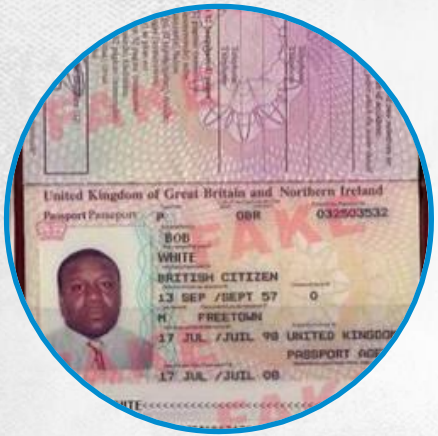

Authentication
IT SECURITY ACADEMY
www.SecAcademy.com

Authentication, Identification and Authorisation



Authentication is verifying the identity of a user

To authenticate, you have to prove you are who you claim to be

Identification is stating who you are

It is enough to simply submit your identity

Authorisation is allowing an authenticated user to take some action

Operating systems authorise each operation users take

Authentication

You can authenticate programs and information as well as users

You can verify the identity of users against:

- Passwords, or information only they should know
- Data only they possess
- Biometrics, or the unique traits of users

Authentication

Every authentication method used must protect the identity of users

Mistake number one is using the same identity across multiple different systems

Authentication

Every authentication method used must protect the identity of users

Mistake number one is using the same identity across multiple different systems

Authentication protocols and services

The verification of a password does not have to involve checking the submitted string against a password stored on a computer

Authentication protocols and services

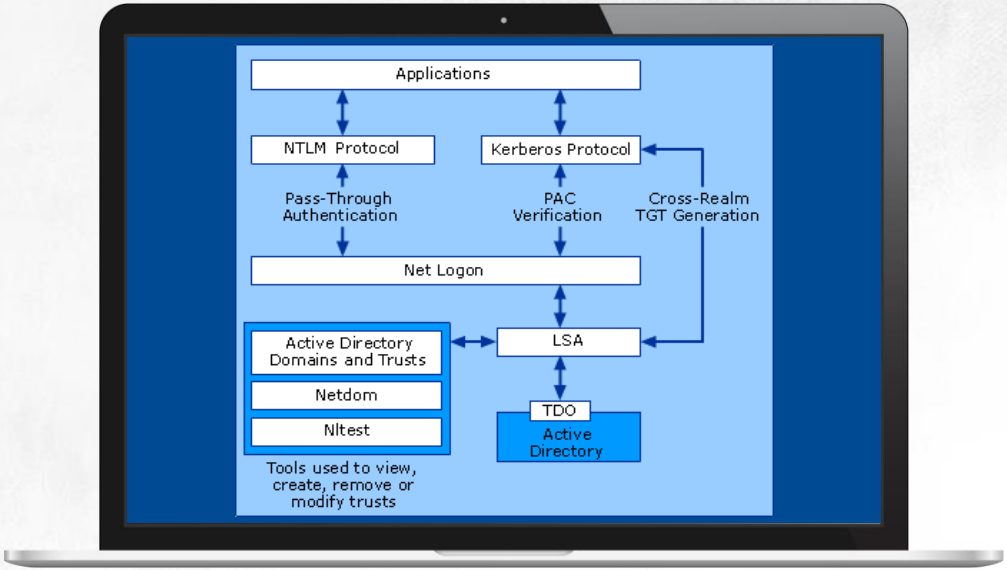
Windows doesn't store user passwords. It only stores credentials generated from a given password. They can have the following formats:

- LM "hash" (the LANMAN hash)
- NT hash (the NT LAN Manager hash, known as the Unicode password)
- Cashed credentials, derivation of NT hashes

Authentication protocols and services

The Winlogon process is responsible for authenticating users. One of its components is the msgina.dll library

