

# **Introduction to Kerberos**

**Kerberos and Domain  
Authentication**

# Key Kerberos Concepts

## Microsoft Kerberos is:

- An authentication protocol
- Based on encrypted “tickets” with client credentials
- The default authentication package in Microsoft® Windows® 2000
- The basis for transitive domain trusts
- Based on RFC 1510 and draft revisions
- More efficient than NTLM
- Extensible

# Kerberos' Goals

- ◆ **Authenticate User's Identity**
  - **User Principal Name**  
(someone@microsoft.com)
- ◆ **Securely Delivers User Credentials in "Ticket"**
  - **Privilege Attribute Certificate (PAC)**
- ◆ **Privacy Through Encryption**
- ◆ **Kerberos Uses Keys for Encryption**
- ◆ **Kerberos Authenticator Prevents Packet Anti-Replay**

# Kerberos Terms

**Authentication Service (AS):** This service runs on the Key Distribution Center (KDC) server. It authenticates a client logon and issues a Ticket Granting Ticket (TGT) for future authentication.

**Ticket Granting Service (TGS):** This service runs on the KDC server. It grants tickets to TGT holding clients for a specific application server or resource.

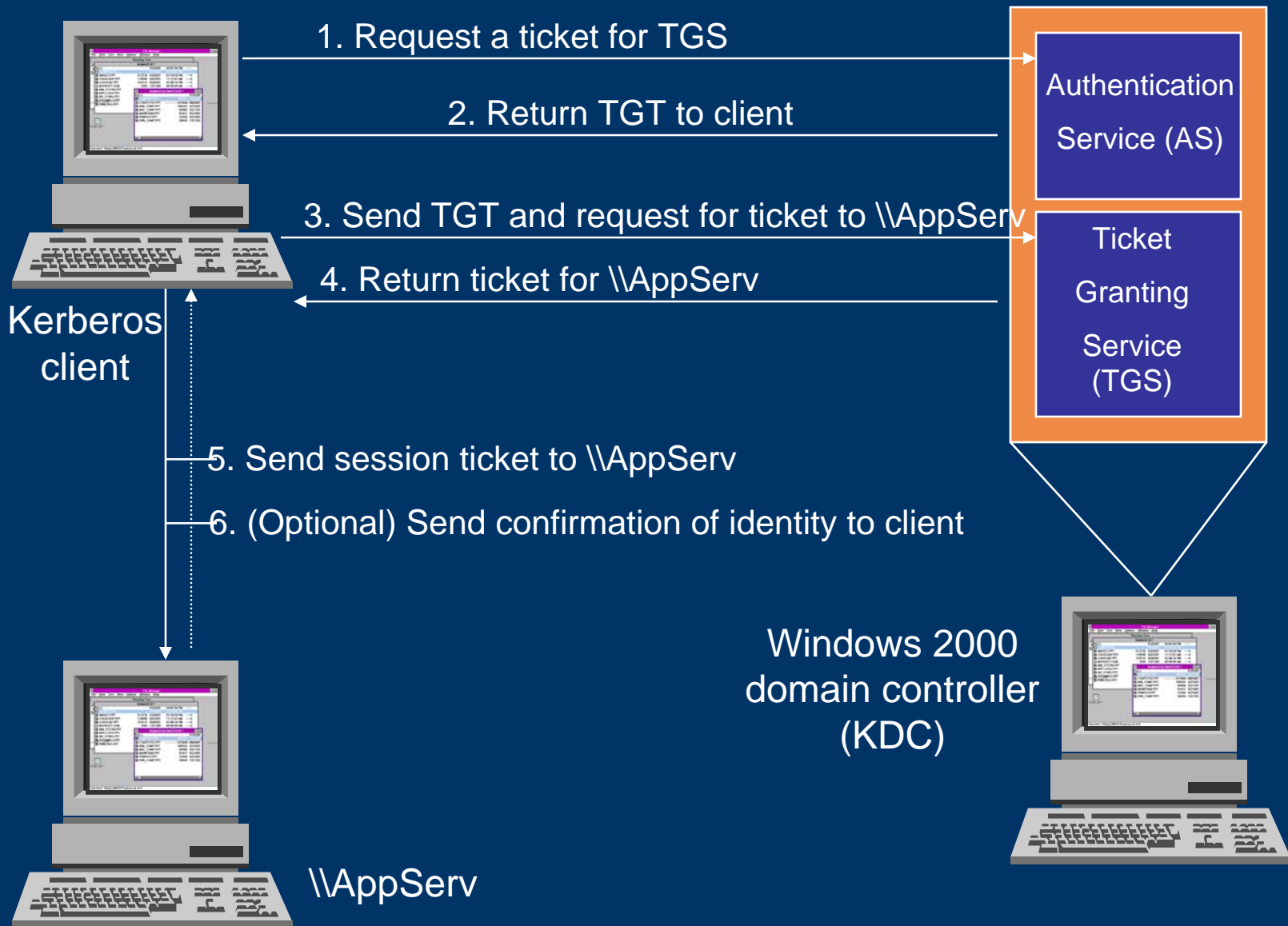
**Ticket Granting Ticket (TGT):** This ticket is received from the Authentication Service (SA) that contains the client's Privilege Attribute Certificate (PAC).

