ASSURED IT SECURITY THROUGH EVALUATION AND CERTIFICATION

AF Security Seminar
University of Oslo 26th of May 2016

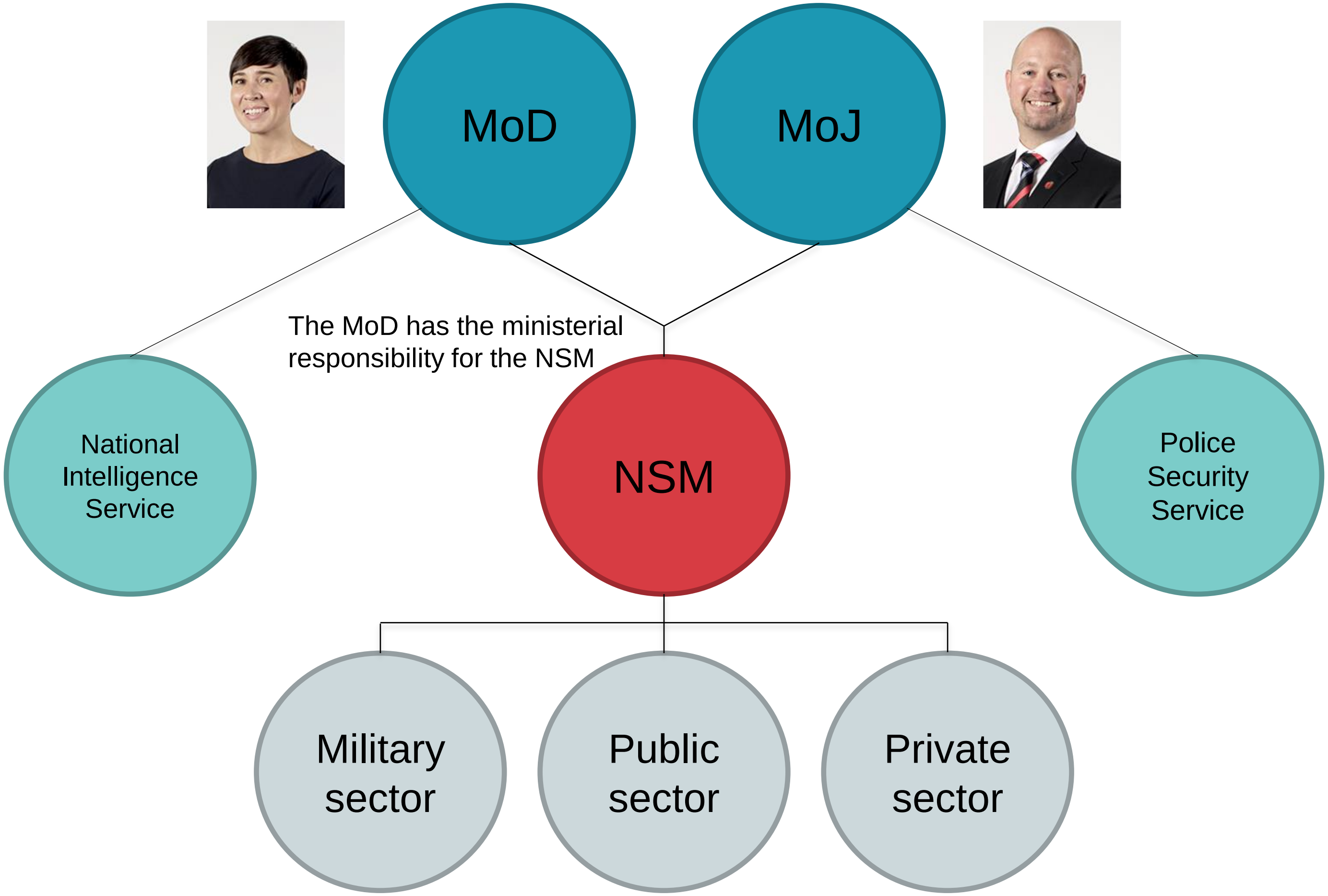
Helge Rager Furuseth
helge.furuseth@nsm.stat.no
post@sertit.no

Norwegian National Security Authority (NSM)

THE NORWEGIAN NATIONAL SECURITY AUTHORITY (NSM)

- Established as a Directorate under the Ministry of Defence and the Ministry of Justice and Public Security in 2003
- Norway's expert organ for information and physical security
- Regulatory body responsible for the Norwegian Security Act
- National Incident coordinator for ICT security
- Norwegian Computer Emergency Response Team (NorCERT)
- National Cryptology Authority
- The Norwegian Certification Authority For It-security

