Utförande av en undersökning

Aspekter att ta hänsyn till vid en incident och efterföljande brottsplatsundersökning

Digitala bevis överväganden (USA)

- Digitala bevis är olikt de flesta andra bevis
  - Digitalt format (1, 0)
  - Lätt att skada (radera)
  - Lätt att modifiera (bit)
  - Digital kopia och original måste vara oskiljaktiga
- De flesta domstolar anser att digitala bevis är detsamma som hörsägen
  - Det vill säga, vanligen inte användbart i rätten
  - Liknande uppsnappade konversationer eller bevis ej under ed
- **Om Digitala bevis skall få betraktas som fysiska bevis:**
  - Speciella undantag från ”hörsägen”-regler måste till för att digitala bevis skall få användas i rätten

Digitala bevis överväganden (USA)

- Affärshändelser anses vara ett undantag till hörsägen regeln
  - E-post, memon, rapporter, händelser, loggfiler
- Affärshändelser måste verifieras
  - Skapade i anslutning till händelsen eller nära den
  - Inrapporterad av en person som har direkt kännedom om incidenten (ej via hörsägen)
- Kan användas om händelserna normalt lagras av organisationen och historik finns

Data-transaktioner och filer (USA)

- Kan användas om de följer standars för information
  - U.S.: Federal Rules of Evicence, 803 (www.usdoj.gov)
  - U.K.: Police and Powers Act and RIPA
- **Faller inom två katergorier:**
  - **Datagenererade** – skapade av systemet själv, t.ex. loggfiler
  - **Datalagrade** – skapade av användare på systemet
- Datagenererade filer anses vanligen inte vara hörsägen
  - Innehållet kan inte misstolkas
- Datalagrade filer **anses normalt vara hörsägen** om de inte hör till en affärshändelse

Data-bevis och integritet

- Kommer ifrågasättas av en domstol när
  - Bevis t.ex. finns i ”slack space” (gammal data) på hårddisk
  - Ingen författare är associerad till dokument
- Datagenererade transaktioner
  - Måste kunna identifieras till datorn ifråga
  - Får inte vara modifierade på något sätt
  - Måste identifiera användaren eller tjänstens konto
- Extra information är ofta nödvändig för att ”koppla” bevisen
  - E-post med samma ord, fraser eller lösen
  - Filers skapande- datum/modifiering eller åtkomst, när en viss användare var inloggad

Digitalt tillåtna bevis

- Generellt gäller att datautskrifter som korrekt beskriver data i datorn betraktas som original dokument
- I USA så är kopior av data erhållet med en tillförlitlig ”bit-stream kopiator” godkända som bevis
- Bit-stream kopian anses vara en tillförlitlig arbetskopia även om originalmediet skulle försvinna, fallera eller skadas
  - Man måste dock kunna uppvisa att man vidtagit nödvändiga säkerhetsåtgärder för att skydda/bevara originalet

Forensiska analys team

- Det finns flera fördelar med låta ett team hantera forensiska analyser
  - Ett team kan dela upp ansvaret med att processa incidenten
  - Om ett team har utfört analysen ökar det trovärdigheten
  - När man stämmer av bevis så har man ett antal olika initialer som verifierar
    - Förenklar när många bevis måste loggas in eller om analysen måste utföras på väldigt kort tid

Forensiska verktyg för incident hantering

- Forensiska utredare bör ha ett antal verktyg redo för utryckningar på ”fältet”
  - PC- / Embedded- / Mobile- Toolkits
  - Bootbar USB eller CD-ROM med forensisk mjukvara och verktyg
  - Handverktyg
  - Digitalkamera
  - Påsar för bevisinsamling
  - Skrivskyddsblockerare

Säkra incident eller brottsplatsen

- Koordinera med avdelningschefer för att förhindra
  - Otillbörlig access till platsen
  - **Manipulering av platsen av misstänkt**
  - Konfrontationer med person/personer vid tillslag
- Bestäm i förväg vad som skall **beslagtas** eller **omhändertas**
  - Hårddiskar eller hela system
  - Skrivarutskrifter eller hela skrivaren
  - Floppys/CD/DVD, bandbackup, flash-minnen etc.
- Kopiering (bit-stream image) direkt på plats är också en möjlighet eller kanske tvunget att göras

Säkra incident eller brottsplatsen – forts.

