a] Kai Rannenberg: Mehrseitige Sicherheit - Schutz für Unternehmen und ihre Partner im Internet; Wirtschaftsinformatik Volume 42, pp. 489-497 (2000), <https://link.springer.com/article/10.1007/BF03250765>
- [Rannenberg 2000b] Kai Rannenberg: Multilateral Security – A concept and examples for balanced security, pp. 151-162 in Proceedings of the 9th ACM New Security Paradigms Workshop 2000, September 19-21, 2000 Cork, Ireland; ACM Press; ISBN 1-58113-260-3, <https://m-chair.de/images/documents/publications/Rannenberg/p151-rannenberg.pdf>
- [Rannenberg 2000c] Kai Rannenberg: How much negotiation and detail can users handle?, pp. 37-54 in Frédéric Cuppens et al.: Computer security: Proceedings of the 6th European Symposium on Research in Computer Security; October 4-6, 2000, Toulouse, France; Lecture Notes in Computer Science 1895, Springer-Verlag; ISBN 3-540-41031-7, <https://m-chair.de/images/documents/publications/Rannenberg/ESORICS-f-1.7.mh.pdf>
- [Schoder, Müller 1999] Detlef Schoder, Günter Müller: Potentiale und Hürden des Electronic Commerce – Eine Momentaufnahme, Informatik-Spektrum Volume 22, pp. 252–260 (1999), <https://link.springer.com/article/10.1007/s002870050142>