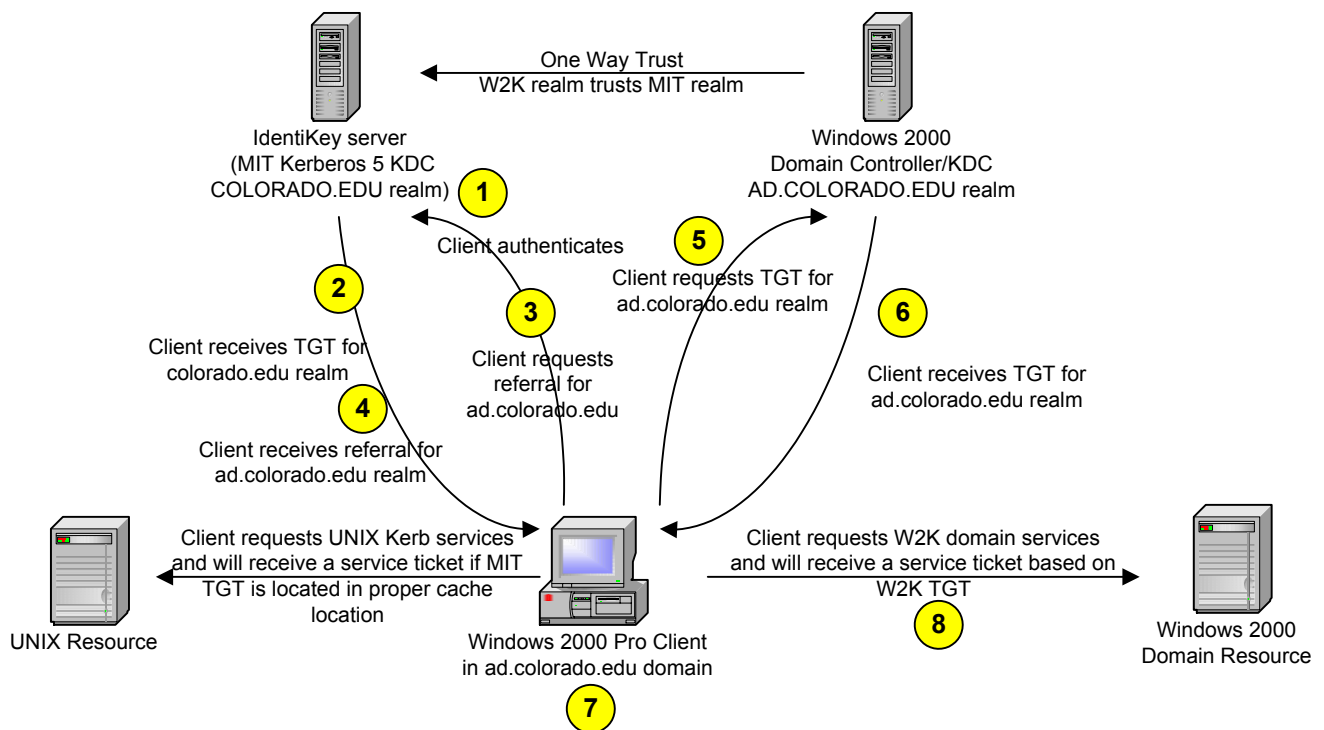


# UCB W2K - MIT Kerberos Interoperability

## Authentication model for W2K Domain Clients

BDJ 1-18-02



1. User logs selects "COLORADO.EDU (Kerberos Realm)" from the login screen and enters their IdentiKey username and password.
2. IdentiKey server confirms username/password match and returns a Kerberos Ticket Granting Ticket (TGT) for the colorado.edu realm to the client.
3. Client requires a TGT for the Active Directory (ad.colorado.edu realm), so it requests a referral from the IdentiKey server.
4. IdentiKey server returns a referral for the ad.colorado.edu realm.
5. Client requests ad.colorado.edu TGT from AD domain controller.
6. AD domain controller checks for a user mapping to an IdentiKey account and issues a TGT for ad.colorado.edu based on the IdentiKey TGT and its trust of the colorado.edu realm. This service ticket contains group membership information.
7. User is authenticated with TGTs for both the IdentiKey resources (colorado.edu realm) and Active Directory resources (ad.colorado.edu realm).
8. When resources within the Active Directory are accessed, a service ticket must first be issued based on the TGT.
9. Using software included in the MIT distribution of Kerberos for Windows, a user can leverage their IdentiKey TGT to access Unix resources that allow Kerberos authentication (like ktelnet) when using client software also capable of Kerberos authentication (like Kermit 95).