COMP3052.SEC Computer Security

Session 11: OS Security II: Windows Security

Acknowledgements

- Some of the materials we use this semester may come directly from previous teachers of this module, and other sources ...
- Thank you to (amongst others):
  - Michel Valstar, Milena Radenkovic, Mike Pound, Dave Towey, …

This Session

- Windows Security
  - Permissions
  - Access Tokens
  - Authentication
- Kerberos

Overview

- The Windows security model has seen a steady evolution
- This lecture is not windows version-specific
- Security in Windows is much more fine-grained than other operating systems

Security Subsystem

- Runs in user mode
- Logon processes (winlogon, LogonUI)
- Local Security Authority (LSA)
  - Checks User Accounts
  - Provides access token
  - Responsible for auditing
- Security Account Manager (SAM)
  - Maintains user account database used by LSA
  - Encrypts / hashes passwords

Windows

- Windows predominantly uses Access Control Lists, and has done since Windows NT
- Extends the usual read, write and execute with:
  - Take ownership
  - Change permissions
  - Delete
- 32-bit access masks (cf. Unix 9-bit)
- A higher degree of control, with the associated complexity increase!

Access Control

- Access control in windows treats more than just files, also:
  - Registry keys
  - Active directory objects
  - Groups
- Inheritance is implemented
  - File can inherit ACLs from parent directories

Microsoft Active Directory

Principals

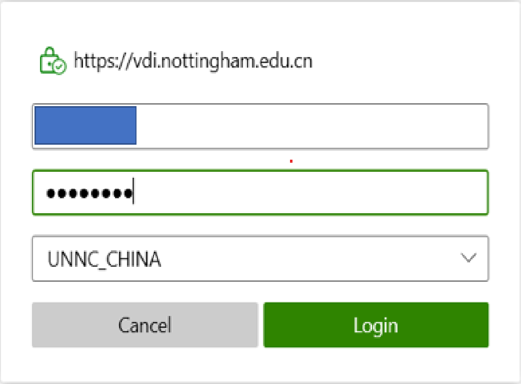
- Principals more broadly defined as well:
  - Local users
  - Domain users
  - Groups
  - Machines
- Each principal has a human-readable name and security ID (SID)

S-1-5-21-2475811070-2421845406-3333283485-1005

S-1-5-21-1664130791-3153540899-3044996548-279530

Local / Domain Principals

- Local Security Authority (LSA) creates local principals
  - principal = MACHINE\principal
    - › E.g., Host\Dave
- Domain principals administered on Domain Controller (DC) by domain admins
  - principal@domain = DOMAIN\principal
    - › net user / domain
    - › net group / domain
    - › net localgroup / domain



https://vdi.nottingham.edu.cn

[redacted]

•••••••••

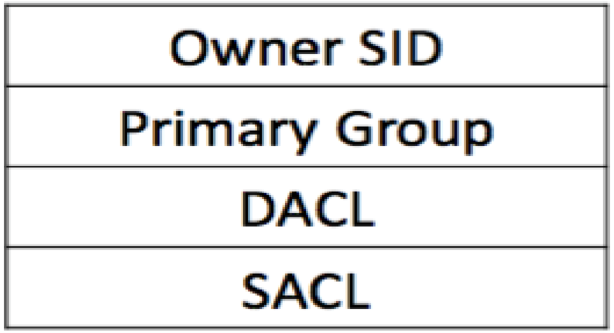
UNNC_CHINA

Groups

- Groups are collections of SIDs
- Group can itself be an SID
- Groups can thus be nested
- Groups are not nest-able on local machines
- Managed by a domain controller within Active Directory

Objects

- Objects are passive entities in access operations
- In Windows:
  - Private objects (files, directories)
  - Executive objects (processes, threads, etc.)
- Securable objects have a security descriptor
  - Private objects managed by application software
  - Built-in securable objects managed by the OS

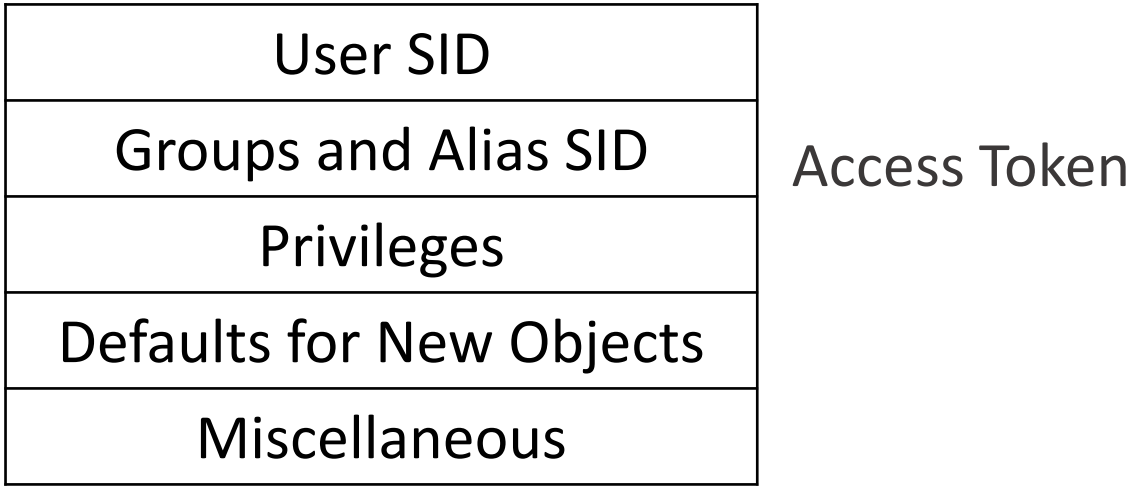


Owner SID
Primary Group
DACL
SACL

Discretionary Access Control List (DACL)
System Access Control List (SACL)

Access Tokens

- Security credentials for a login session stored in access token
- Identifies the user, the user's groups, and the user's privileges



User SID

Groups and Alias SID

Privileges

Defaults for New Objects

Miscellaneous

Access Token

Subjects

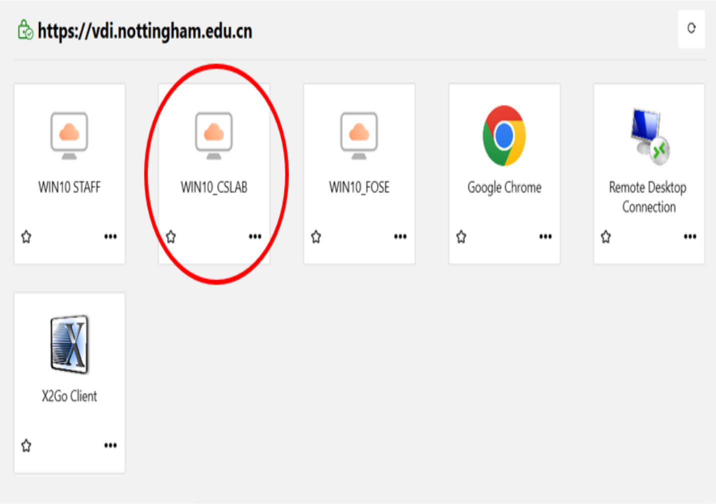
- Windows subjects: Processes and threads
- New processes get a copy of the parent access token, possibly modified
- Individual access tokens are immutable, and can live beyond policy changes (TOCTTOU issue)