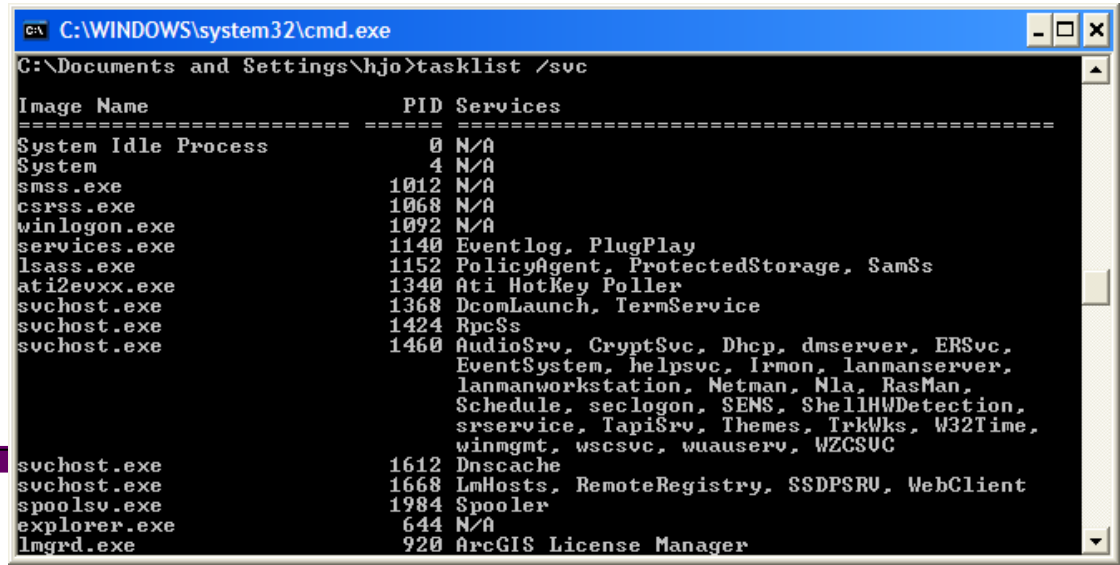
- Avdelningschefer vill ibland inte att arbetstagaren skall veta att vederbörande är under utredning
  - Gör image av hårddisk med bit-stream program – lämna inga spår av att du ”varit där”
  - Det kan vara ide att lämna en keystroke logger (KeyPhantom, KeyCatcher)
    - Både hårdvaru- och mjukvaruversioner finns
  - Fotografera hela platsen
    - Prylars placering, post-it lappar etc.
    - Förvissa dig om att **allt** hamnar på samma plats igen
  - Ändra inte på belysning, stol eller annat!

Minimera driftsavbrott eller störning

- Koordinera med chefer för att förvissa dig om att störningar blir minimerade
- Om en server behöver kopieras
  - Genomför kopieringen ASAP!
  - Ta upp servern online igen
- Om servern måste beslagtas/omhändertas
  - Koordinera detta med en backup/redundant server
  - Om servern är allvarligt skadad måste kanske den byggas upp från gammal backup
- Genom att minimera effekterna av en undersökning kan framtida händelser analyseras och hanteras i tid
  - Chefer får större ”förtroende” att verkligen anmäla incidenter i framtiden

Tidssynkronisering

- Tidssynkronisering är nödvändigt för att rekonstruera i vilken ordning utrustning och filer accessats
- Tidssynkronisering bör ske automatiskt i ett domännätverk
- W32time service finns i Windows Server
- W32time tråd kör inuti svchost
  - Svchost laddar .dll filer som tillhandahåller tjänster i systemet
  - Lista finns i registret
- UNIX/Linux etc.
  - NTPD
  - **set date ntp** *<ntp-server>*
  - CRON-jobb



