Windows 2000 Security Architecture

Peter Brundrett
Program Manager
Windows 2000 Security
Microsoft Corporation

Topics

- Single Sign-on
- Kerberos v5 integration
- Active Directory security
- Delegation of authentication
- Public key infrastructure
- Encrypting file system
- Network security
- Security policy
- Secure Windows

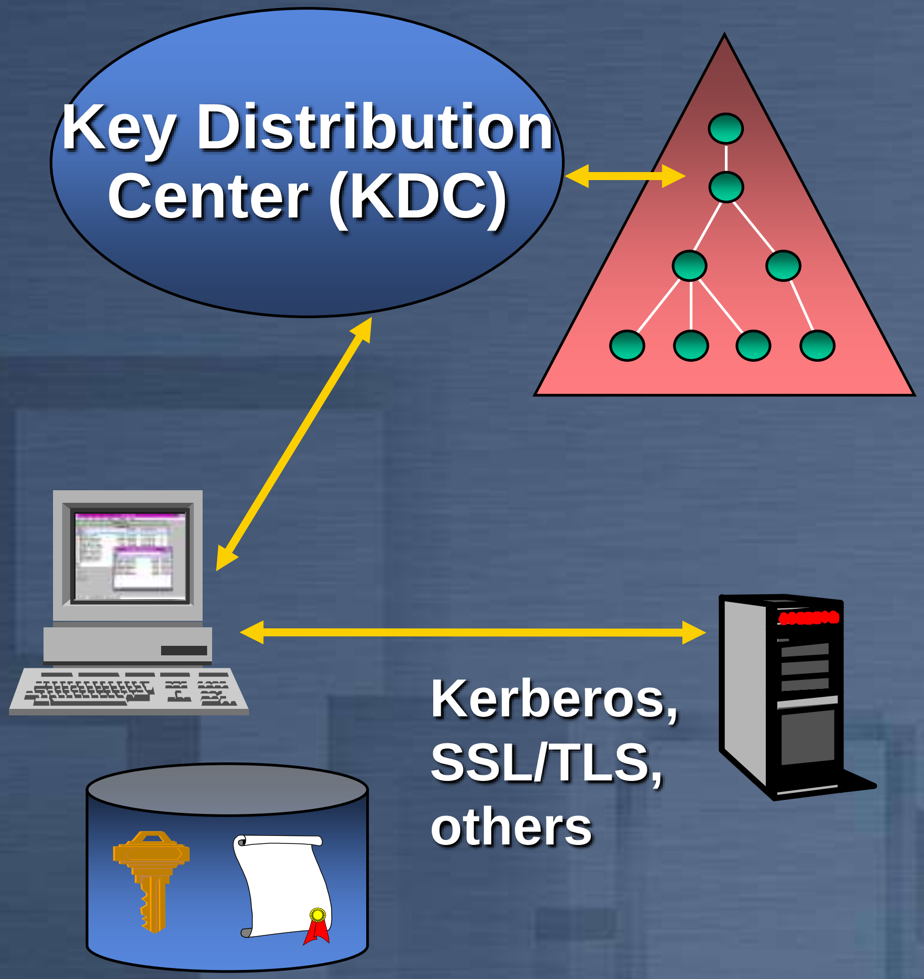
Platform Security Requirements

- Single enterprise logon
- Strong authentication
- Authorization
- Secure communications
- Mandatory policy
- Auditing
- Interoperability
- Extensible architecture

***Goal:* Deliver Windows 2000 as the most secure high volume OS**

Windows 2000
Single Sign On

- Single account store in Active Directory
- Integrated Kerberos v5 logon
- Protected store for public key credentials
- Industry standard network security protocols

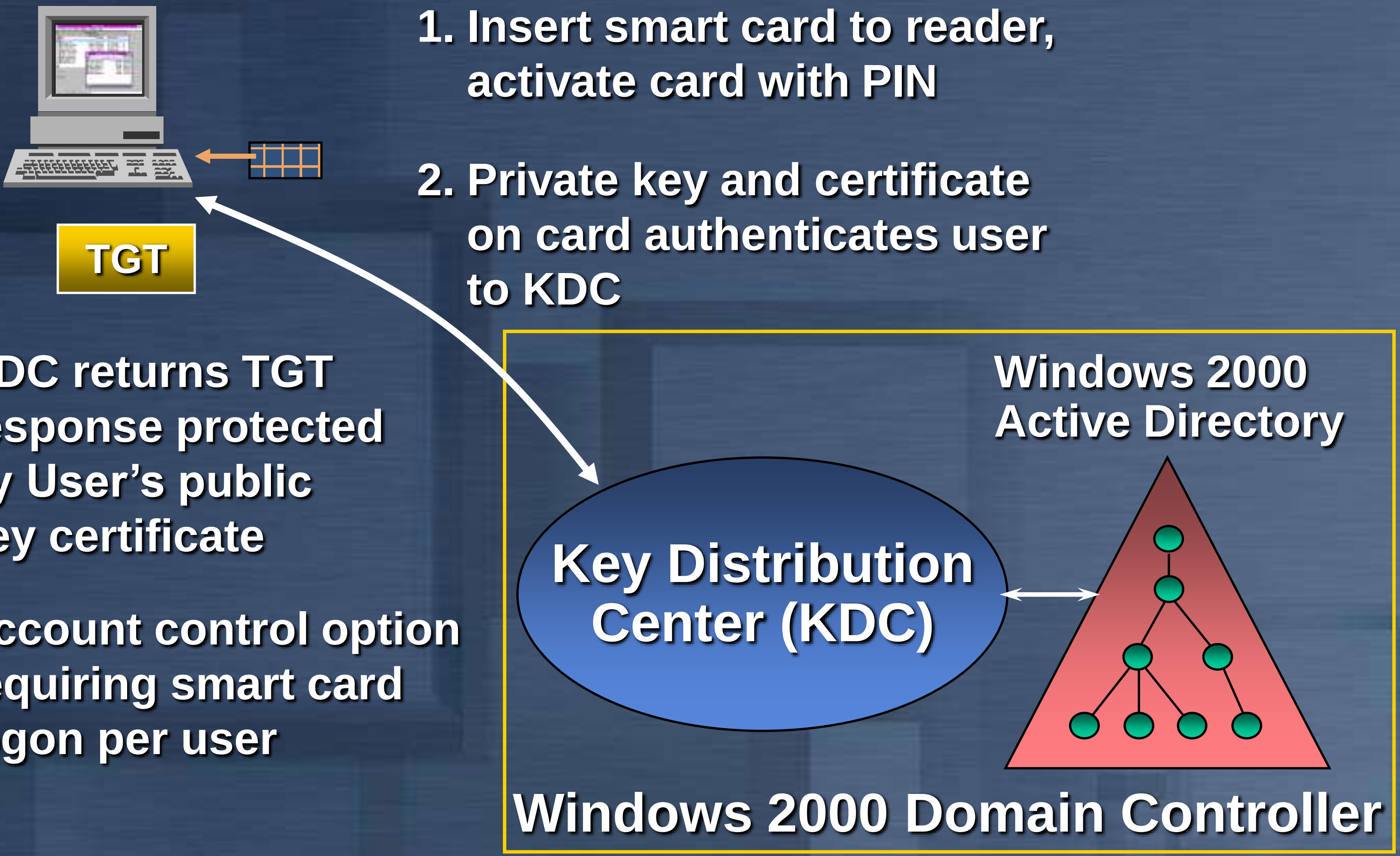


Key Distribution Center (KDC)

Kerberos, SSL/TLS, others

Smart Card Logon

1. Insert smart card to reader, activate card with PIN
2. Private key and certificate on card authenticates user to KDC
3. KDC returns TGT response protected by User’s public key certificate
4. Account control option requiring smart card logon per user



TGT

Key Distribution Center (KDC)

Windows 2000 Active Directory

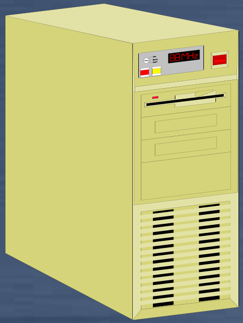
Windows 2000 Domain Controller

Kerberos V5 Integration

Client

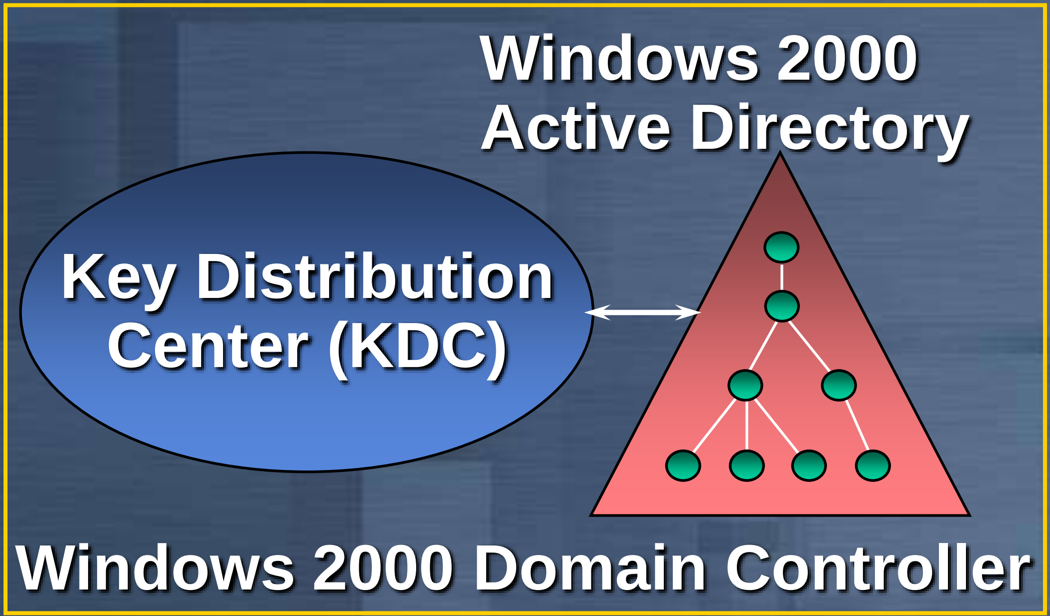
Kerberos SSPI provider manages credentials and security contexts