**Ticket:** This ticket is received from the TGS that provides authentication for a specific application server or resource.

**Session Key:** This is the derived value used strictly for the immediate session between a client and a resource.

**Privilege Attribute Certificate (PAC):** This is strictly used in Windows 2000 Kerberos authentication. Contains information such as the user's Security ID (SID), group membership SIDs, and users' rights on the domain.

# Domain Authentication and Resource Access



# Keys Used in Kerberos

- ◆ Long-Term Symmetric Keys
- ◆ Short-Term Symmetric Keys
- ◆ Asymmetric Keys

# Kerberos and Internet Protocol (IP)

## Transport: UDP/TCP

- ◆ **RFC 1510 specifies UDP for transport.**
- ◆ **Kerberos adds user credentials to messages called by the PAC.**
- ◆ **Messages of less than 2,000 bytes, such as interaction with MIT KDC server or client, are sent over UDP.**
- ◆ **Messages of 2,000 bytes or more, such as interaction with Microsoft KDC server or client, are sent over TCP.**

# Locating a KDC

- ◆ The Kerberos KDC runs on every Windows 2000 domain controller.
- ◆ Kerberos client queries for a domain controller:
  - ◆ Queries Netlogon if it is running
  - ◆ Queries DNS
- ◆ Kerberos client attempts to contact three times, and then rediscovers KDCs.

