

The British
Museum
In London

Access Control From Jerry Scott

Access Control Controls

Access Control Category	Done Before or After	Access Control Category	Done Before or After
Preventive	Before	Detective	After
Corrective	After	Directive	Before
Deterrent	Before	Recovery	After

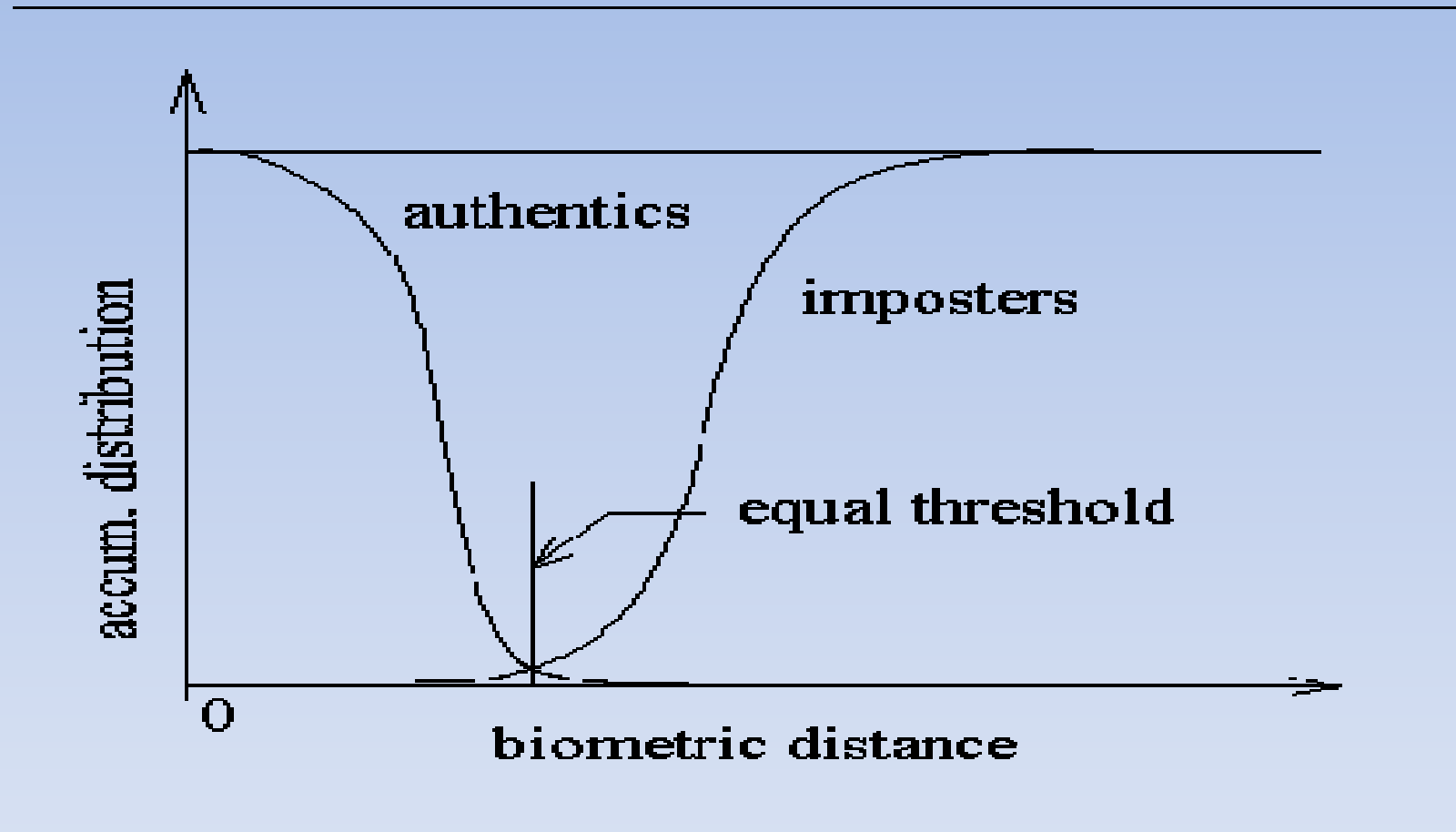
Compensating Controls reinforce or replace normal controls that are available for some reason. An example of a compensating control is something like a \$5,000 limit on a corporate credit card for a new manager.

