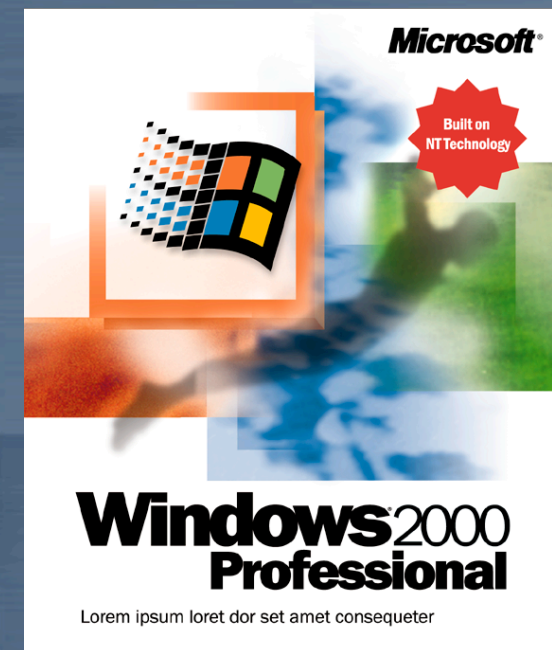# Unit 6: Protection and Security

6.6. Windows 2000 – Standards-based Security

Windows 2000 Professional
Standards Based Security

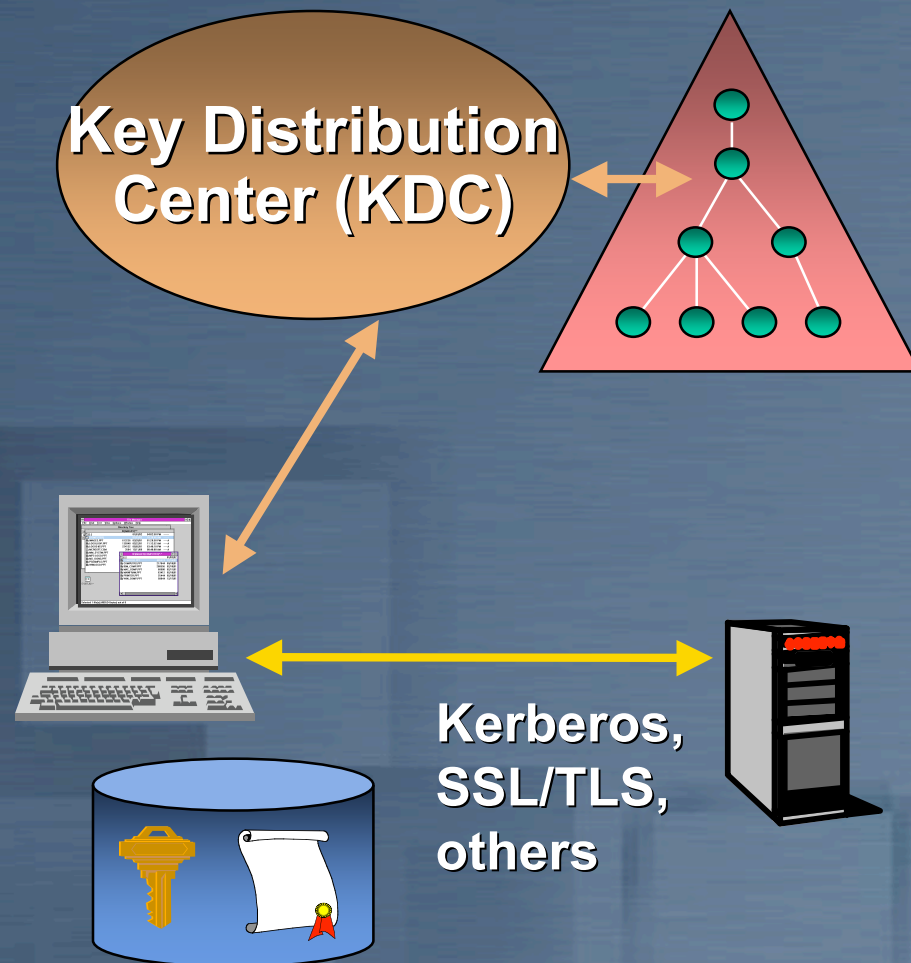# More Secure Information Access

- **NTFS requires authentication to access file system**

- **Encrypted File Systems protects sensitive data**

- **Native support for Kerberos authentication**

- **Public Key infrastructure to pass digital certificates**

- **IP Security to avoid access to sensitive data traveling across the wire**

NTFS Encryption (EFS)