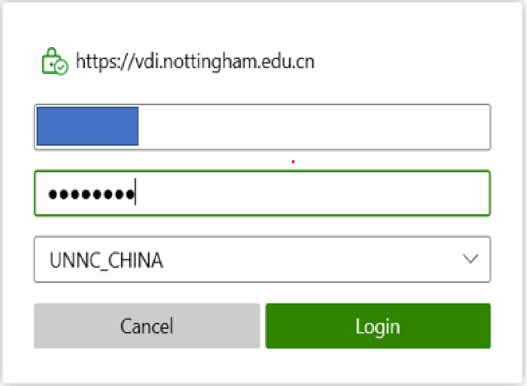
User Account Control

- After Vista, administrator users do not use an administrative access token by default
- Users have two tokens, one heavily restricted and used by default
- A prompt allows a user to spawn a process with the other token, or switch a process’ token

Domains

- Single sign-on for network resources
- Centralised security administration
- Domain
  - A group of machines, sharing a common user account database and security policies
- Domain Controller (DC)
  - Handles user accounts and access control
- Multiple DCs allow for decentralisation by design




https://vdi.nottingham.edu.cn

[redacted]

••••••••

UNNC_CHINA

Interactive Logon

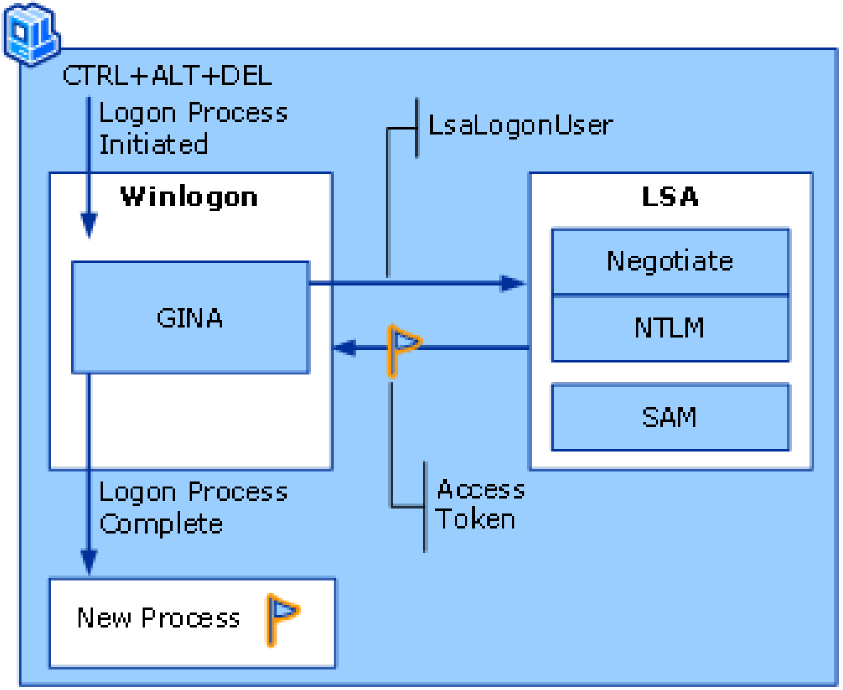
- The windows interactive logon allows a user to authenticate
- Windows logon begins with the Secure Attention Sequence – Ctrl + Alt + Delete
  - Can prevent spoofing – is tied directly to winlogon
- The logon process differs slightly for local and domain authentication

Interactive Logon

- The logon process contains:
  - Winlogon – the process responsible for authenticating users
    - Graphical Identification and Authentication (GINA)
  - The Local Security Authority (LSA)
    - An authentication package (NTLM)
    - Security Account Manager (SAM)
  - Since Vista, additional Credential Providers are allowed

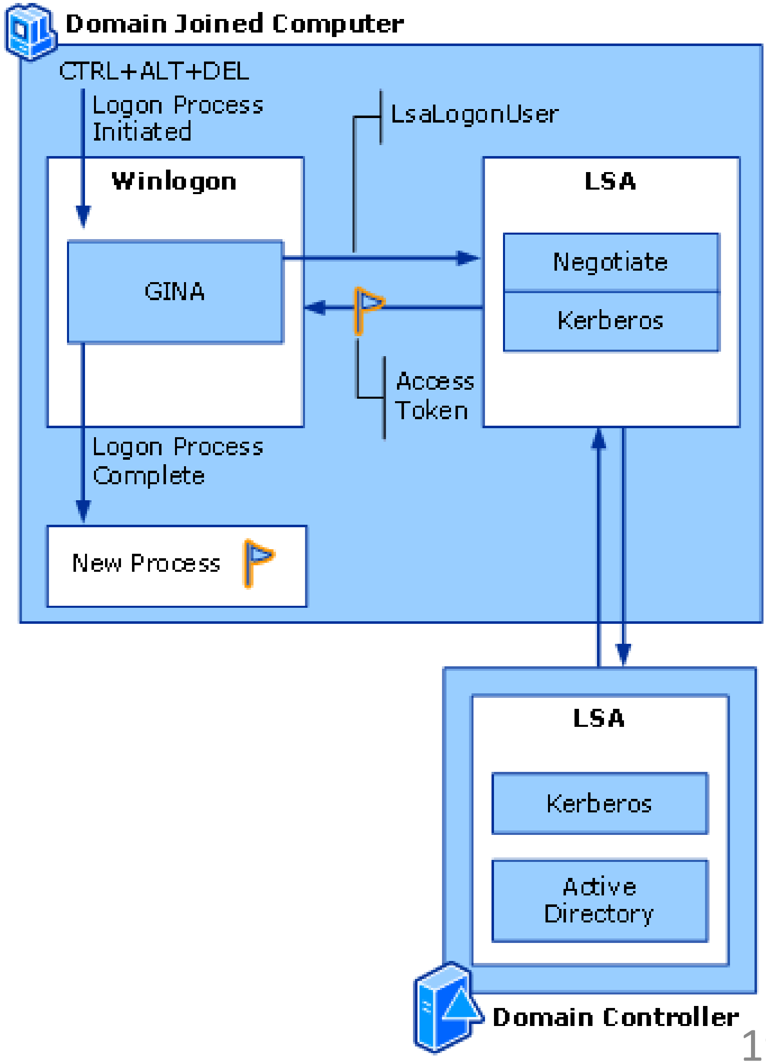
Local Logon – Pre vista

1. Ctrl+Alt+Delete initiates a login prompt using GINA
2. These collect credentials which are passed to the LSA
3. The LSA uses NTLM to check the credentials against the SAM database
4. Successful login provides an access token, which is used to spawn a shell (explorer.exe)



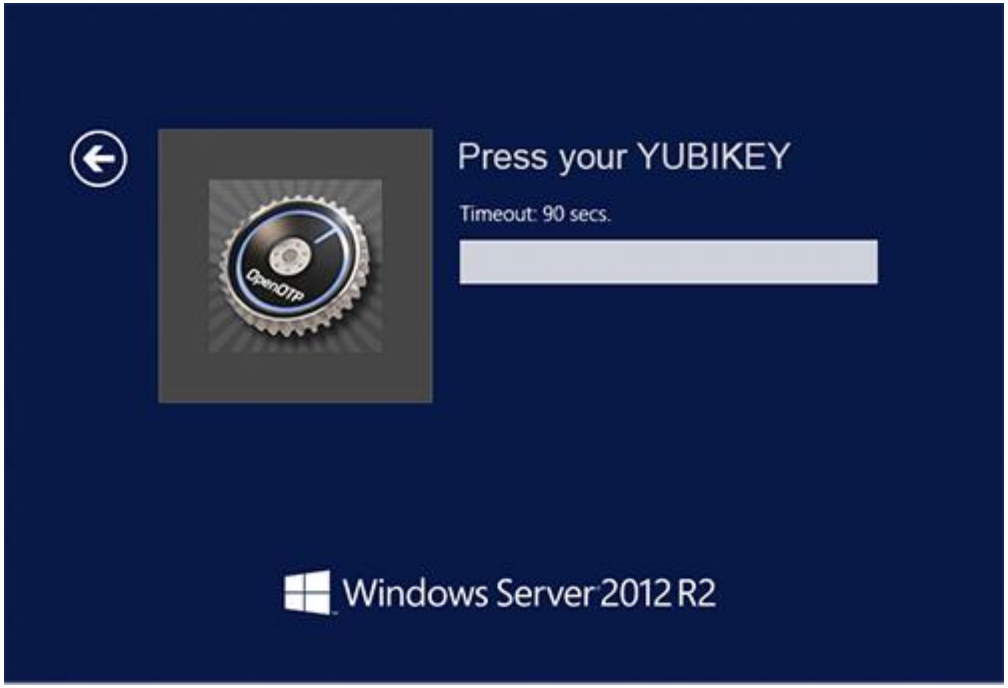
Domain Logon

- Replaces NTLM with Kerberos
- Replaces SAM with an Active Directory Domain Controller
- Checks of a user are now performed on the remote LSA