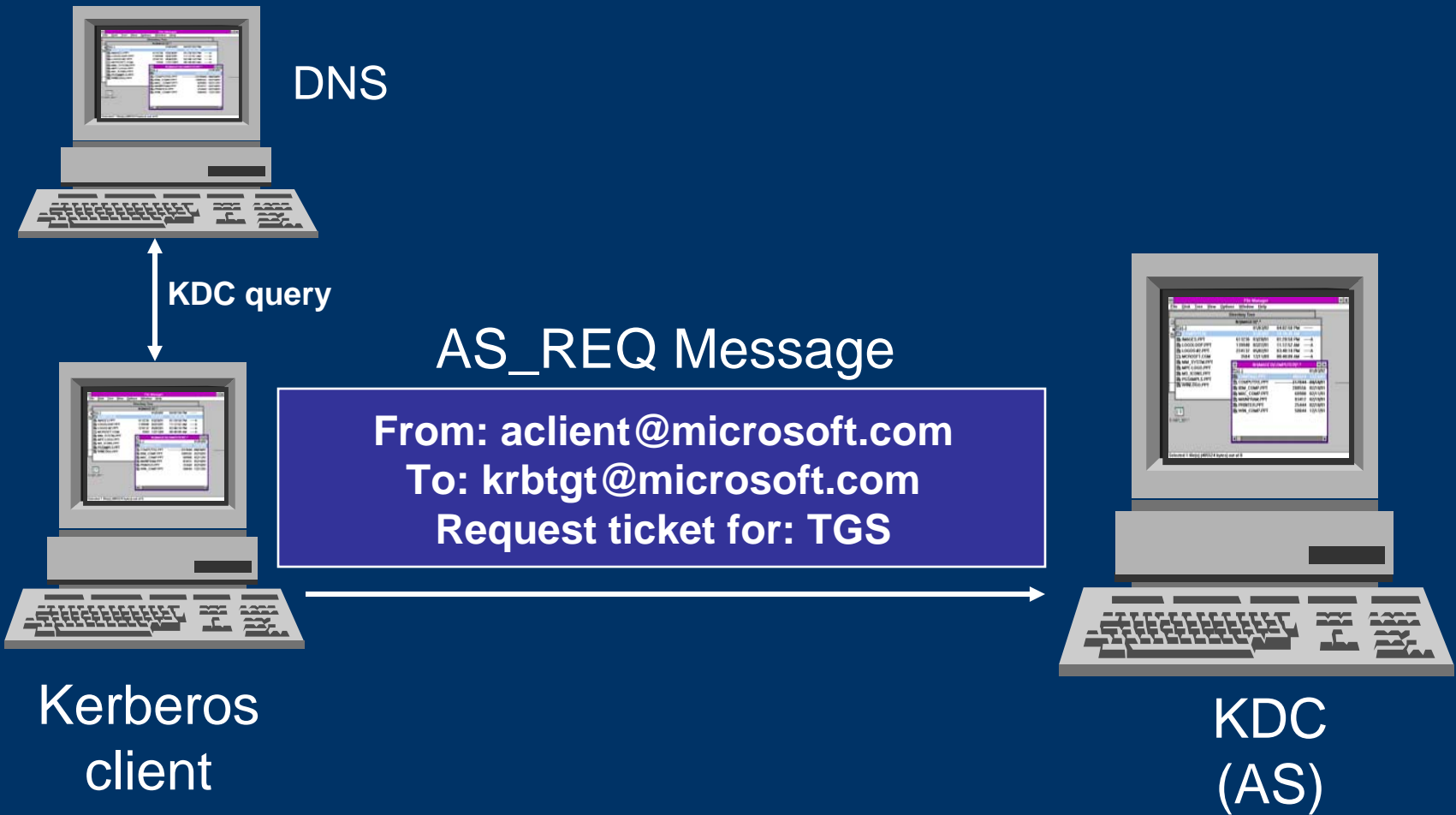
# Requesting a Ticket

- ◆ Requests go to the KDC:
  - TGT sends requests to the AS
  - Session ticket sends requests to the TGS
- ◆ Contents of ticket requests:
  - Names
  - Times
  - Encryption method
  - Properties

# The Authenticator

- ◆ Authenticator Authenticates Ticket
- ◆ Why Is This Necessary?
- ◆ How Does This Work?
- ◆ The Authenticator's Time Stamp
- ◆ Authenticator Field Contents

# Message 1: The Authentication Server Request



# Message 2: The Authentication Server Response

## AS\_REP Message

From: krbtgt@microsoft.com  
To: aclient@microsoft.com  
Contains ticket for: TGS (TGT)  
Contains: Session key for TGS



Kerberos  
client



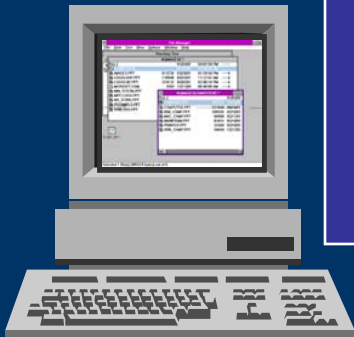
KDC  
(AS)