- **Integral part of NTFS v5**
- **Encryption using unique key per file**
- **Enterprise data recovery using public key technology**
  - **Recovers individual file encryption key, not user's encryption key**
- **Transparent to users and applications**
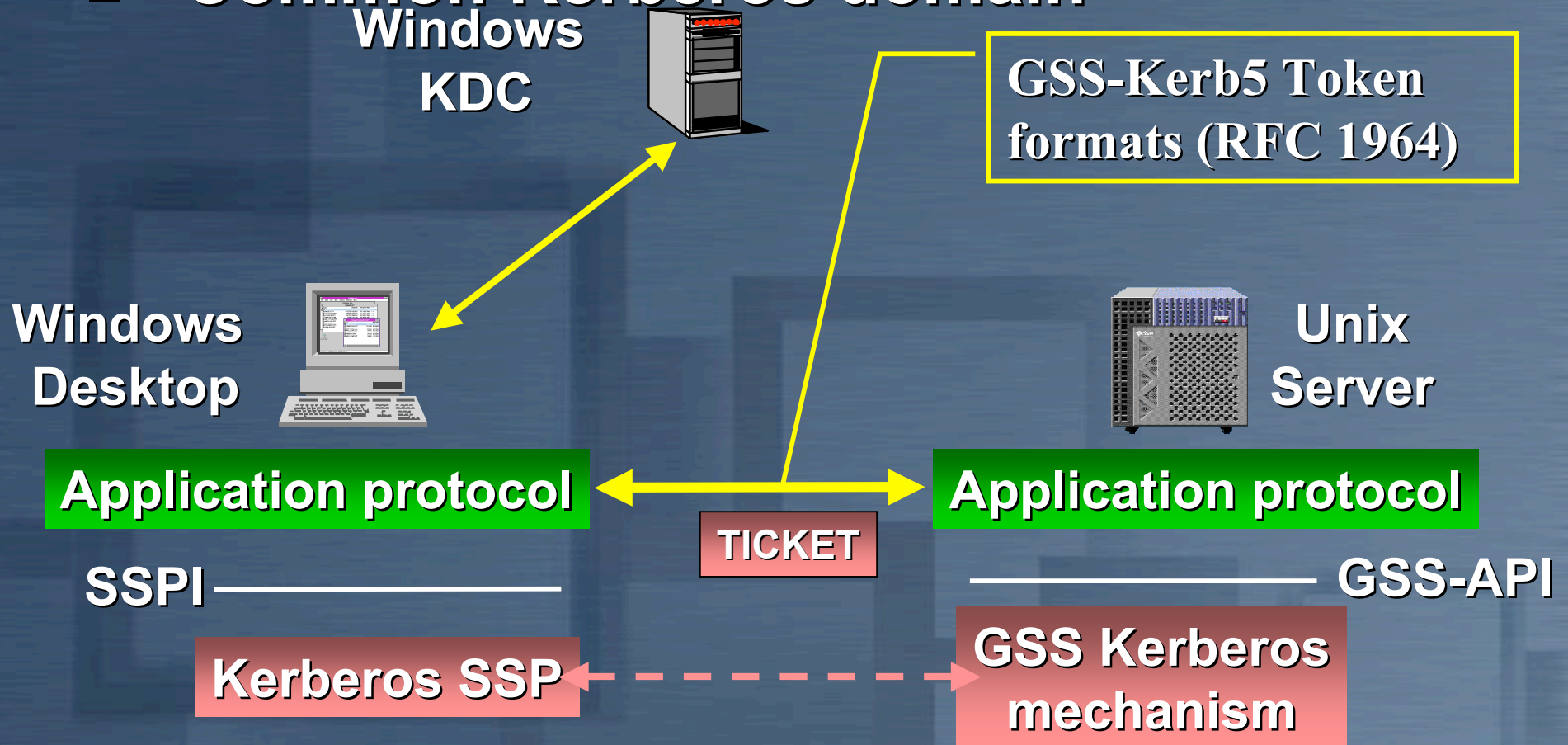- **Very fast operation**

Kerberos Authentication

- **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

Cross-platform Strategy

- **Common Kerberos domain**

Windows KDC

GSS-Kerb5 Token formats (RFC 1964)

Windows Desktop

Unix Server

Application protocol ⟷ **Application protocol**

TICKET

SSPI

GSS-API

**Kerberos SSP** ⤙ ⤚ ➔ **GSS Kerberos mechanism**

Public Key Services

- **Flexible, comprehensive, and efficient security infrastructure**
  - **Enterprise, Intranet, and Internet apps**
- **Standards based**
- **Simplifies deployment of PK-based functionality**