Kerberos autentisering – I

- Kerberos autentisering kräver tidssynkronisering
  - Förhindrar Domänkontrollanter att acceptera gamla eller inspelade login sessioner i autentiseringsförfrågan
- Förhindrar datorer att accessa utdelningar, skrivare etc. utan en giltig svit av Kerberos credentials
- Att slå av tidssynkroniseringen har därför i vanligaste fallet motsatt effekt mot vad inkräktare vill – om inte DoS är deras mål
- Tidssynkronisering tillåter korrelation av loggfiler på ett stort antal datorer
  - Datorer bör vara mindre än 5 minuter ifrån varandra i tid
  - Baserat på kerberos autentiseringsstandard
- Tidssynkronisering sker automatiskt vid login eller när en nätverksresurs används
  - Uppdateringstiden kan även sättas med policys i domänen
  - Kan också göras manuellt med kommandot net time

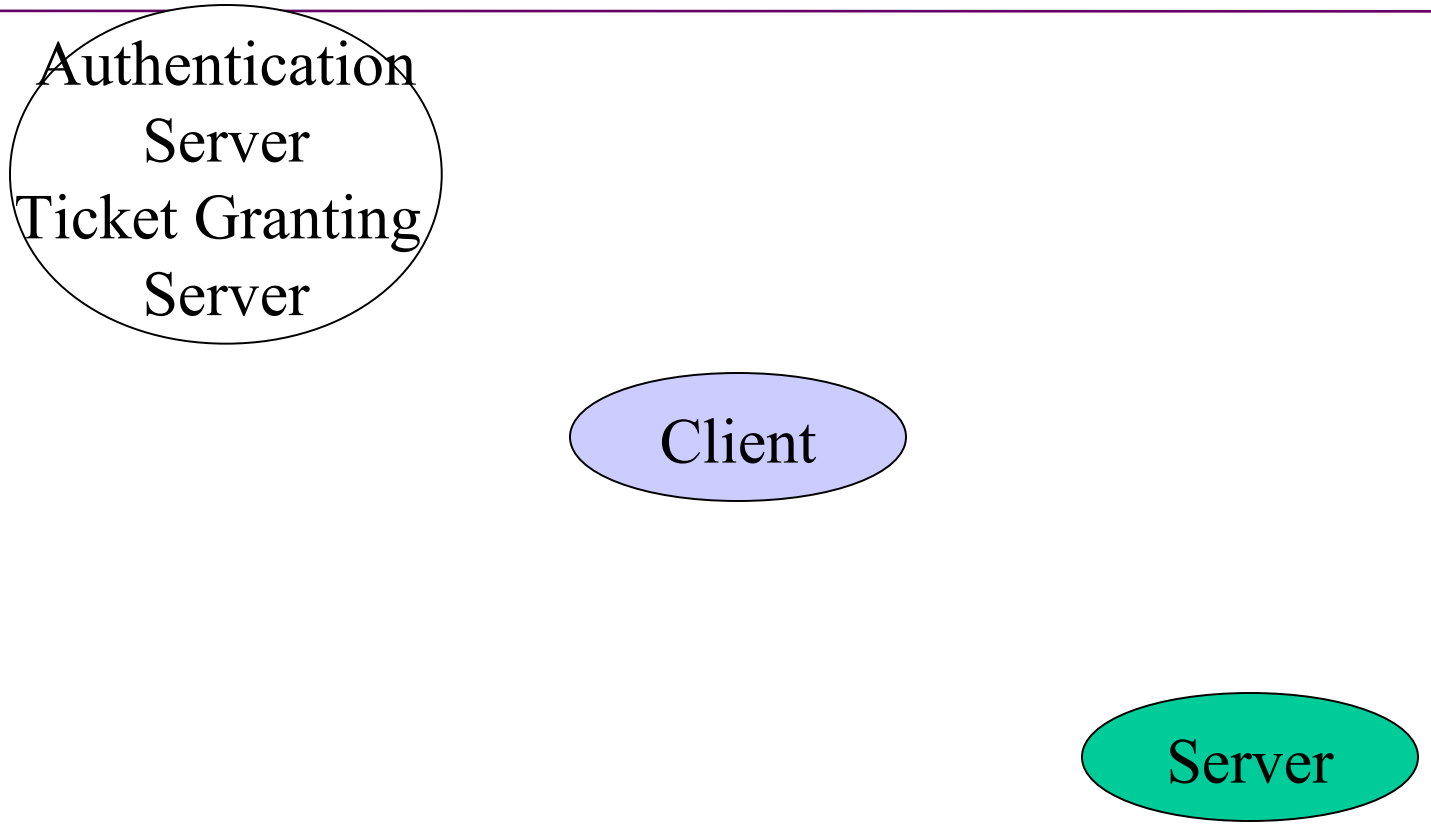
Kerberos autentisering – II

- Utvecklat av Massachusetts Institute of Technology
- Windows 2000/XP/Vista/7 logon använder Kerberos
- Kerberos hanterar en databas av hemliga nycklar där varje klient (tjänst eller användare) på nätet delar en nyckel med sig själv och Kerberos
  - Bevisar identiteten
- Datorn autentiserar sig mot Kerberos servern när den bootar upp eller när någon loggar på
  - Sessionsnycklar skapas för att säkra interaktionen när enheter skall kommunicera med varandra
- 3 nivåer av säkerhet stöds
  - Autentisering, signering och kryptering
- Kerberos bygger på symmetriska nycklar och en betrodd tredje part KDC (Key Distribution Center)
  - Består av en Authentication Server (AS) och en Ticket Granting Server (TGS)