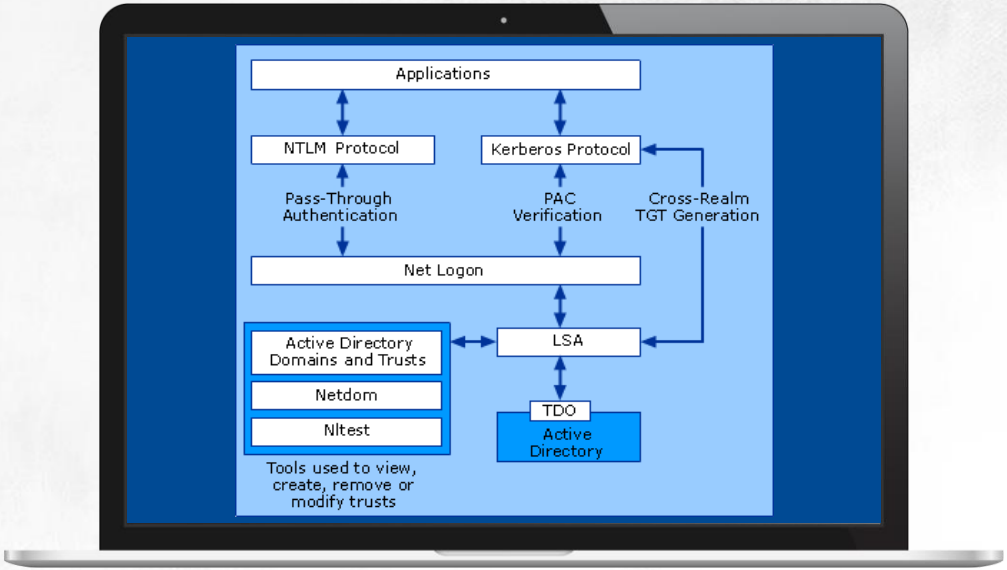
GINA sends submitted data to the LSA subsystem service, and LSA forwards them to a default Security Support Provider (SSP)



Authentication protocols and services

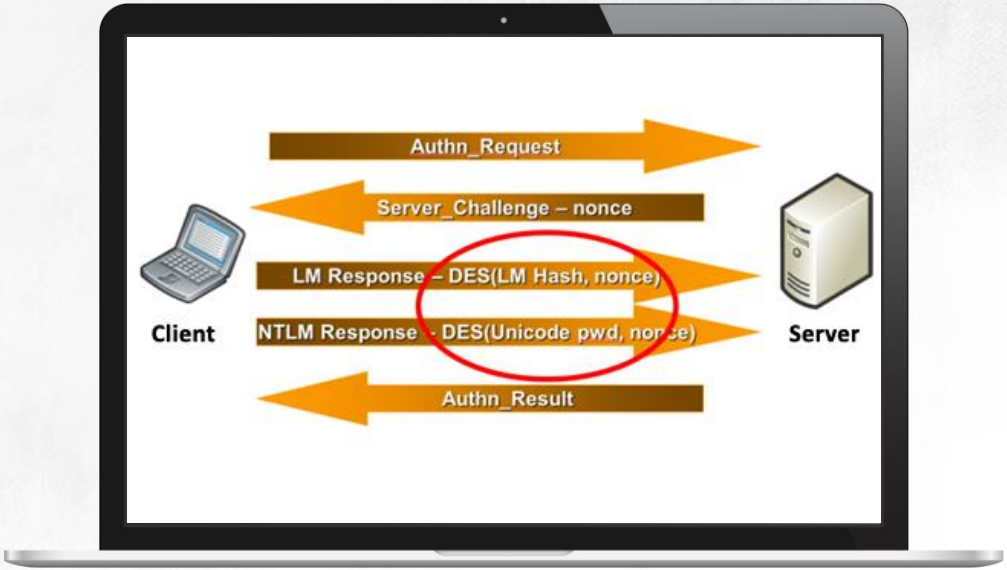
Kerberos is the default SSP in Windows 2000 and newer systems

If Kerberos cannot authenticate a user, user credentials will be sent to the next SSP, NT LAN Manager (NTLM)



Authentication protocols and services

If a local client is to be authenticated, credentials are sent in the MSV1_0 authentication package to the Security Accounts Manager (SAM) file, where they are checked against an encrypted list of passwords



Authentication protocols and services

But if the authentication process is to be applied to a remote client, credentials are sent over a network and checked against data saved in a domain controller's or a remote client computer's SAM

