Elective Subjects/ Semester 2,3 or 4:	
Title of the course	Identity and Access Management
Coordinator of the course:	Henning Olesen, Samant Khajuria
Objectives	**Students who complete the module:** **Knowledge** - Must be able to explain the concepts of security, privacy and trust - Must be able to explain the concepts of attributes, claims, assertion and claims-based identities - Must have knowledge about the principles and methods for access control, authentication, authorization and identification - Must be able to explain the key concepts and principles of identity management - Must have knowledge of key management, certificates, tokens and credentials - Must have knowledge about state-of-the-art principles and guidelines for protecting users privacy - Must have knowledge of state-of-the-art technologies and frameworks for fine-grained management of personal attributes - Must be able to understand the concepts of linkability and unlinkability and state-of-the-art principles for establishing trust - Must have knowledge about security architectures, including policies and policy management - Must have knowledge of national identity management frameworks such as NemID **Skills** - Must be able to discuss the differences between physical identities and online digital, virtual and partial identities - Must be able to identify the personal attributes that are needed to perform a given task - Must be able to apply methods for privacy protection, encryption, access control, authentication and authorization as a part of service development, including privacy by design principles - Must be apply to apply state-of-the-art technologies for realizing advanced services with privacy protection, e.g. OAuth and OpenID Connect - Must be able to analyse and design information flow and architectures for secure ICT services and solutions - Must be able to design applications and services incorporating security elements (e.g. payment, authentication), different assurance levels, and management of user identities (authentication, authorization, privacy protection) **Competencies** - Must have the competency to design secure services and security architectures with controlled exchange of attributes between stakeholders and minimal disclosure of personal information

	- Must be able to discuss and reflect on management of personal information for access to - resources and for personalization of services
Workload: ECTS	5 ECTS Credits

Important note

This syllabus describes the course as it was delivered in **Summer Semester 2016** Readers should note that courses of the DCLead programme are changed and adapted every year, also taking into consideration the feedback of the participants. This syllabus is for informational purposes only. The administration of the DCLead programme does not guarantee that the entirety of the information contained in this document clearly applies to any course that is delivered during another semester, also with the same title.