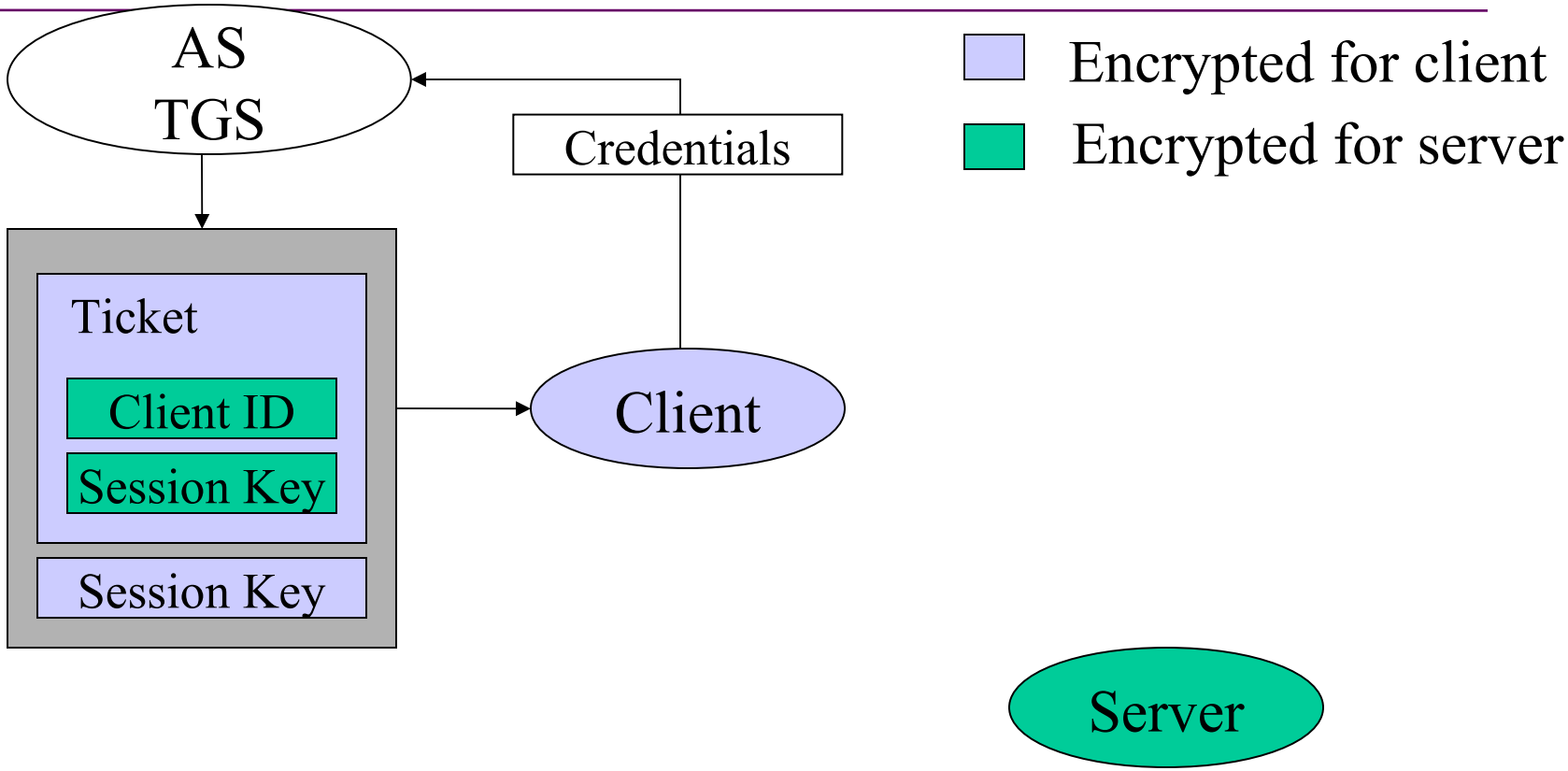
Kerberos autentisering – III

- Kerberos använder 3 sub-protokoll för sin funktion
  - **Authentication Service (AS) Exchange**
    - Används av Key Distribution Center (KDC) för att erbjuda klienter ticket-granting tickets (TGTs) och logon sessions nycklar
  - **Ticket-Granting Service (TGS) Exchange**
    - Används av KDC för att distributera service session nycklar och deras associerade tickets
  - **Service/Client Server ((S)CS) Exchange**
    - Används av klienten för att sända en ticket i syfte att få tillgång till en service
- ”Tickets” representerar identiteten hos användare eller tjänster
- Sessionsnycklarna har relativt kort livslängd