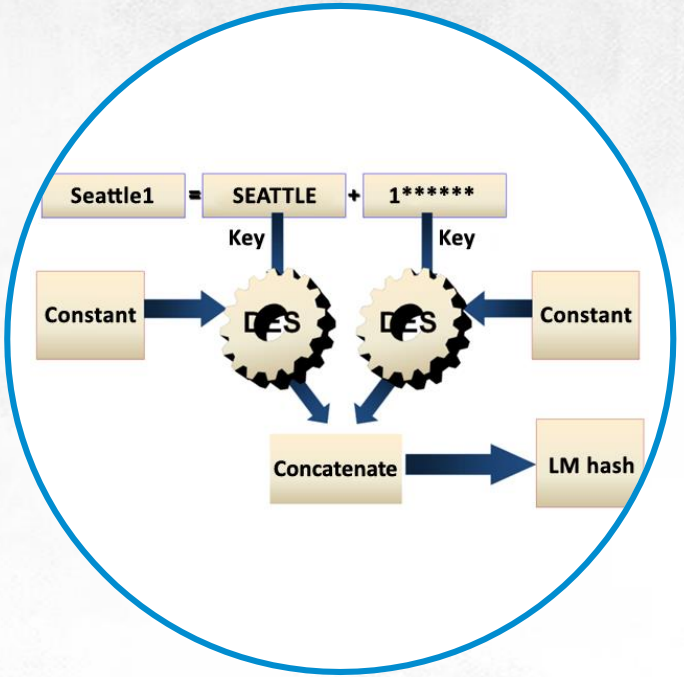
Authentication protocols and services

In Microsoft Windows networks user identity may be verified using the following protocols:

- LM, which should not be used
- NTLM, which also should not be used today
- NTLM v2, which ensures a basic level of security, including the mutual authentication feature. NTLM v2 should be used in workgroups
- Kerberos v5, which is the default authentication protocol in Windows 2000 systems that are members of an AD domain

LM

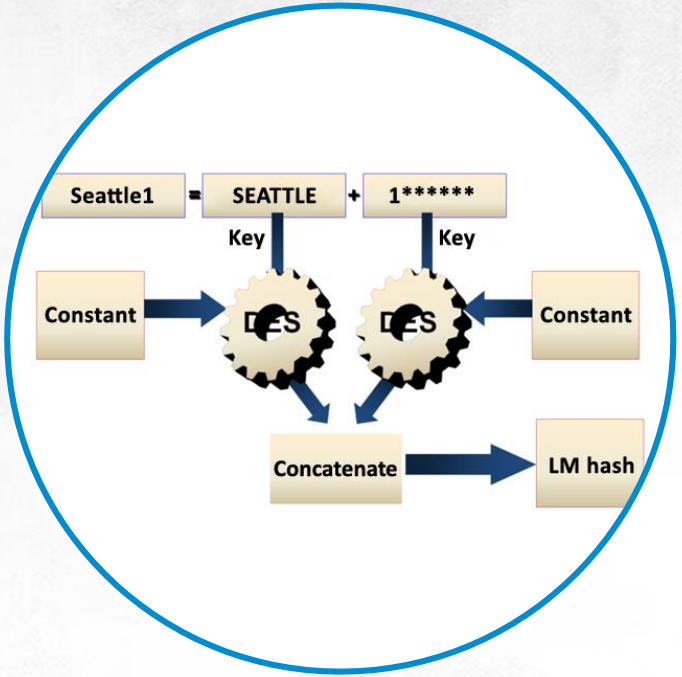
This protocol makes use of the DES algorithm and a fixed key (constant) to encrypt passwords



LM

The list of faults is pretty long:

- Passwords are converted to uppercase before encryption
- Only alphanumeric characters are allowed
- Padded with NULL (ASCII 0 code) to 14 characters if a password is shorter. Because LM hashes are deterministic, they do reveal the password's real length (the padding in the passwords always gets the same LM hash characters)
- Split a password into two seven-character halves. Because both parts are DES-encrypted independently and resultant ciphertexts are concatenated, the password parts may be cracked independently. This means that:
    - The LM hash is not 14-character, it has two 7-character parts
    - To go over all passwords, a brute-force attack needs to only do about $6.8*10^{12}$ operations