Access Control Threats

Time of check vs. Time of Use

- When you login to a Microsoft system, you get a SID or Security Access Token, which you will use for all access to the system.
- Suppose that while you are logged in, the owner of an object grants RWX access to that object to a group you belong to. Since the group SID is in your token, when you try to access the object, you will then get a handle to it. Why? Because the object check is at Time of Use, and even though you did not have this at login, you now have access.
- Suppose that you login and are a member of the Widgets group. While you are logged in, the system administrator removes you from the Widget group. Do you still have access to what the Widgets group had access to? Yes, because the TOC was login.

Biometric Crossover Thresholds



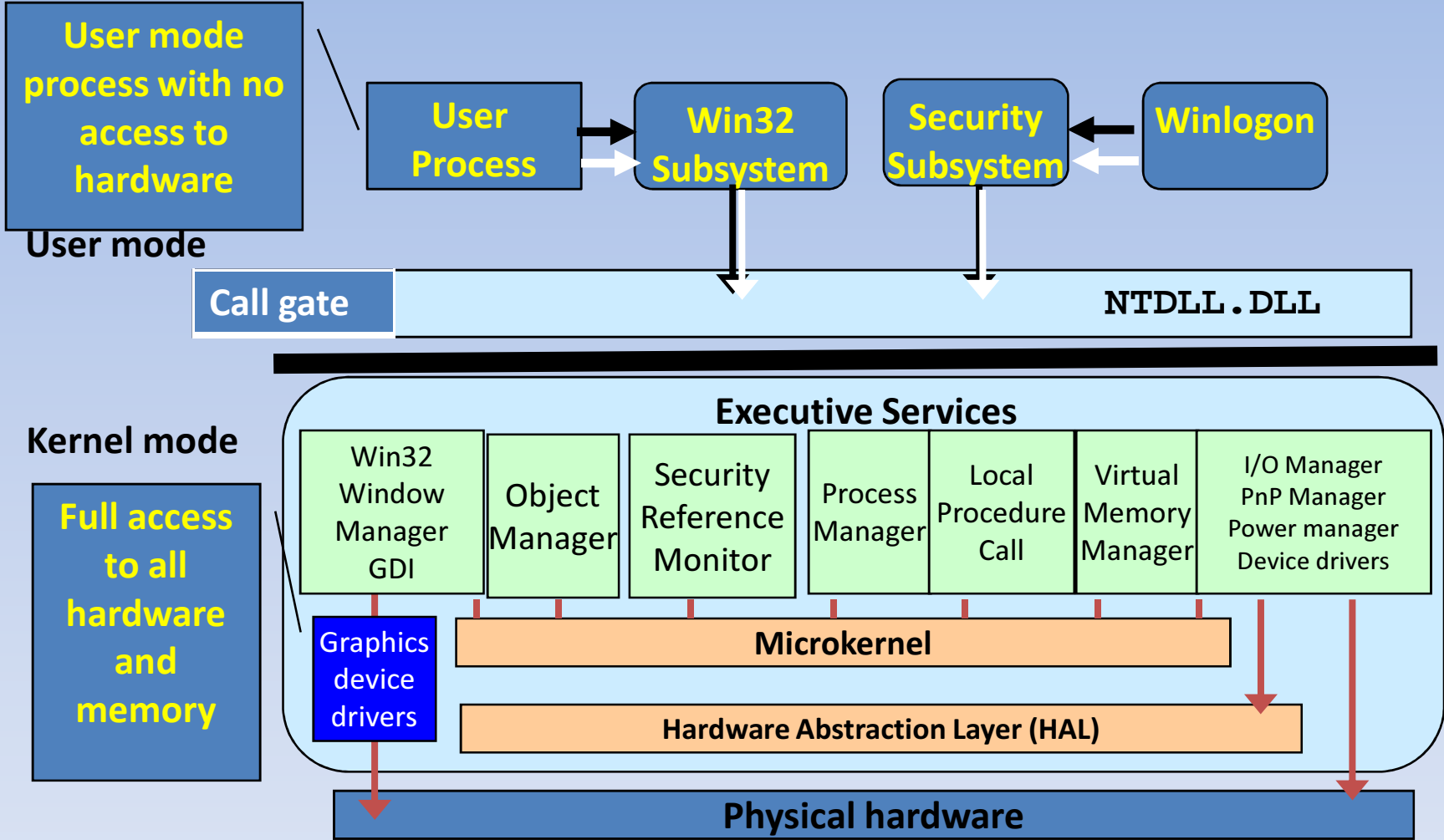
Sensitivity → → → → → → → → → → → → → → →