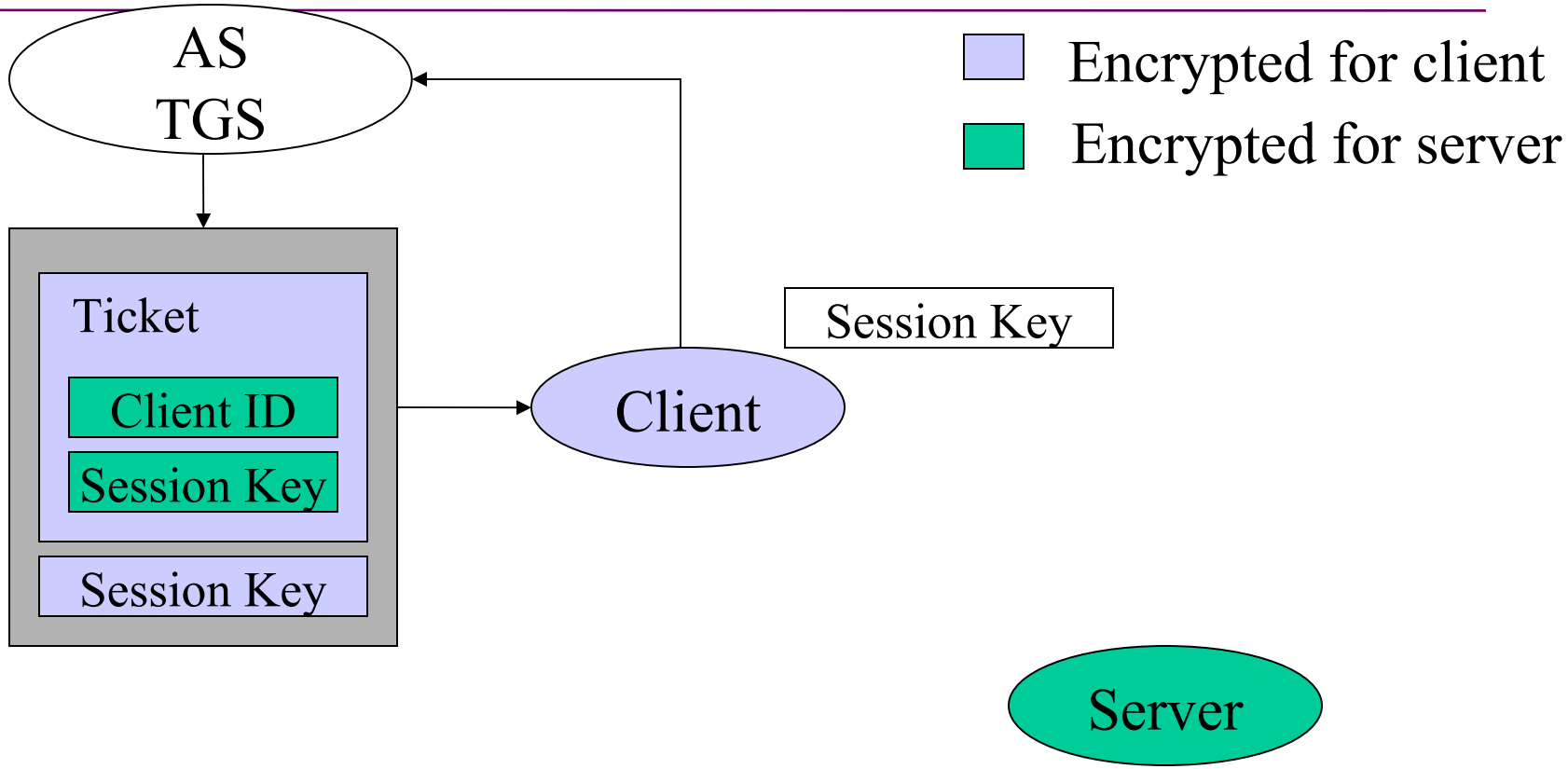
Kerberos IV


Authentication
Server
Ticket Granting
Server
Client
Server

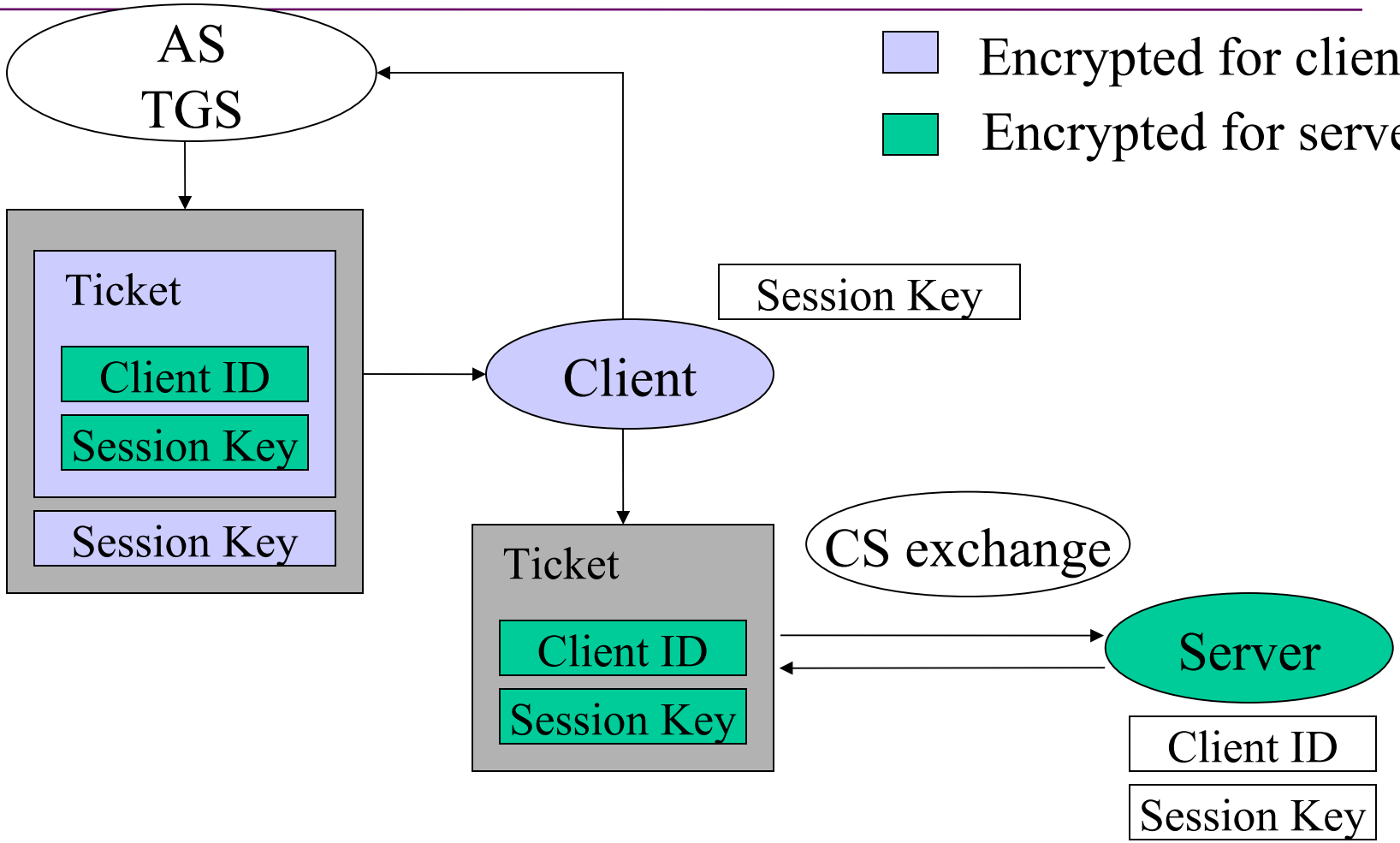
Kerberos V


AS
TGS
Credentials
Ticket
Client ID
Session Key
Session Key
Client
Encrypted for client
Encrypted for server
Server

Kerberos VI


AS
TGS
Encrypted for client
Encrypted for server
Ticket
Client ID
Session Key
Session Key
Session Key
Client
Server