Server



Service ticket authorization data supports NT access control model

KDC relies on the Active Directory as the store for security principals and policy



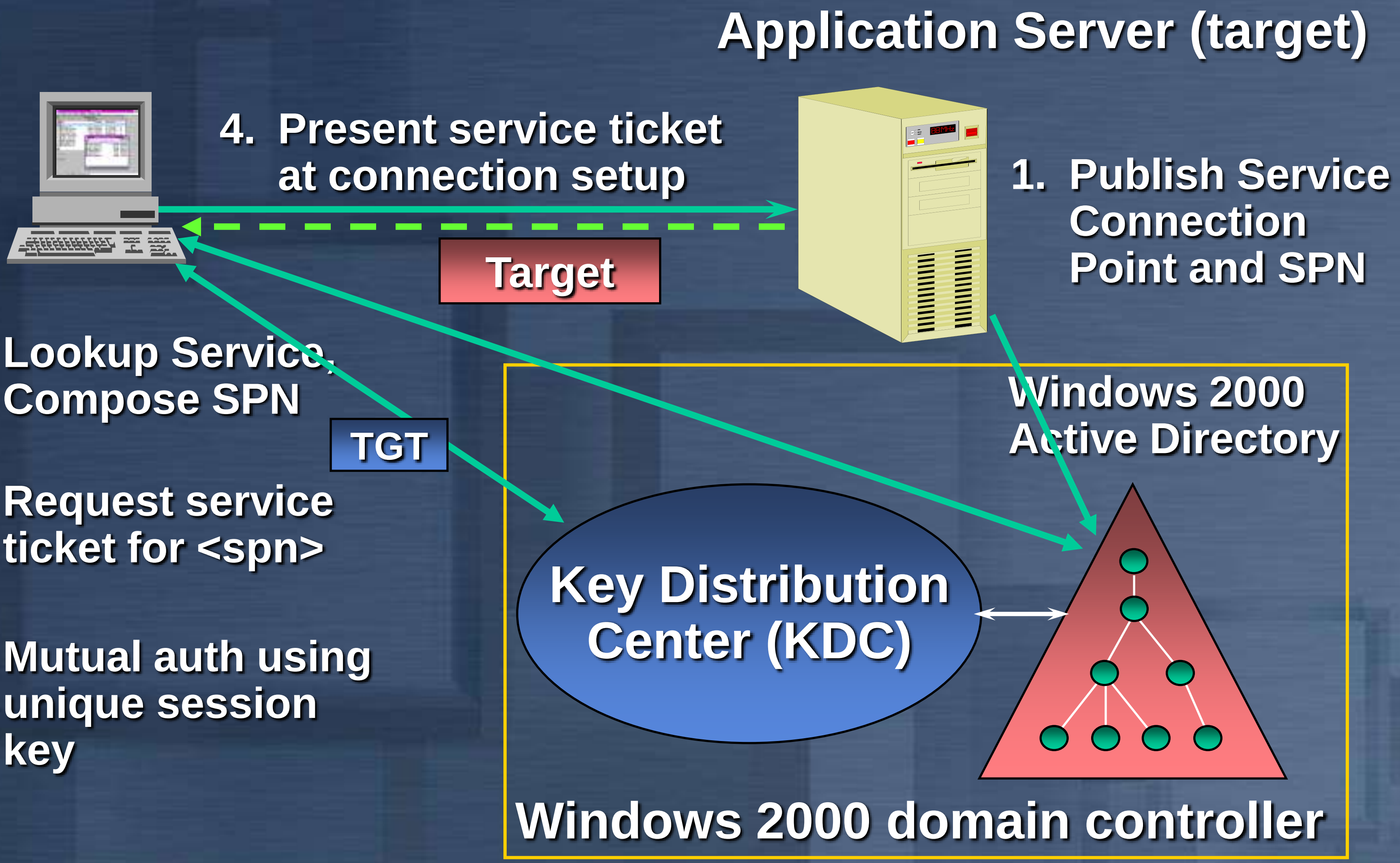
Windows 2000 Active Directory

Key Distribution Center (KDC)

