NTNU
Institutt for datateknikk
og informasjonsvitenskap

**Exam**

# TDT4237 – Software Security (Programvaresikkerhet)

**Monday December 16th 2012, 09:00 - 13:00**

Oppgaven er utarbeidet av faglærer Lillian Røstad og kvalitetssikrer er Torbjørn Skramstad.
Kontaktperson under eksamen er Lillian Røstad (mobil 994 00 628)

Språkform: Engelsk

Tillatte hjelpemidler: D

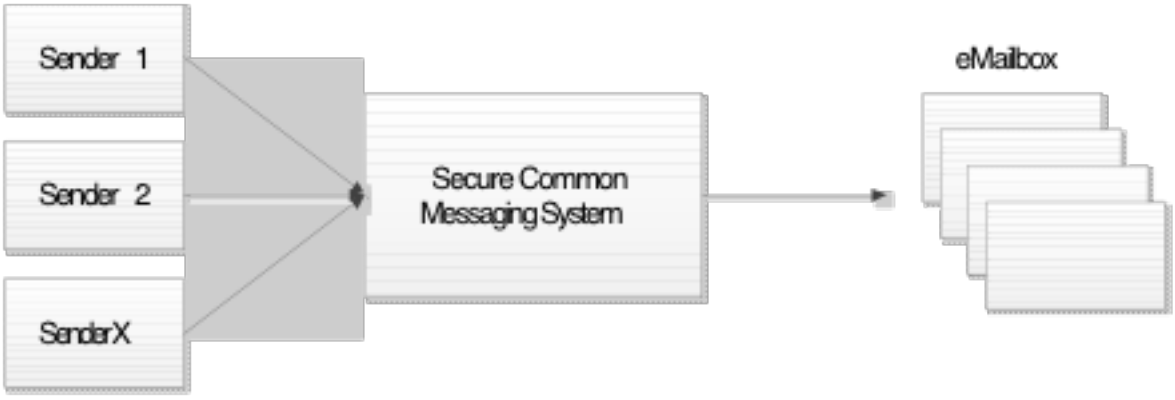
Ingen trykte eller håndskrevne hjelpemidler tillatt. Bestemt, enkel kalkulator tillatt.
No printed or hand-written materials allowed. Approved calculator allowed.

*Results available (sensurfrist): Thursday January 16th 2014*

*Read each task carefully. Identify what the task asks for.*
*If you find that information is missing in a task you are free to make the assumptions you consider necessary, but remember to explain and clearly mark your assumptions.*

*Les oppgaveteksten nøye. Finn ut hva det spørres etter i hver oppgave.*
Dersom du mener at opplysninger mangler i en oppgaveformulering gjør kort rede for de antagelser og forutsetninger som du finner det nødvendig å gjøre.

## Task 1 (40%)




Above is a high-level sketch for a system which purpose is to provide secure messaging services, to send messages from government to citizens. Depending on the sender, these messages may contain personal and sensitive data, so it is important for the system to be secure. The messages should only be readable by the intended receiver and it is very important also to protect the integrity of the messages.

The central component in the system has been given the name Secure Common Messaging System (SCMS). The purpose of the SCMS is to enable secure communication of messages from government to citizens:

- By providing addressing services for citizens. So government need only know who they are sending a message to, but not to which address or mailbox. A citizen may have one or several mailboxes.
- By providing services that ensures that government can know, with reasonable certainty, that messages have been delivered to, and opened by, the citizen.
- The SCMS should not be able to see the content of messages from government to citizens.

The task of your project is to create security requirements for the SCMS using the Risk Management Framework.

## Task 2 (30%)

a) When creating a software system, when and for what would you use threat modeling?

b) How does an XSS-attack work? Explain using an example.
c) What is a one-time pad?

d) What is the attack surface of a system?

e) What is the purpose of creating a risk-based test plan?

f) What are the main pros and cons of manual code review vs code review with a tool?

**Task 3 (30%)**

Authentication and password management is a key feature of many systems, but also something easily done wrong. For this task we will use an online ticket ordering system as our case. In this system a user has to create an account in order to be able to order tickets.

Authentication and password management is a key feature of many systems, but also something easily done wrong. For this task we will use an online ticket ordering system as our case. In this system a user has to create an account in order to be able to order tickets.

a) Create a password policy for the ticket ordering system.
b) Explain how you would:
    a. Store passwords.
    b. Perform password checks.
    c. Allow users to reset their password.

You may provide pseudo-code examples to explain your thinking.