REVA UNIVERSITY
Bengaluru, India

School of Computing and Information Technology

Course Delivery

Prof. Raghavendra Nayaka P

B.Tech – VI Semester

Kerberos

- ***A SIMPLE AUTHENTICATION DIALOGUE***

(1) $C \rightarrow AS: \quad ID_C \| P_C \| ID_V$

(2) $AS \rightarrow C: \quad Ticket$

(3) $C \rightarrow V: \quad ID_C \| Ticket$

$Ticket = E(K_v, [ID_C \| AD_C \| ID_V])$

Kerberos(contd.)

REVA UNIVERSITY
Bengaluru, India

- ***A MORE SECURE AUTHENTICATION DIALOGUE***

Once per user logon session:

(1) C → AS: $ID_C \| ID_{tgs}$

(2) AS → C: $E(K_c, Ticket_{tgs})$

Once per type of service:

(3) C → TGS: $ID_C \| ID_V \| Ticket_{tgs}$

(4) TGS → C: $Ticket_v$

Once per service session:

(5) C → V: $ID_C \| Ticket_v$

$Ticket_{tgs} = E(K_{tgs}, [ID_C \| AD_C \| ID_{tgs} \| TS_1 \| Lifetime_1])$

$Ticket_v = E(K_v, [ID_C \| AD_C \| ID_v \| TS_2 \| Lifetime_2])$

Kerberos (contd.)

REVA UNIVERSITY
Bengaluru, India

- ***THE VERSION 4 AUTHENTICATION DIALOGUE***

(1) C → AS $ID_c \| ID_{tgs} \| TS_1$

(2) AS → C $E(K_c, [K_{c,tgs} \| ID_{tgs} \| TS_2 \| Lifetime_2 \| Ticket_{tgs}])$