Ticket (TGT) encrypted with TGS server key  
Session key encrypted with user key

# Message 3: The Ticket Granting Server Request

## TGS\_REQ Message

From: aclient@microsoft.com  
To: krbtgt@microsoft.com  
Contains ticket: TGT  
Contains Authenticator  
Request ticket for: AppServ



Kerberos  
client



KDC  
(TGS)

TGT encrypted with TGS server key  
Authenticator encrypted with TGS session key

# Message 4: The Ticket Granting Server Response

## TGS\_REP Message

From: krbtgt@microsoft.com  
To: aclient@microsoft.com  
Contains ticket for: AppServ  
Contains: Session Key for AppServ



Kerberos  
client



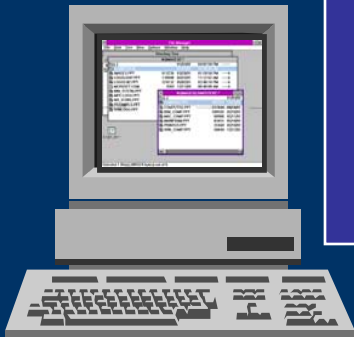
KDC  
(TGS)

Ticket encrypted with AppServ server key  
AppServ session key encrypted with TGS session key

# Message 5: The Application Server Request

## AP\_REQ Message

From: aclient@microsoft.com  
To: appserv@microsoft.com  
Contains ticket for: AppServ  
Contains Authenticator  
Contains: Mutual Authentication  
Request (optional)



Kerberos  
client



AppServ

Ticket encrypted with AppServ server key  
Authenticator encrypted with AppServ session key

# Message 6: The Optional Application Server Response

## AP\_REP Message

From: appserv@microsoft.com  
To: aclient@microsoft.com  
Contains: Mutual Authentication  
Response

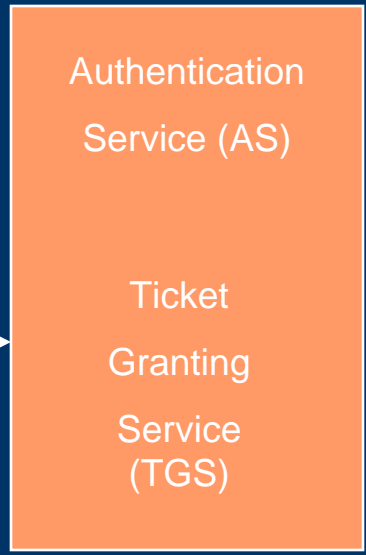
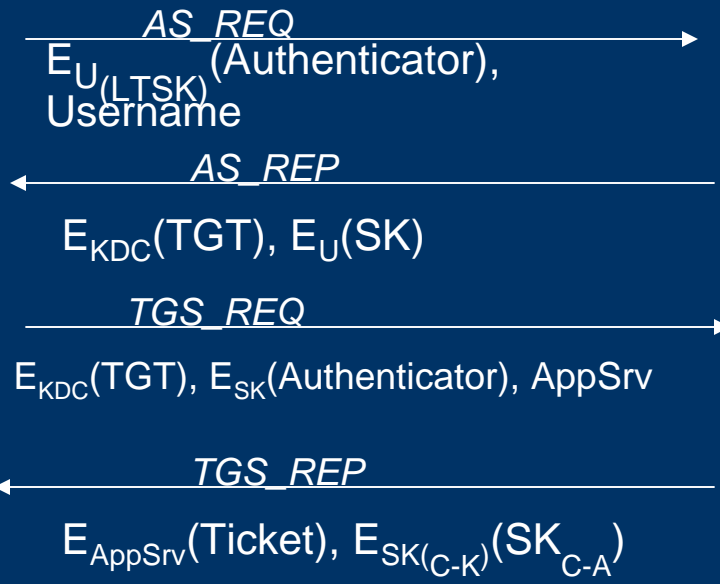
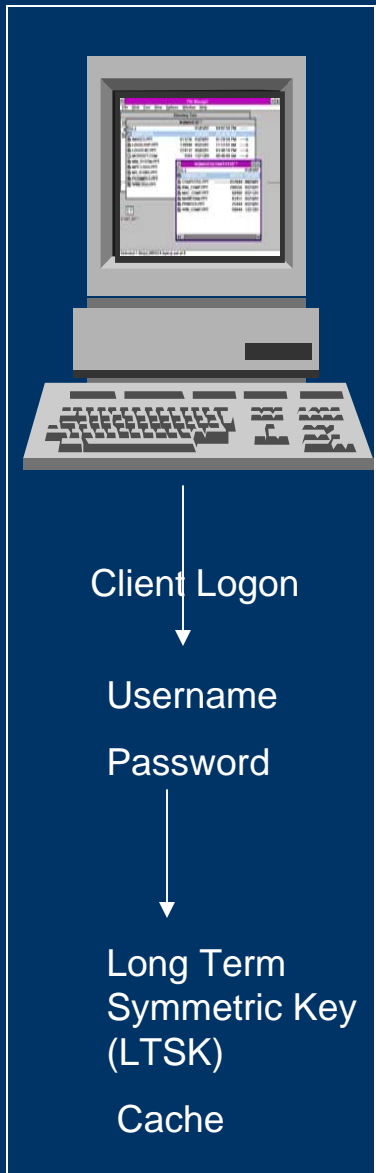