Windows 2000 Domain Controller

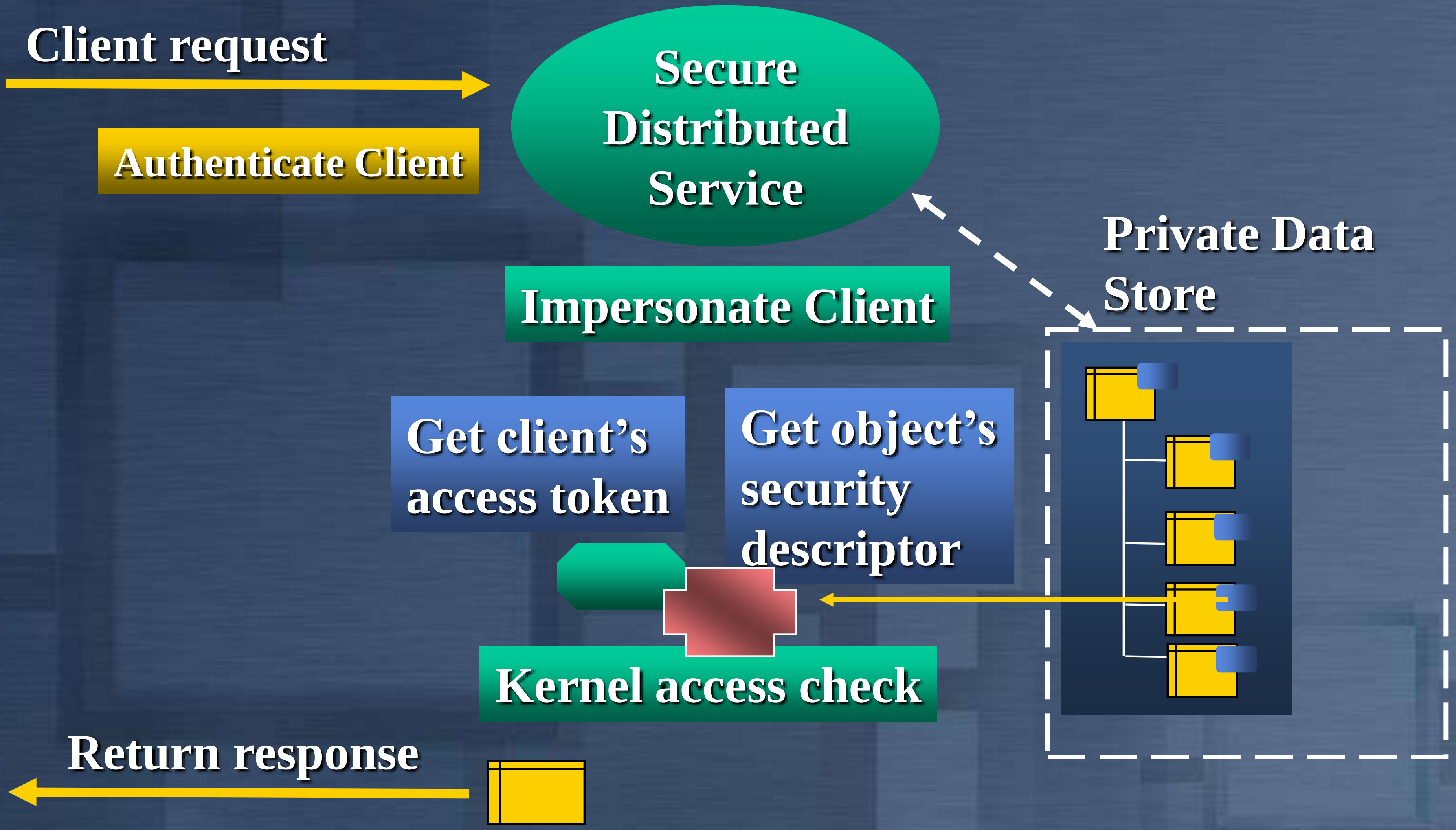
Kerberos Authentication

Mutual Authentication

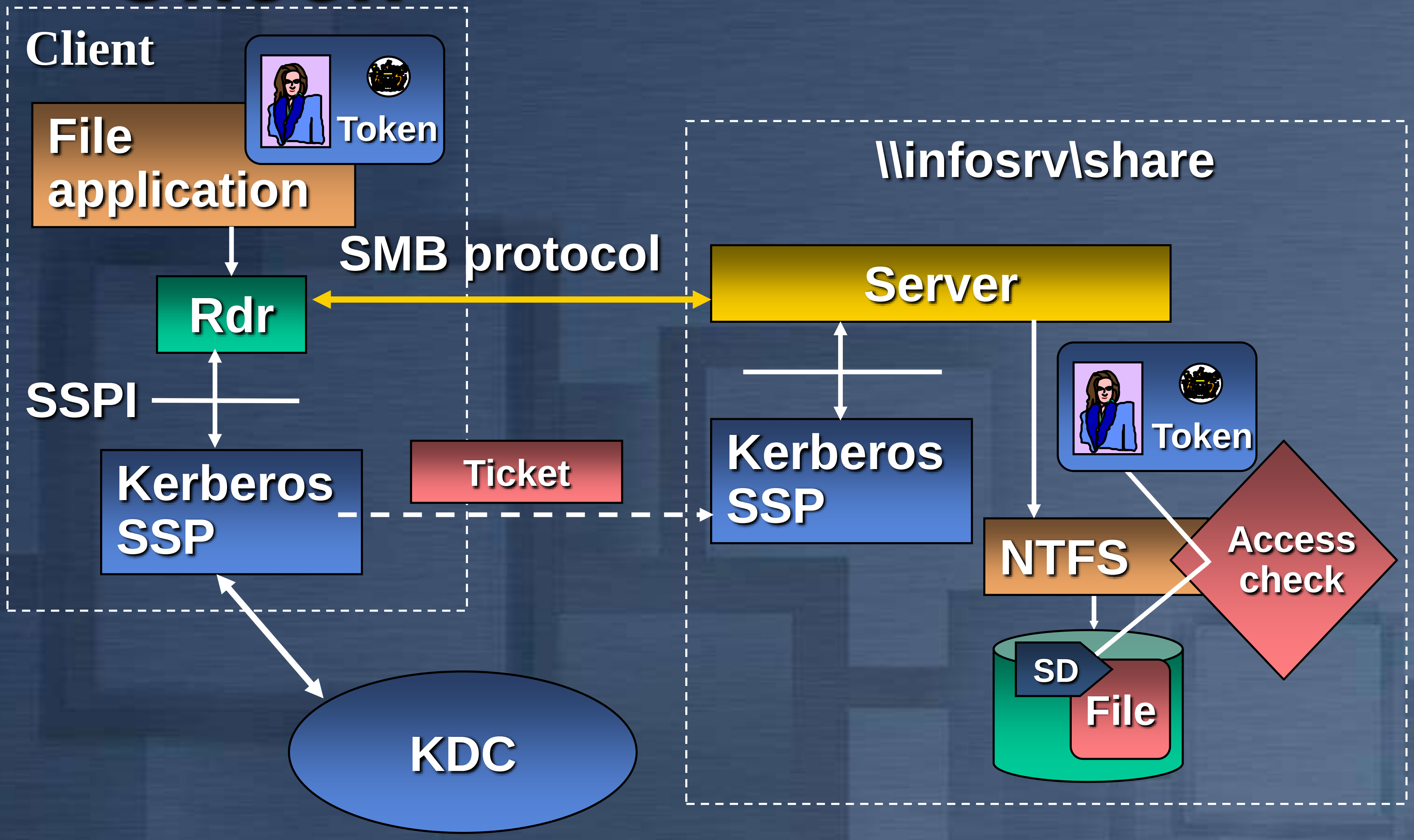

Application Server (target)
Target
TGT
Windows 2000 Active Directory
Key Distribution Center (KDC)
Windows 2000 domain controller

1. Publish Service Connection Point and SPN
2. Lookup Service, Compose SPN
3. Request service ticket for <spn>
4. Present service ticket at connection setup
5. Mutual auth using unique session key

Secure Distributed Services Model



Remote File Access Check



Windows 2000 Integration

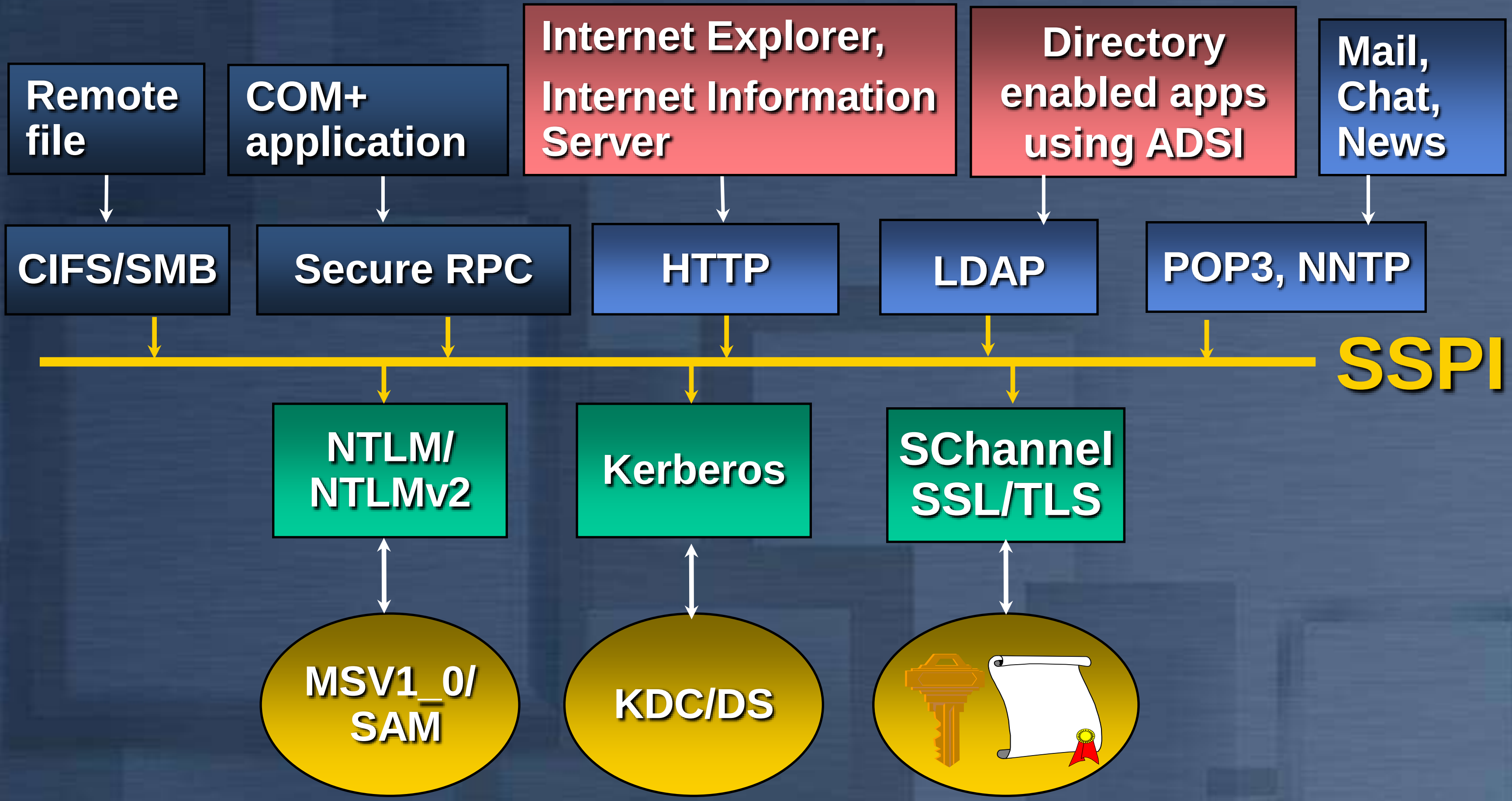
Kerberos Authentication Use

- LDAP to Active Directory
- CIFS/SMB remote file access
- Secure dynamic DNS update
- System management tools
- Host-host IP security using IKE
- Secure Intranet web services in IIS
- Authenticate certificate request to Enterprise CA
- COM+/RPC security provider

Cross-platform Interoperability

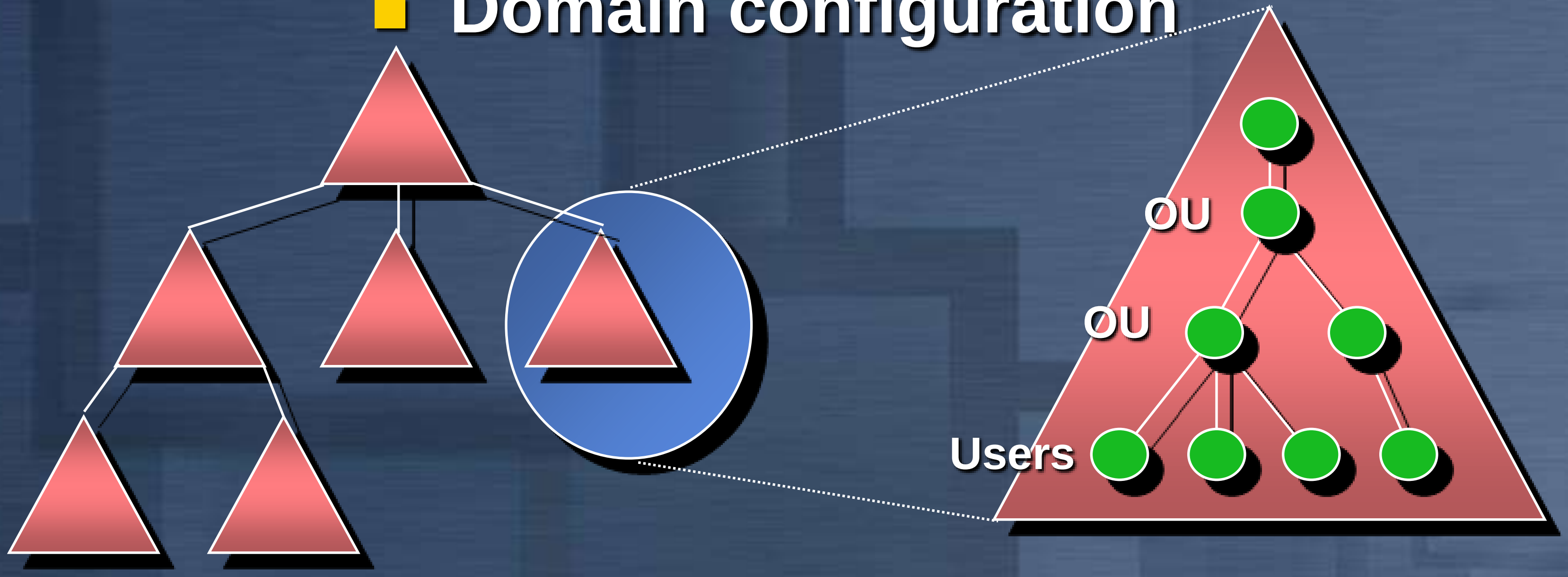
- Based on Kerberos V5 Protocol
  - RFC 1510 and RFC 1964 token format
  - Testing with MIT Kerb V5
- Windows 2000 hosts the KDC
  - UNIX clients to Unix Servers
  - UNIX clients to Windows Servers
  - NT clients to UNIX Servers
- Cross-realm authentication
  - UNIX realm to Windows domain