Credential Providers

- Since Vista, winlogon uses a LogonUI to query Credential Providers
- These don’t actually log you in, they simply serialize your credentials and pass them to the LSA

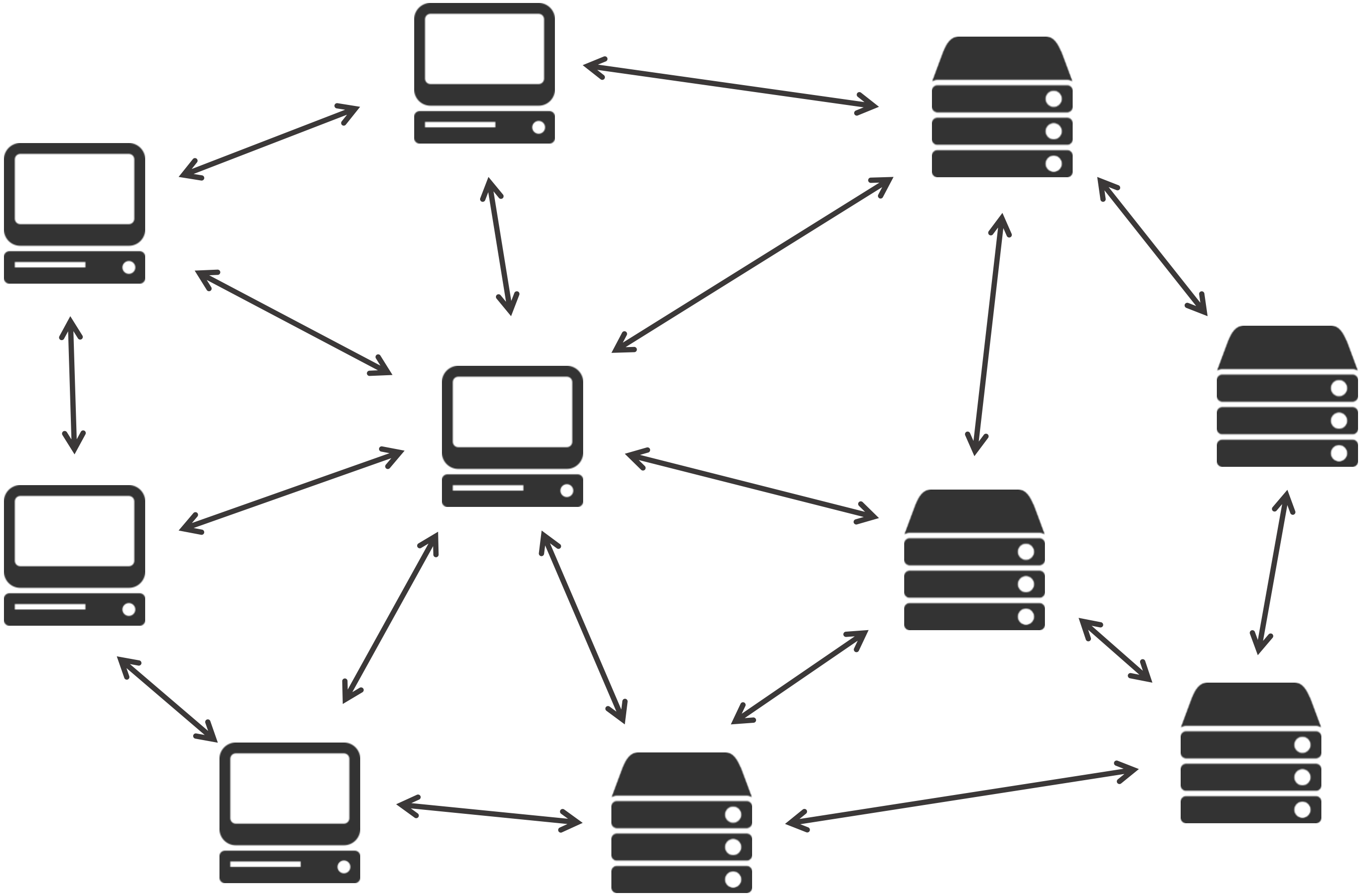

Press your YUBIKEY

Timeout: 90 secs.