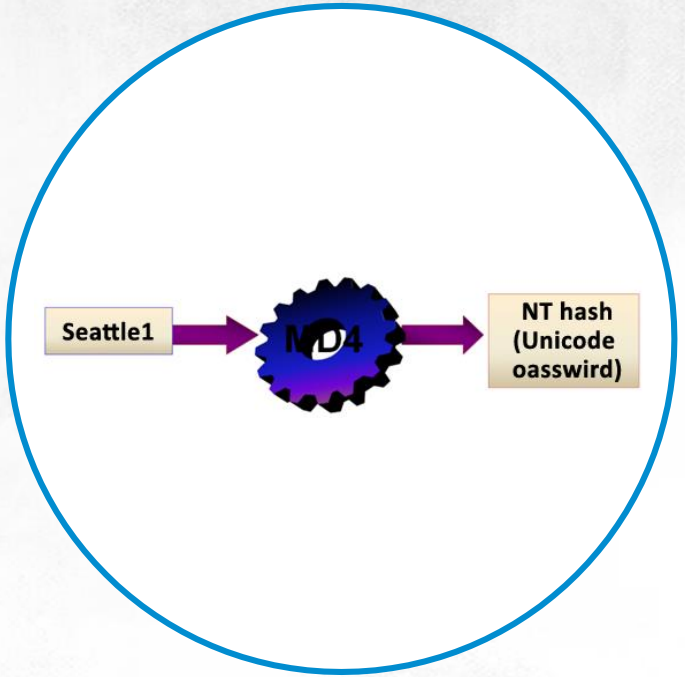


NTLM

NTLM uses a hash function to encrypt passwords

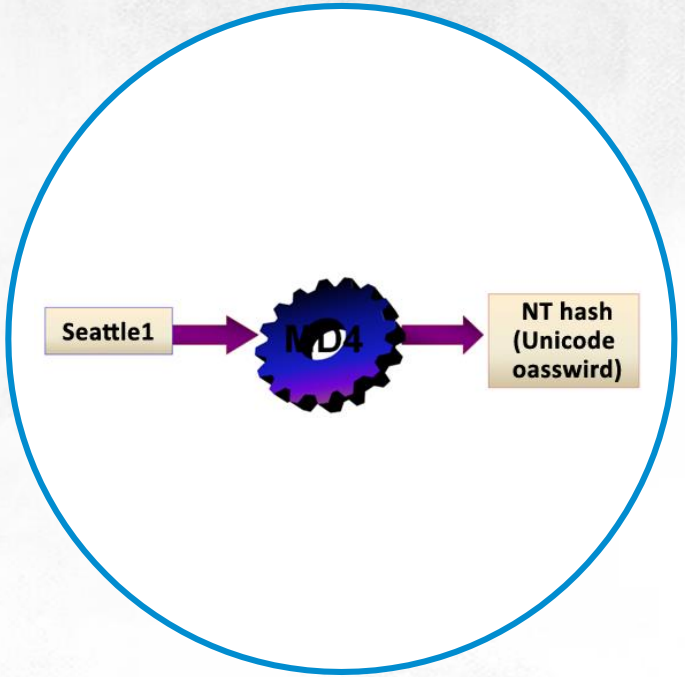
NT hashes:

- Are case-sensitive
- Allow passwords to be longer than 14 characters (the maximum length is 127 characters)
- Brute-force attacks need to go over more possibilities to succeed:
    - For passwords that contain the same character set as LM hash there are about $4.6*10^{25}$ passwords to check
    - For a 14-character passwords containing any characters there are about $2.7*10^{67}$ passwords to check
    - For a 127-character password there are about $4.9*10^{611}$ passwords to check
- Are also deterministic