$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| Lifetime_2])$

(a) Authentication Service Exchange to obtain ticket-granting ticket

(3) C → TGS $ID_v \| Ticket_{tgs} \| Authenticator_c$

(4) TGS → C $E(K_{c,tgs}, [K_{c,v} \| ID_v \| TS_4 \| Ticket_v])$

$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| Lifetime_2])$

$Ticket_v = E(K_v, [K_{c,v} \| ID_C \| AD_C \| ID_v \| TS_4 \| Lifetime_4])$

$Authenticator_c = E(K_{c,tgs}, [ID_C \| AD_C \| TS_3])$

(b) Ticket-Granting Service Exchange to obtain service-granting ticket

(5) C → V $Ticket_v \| Authenticator_c$

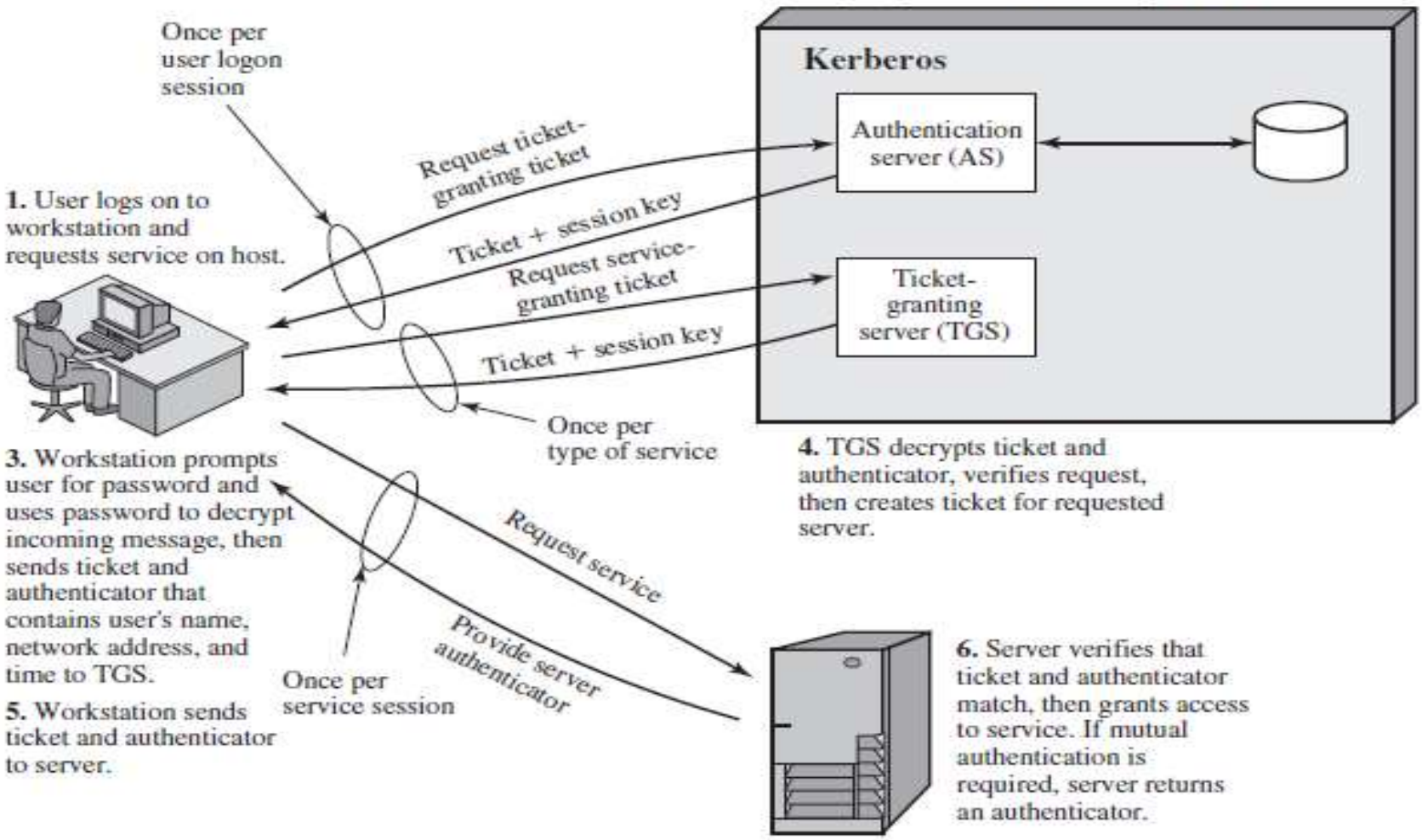
(6) V → C $E(K_{c,v}, [TS_5 + 1])$ (for mutual authentication)