Actual Biometric Crossover Rates

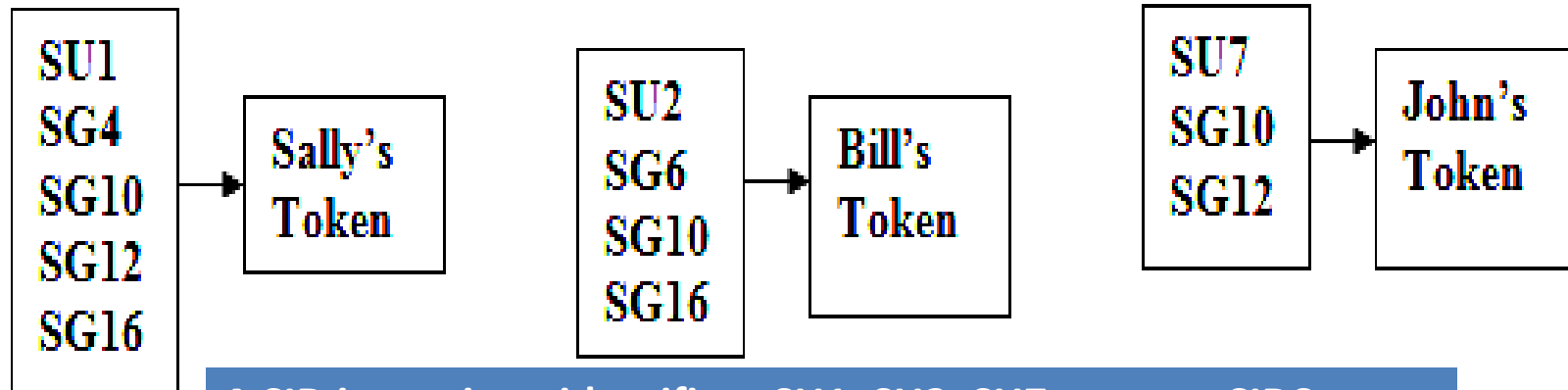
Biometric Solution	Biometric Crossover Point	Biometric Solution	Biometric Crossover Point
Digital Fingerprints	< 0.00001 or < $1 * 10^{-5}$	Forensic Fingerprints	0.0000001 or < $1 * 10^{-7}$
Face Recognition	Best is <0.01 or $1 * 10^{-2}$	Iris Scan	< 0.0000001 or < $1 * 10^{-7}$
Speaker Recognition	Best is <0.01 or $1 * 10^{-2}$	Retina Scan	<0.0001 or $1 * 10^{-4}$
Signature Analysis	<0.02 or $2 * 10^{-2}$		

A BCP of 10^{-2} is 1,000 times worse than one of 10^{-5} !

Windows Server 2003 OS Functional Diagram



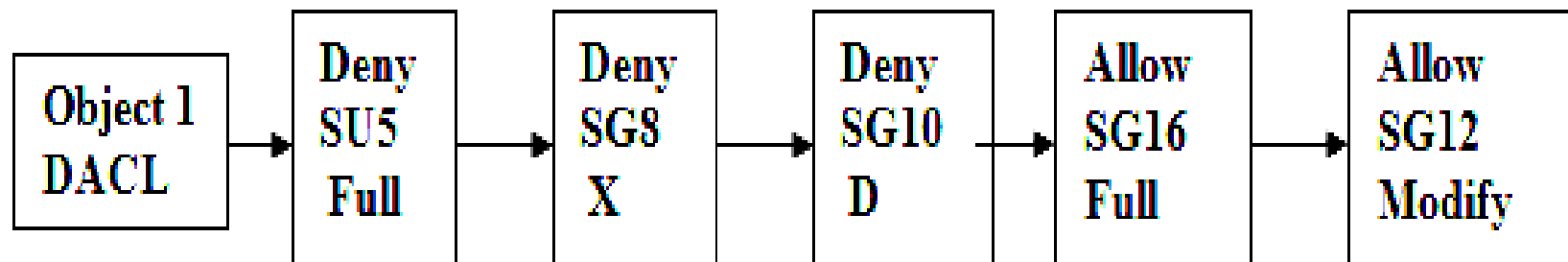
Windows User SIDs and Tokens and An Object's Access Control List



A SID is a unique identifier; SU1, SU2, SU7 are user SIDs.