Kerberos  
client

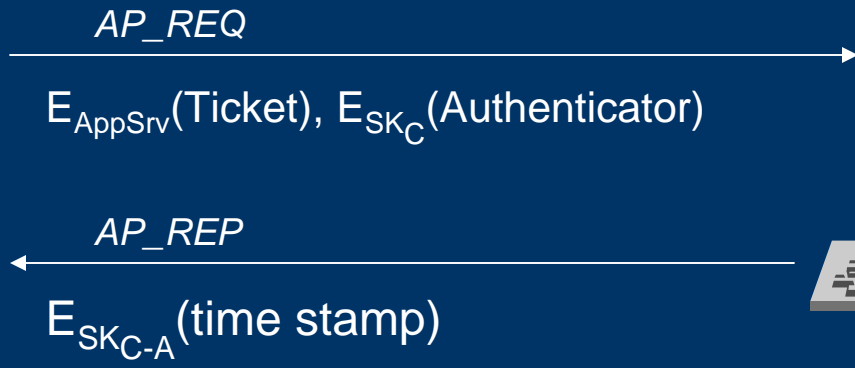


AppServ

Message encrypted with session key



Windows 2000 domain controller (KDC)



\\AppServ

**Legend**

LTSK: Long Term Symmetric Key

SK: Session Key

E: Encrypted

C: Client

K: KDC

A: AppSrv

# Kerberos Policy

## ◆ Kerberos Policy Settings

On a domain controller in your domain in Administrative Tools, click Domain Security Policy, click Windows Settings, click Security Settings, click Account Policies, and then click Kerberos Policy.

- Enforce logon restrictions: Yes
- Maximum lifetime that a user ticket can be renewed: 7 days
- Maximum service ticket lifetime: 60 minutes
- Maximum tolerance for synchronization of computer clocks: 5 minutes
- Maximum TGT lifetime: 10 hours

# Kerberos Tools

- ◆ **KerbTray**
  - **Displays ticket information**
  - **Runs on the taskbar**
  - **Lists or purges tickets**

# Kerberos Tools (2)

## ◆ NetDom

- Included with Microsoft® Windows® 2000 Server
- Displays domain information
- Resets broken Kerberos transitive trusts

# Review

- ◆ Kerberos Concepts
- ◆ Authentication
- ◆ Resource Authentication
- ◆ Kerberos Tools

***Microsoft***<sup>®</sup>

**Where do you want to go today?**<sup>®</sup>

