03-IMAP-ISPS	**Informationssicherheit – Prozesse und Systeme**
	Information Security - Processes and Systems

Lehrform *(teaching format)* / **SWS** *(hours per week)*: 4K

Kreditpunkte *(credit points)*: 6

Turnus *(frequency)*: i.d.R. jedes SoSe

Inhaltliche Voraussetzungen *(content-related prior knowledge/skills)*: Informationssicherheit

Sprache *(language)*: Deutsch

Lehrende *(teaching staff)*: AG Rechnernetze (Prof. Dr. Carsten Bormann, Dr. Stefanie Gerdes)

Studiengang *(degree program)*	**Module**	**Semester**
Informatik (Master)	IMAP, IMAP-SQ	ab 1.Sem.
Digital Media (Master)	*Free Choice*	ab 1.Sem.
Systems Engineering I/II (Master)	M07-VT-ESS	ab 1./2.Sem.
Management Information Systems (Master)	MIS-INF2	ab 1.Sem.
Informatik (Bachelor)	(nur *Freie Wahl*)	
Zertifikatsstudium DiMePäd	DM in Lernumgebungen	ab 1.Sem.

Lernergebnisse: Studierende

- haben vertiefte Kenntnisse in der Sicherung komplexer soziotechnischer Systeme
- können komplexe kryptographische Sicherheitsprotokolle bewerten und in ihrem Einsatzbereich weiterentwickeln
- verstehen Sicherheit als Prozess mit ihren technischen und nicht-technischen Komponenten
- kennen wichtige Sicherheitsprozesse, so wie sie heute in ISMS eingesetzt werden, und können diese weiterentwickeln

Learning Outcome:

Inhalte:

Systeme:

1 Fortgeschrittene Anwendung von Kryptographie

- ECC und seine Varianten
- Lebenszyklus kryptographischer Verfahren; Stand aktueller Verfahren
- Zero-Knowledge-Protokolle, Zero-Knowledge-Password-Proof
- Zertifikate, Beweiswerterhaltung/LTANS
- Composability von Sicherheitsprotokollen
- Browserbasierte Sicherheitsprotokolle (SAML/Liberty, OpenID, OAuth)

2 Grundlagen manipulationssicherer Systeme (tamperproof systems)

Prozesse:

1 Softwaresicherheit

- Sicherheit im Software-Lifecycle
- Statische Analyse, Symbolic Execution, Fuzzers usw.

2 Security Management

- Awareness
- Incident-Response
- Logging/Auditing

3 Risk-Assessment

- Risiko-Wahrnehmung
- Qualitative und quantitative Modelle
- Insider-Threat-Modelle

4 Security Usability

- Usability als Sicherheitsfaktor
- Benutzbare Autorisierung

Contents:

Hinweise *(remarks)*: In der Tabelle sind nur die primären/spezifischsten Module aufgelistet, denen diese Veranstaltung zugeordnet ist.