Permissions are: R=Read, W=Write, X=Execute, D=Delete, O=Take Ownership, P=Change Permissions, Modify=RWXD, and Full=RWXDOP.

The Group SIDs are designated as SG4, SG6, SG10, SG12 and SG16



Question 1: Can Sally delete Object 1?

Question 2: Can Bill Execute Object 1?

Understanding Windows User and Data Protection

There are three rules that Windows systems use to determine user access to an object. These rules are “*mutually exclusive and exhaustive*” so that only one rule occurs in each request to access an object, no matter what the request is. In each case, your search starts at the first Access Control Entry in the object’s DACL and compares SIDs to Access Control Entries, one at a time.

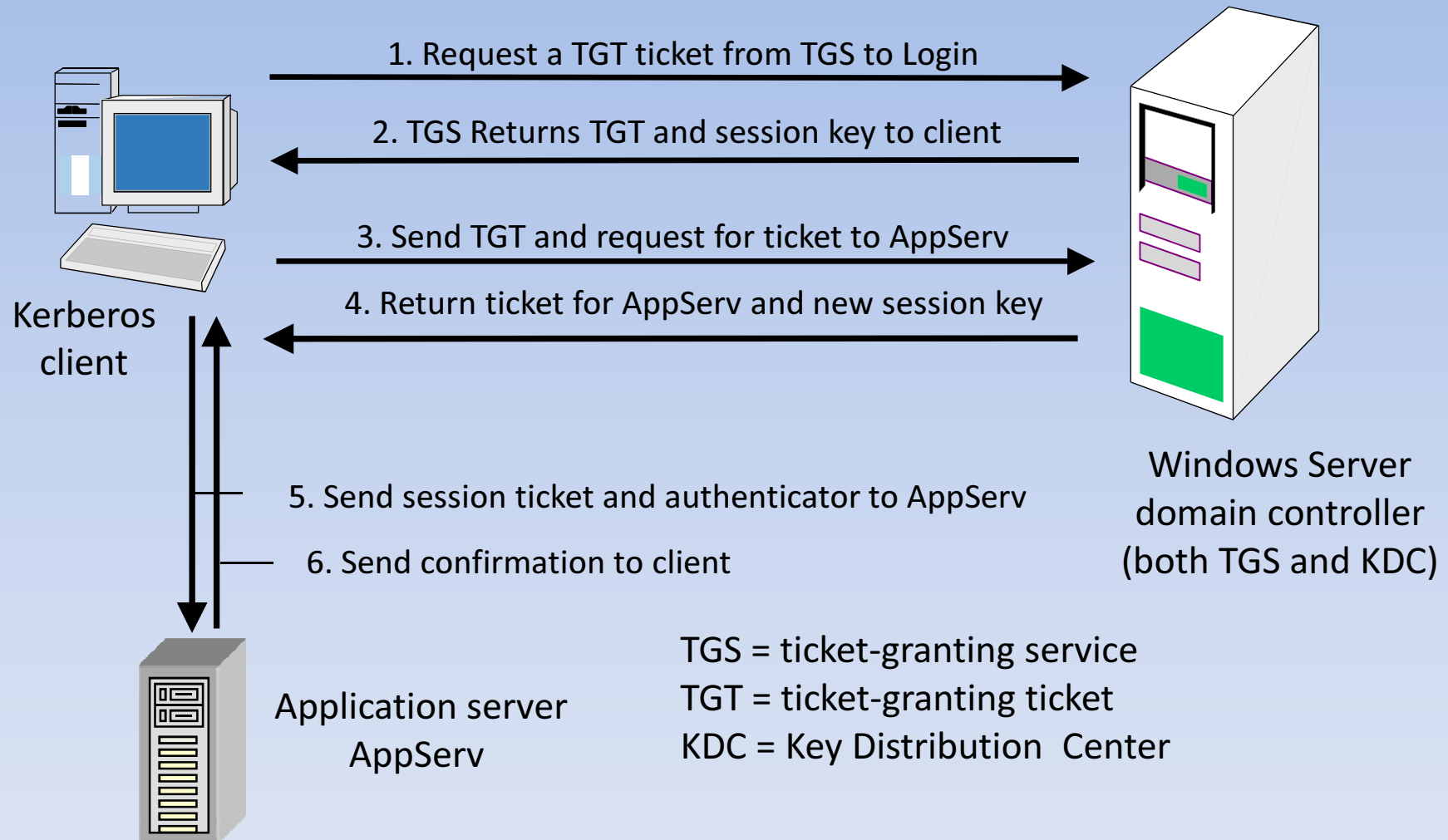
Rule 1: As you go through the DACL, before getting all the permissions you seek, you find an ACE that denies you a permission you seek. In this case, you are denied access to that object. **North Georgia Version: No means No!**

