HOCHSCHULE DEGGENDORF
University of Applied Sciences



Subjective Security and Safety

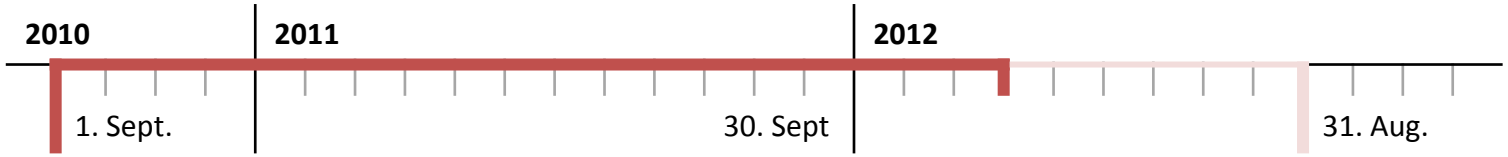
BPM as a Base for the Description of Security and Safety Objectives

Max Dirndorfer – Forschungsprojekt STERN

Projekt STERN

STERN

- "Sichere Teilnahme am elektronischen Rechtsverkehr für Notare"
  i.e. "Secure Partizipation in electronic legal Transactions for Notaries"
- Scope:



- Partners:

BNotK Bundesnotarkammer · Notarnet · Westernacher · Bayerisches Staatsministerium für Wissenschaft, Forschung und Kunst

STERN
www.stern-projekt.de

Goals of Project STERN

Main Goal is to facilitate and improve electronic communication for notaries

- Support to integrate central middleware
- Reference model for communication in the context of notaries
- Analysis of communication intensive processes
- Guarantee high software quality (software test)
  - Black and white box tests
  - Usability tests

STERN
www.stern-projekt.de

IT Security Costs Money

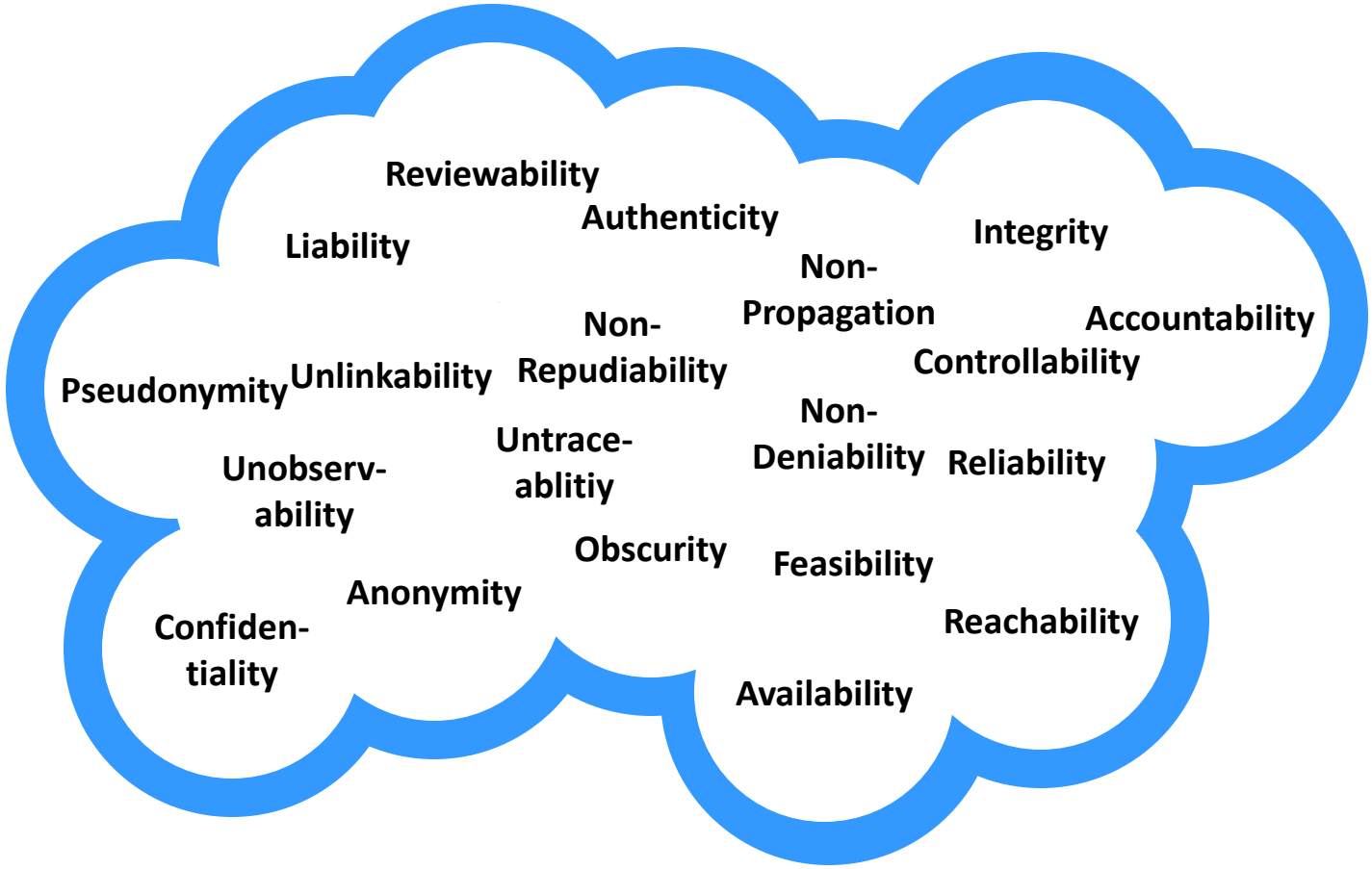
- To much security?
- Who decides about the proper amount of security?
- Wouldn‘t it be better, when the process involved subjects descide?