Architecture For Multiple Authentication Services



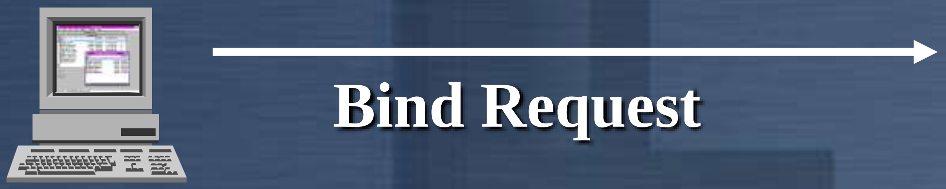
Windows 2000 Active Directory

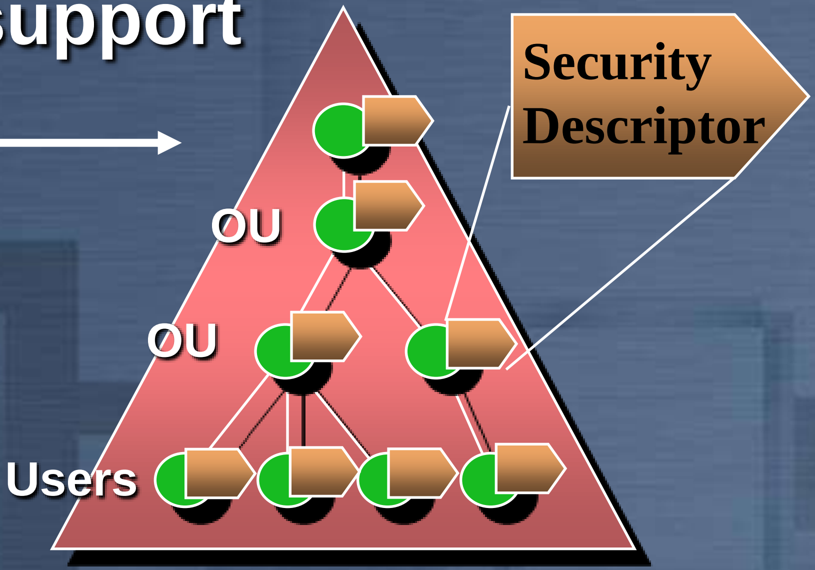
- Domain hierarchy: *domain tree*
  - Organizational Unit (OU) hierarchy within a domain
    - Users, groups, machines
    - Domain configuration



Active Directory
Authentication and Access Control

- LDAP v3 is core directory access protocol
  - Authenticate using SASL and Kerberos protocol
  - LDAP with SSL/TLS support





- Every object has a unique ACL
  - Like NTFS folders and files

Active Directory

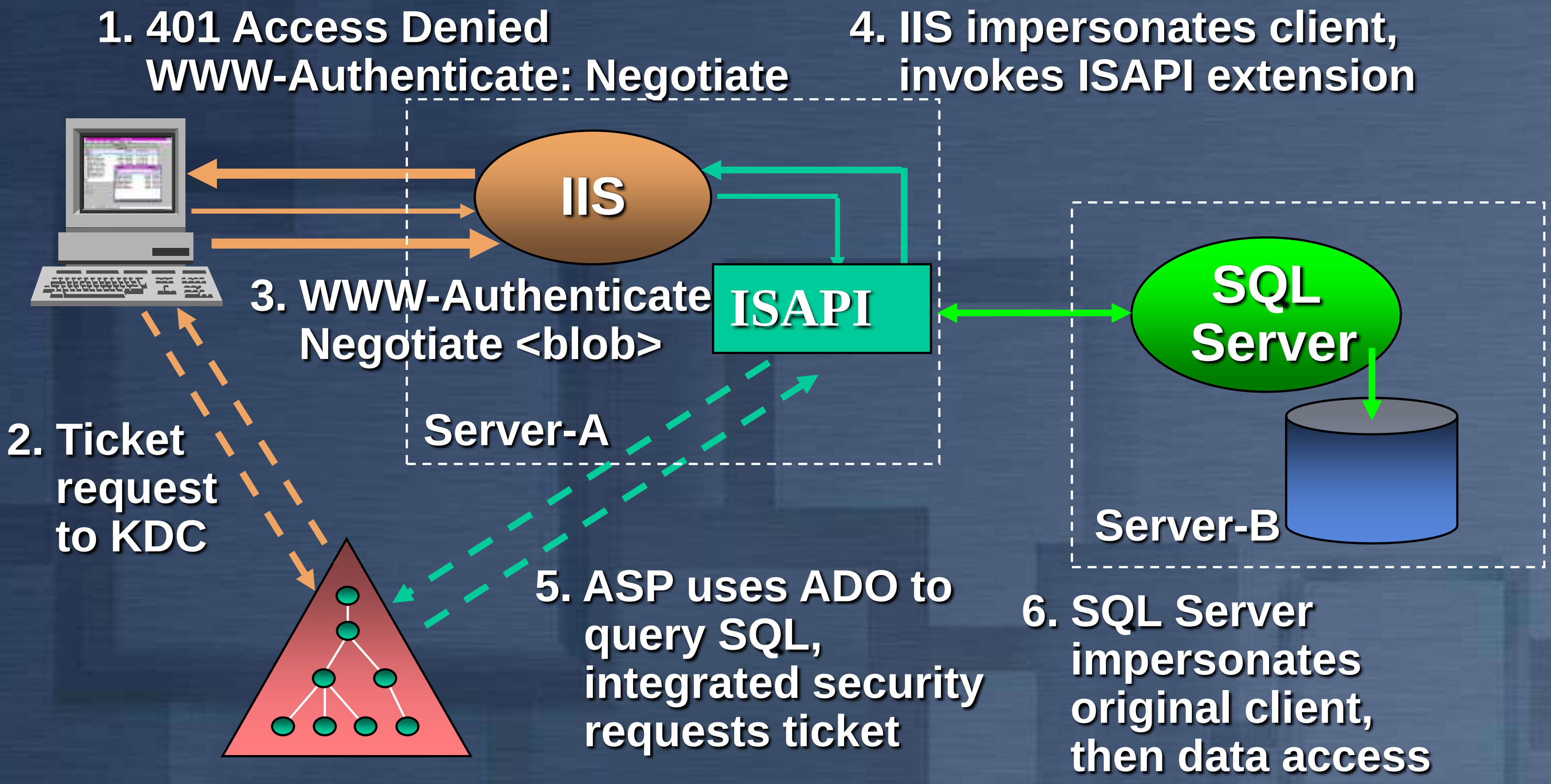
Security administration

- Delegation of administration
  - Grant permissions at organizational unit (OU) level
  - Who creates OUs, users, groups, etc.
- Fine-grain access control
  - Grant or deny permissions on per-property level, or a group of properties
    - Read property
    - Write property
- Per-property auditing

Secure Applications

- Connection Authentication
  - Establish Credentials
  - Mutual authentication of client and server
- Secure Communication
  - Message privacy and integrity
- Impersonation and Delegation
  - Assuming client’s identity
- Authorization and Auditing
  - Using security descriptors

Example: Delegation in Action



1. 401 Access Denied
   WWW-Authenticate: Negotiate

2. Ticket
   request
   to KDC

3. WWW-Authenticate
   Negotiate <blob>

4. IIS impersonates client,
   invokes ISAPI extension

5. ASP uses ADO to
   query SQL,
   integrated security
   requests ticket

6. SQL Server
   impersonates
   original client,
   then data access

Interoperability

Cross Platform Secure 3-Tier App

Windows 2000
Professional

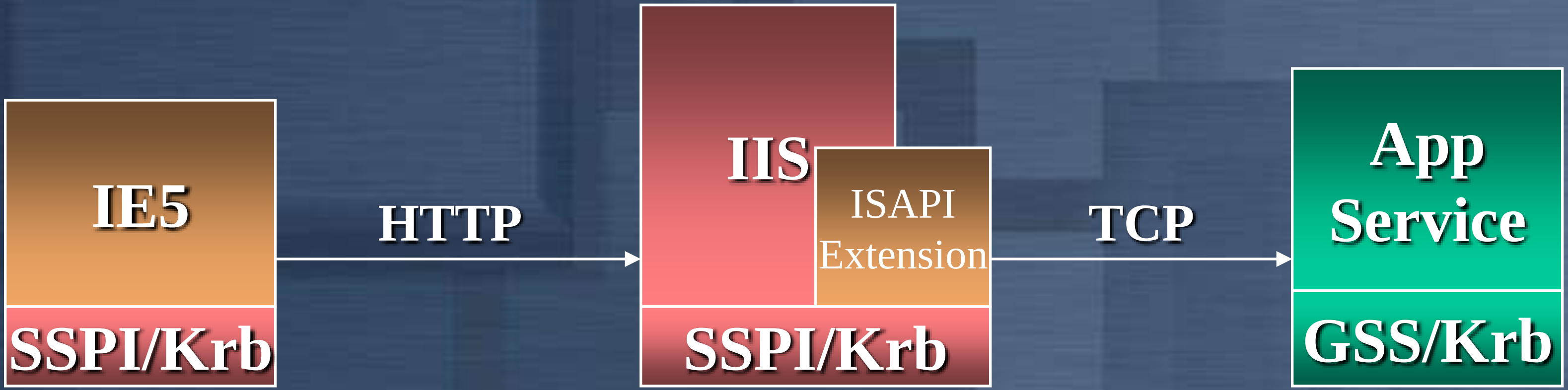
Smart Card Logon

Windows 2000
Server

Web Server

Solaris
UNIX Server

Oracle DB Application



IE5

SSPI/Krb

HTTP

IIS

ISAPI Extension

SSPI/Krb

TCP

App Service

GSS/Krb

Public Key Components

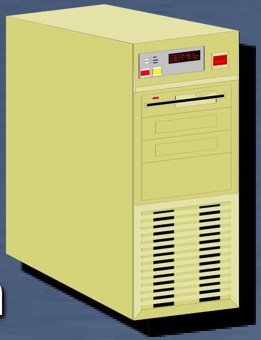
For clients

- User key and certificate mgmt
- Secure channel
- Secure storage
- CA enrollment