NATIONAL ORGANIZATION



MoD

MoJ

The MoD has the ministerial responsibility for the NSM

National Intelligence Service

NSM

Police Security Service

Military sector

Public sector

Private sector

THE NORWEGIAN NATIONAL SECURITY AUTHORITY

- Headquarters at Kolsås Base

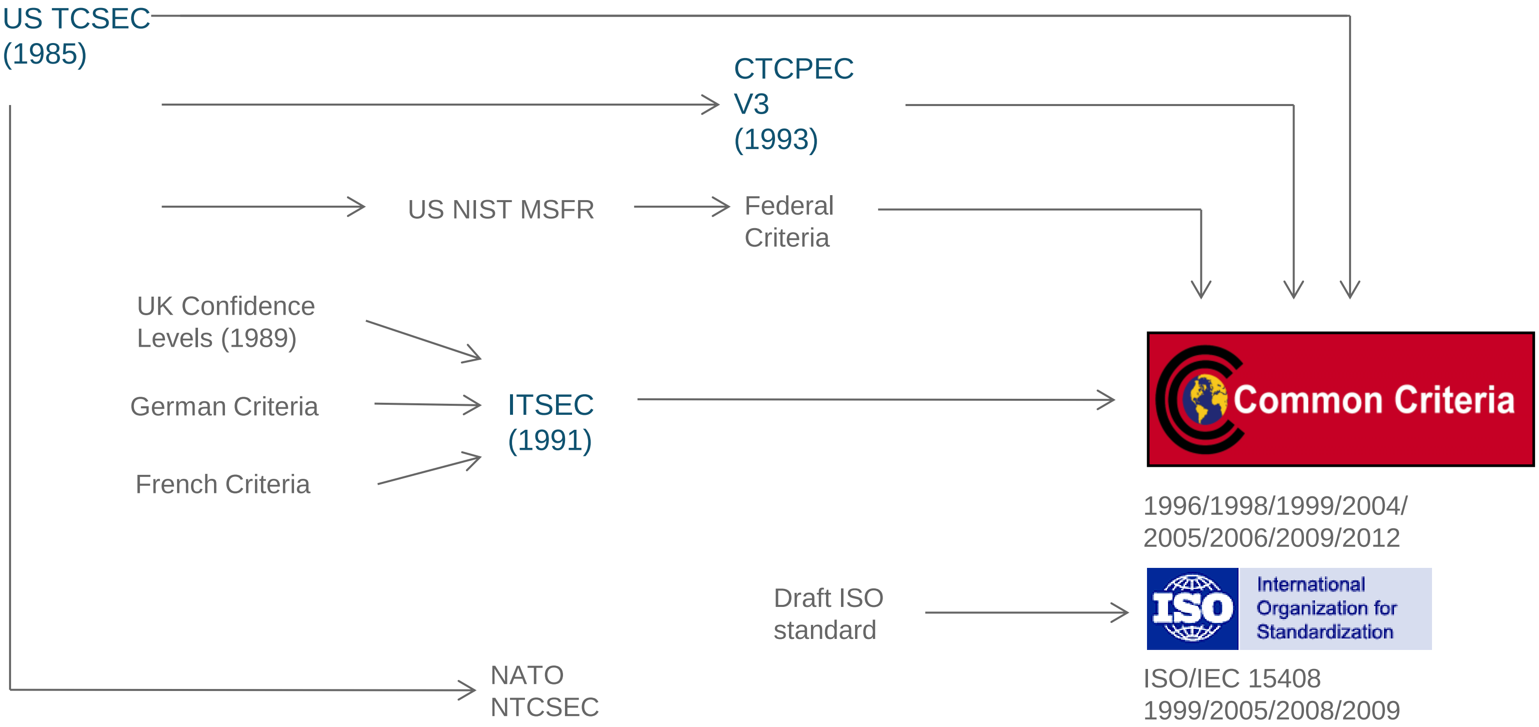
- Offices in Sandvika and Oslo

THE NORWEGIAN CERTIFICATION AUTHORITY FOR IT-SECURITY (SERTIT)

SERTIT

- The official Norwegian Certification Scheme for ICT-security
- Neutral third party
- Established in 2000
- Part of Norwegian National Security Authority (NSM)
- Common Criteria (ISO/IEC 15408)
- 4 approved IT Security Evaluation Facilities (ITSEFs)

COMMON CRITERIA STANDARD - DEVELOPMENT



1996/1998/1999/2004/ 2005/2006/2009/2012

ISO/IEC 15408 1999/2005/2008/2009

EVALUATION OF IT-SECURITY

- There are at least three approaches to the evaluation of IT security:
  - The first approach is to trust in the supplier's assurances
  - The second approach is to conduct one's own tests and evaluations
  - The third approach is to assign the task of assessing the product to an independent third party with the necessary competence
- The purpose of the Norwegian Certification Scheme is to provide services that support the third approach.
- Evaluation results shall be:
  - Provided on basis of unbiased judgement
  - Repeatable and reproducible
  - Complete and technical correctness
- A certificate is issued on the basis of the evaluation.

