1. Kerberos Process
2. Encryption Algorithm
3. Kerberos Delegation
4. NTLM Process

Windows New Technology LAN Manager (NTLM)

验证流程：

协商

1. 确认版本协议
2. df

质询、验证

1. NTLM Negotiate
2. Session Key
3. NTLM Protocol (4), how to identify which protocol was used

Response length

1. Restriction of NTLM

* Application
* Specified Members
* Devices
* Bugs

Delegation

有时需要Application或Service代表Client连接其他Servers或Services。在一些多层级情况下，需要第一个Server连接第二个Server，因此第一个Server需要到第二个Server的Ticket，同时希望第一个Server仅代表Client权限而非自身权限。此时，便需要Delegation。

Kerberos提供两种方式完成Delegation

* Proxy Tickets

The client can get a ticket for the back-end server and then give it to the front-end server. Tickets obtained in this way—by a client for a proxy—are called proxy tickets. The difficulty with proxy tickets is that the client must have information about the name of the back-end server.

* Forwarded Tickets

The client can give the front-end server a TGT that the server can use to request tickets as needed. Tickets obtained in this way—with credentials forwarded by a client—are called forwarded tickets. This second method overcomes the difficulty (that the client must have information about the name of the back-end server) presented by the first method.

For delegation of authentication to work, three conditions must be met:

* The computers that host the client process, the service process, and the processes for back-end services must all be running Windows 2000, Windows XP, or Windows Server 2003 in an Active Directory domain.
* The client's account must be enabled for delegation.
* The service's account must be enabled for delegation.

**NTLM版本种类**

LM；V1；Session Security；V2。

**Encryption Algorithm**

DES – Data Encryption Standard

RC4 – Rivest Cipher 4

AES – Advanced Encryption Standard

**Cryptographic Hash Functions**

SHA – Security Hash Algorithm

MDA5 – Message Digest Algorithm 5

注意DES被认为不安全，尽量避免使用。