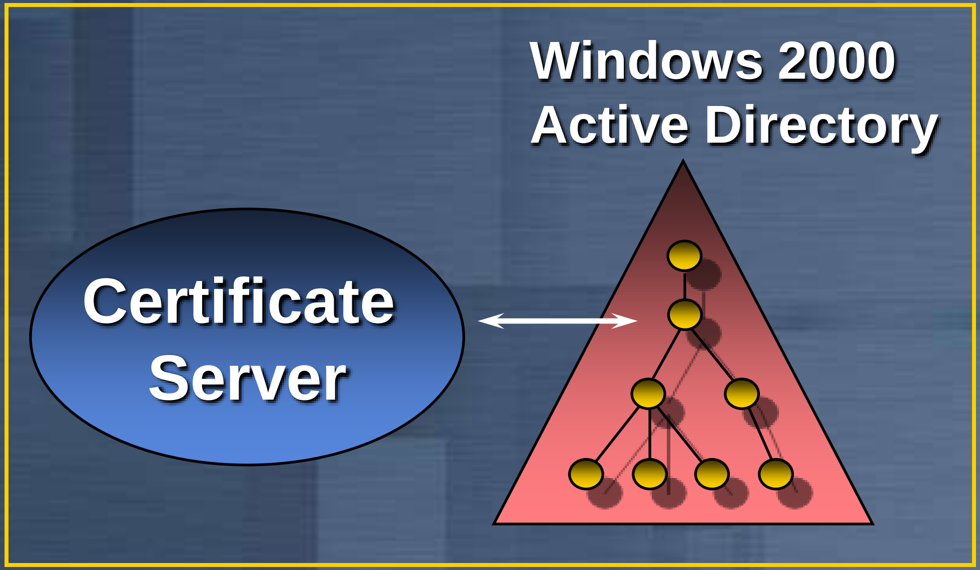
Enterprise

- Certificate services
- Trust policy

For servers



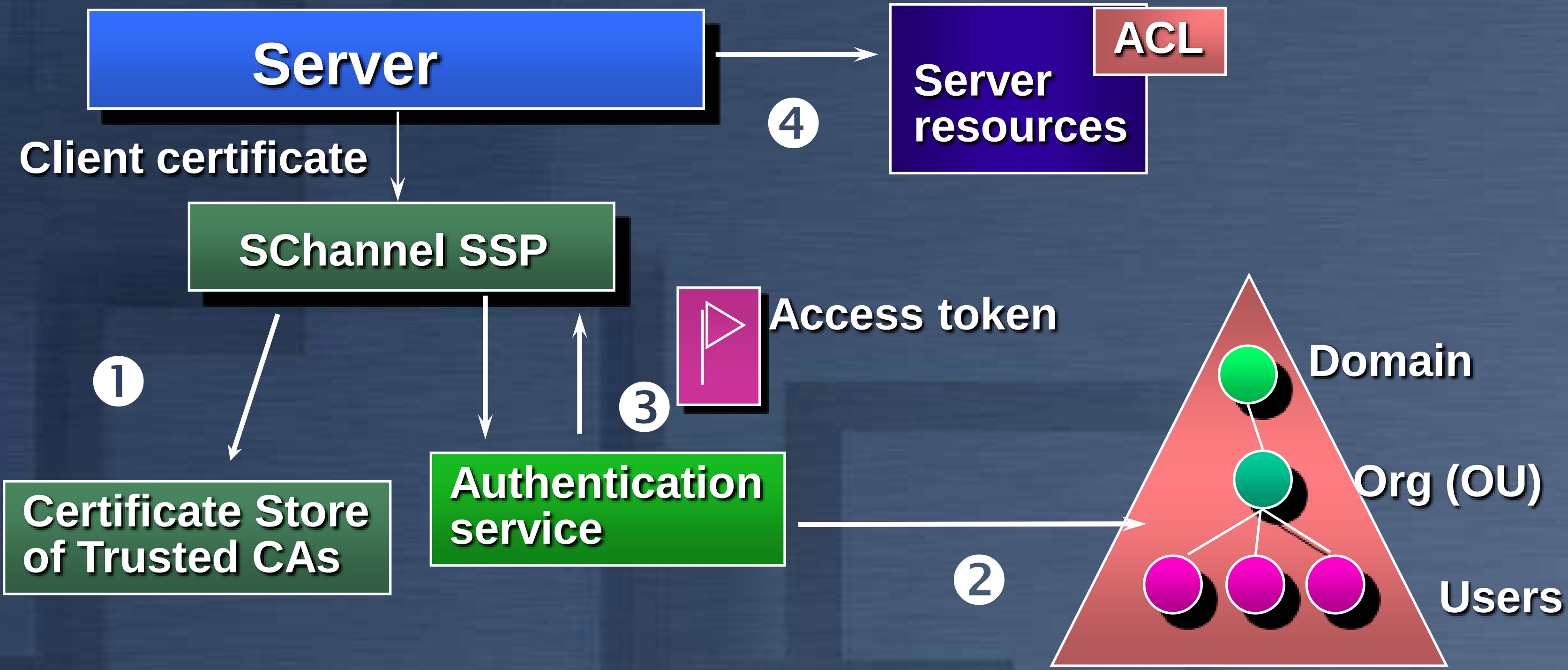
- Key and certificate management
- Secure channel with Client authentication
- Auto enrollment



Windows 2000 Active Directory

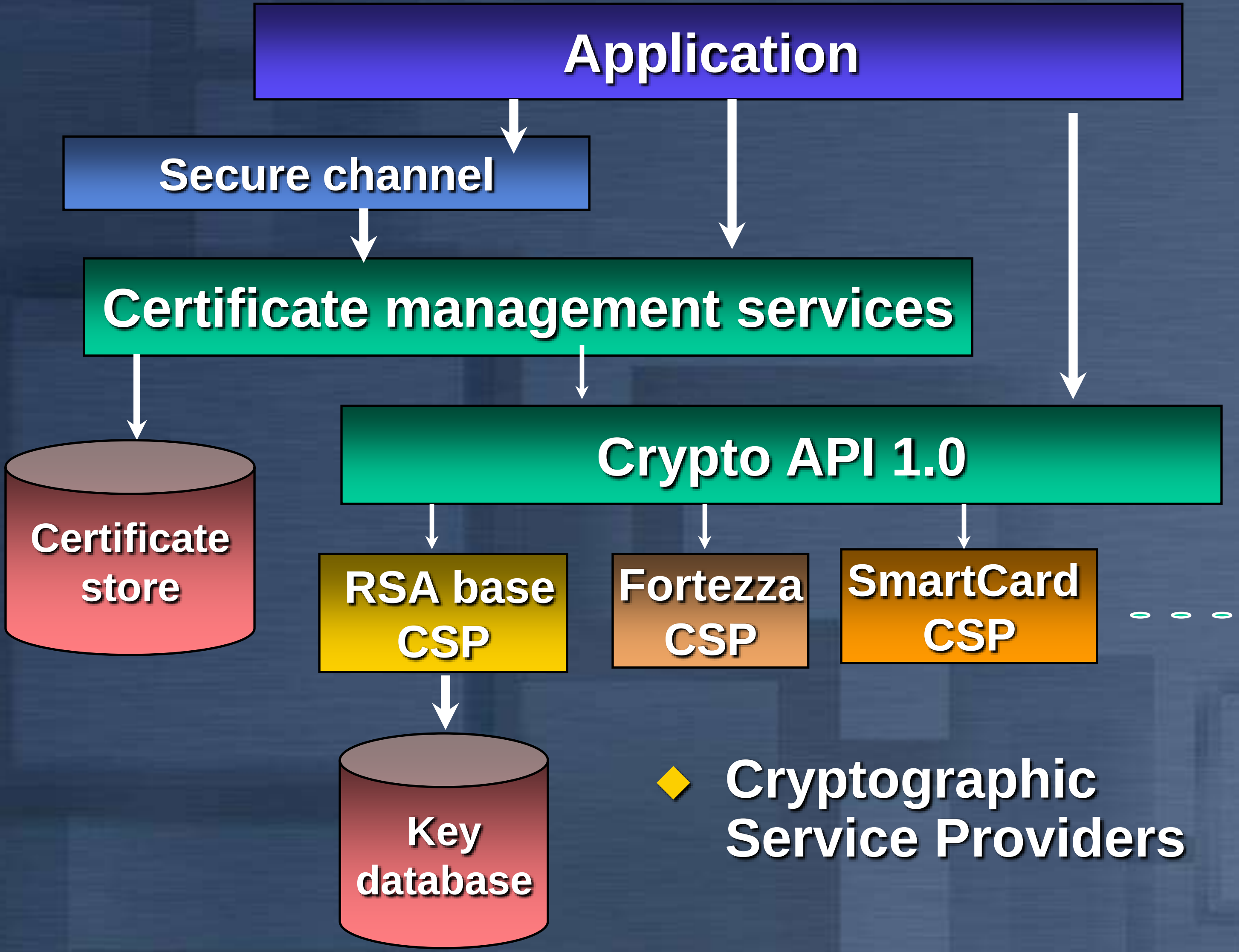
Certificate Server

SSL Client Authentication



1. Verify user certificate based on trusted CA, CRL
2. Locate user object in directory by subject name
3. Build NT access token based on group membership
4. Impersonate client, object access verification