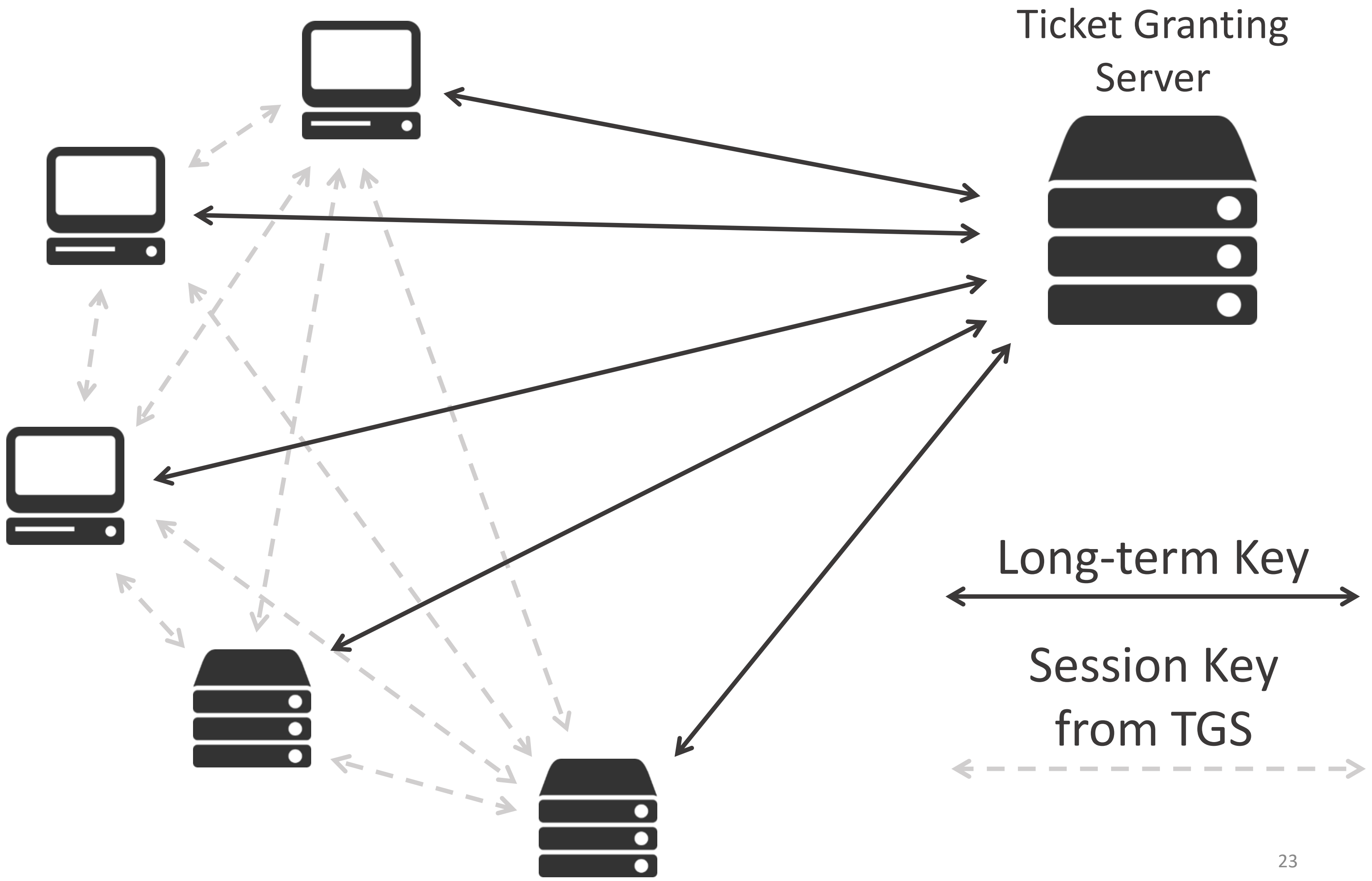
Kerberos

- Originally developed at MIT
- Widely supported, in particular is the default authentication for network logon in Windows
- Uses symmetric encryption
- Requires a trusted third party