S-BPM

- Offers no possibility to define security goals
- Subjective view on business processes

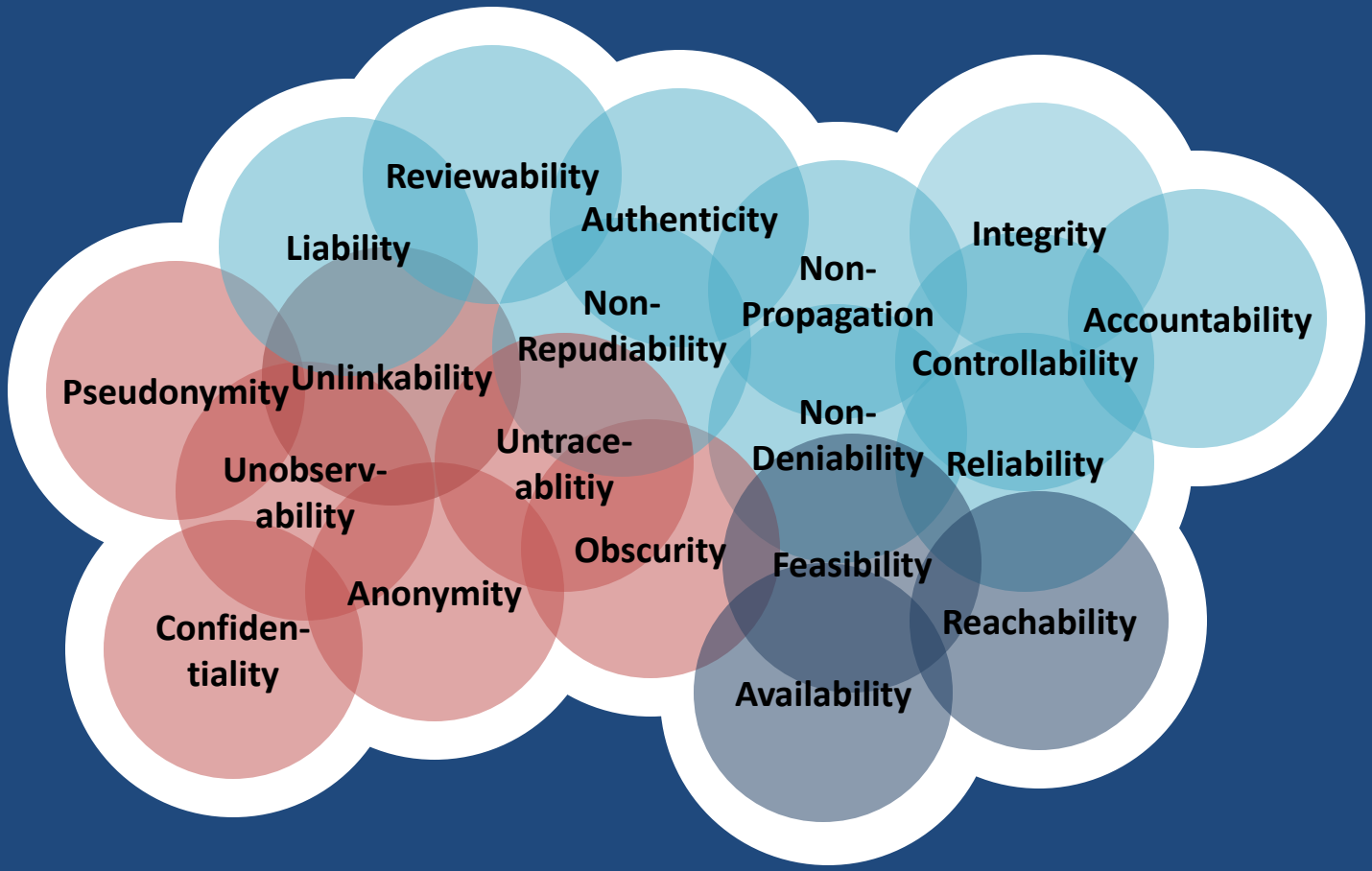
- Why not combining both parts?

Classification System For Security Goals



STERN
www.stern-projekt.de

Classification System For Security Goals



Classification System For Security Goals

Confidentiality: Anonymity, Pseudonymity, Obscurity, Unobservability, Untraceablitiy, Unlinkability