$Ticket_v = E(K_v, [K_{c,v} \| ID_C \| AD_C \| ID_v \| TS_4 \| Lifetime_4])$

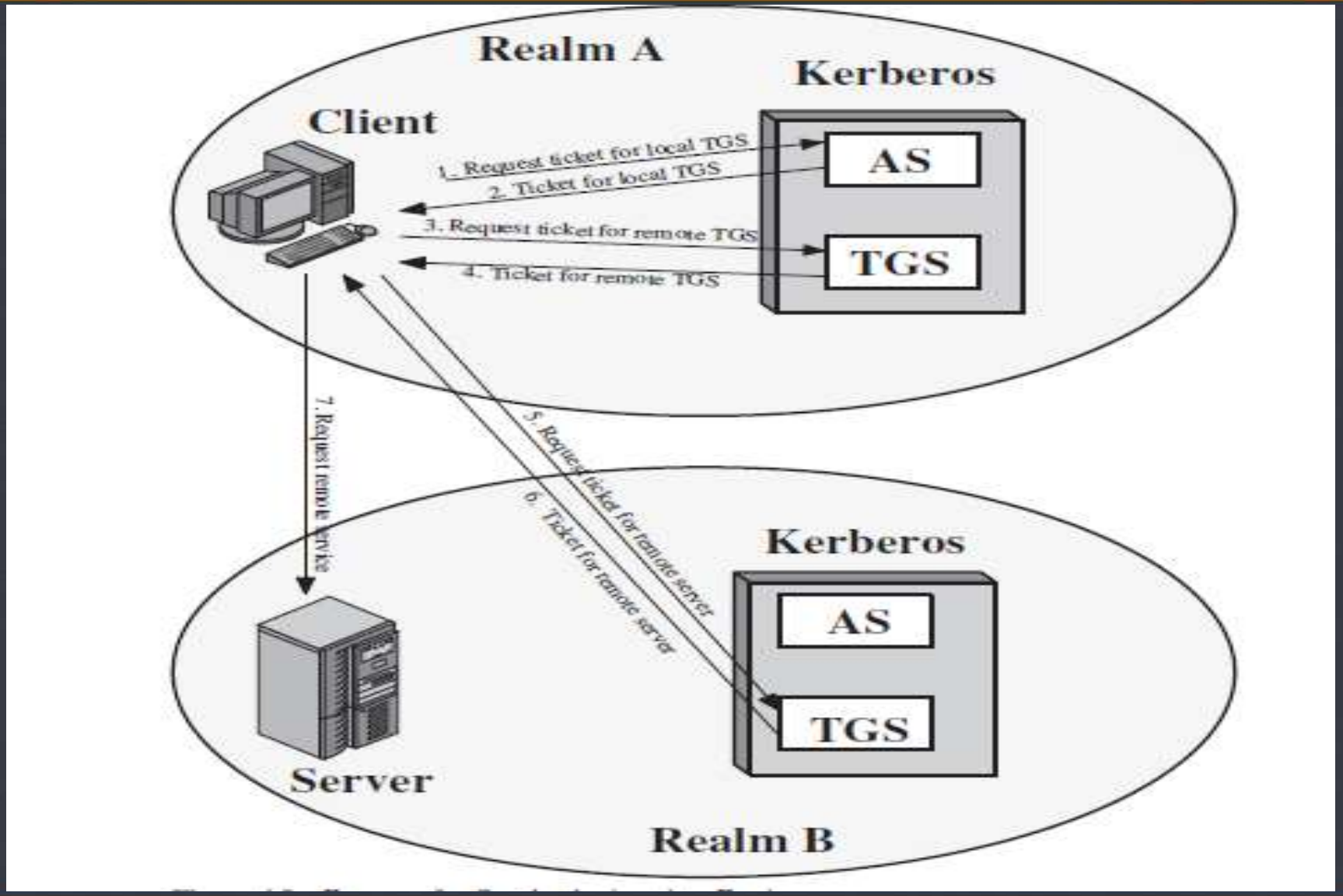
$Authenticator_c = E(K_{c,v}, [ID_C \| AD_C \| TS_5])$

(c) Client/Server Authentication Exchange to obtain service

Overview of Kerberos



Request for Service in Another Realm



Request for Service in Another Realm

REVA UNIVERSITY
Bengaluru, India

(1) $C \rightarrow AS$: $ID_C \| ID_{tgs} \| TS_1$

(2) $AS \rightarrow C$: $E(K_C, [K_{C,tgs} \| ID_{tgs} \| TS_2 \| Lifetime_2 \| Ticket_{tgs}])$

(3) $C \rightarrow TGS$: $ID_{tgsrem} \| Ticket_{tgs} \| Authenticator_C$

(4) $TGS \rightarrow C$: $E(K_{C,tgs}, [K_{C,tgsrem} \| ID_{tgsrem} \| TS_4 \| Ticket_{tgsrem}])$

(5) $C \rightarrow TGS_{rem}$: $ID_{Vrem} \| Ticket_{tgsrem} \| Authenticator_C$

(6) $TGS_{rem} \rightarrow C$: $E(K_{C,tgsrem}, [K_{C,Vrem} \| ID_{Vrem} \| TS_6 \| Ticket_{Vrem}])$

(7) $C \rightarrow V_{rem}$: $Ticket_{Vrem} \| Authenticator_C$