



(1)

Voornaam: .....

Naam: .....

Studentennummer: .....

Klasgroep: .....

Datum: .....

Opleidingsonderdeel (OPO): .....

Onderwijsleeractiviteit (OLA): .....

Examinator: Kerberos

- 1) Gebruiker X wil resources op server  $\alpha$
- 2) Netwerk is niet te vertrouwen
- 3) Gebruiker X wil identiteit  $\alpha$  heen bewijzen  
→ Single-sign-on

- ! Hoe kan X bewijzen aan  $\alpha$  dat ze X is?
- ! Hoe weet X dat ze met  $\alpha$  „praet“?

Kerberos  $\Rightarrow$  werkt met eenvoudige  
Symm sleutels.

- 1) KDC = key distr. center  
AS = auth. service (server)  
TGS = ticket granting service (server)

2) X = gebruikers X

3)  $\alpha$  = server  $\alpha$



$\alpha$

$\alpha$



2

Voornaam: .....

Naam: .....

Studentennummer: .....

Klasgroep: .....

Datum: .....

Opleidingsonderdeel (OPO): .....

Onderwijsleeractiviteit (OLA): .....

Examinator: .....

Hoe komen we aan die sym. sleutels?  
(heeft lange sym sleutel)

1) Gebruiker X

- password  $\Rightarrow H(\text{password}) =$  

2) Server X

- key-file = random sleutel 

3) TGS

- random key 

4) AS heeft een kopie van de 3 sleutels



De kracht van Kerberos ligt in het feit dat de sleutels alleen op 2 plaatsen in het netwerk te vinden zijn.



Voornaam: .....

Naam: .....

Studentennummer: .....

Klasgroep: .....

Datum: .....

Opleidingsonderdeel (OPO): .....

Onderwijsleeractiviteit (OLA): .....

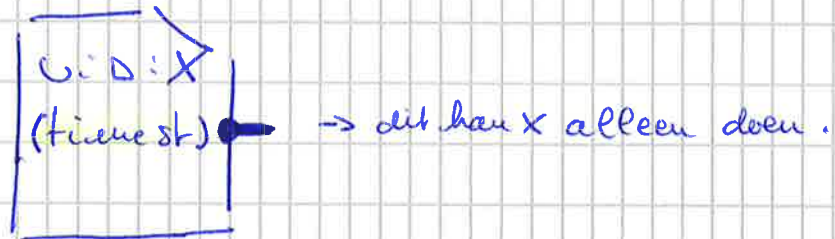
Examinator: .....

3

zie

Tekening

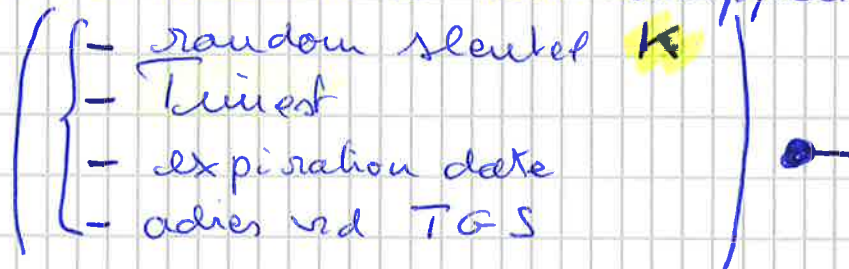
- User X wil toegang tot X? X wil zich 1 maal authenticeren of identificeren (SSO)!
- 1) User X maakt een bericht



en stuurt dat naar AS

- 2) AS ontvangt het bericht leest welke UID er in zit X en neemt de sleutel van X erbij. Hiermee ontsteltelt die de (Timestamp) tot Timestamp.

- 3) De AS maakt 2 boodschappen en stuurt die naar X



TGT

ticket  
granting  
ticket





4

Voornaam: .....

Naam: .....

Studentennummer: .....

Klasgroep: .....

Datum: .....

Opleidingsonderdeel (OPO): .....

Onderwijsleeractiviteit (OLA): .....

Examinator: .....

4) User X gebruikt de  $\bullet$ -sleutel om het eerste bericht te ontcijferen en  $K^{\text{te}}$  krijgen. Omdat de Timestr dezelfde is als dat zij hij naar de AS gestuurd heeft; Weet X dat enkel de AS met haar  $\bullet$ -sleutel haar bericht in 1) kan lezen. X weet nu ook het adres van de TGS.

5) Gebruiker X maakt 2 nieuwe boodschappen.

$\left( \begin{array}{l} \text{- UID: X} \\ \text{- Timestr} \end{array} \right) K$

$\left\{ \begin{array}{l} \text{- UID} \\ \text{- Samen X} \end{array} \right\} \Rightarrow \text{KLAAR TEKST}$

en stuurt deze samen met de TGT naar de TGS

6) De TGS neemt zijn  $\bullet$ -sleutel en haalt uit het TGT de sleutel  $K$ . Die gebruikt hij (zij) om de UID: X en de Timestr te verkrijgen. De TGS vergelijkt of bekijkt de 2 ontsleutelde berichten. Enkel X shouldie boodschappen gemaakt hebben nadat die zich ~~geauthenticeerd~~ heeft bij een AS. De TGS gaat nu "vragen" aan de vraag van X om toegang te krijgen tot X en haalt de  $\bullet$ -sleutel van X op in de AS.

5


Voornaam: .....  
 Naam: .....  
 Studentnummer: .....  
 Klasgroep: .....  
 Datum: .....  
 Opleidingsonderdeel (OPO): .....  
 Onderwijsleeractiviteit (OLA): .....  
 Examinator: .....

7) De TGS vraagt aan de AS de server X zijn -sleutel en maakt 2 boodschappen.

Service ticket

{
 

- random sessie sleutel  $K_x$
- UID: X
- time st
- expiration date

 } 

{
 

- random sessie sleutel  $K_x$
- server naam X
- ~~time st~~
- expiration date

 }  $K$

en stuurt ze naar gebruiker X

8) Gebruiker X kan het tweede pakket uit 7) ontsleutelen en krijgt de sessie sleutel  $K_x$  en krijgt na dat de time st die in dat pakket is, de time st is die zegt hij na de TGS heeft gestaan?





6

Voornaam: .....

Naam: .....

Studentennummer: .....

Klasgroep: .....

Datum: .....

Opleidingsonderdeel (OPO): .....


Onderwijsleeractiviteit (OLA): .....

Examinator: .....

9) User X creëert een boodschap

( { - UID: X  
          - ~~timestamp~~ } ) ~~K<sub>X</sub>~~

en stuurt dit samen met de service ticket naar server X omdat X aan X wil bewijzen dat ze X is.

10) de server X gebruikt zijn  - sleutel om uit de sessie ticket de ~~K<sub>X</sub>~~ te halen.

Het gebruikt de sessie ticket sleutel ~~K<sub>X</sub>~~ om het eerste bericht in 9) te ontsleutelen. Als de info in de 2 boodschappen kloppen / overeenkomen dan moet X ze gekregen hebben van X.

11) om de server X zich te laten authenticeren bij X stuurt deze een boodschap

( { - servernaam X  
          - ~~timestamp~~ } ) ~~K<sub>X</sub>~~

en stuurt het naar X omdat X wil bewijzen aan X dat het X is.

12) Als X het bericht uit 11) kan ontsleutelen moet de boodschap komen van server X.