NTLM

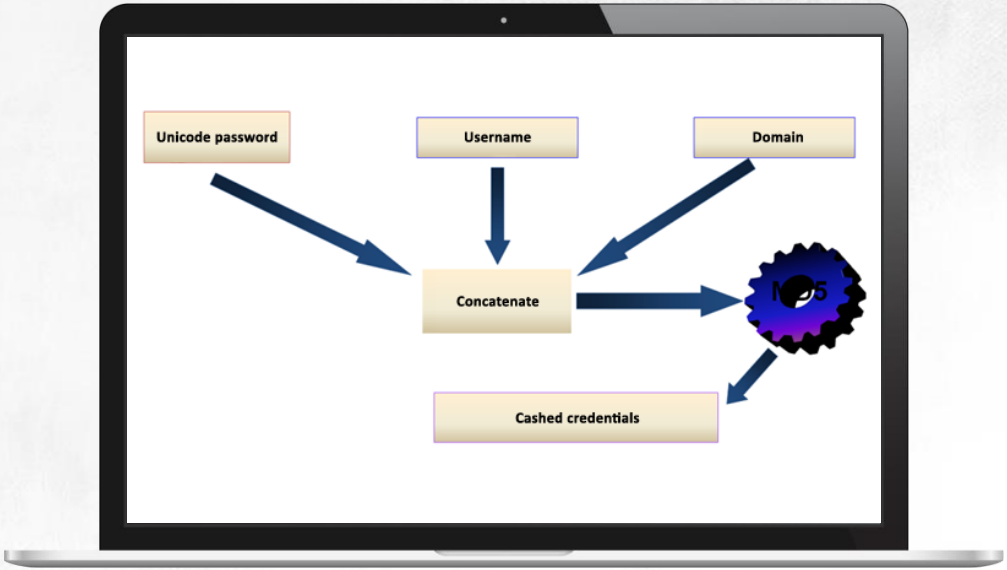
Windows 2000 and Windows XP systems with default settings store both NT and LM hashes. From Vista onwards the Windows systems only store NT hashes



Cashed Credentials

Cashed credentials can be used to allow users to reconnect to remote computers, if the users have been authenticated before

Unlike LM and NT hashes, cashed credentials stored on a local computer are not susceptible to cracking



Cashed Credentials

Even if attackers succeed in reversing a twice-used hash function, it only gives them the ability to log onto a specific remote host, and as thee user whose NT hash was used to calculate the cashed credential

The SAM is also fully encrypted using a Windows startup key

Kerberos

Kerberos V5:

- Is developed on the basis of open standards (RFC 1510 and RFC 1964)
- Enables delegating credentials
- Enables creating cross-realm trust relationships between Windows domains and any Kerberos V5 realms
- Enables creating cross-domain bidirectional, transitive trust relationships
- Doesn't force servers to connect to a domain controller to verify the identity of a client

Kerberos

In AD domains each principal has its own secret: either a long-term key derived from a hash or a private key stored in a certificate issued for the principal

Kerberos

With long-term keys, a shared secret is encrypted by one principal, while another principal decrypts it using the same key

If a user logs on using a smart card, the credential is encrypted using a public key, and decrypted by a KDC with a private key

Every domain controller is a key distribution centre (KDC)

A KDC stores long-term keys as well as grants TGTs and service tickets. Ticket-granting-tickets (TGT) are used to authenticate users, while service tickets are used to enable authenticated users to use a given network service

Kerberos

Every principal (including KDCs) must have the same name: the name is krbtgt

The krbtgt user password is generated automatically and changed on a regular basis