PRINCIPLES FOR THE CERTIFICATION SCHEME

- The Scheme is open and accessible for any applicants
- Evaluation and Certification shall take place in an impartial and cost-effective way
- The security evaluation is performed by approved evaluation facilities which operates according to regular business principles
- SERTIT approves and oversees the evaluation facilities
- SERTIT decides whether a TOE is appropriate for certification
- Certificates satisfying the criteria under CCRA or SOGIS MRA are offered mutual recognition

MUTUAL RECOGNITION

- Arrangement on the Recognition of the Common Criteria Certificates in the field of Information Technology Security (CCRA)
- 25 countries internationally
  - 17 certificate authorizing
  - 8 certificate consuming
- Mutual Recognition Agreement of Information Technology Security Evaluation Certficates (SOGIS MRA)
- 10 countries from EU or EFTA
  - 8 certificate authorizing
  - 2 certificate consuming

CERTIFICATION OF PRODUCTS

- Products to be evaluated are described as *Target of evaluation (TOE)*
- The TOE may consist of the entire or a part of the IT product, including user- and administrative guides
- TOE typically describes a given configuration or several configurations
- A formal description of the security functions is a prerequisites to start a product certification
- The security functions of the product are defined in:
  - *Protection Profile (PP)*
  - *collaborative Protection Profile (cPP)*
  - *Security Target (ST)*
- A ST can consist of one or more PPs or based on a cPP.

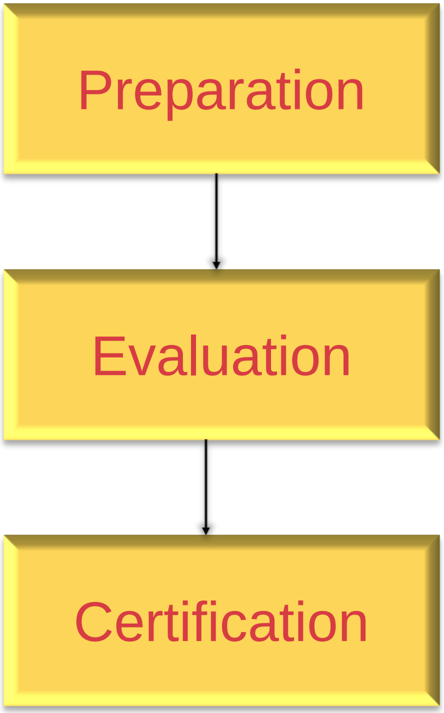
CERTIFICATION OF PROTECTION PROFILES

- Protection Profiles formed as PPs or cPPs describes the generic requirements of a distinct technology area
- The Security Target (ST) describes the implementation and realisation of the security functions in a specific product
- In order to achieve mutual recognition according to CCRA, the ST is required to contain a PP or a cPP

IT SECURITY EVALUATION FACILITIES (ITSEFS)

- ITSEFs perform evaluations of PPs, cPPs and TOE on a commercial basis and documented procedures
- SERTIT is responsible for oversigth of the ITSEFs
  - approving evaluation activities
  - verification of the evaluation facility and of all evaluation activities
- Evaluation activities are regulated by the provisions of the CCRA, SOGIS MRA and national framework conditions
- ITSEFs must have accreditation according to ISO/IEC 17025
- ITSEFs under SERTIT:
  - Advanced Data Security (US)
  - Brightsight BV (NL)
  - Norconsult AS (NO)
  - NTT Com Security Norway AS (NO)

THE CERTIFICATION PROCESS



Preparation

Evaluation

Certification

- Fundament for the evaluation
  - Sponsor(s), developer
- Security Target (ST)
- Protection Profiles (PP)

- Progress meetings
- Observation reports and activity reports
- Evaluation Technical Report (ETR)

- Assessment of ETR
- Certification Report (CR)

EVALUATION ASSURANCE LEVEL (EAL)