Rule 2: Rule 1 does not apply, and you go through the entire DACL and still do not discover an ACE that gives you a desired permission. You are denied access to that object. **North Georgia Version: No Yes means No!**

Rule 3: As you go through the DACL, Rule 1 never applies, i.e., you are not denied a permission you seek. You find each and every permission you seek. You are granted a handle to that object.

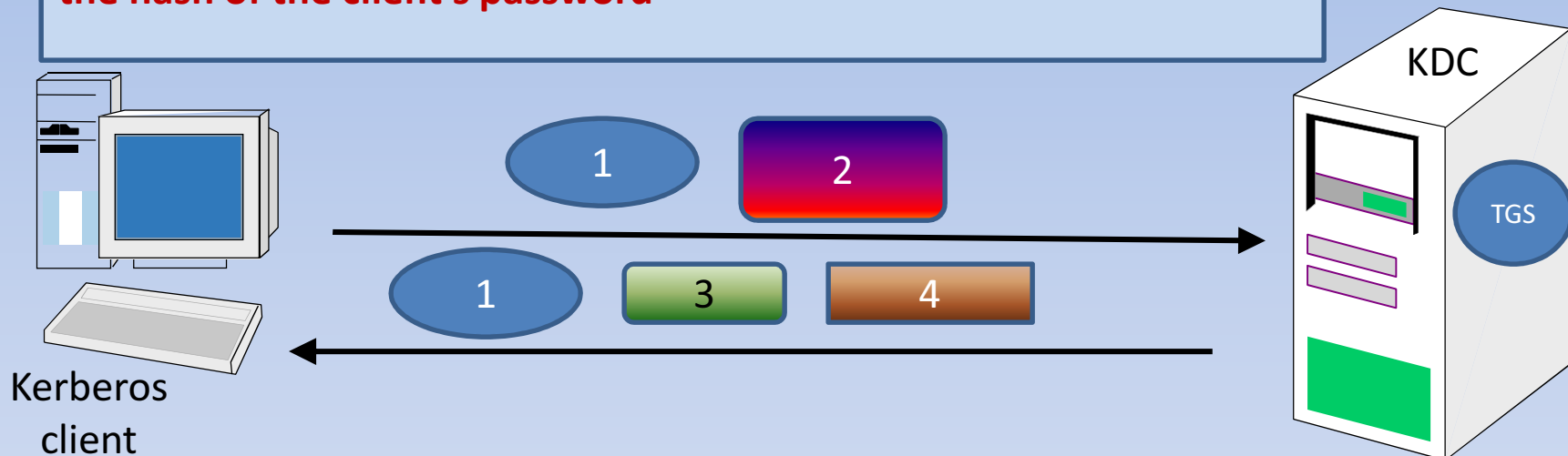
North Georgia Version: Yes means Yes.

Domain Authentication via Kerberos



Microsoft Kerberos Authentication

- 1 is a plaintext containing [name, domain, timestamp]
- 2 is an encrypted version of { name, domain, timestamp, ...} encrypted with the client's Long Term Symmetric key, which may be the hash of the client's password



- 1 Is the same Plaintext that the client sent to the KDC.
- 3 Is the Ticket Granting Ticket encrypted with the KDC's secret key. This key is not known to the client, who can never read the TGT. It only gets sent back to the KDC when the client needs to access an App Server in the domain.
- 4 is the special packet sent back to the client, encrypted with the key the client used in 2 but it contains the client's SIDs, etc., for the client authentication token, and the session key the client will use to talk to the KDC during the rest of this login session.