Integrity: Authenticity, Accountability, Non-Repudiability, Liability, Non-Deniability, Reviewability, Reliability, Controllability, Non-Propagation

Availability: Reachability, Feasibility

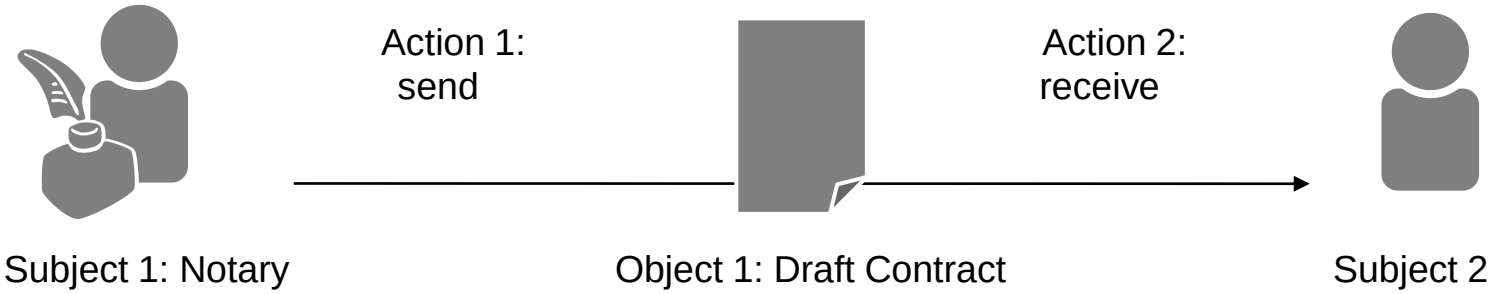
»*Anonymity of a subject means that the subject is not identifiable …*«
(Pfitzmann & Hansen 2010)