Crypto API Architecture



Application

Secure channel

Certificate management services

Certificate store

Crypto API 1.0

RSA base CSP

Fortezza CSP

SmartCard CSP

- - -

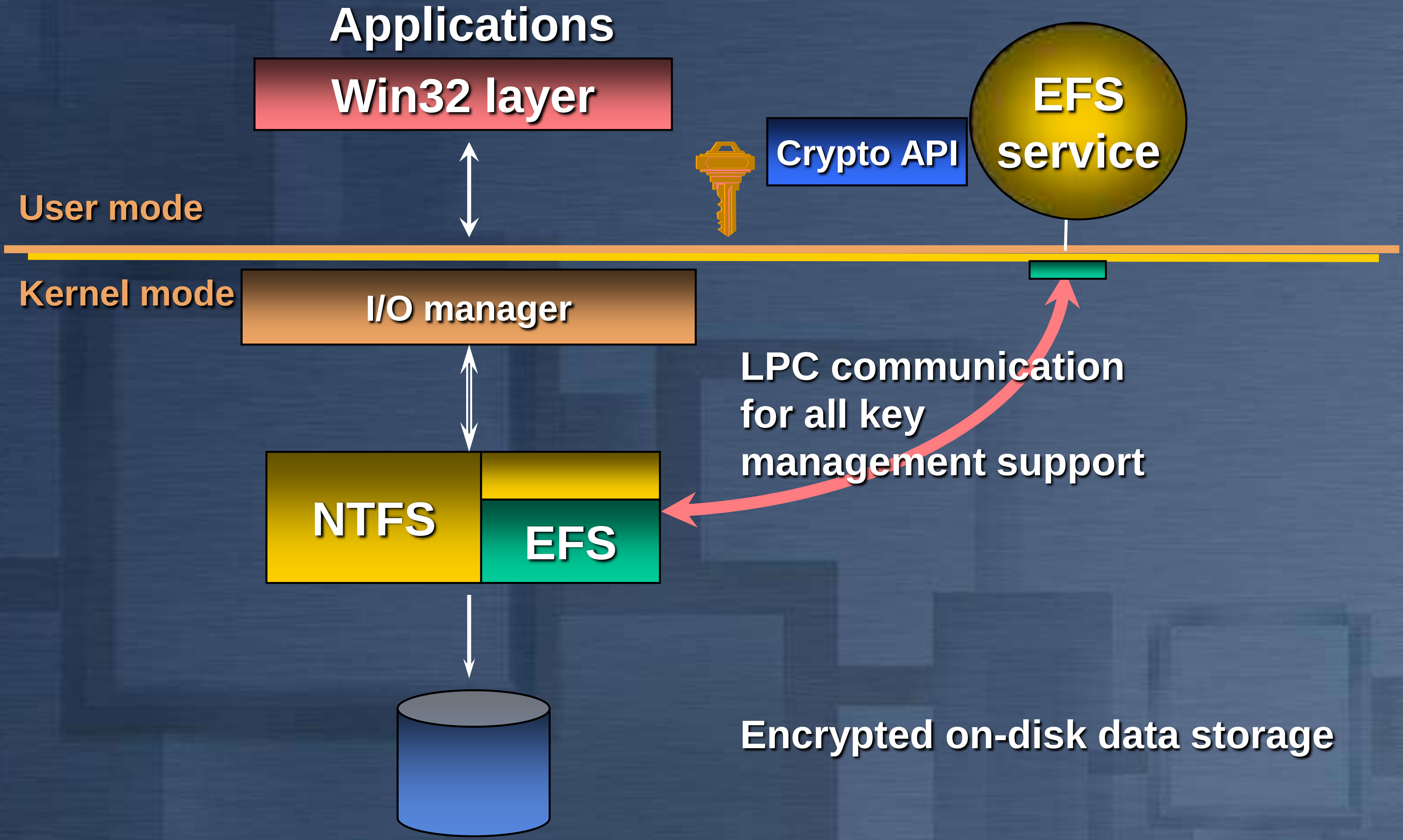
Key database

- Cryptographic Service Providers

Encrypting File System

- Privacy of data that goes beyond access control
  - Protect confidential data on laptops
  - Configurable approach to data recovery
- Integrated with core operating system components
  - Windows NT File System - NTFS
  - Crypto API key management
  - LSA security policy
- Transparent and very high performance

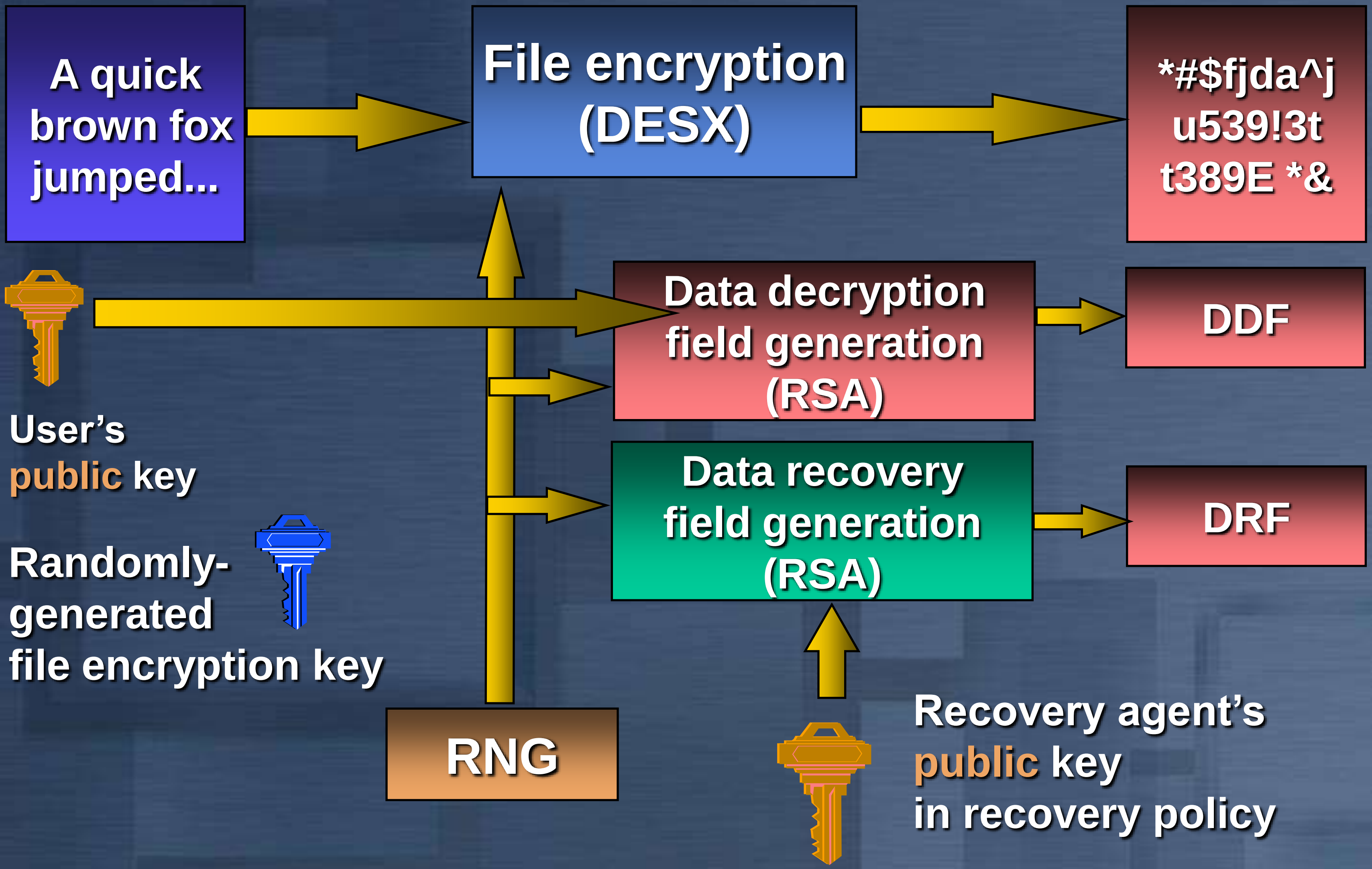
EFS Architecture



LPC communication for all key management support

Encrypted on-disk data storage

File Encryption



A quick brown fox jumped...

File encryption (DESX)

*#$fjda^j u539!3t t389E *&

Data decryption field generation (RSA)

DDF

Data recovery field generation (RSA)

DRF

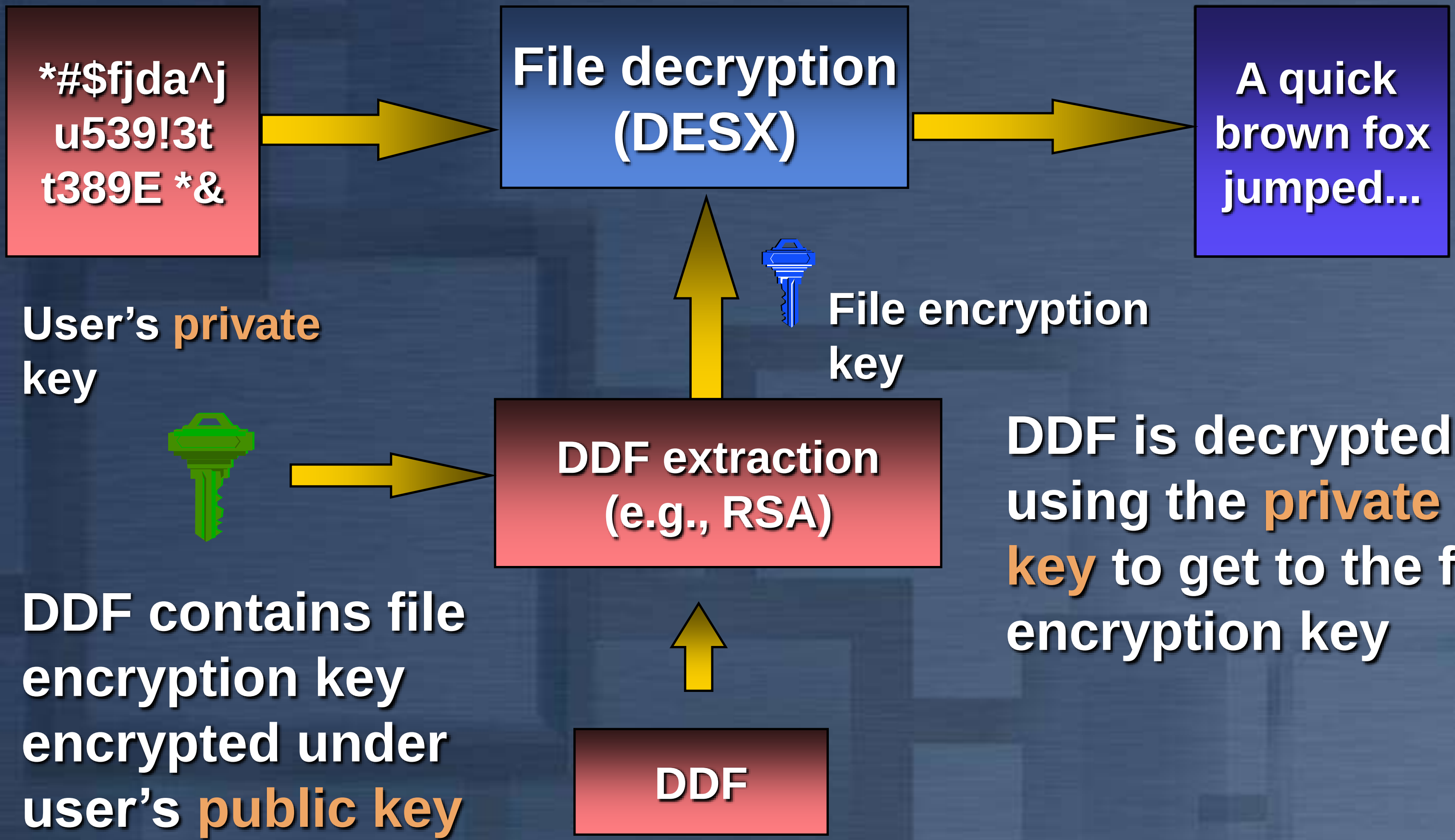
User's public key

Randomly-generated file encryption key

RNG

Recovery agent's public key in recovery policy

File Decryption



*#$fjda^j
u539!3t
t389E *&

File decryption
(DESX)

A quick
brown fox
jumped...