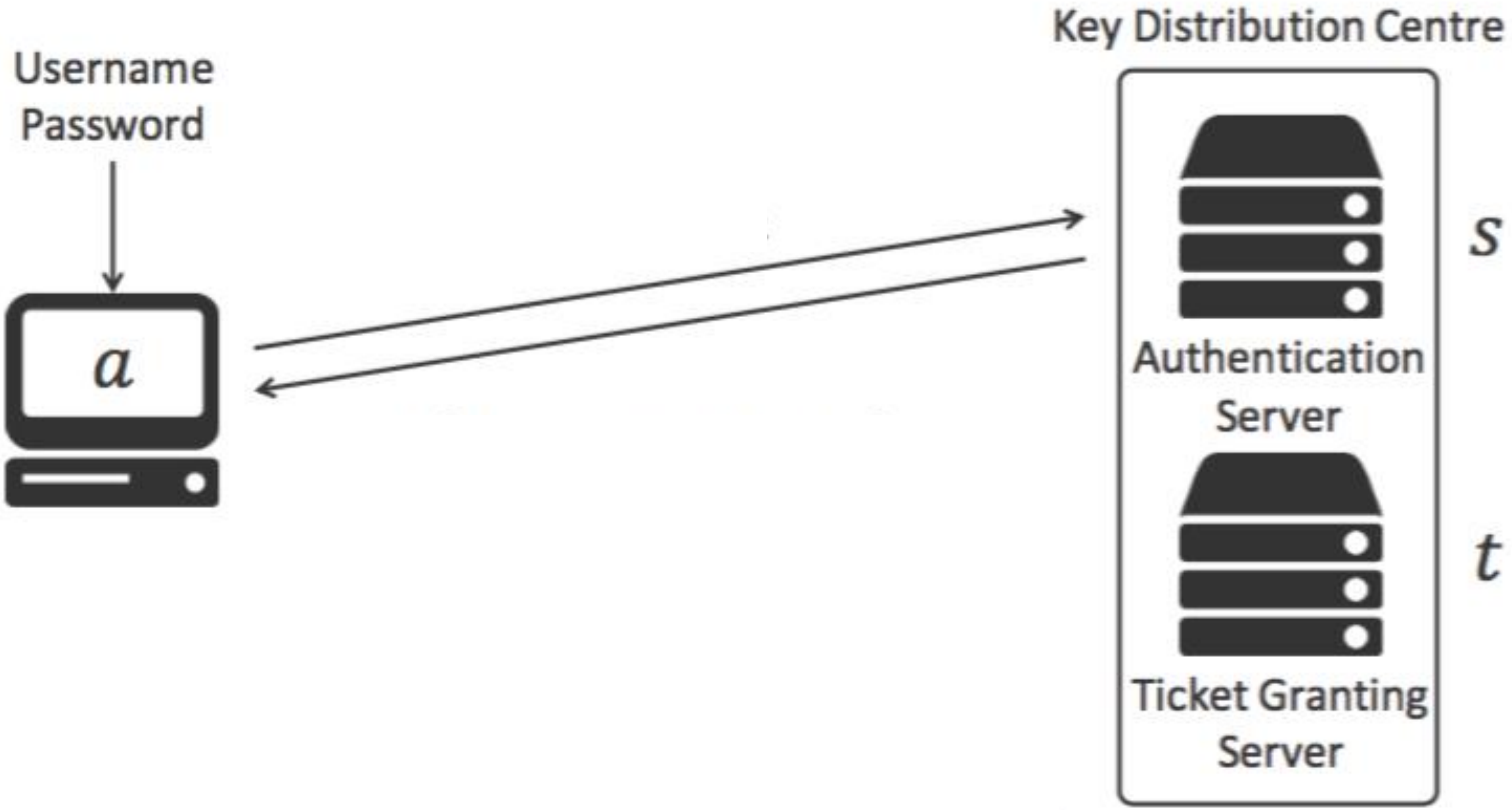
Encrypting Large-scale Networks



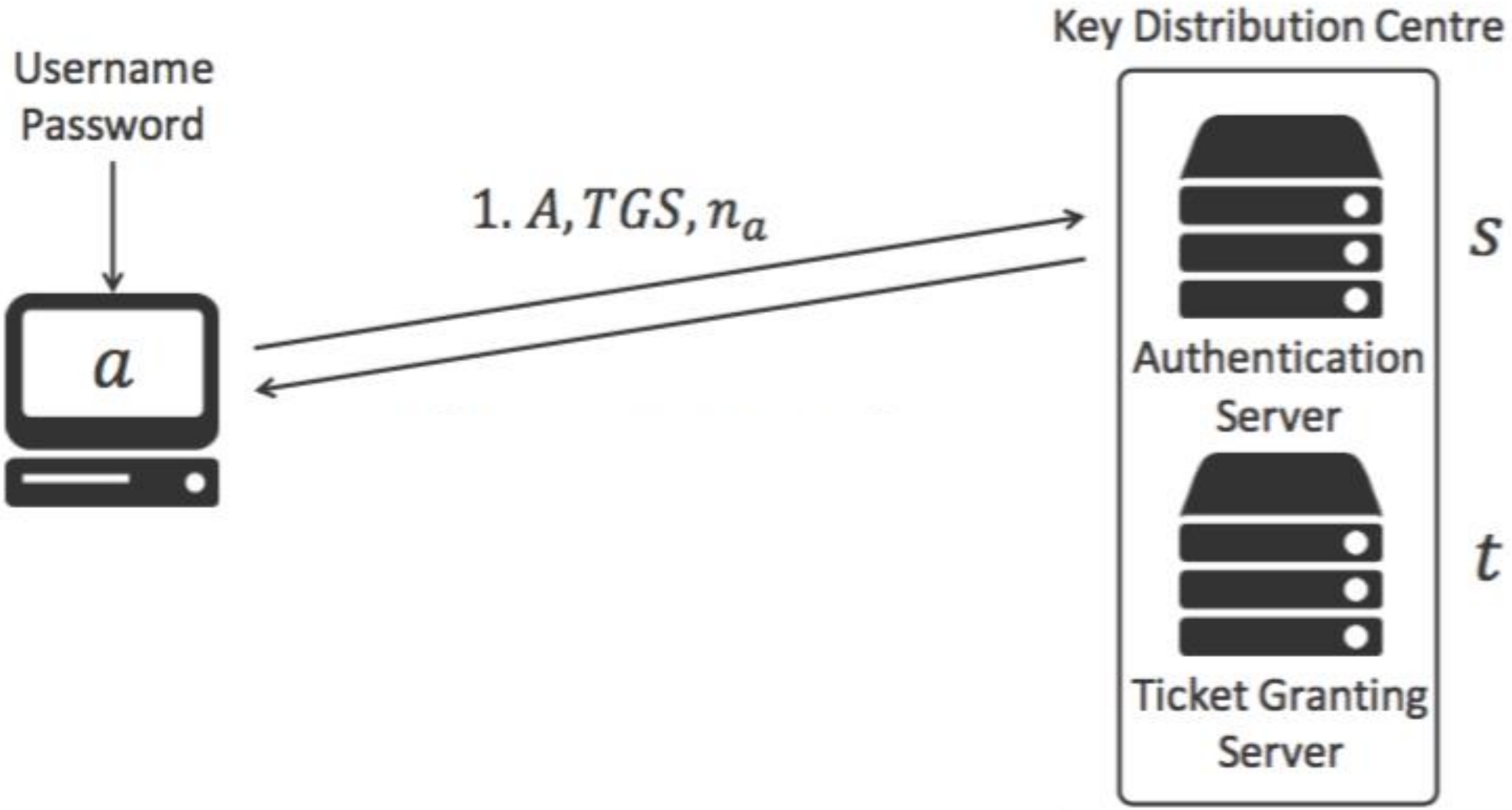
Ticket Granting Servers



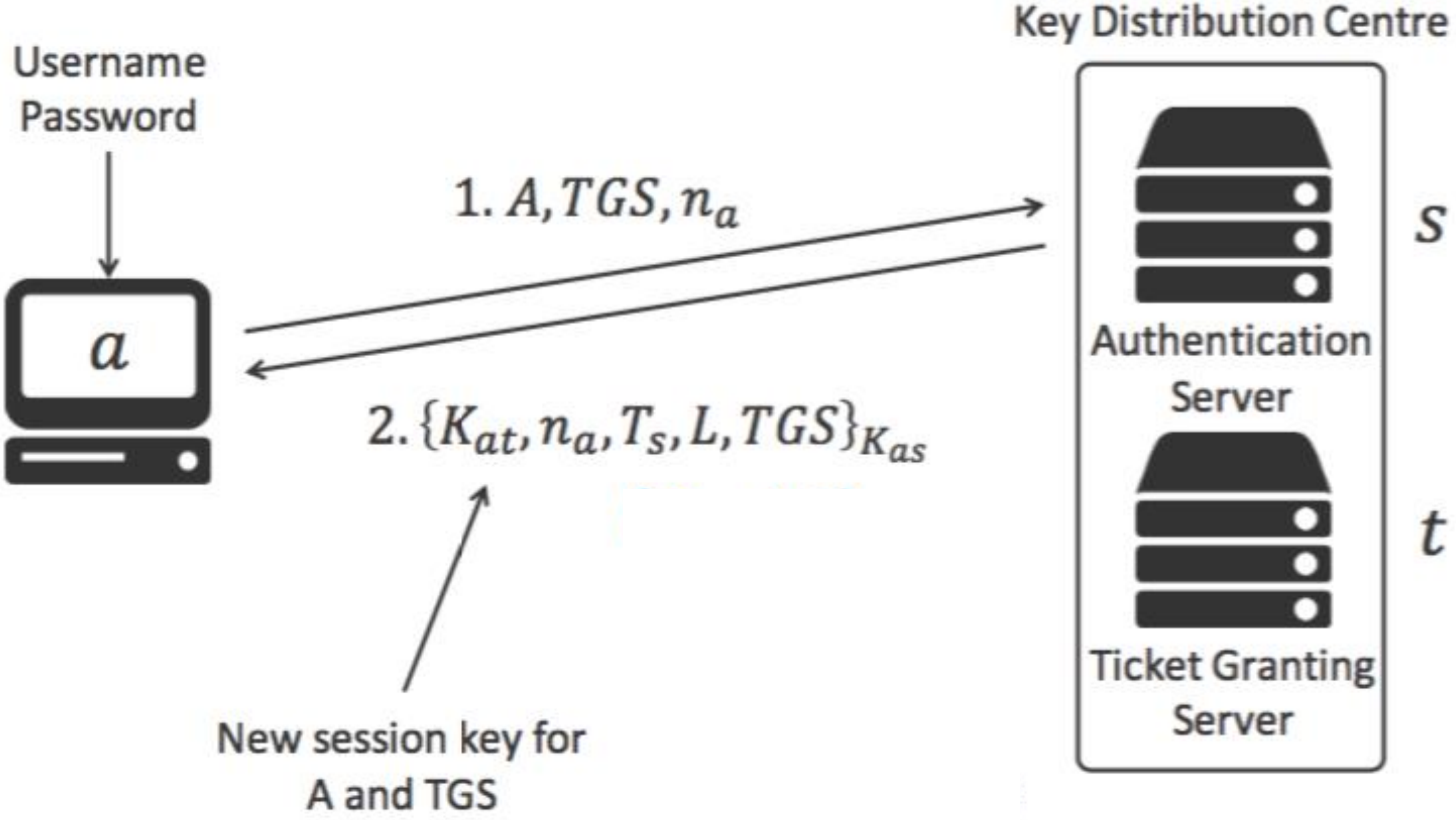
Kerberos: Step 1, Authentication



Kerberos: Step 1, Authentication



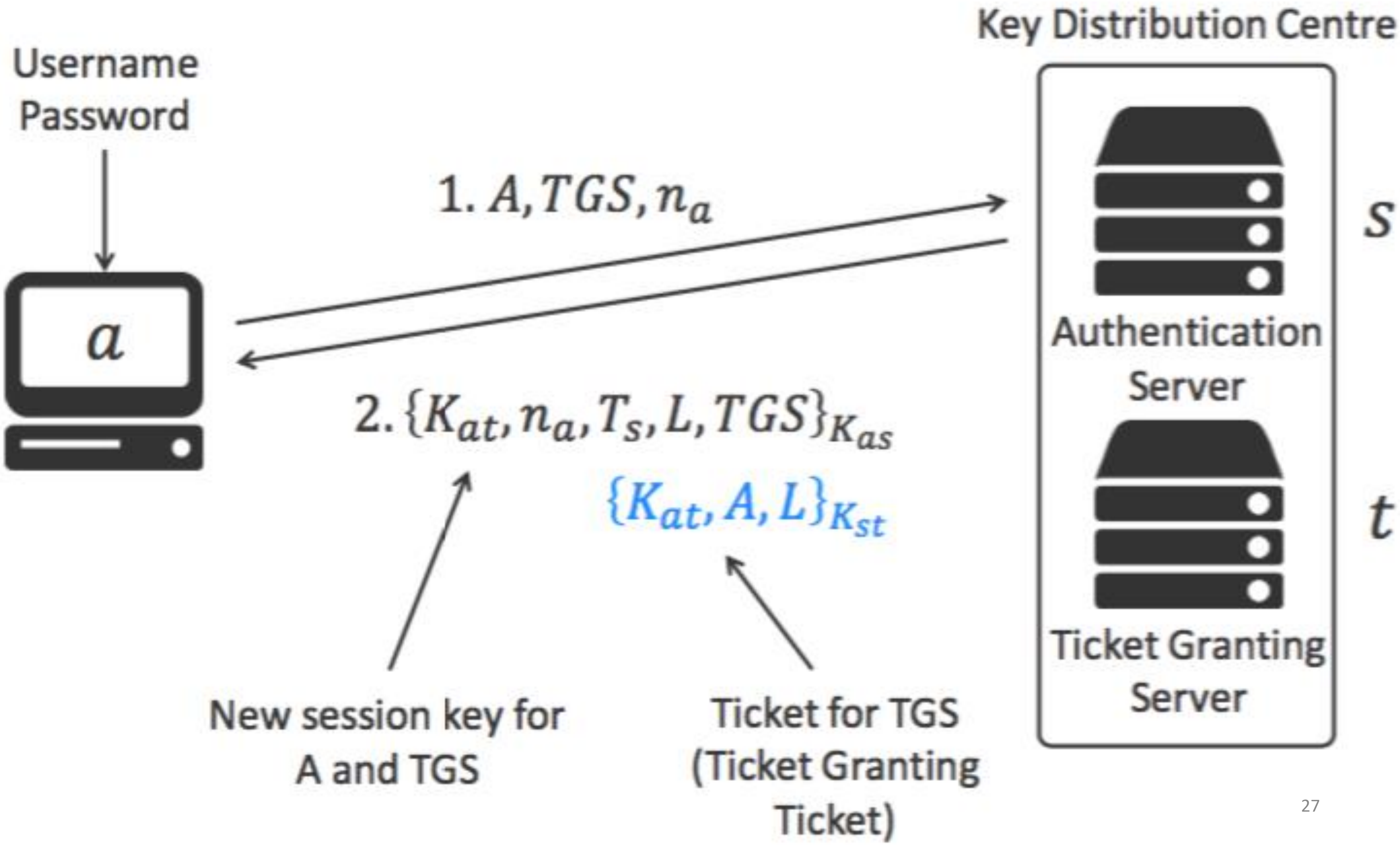
Kerberos: Step 1, Authentication



1. A, TGS, n_a

2. $\{K_{at}, n_a, T_s, L, TGS\}_{K_{as}}$

Kerberos: Step 1, Authentication



Username
Password

a

$1. A, TGS, n_a$

$2. \{K_{at}, n_a, T_s, L, TGS\}_{K_{as}}$

$\{K_{at}, A, L\}_{K_{st}}$

New session key for A and TGS

Ticket for TGS (Ticket Granting Ticket)