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

PA
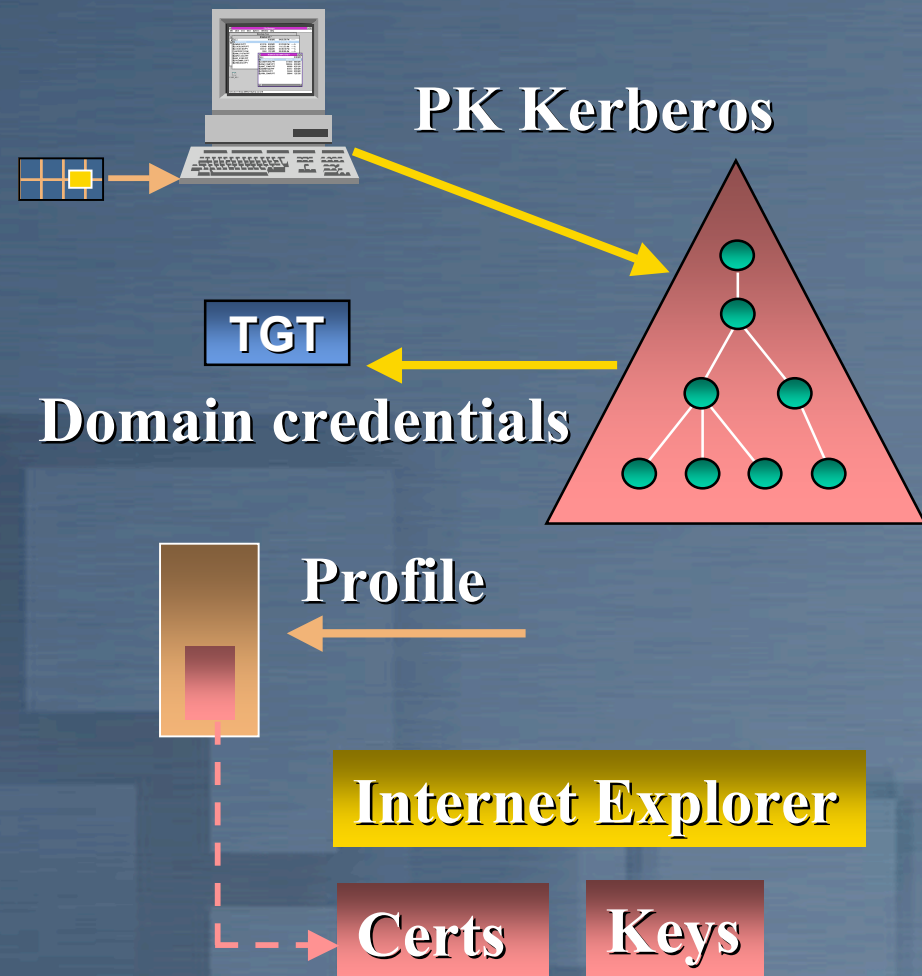
PA
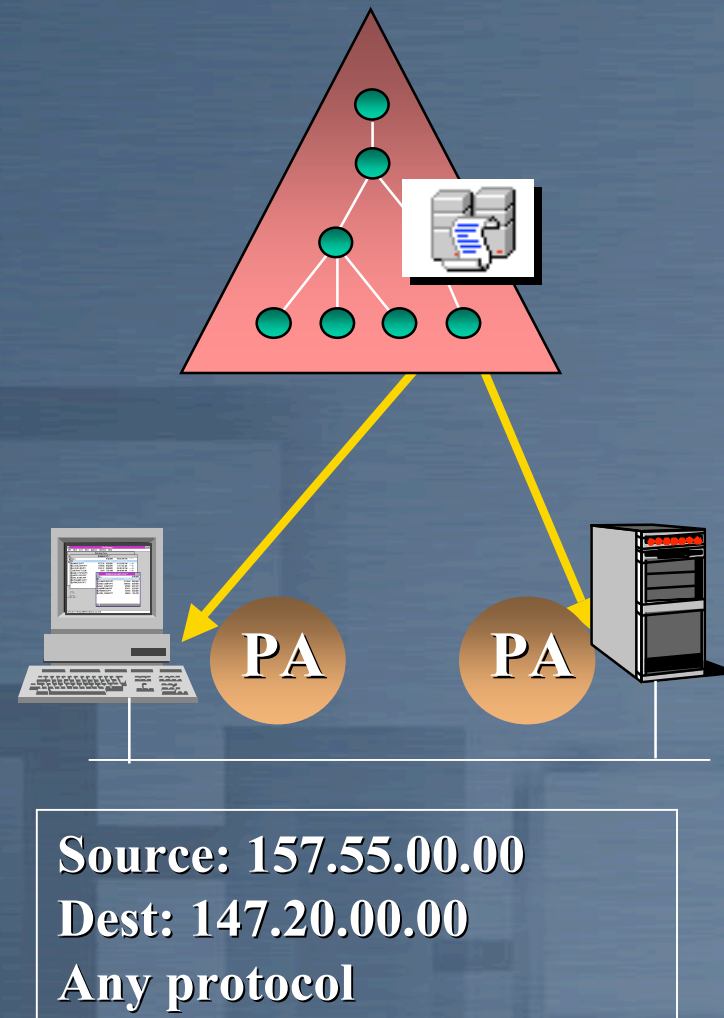
More Secure Resource Access

- **Latest machine access support via Smart Cards**

- **Secure Virtual Private Networking (VPN) support to tunnel in to private LAN over public**

- **Easier management of security settings with Security Configuration Manager**

Smart Card for Windows

- **A logical extension to the Windows environment**

- **Low cost, 8-bit solution**

- **Common development tools**

- **Language neutral run-time environment**

- **Strong security**

- **Partitioned file system**

- **Unicode character support**

Smart Card Logon

- **Private key and certificate on card**

- **Public key domain authentication**

- **Obtain Kerberos TGT and NTLM credentials**

- **User profile for other keys and certificates**

PK Kerberos

TGT

Domain credentials

Profile

Internet Explorer

Certs   **Keys**