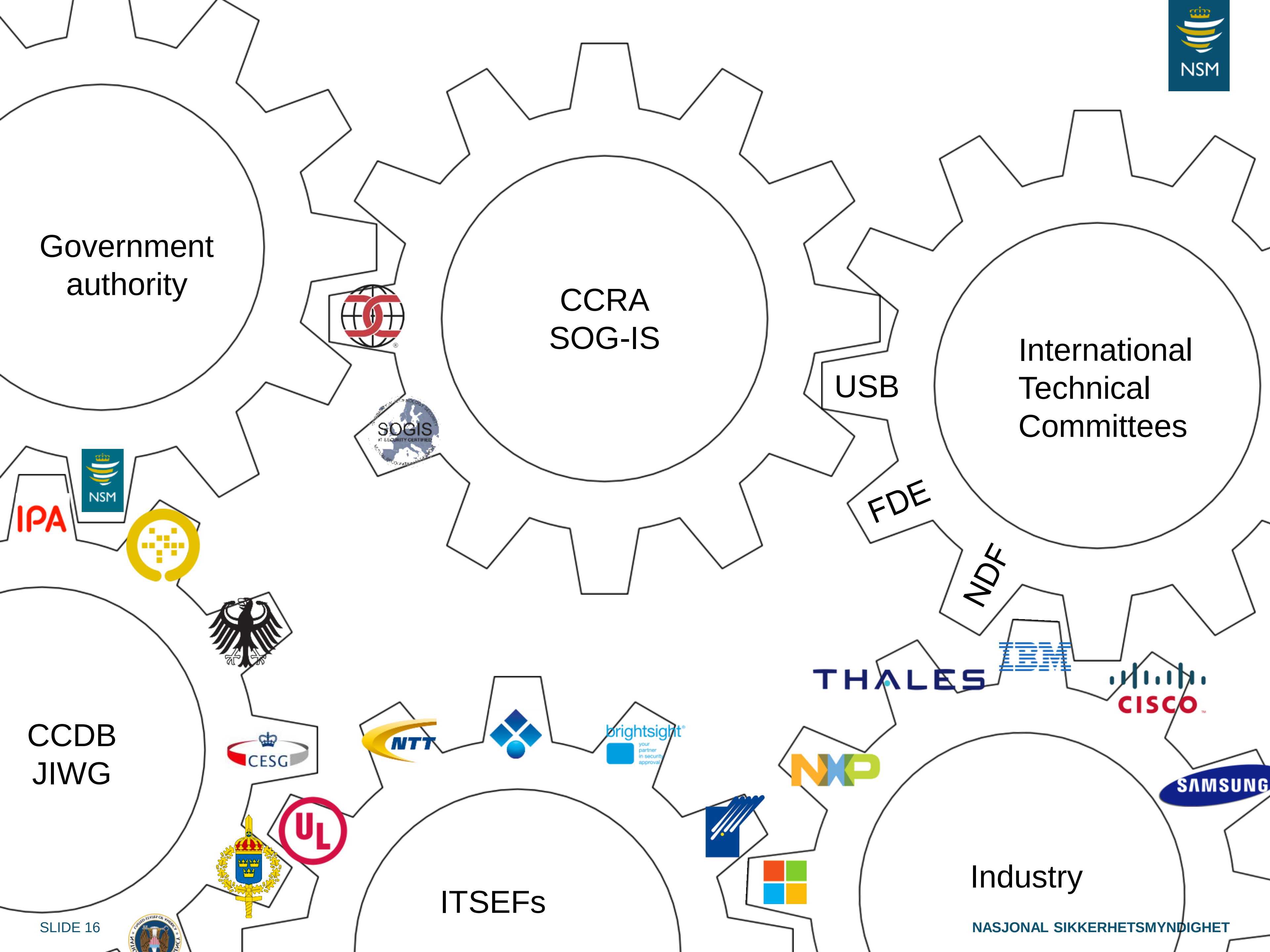
The Common Criteria has seven assurance levels:

- EAL1: Functionally tested
- EAL2: Structurally tested
- EAL3: Methodically tested and checked
- EAL4: Methodically designed, tested and reviewed
- EAL5: Semiformally designed and tested
- EAL6: Semiformally verified design and tested
- EAL7: Formally verified design and tested.

REFORM OF THE CCRA

Common Criteria

- Increase general security in COTS through certification
- Use of standards for security requirements
- Establishing technical committees
- Develop «collaborative Protection Profiles» and supporting documents
- Maintain the CC toolbox
- Recognition only up to EAL2 or certification based on cPP



Government authority

CCRA SOG-IS

International Technical Committees

USB

FDE

NDF

CCDB JIWG

ITSEFs

Industry

HOW CAN YOU BENEFIT?

- Having assured IT-security may be a competitive advantage
- Mutual recognition gives acccess to markets
- Procurers can use it in requirements for bids
- Government can use it to regulate critical and sensitive systems
- All parties benefit on collaboration on development of PPs
- Is a requirement for national classified systems
- Many nations mandates certified products for other areas

C:\> Questions?

www.sertit.no