Key Distribution Centre

Authentication Server

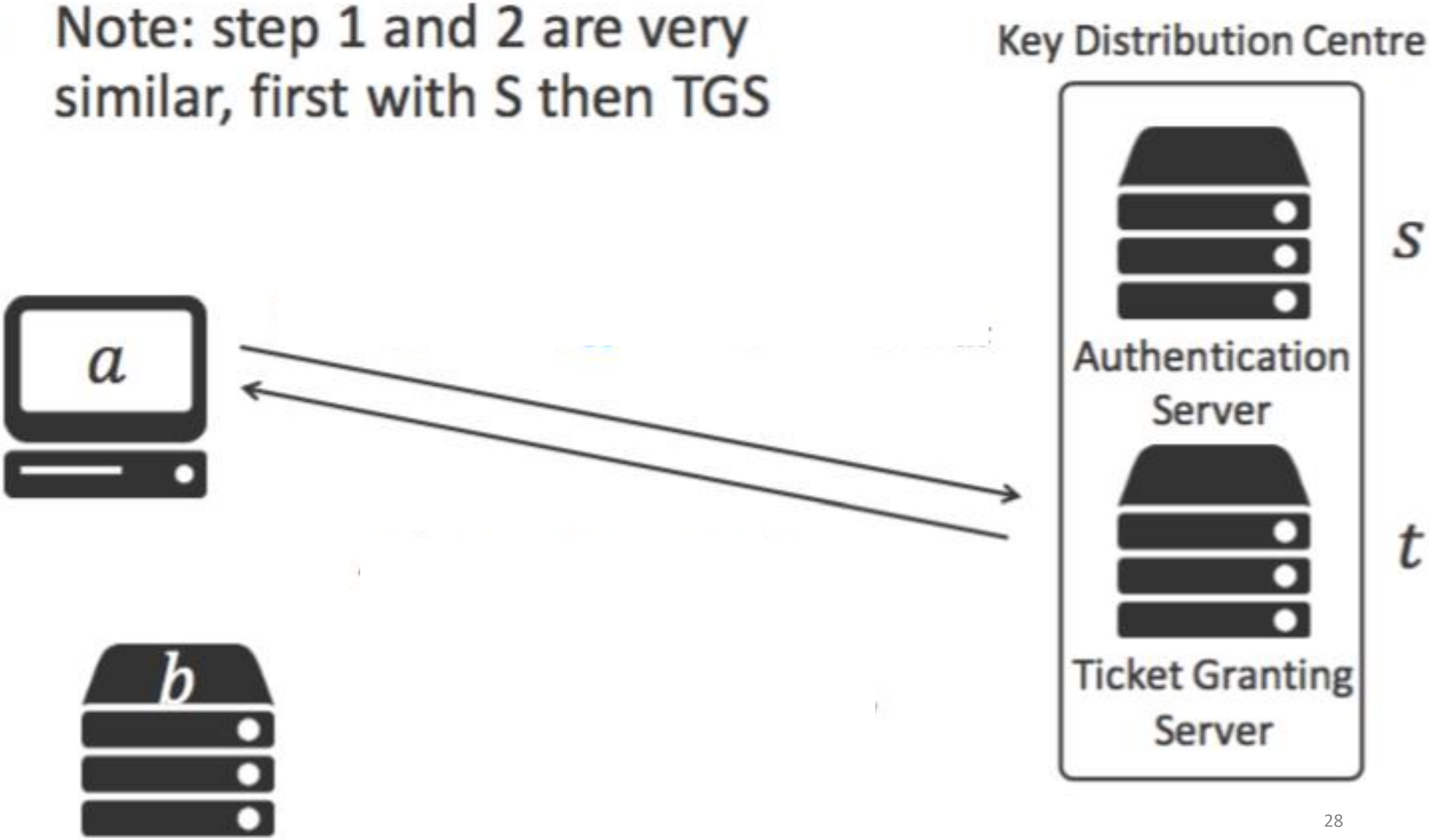
s

Ticket Granting Server

t

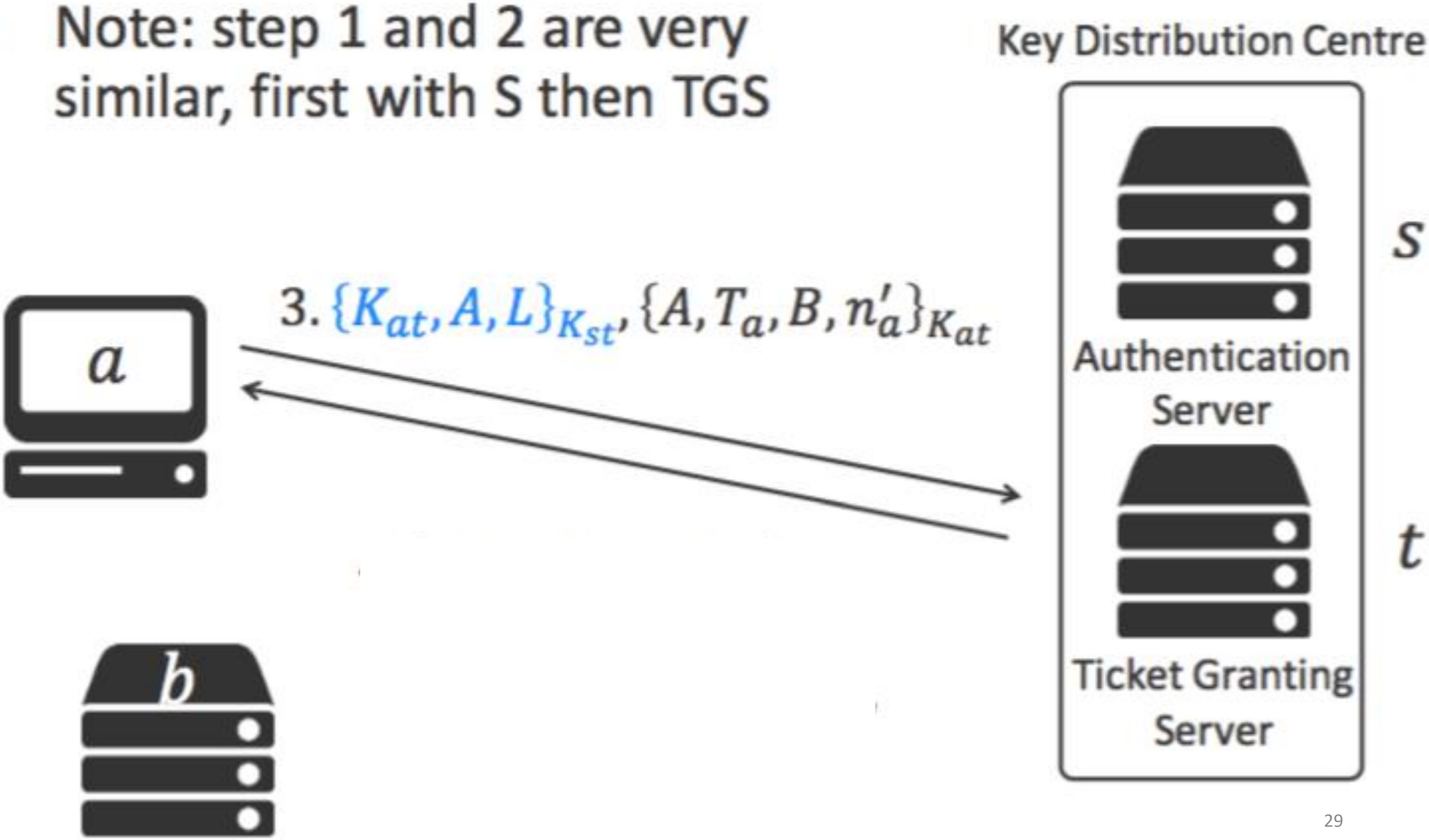
Step 2, Obtaining Tickets

- Note: step 1 and 2 are very similar, first with S then TGS



Step 2, Obtaining Tickets

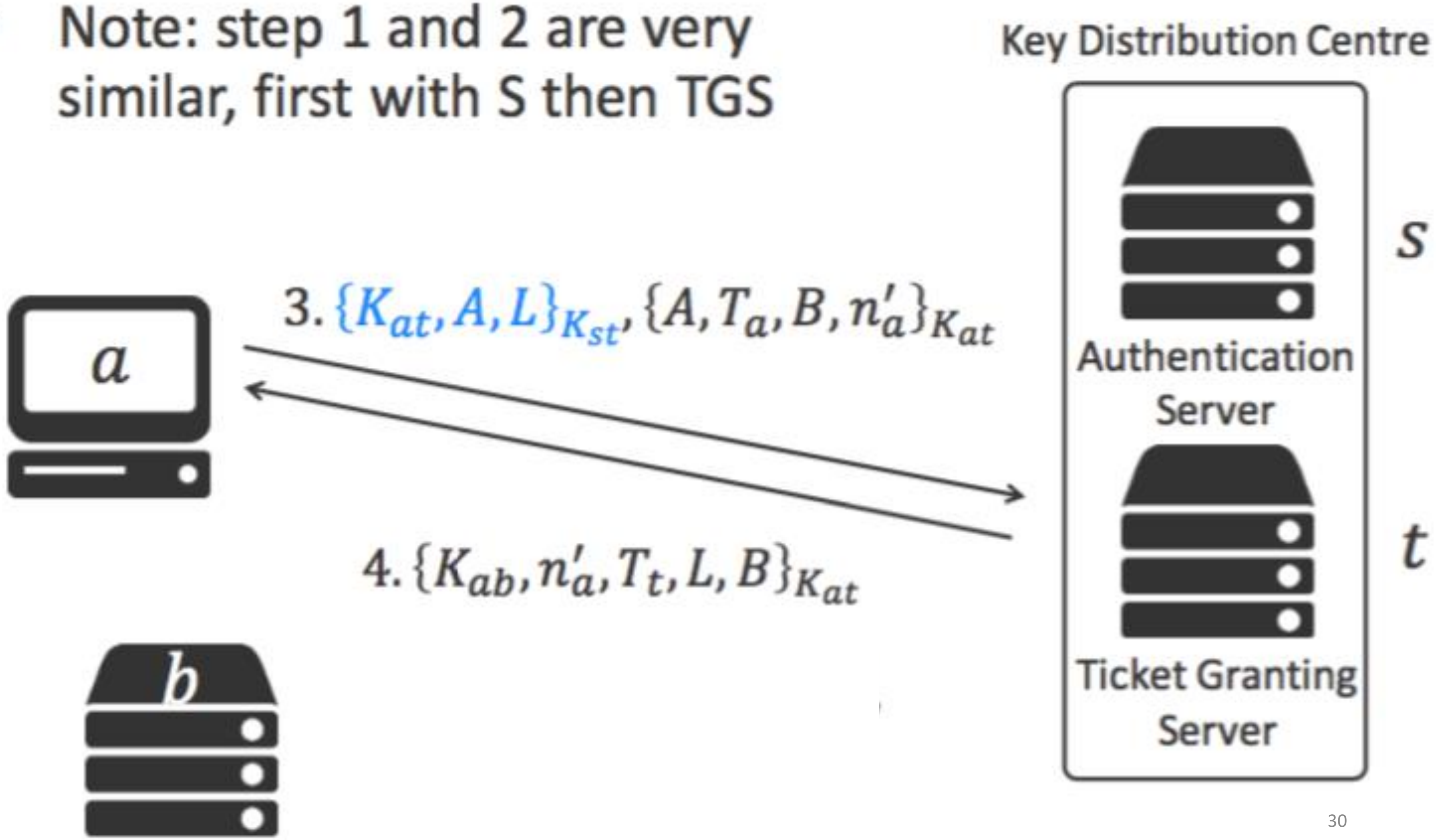
- Note: step 1 and 2 are very similar, first with S then TGS