»*Wir sagen, dass ein System die Verbindlichkeit bzw. Zuordenbarkeit … gewährleistet, wenn es nicht möglich ist, dass ein Subjekt … die Durchführung einer … Aktion abstreiten kann*«
(Eckert 2012)

»*In access control module, the entities that can perform actions in the system are called subjects, and the entities representing resources to which access may need to be controlled are called objects.*«
(Zhu & Lee 2009)

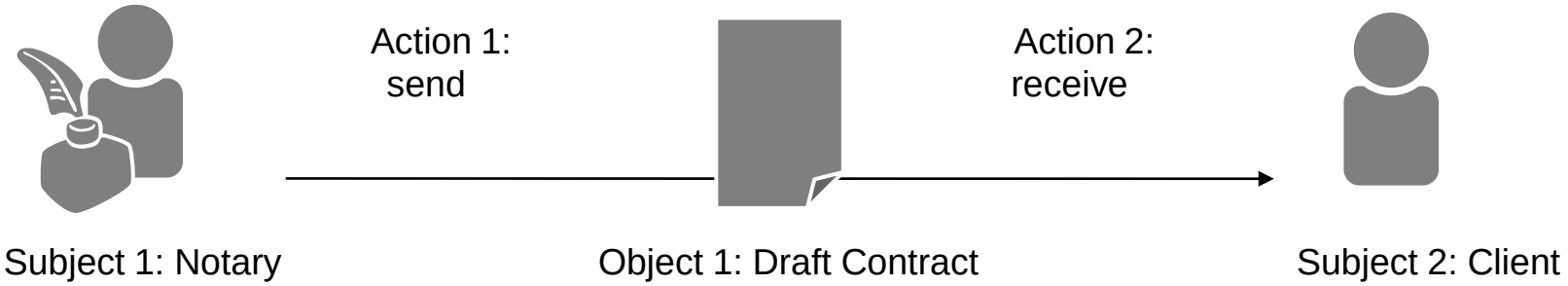
STERN
www.stern-projekt.de

OSA-CIA-Matrix



	Confidentiality	**Integrity**	**Availability**
Object (O)	Confidentiality	Integrity [, Non-Propa-gation]	Availability
Subject (S)	Anonymity [, Pseudonymity]	Authenticity	Reachability
Action (A)	Obscurity [, Unobservability, Untraceablitiy , Unlinkability]	Accountability [, Non-Repu-diability, Liability, Review-ability, Non-Propagation], Reliability [, Controllability]	Feasibility