This password is used to calculate the KDC long-term key

This key in turn is used to encrypt TGTs issued by the KDC

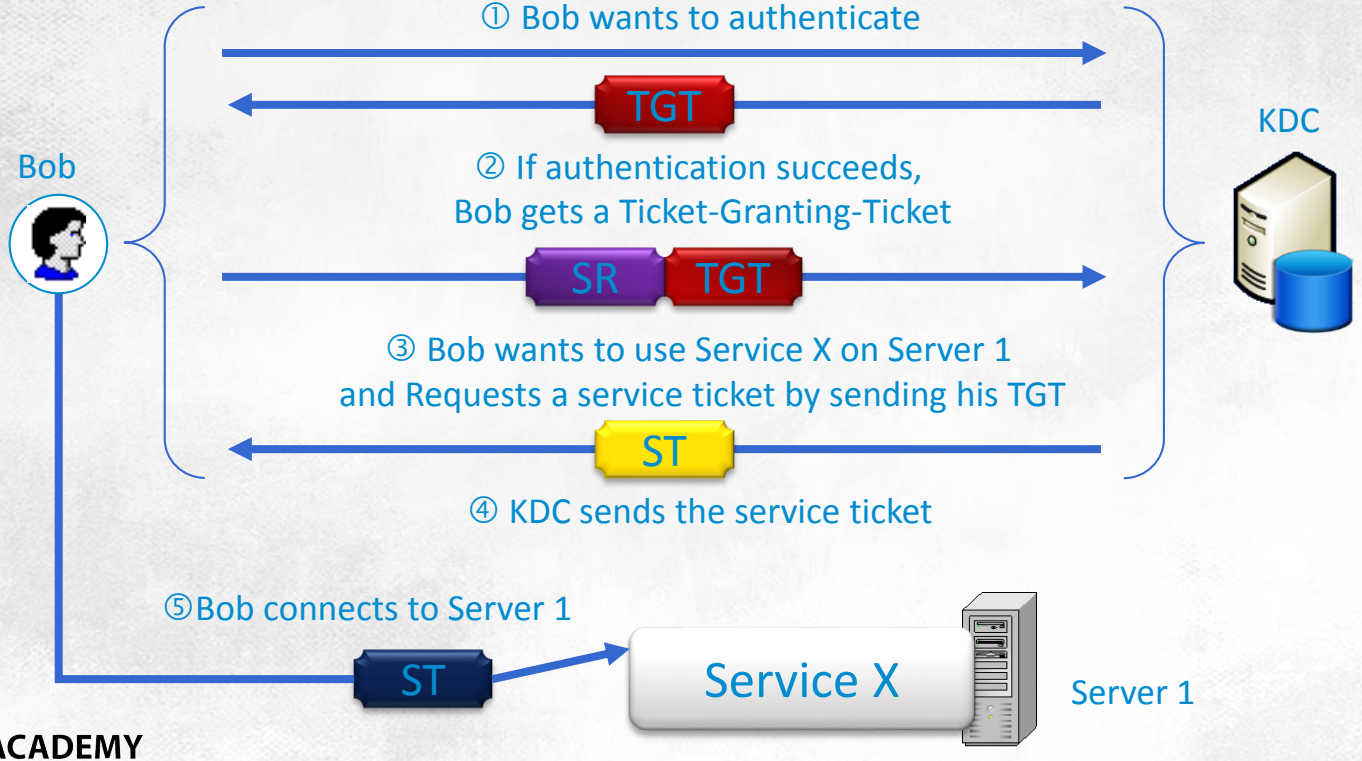
Since all KDCs in a domain use the same krbtgt account, all TGT tickets in a domain are encrypted with the same long-term key

One TGT may be reused multiple times until it expires

TGTs are encrypted with a user's long-term key, and the SIDs they contain are additionally signed by a KDC