User's private
key

File encryption
key

DDF extraction
(e.g., RSA)

DDF

DDF contains file encryption key encrypted under user's public key

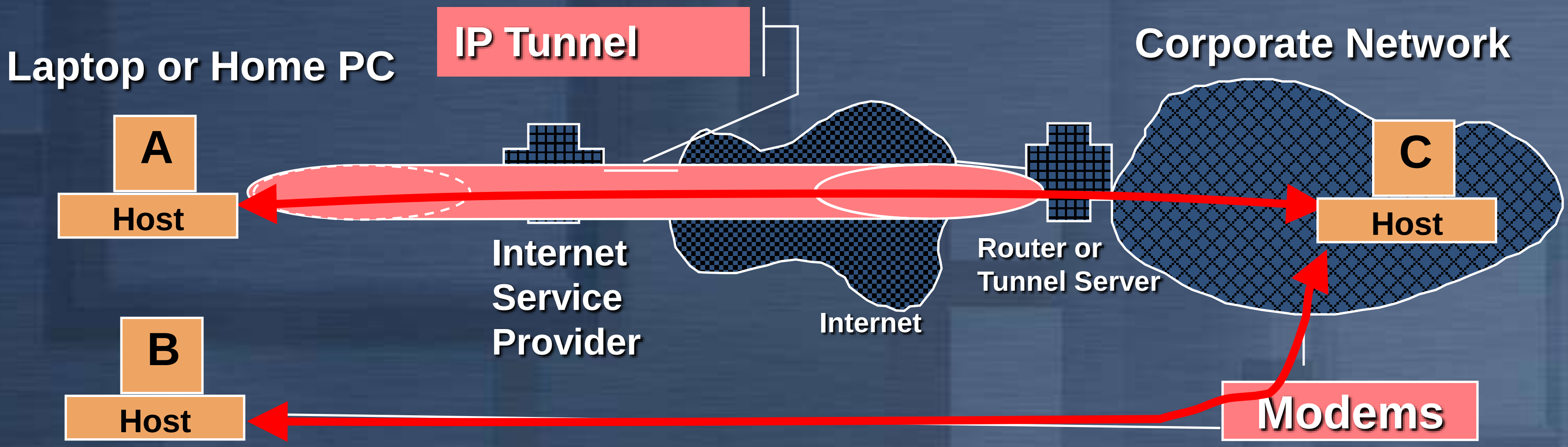
DDF is decrypted using the private key to get to the file encryption key

Secure Networking

- Internet Protocol Security (IPSec)
- Extended Authentication Protocol/PPP
  - Token and SmartCard support
- Remote Authentication Dial In User Service (RADIUS)
- Kerberos security package
- Public key (SSL/TLS) security package

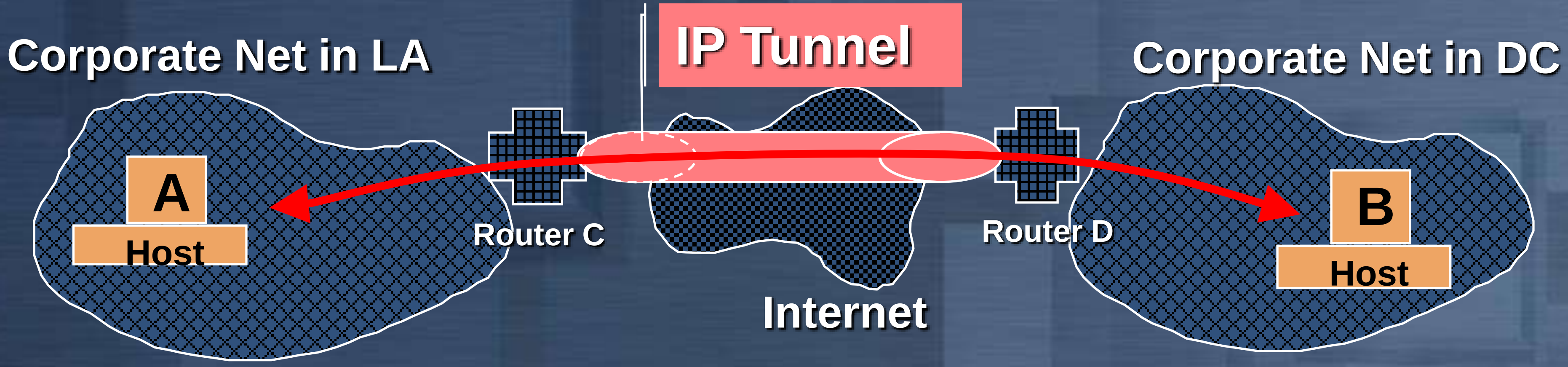
Windows 2000 IPSec
Target Scenarios

- Remote Access User to Corporate Network
  - Dial Up from Laptop or Home
  - Using existing network connectivity to Internet



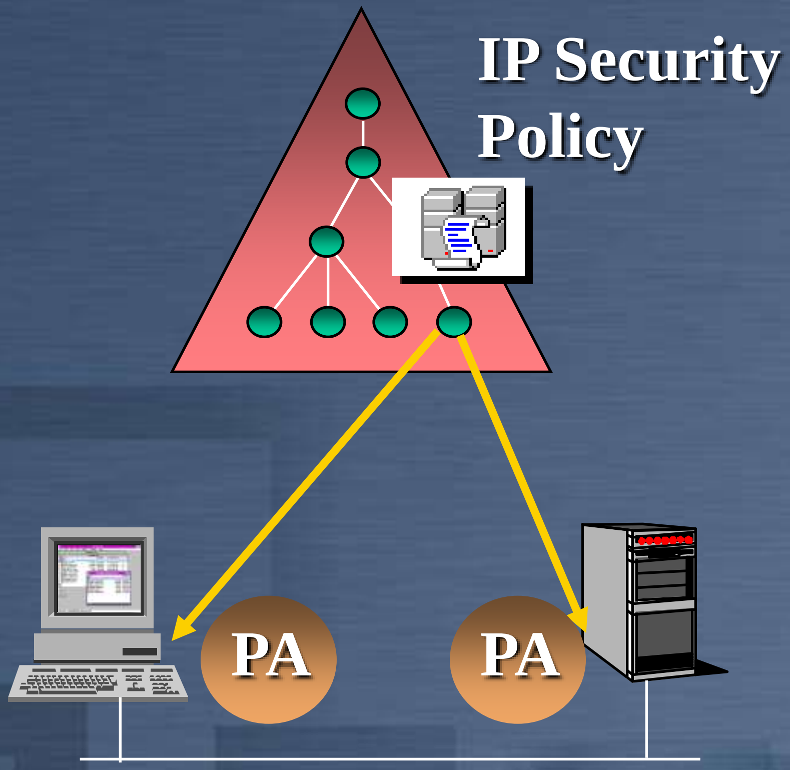
Windows 2000 IPSec
Target Scenarios

- LAN Edge Gateway to Edge Gateway of Another LAN
  - Across Internet or private network with Windows 2000 <-> Windows 2000 routers using IP tunnels
    - IPSec Tunnel Mode
    - L2TP/IPSec integrated tunneling



IP Security

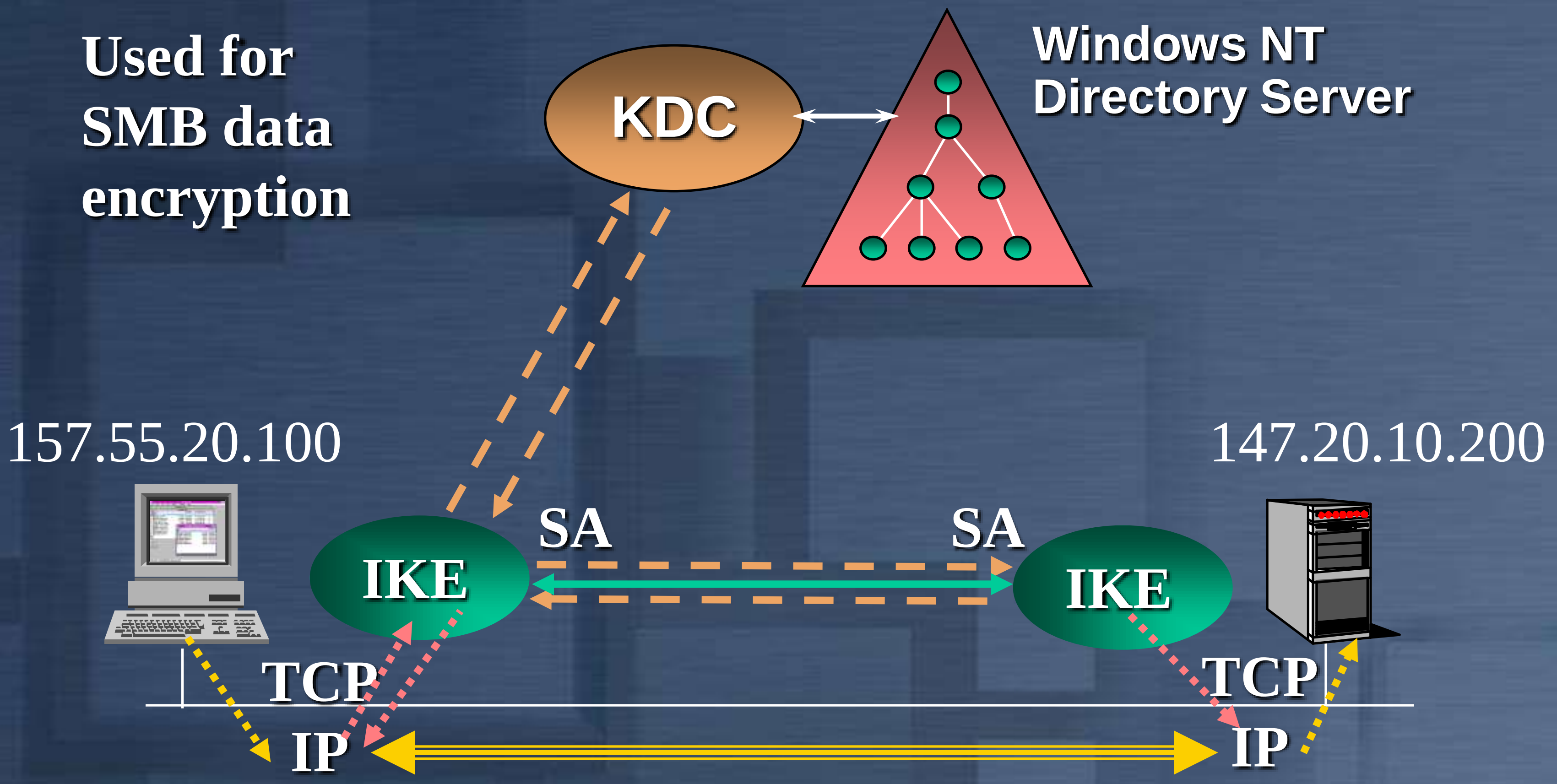
- Host-to-host authentication and encryption
  - Network layer
- IP security policy with domain policy
  - Negotiation policies, IP filters
- Policy Agent
  - Downloads IPSEC policy