STERN
www.stern-projekt.de

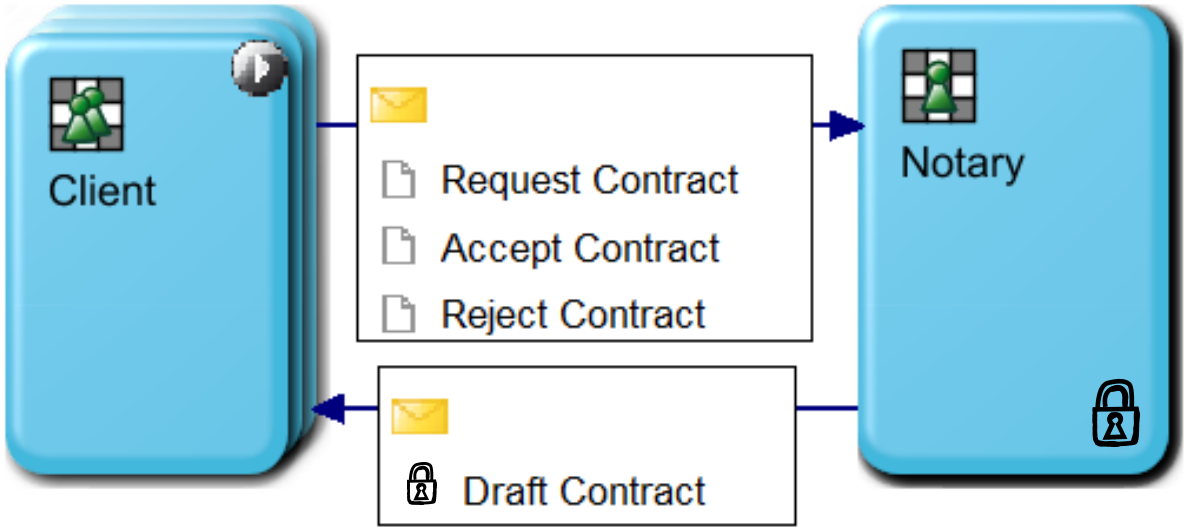


Confidentiality	Objects (Confidentiality)	Subjects (Anonymity)		Actions (Unobservability)	
View of subject:	Draft Contract	Notary	Client	Send	Receive
Notary	Internal	Public	Public	Internal	Internal
Client	Confidential	Public	Public	Internal	Internal

STERN
www.stern-projekt.de

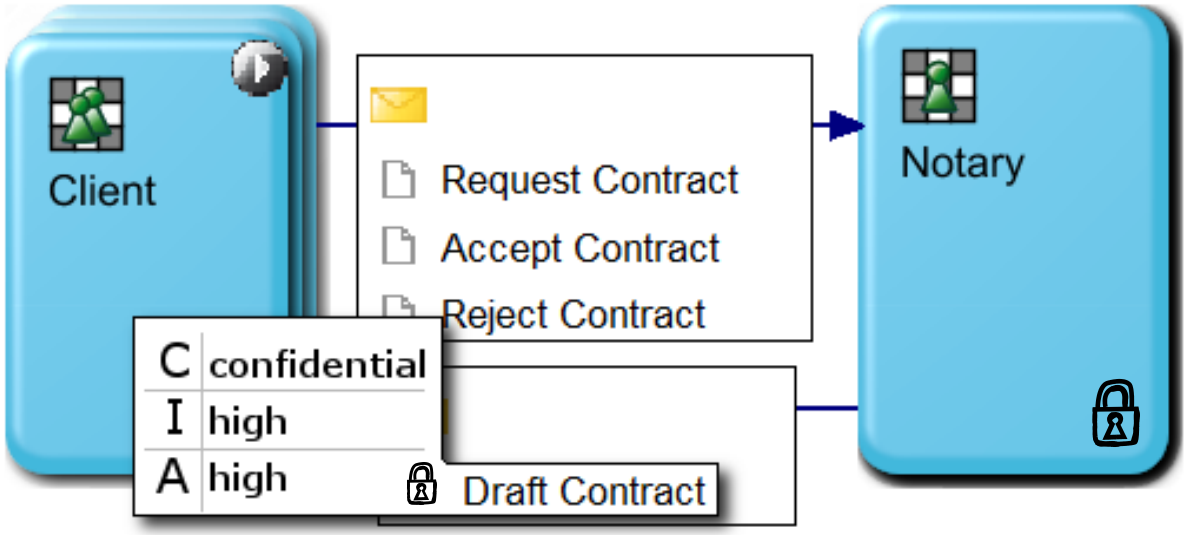
S-BPM

- Assign security requirements to each subject, object, and action of the S-BPM model.
- Rate these requirements using adequate scales.



S-BPM

- Assign security requirements to each subject, object, and action of the S-BPM model.
- Rate these requirements using adequate scales.



STERN
www.stern-projekt.de

Conclusion and Prospects

- Subjectoriented security concept
- Methode to describe security goals with S-BPM

- Concept has to be evaluated
- Concept could be used in workflow engine