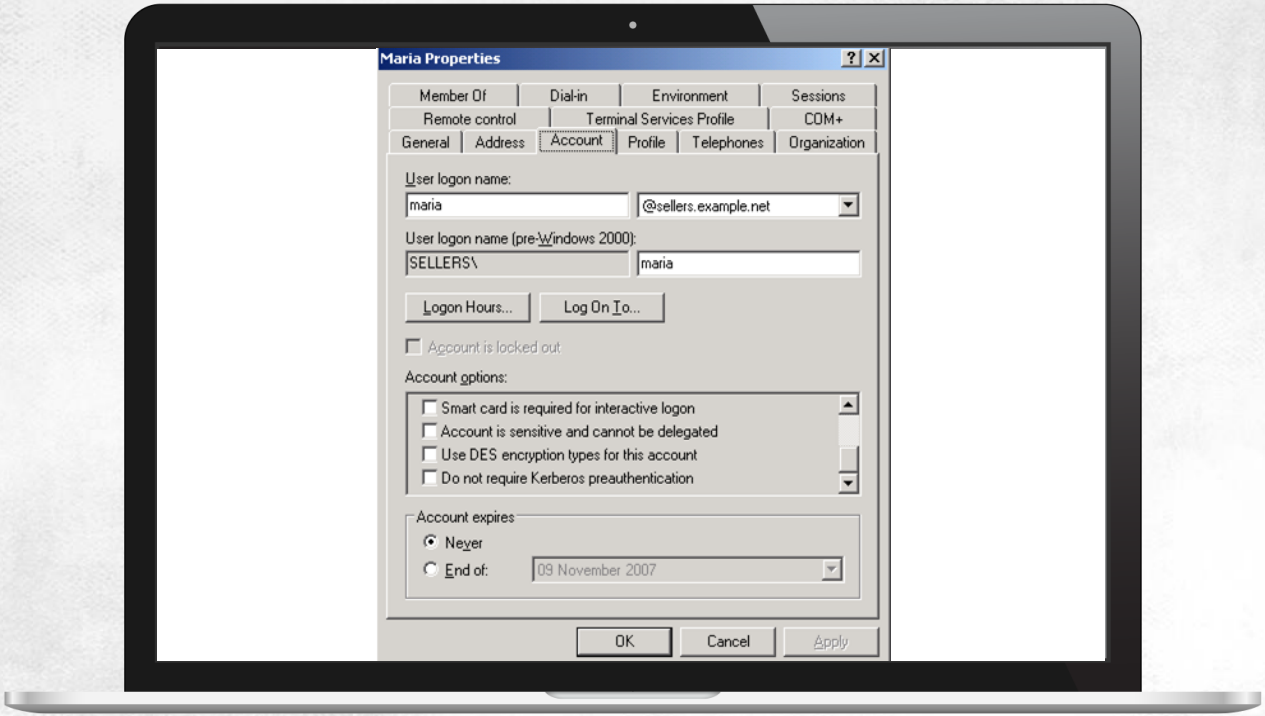
Kerberos

User authentication process



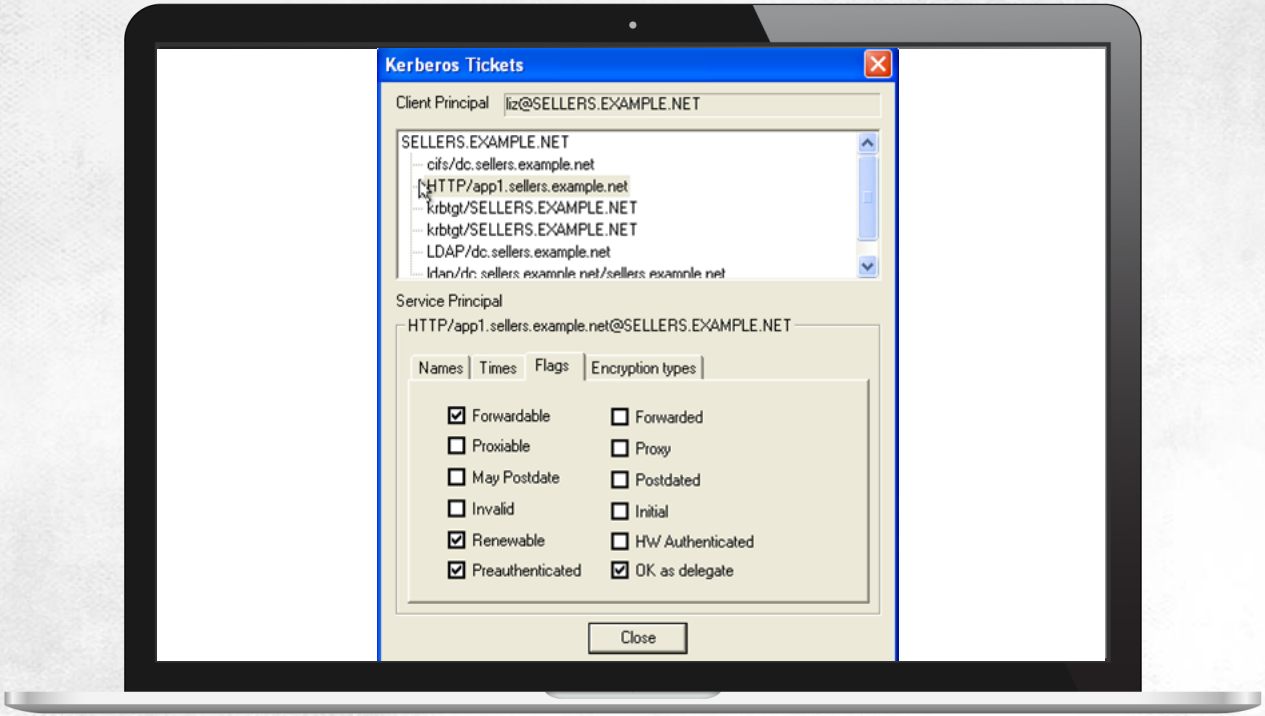
Kerberos

Credential Delegation



Kerberos

Credential Delegation



THANKS