Indhold

[SikkerHed 2](#_Toc501454799)

[Hemmeligholdelse 2](#_Toc501454800)

[SSL 2](#_Toc501454801)

[RSA 3](#_Toc501454802)

[One-Time-Pad 4](#_Toc501454803)

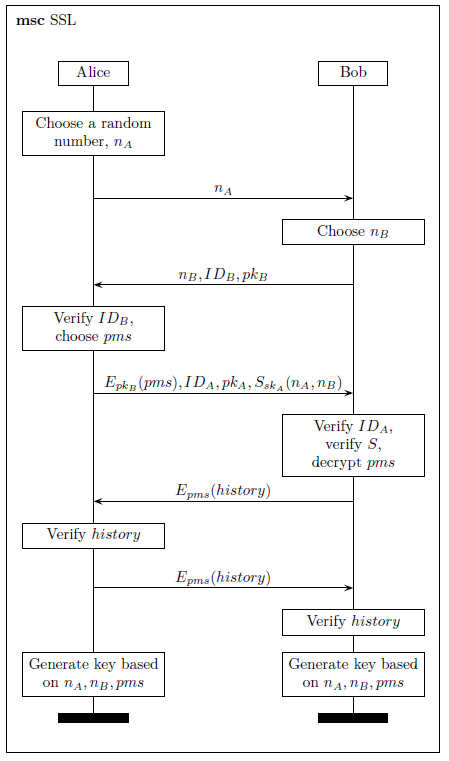
[Autenticitet 5](#_Toc501454804)

[JWT 5](#_Toc501454805)

# SikkerHed

## Hemmeligholdelse

### SSL



Hvad bruger man det til?

Man bruger SSL til at verificere en sikker forbindelse mellem to parter.

Man verificerer hvem man taler med.

Man sikre at forbindelsen mellem de to parter er sikker.

Client server.

Hvordan fungerer det?

Fordele/ulemper/alternativer?

Fordelen er at, hvis beskeder bliver opsnappet kan man kun læse den krypterede besked og ikke selve beskeden.

Ulempe: krypteringen tager ekstra resourcer.

Fordele: tillid, verification, hemmeligholdelse og

### RSA

Hvad bruger man det til?

RSA bruges til at genereet et Public key system

Hvordan fungerer det?

Fordele/ulemper/alternativer?

Alternativ: One Time Pad

### One-Time-Pad

Hvad bruger man det til?

Hvordan fungerer det?

Fordele/ulemper/alternativer?

## Autenticitet

### JWT

Hvad bruger man det til?

Når brugeren er logget ind, vil hver efterfølgende forespørgsel inkludere JWT, så brugeren får adgang til ruter, tjenester og ressourcer, der er tilladt med det token.

Hvordan fungerer det?

Hvad består den af?

JSON Web Tokens består af tre dele separateret af punktum (.) som er:

* Header
* Payload
* Signature

Derfor ser en JWT typisk således ud: xxxxx.yyyyy.zzzzz

Header indeholder: hvilken type token det er og hvilken hashing metode der er blevet brugt.

Payload indeholder: hvilken

Når en client kontakter en server for at logge ind

Fordele/ulemper/alternativer?

# Hacking

## Cross Site Scripting

## JavaScript Injection

## SQL Injection

## Buffer Overflow