3. $\{K_{at}, A, L\}_{K_{st}}, \{A, T_a, B, n'_a\}_{K_{at}}$

Step 2, Obtaining Tickets

- Note: step 1 and 2 are very similar, first with S then TGS



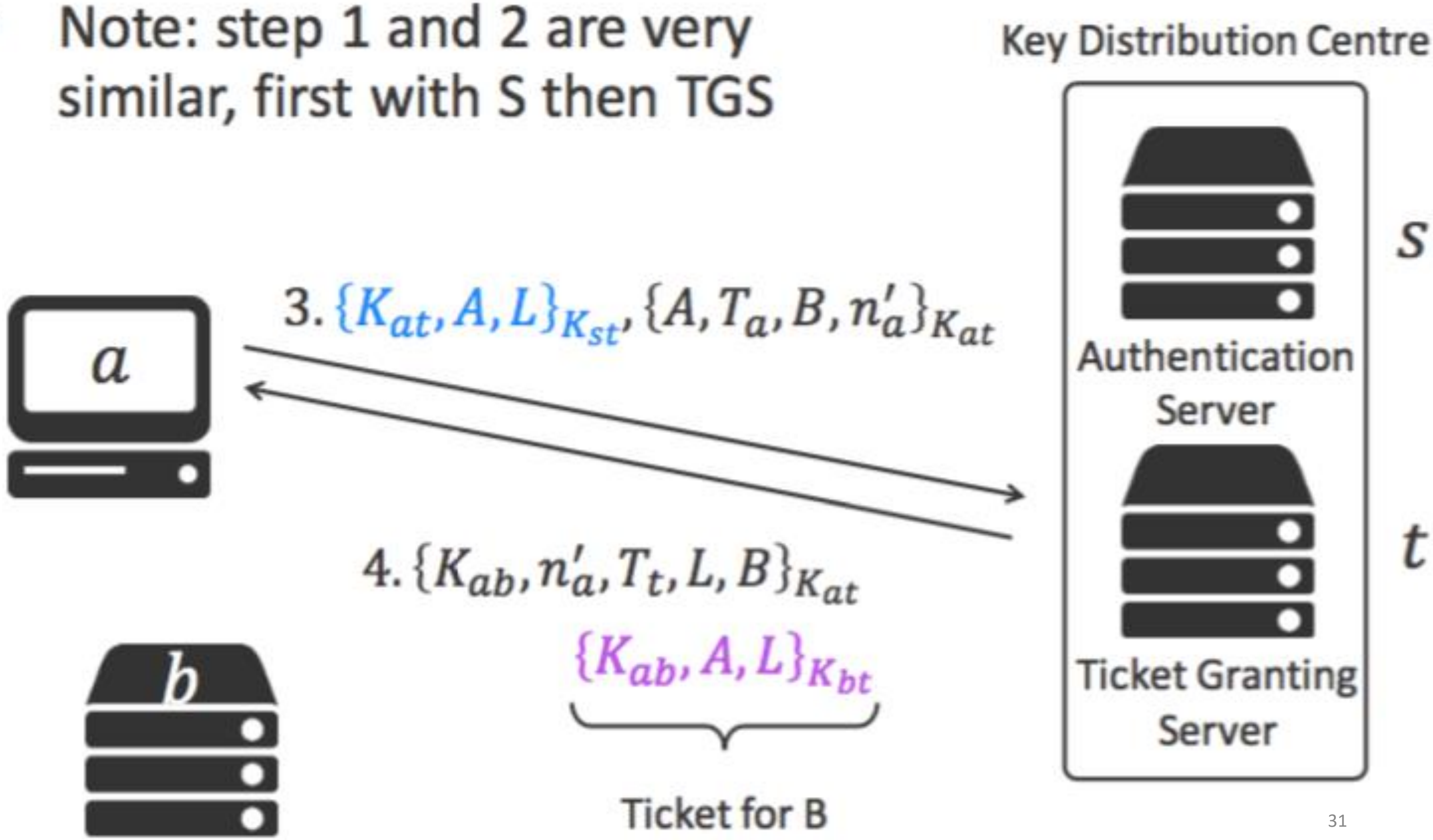
Key Distribution Centre

3. $\{K_{at}, A, L\}_{K_{st}}, \{A, T_a, B, n'_a\}_{K_{at}}$

4. $\{K_{ab}, n'_a, T_t, L, B\}_{K_{at}}$

Step 2, Obtaining Tickets

- Note: step 1 and 2 are very similar, first with S then TGS



Key Distribution Centre

a

b

s

Authentication Server

t

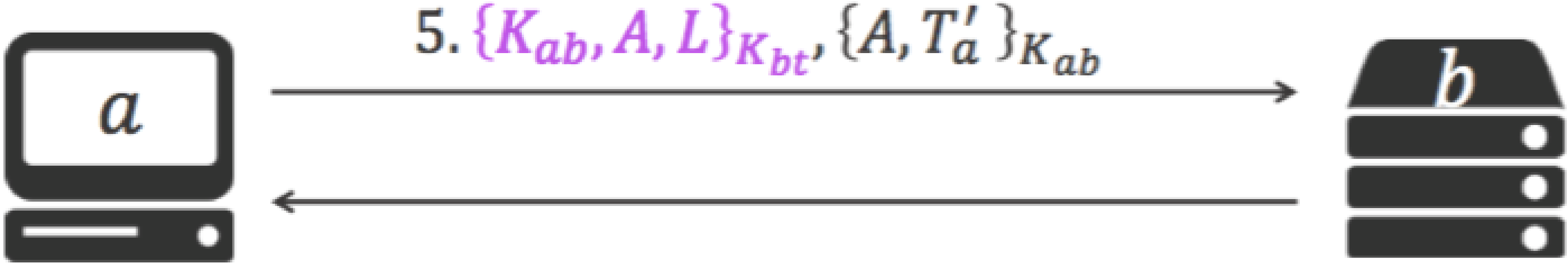
Ticket Granting Server

3. $\{K_{at}, A, L\}_{K_{st}}, \{A, T_a, B, n'_a\}_{K_{at}}$

4. $\{K_{ab}, n'_a, T_t, L, B\}_{K_{at}}$

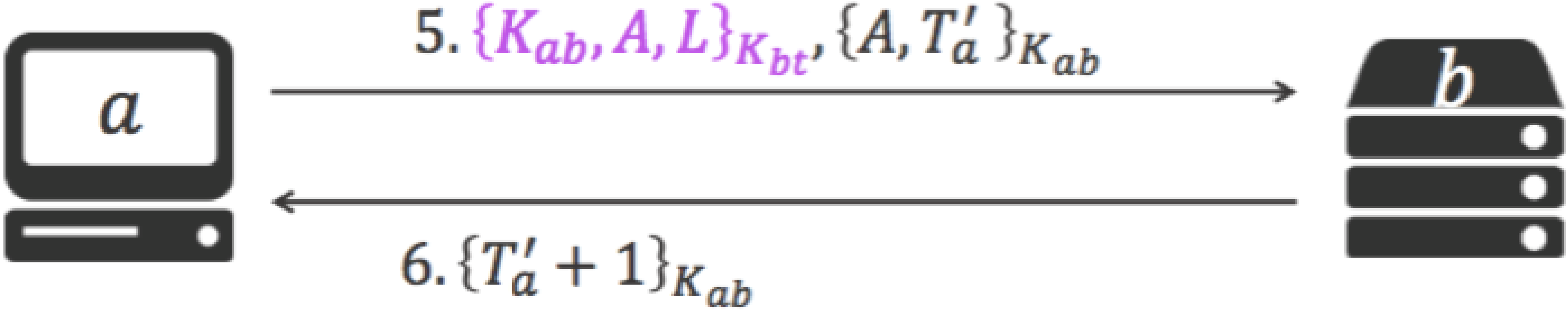
$\underbrace{\{K_{ab}, A, L\}_{K_{bt}}}_{\text{Ticket for B}}$

Step 3, Using A Service



5. $\{K_{ab}, A, L\}_{K_{bt}}, \{A, T'_a\}_{K_{ab}}$

Step 3, Using A Service



5. $\{K_{ab}, A, L\}_{K_{bt}}, \{A, T'_a\}_{K_{ab}}$

6. $\{T'_a + 1\}_{K_{ab}}$

Important Features

- Including nonces and timestamps prevents replay attacks
  - But, clocks must be synchronised between principals
- Windows Kerberos buries domain group IDs inside tickets, for access checks
- The ticket granting ticket usually exists until log-off, or rotates daily
  - A problem if user rights have been changed - TOCTTOU

Summary

- Windows Security
  - Permissions
  - Access Tokens
  - Authentication
- Kerberos

Gollmann
Chapter 8, 15.4