Source: 157.55.00.00
Dest: 147.20.00.00
Any protocol

IP Security Association
using Kerberos Authentication

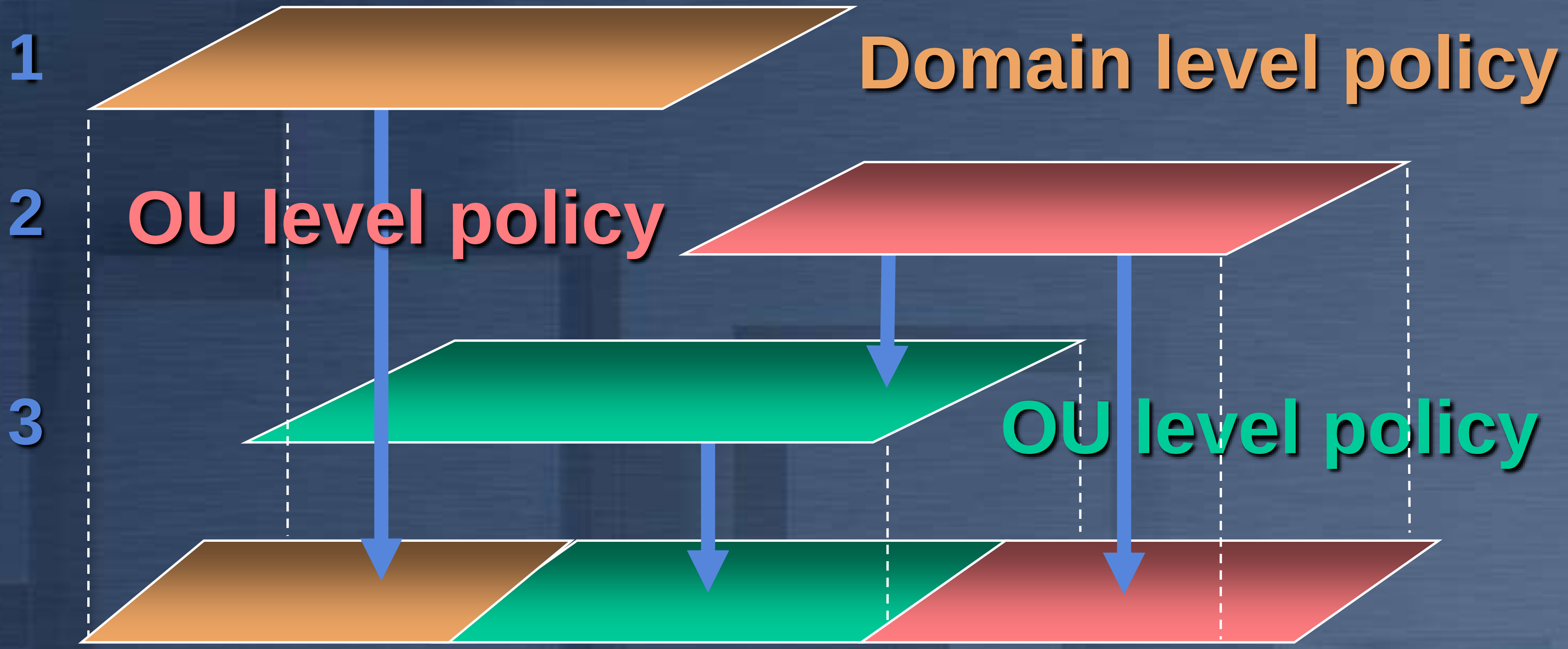
Used for SMB data encryption



Managing Security Policy

- Security settings in local or group policy
- Local computer policy
  - Audit policy, rights, security options
- Group Policy in the directory
  - Common computer policies
- Domain level policies
  - Account policies
  - Public key trust policies

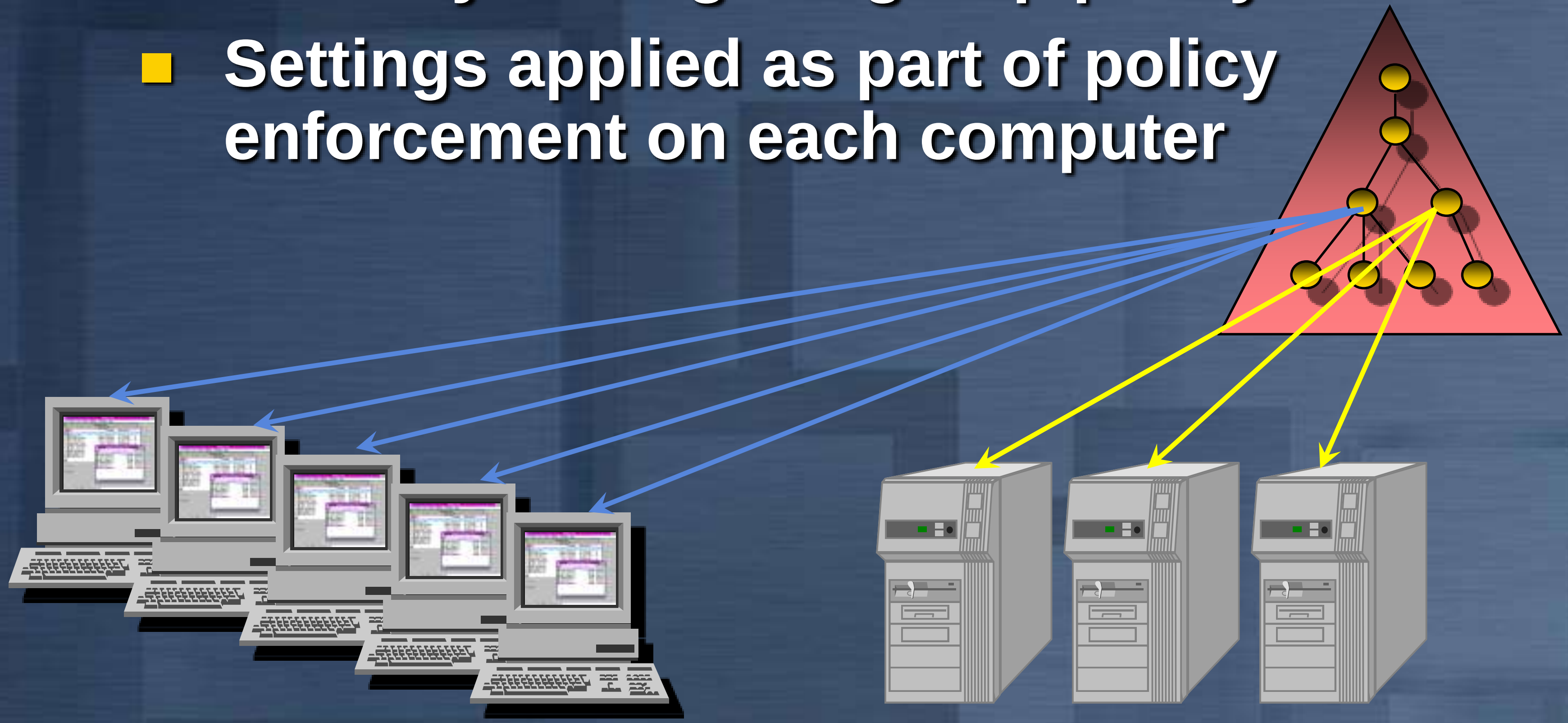
Hierarchical Policy Settings



- Applied policy for a computer combines multiple policy objects

Enterprise Framework

- Integrated with Group Policy management
  - Security settings in group policy
  - Settings applied as part of policy enforcement on each computer



Secure Windows

- Goals
  - Secure out-of-the-box
  - Definition of secure system settings
  - Backward compatible user experience
- Clean install of Windows 2000
  - Upgrade can apply security configuration
- Who can do what?
  - Administrators, Power Users, Users
  - Group membership defines access

Administrators vs. Users

- Administrators
  - Full control of the operating system
  - Install system components, drivers
  - Upgrade or repair the system
- Users
  - Cannot compromise system integrity
  - Read-only access to system resources
  - Interactive and network logon rights
  - Can shutdown desktop system
  - Legacy application issues

Security Features Summary

- Single sign on with standard protocols
  - Kerberos V5 and X.509 V3 certificates
- Public key certificate management
  - Enterprise services for PKI rollout
- Distributed security for applications
  - Authentication, authorization, auditing
- Active Directory integration
  - Scalable, extensible user account directory

For More Information

- White papers
  - http://www.microsoft.com/windows2000/library
  - Active Directory
  - Security Services
- Windows 2000 Resource Kit
  - Deployment Guide
  - Detail technical material
- Microsoft Security Advisor
  - http://www.microsoft.com/security

Where do you want to go today?®

Microsoft®