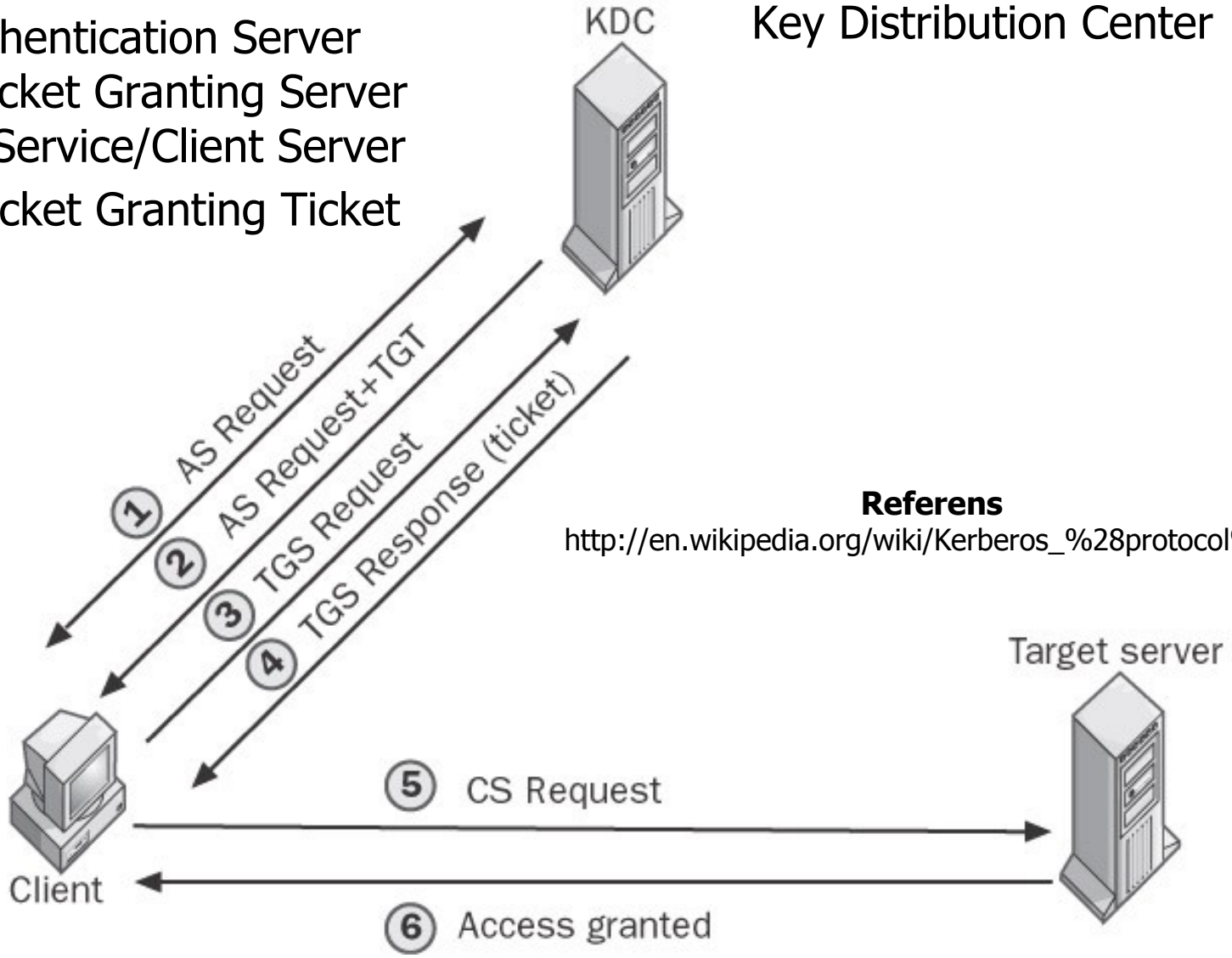
Kerberos VII



Kerberos autentisering - 1

- AS = Authentication Server
- TGS = Ticket Granting Server
- (S)CS = Service/Client Server
- TGT = Ticket Granting Ticket

Key Distribution Center



Referens
http://en.wikipedia.org/wiki/Kerberos_%28protocol%29

Kerberos autentisering – 2

1. The user's credentials are entered on the client, which submits a request to the KDC to access the TGS using the AS Exchange protocol. The request includes encrypted proof of the user's identity.
2. The KDC receives the request, looks up the master key of the user in Active Directory directory service, and decrypts the identify information contained in the request. If the user's identity is verified, the KDC responds by granting the user a TGT and a session key using the AS Exchange protocol.
3. The client then sends the KDC a TGS request containing the TGT granted earlier and requesting access to some service on a target server using the TGS Exchange protocol.
4. The KDC receives the request, authenticates the user, and responds by granting the user a ticket and a session key for accessing the target server using the TGS Exchange protocol.
5. The client then sends the target server a request containing the ticket granted earlier using the CS Exchange protocol. The server authenticates the ticket, replies with a session key, and the client can now access the server.

Regler för konfiskering

- Vad du legalt kan konfiskera beror av
  - De lokala juridiska reglerna för bevis
    - Omhänderta vs. beslagta
  - Om det finns en underförstådd privat frihet för användare
    - Login banners kan komma runt det i viss mån
  - Om systemen är privata eller statliga/kommunala
  - Om enheten är privat eller ägd av organisationen
    - Flashminnen, USB enheter, mobiltelefoner, surfplattor etc.
- Vid tveksamhet är det **TVUNGET** att rådfråga juridisk personal inom organisationen eller utanför
  - Att gå över gränsen kan få allvarliga följder både för dig och din organisation
- **IT-säkerhetspolicyn är viktig… synliggör den!**

Hur hanterar vi personer vars utrustning är föremål för en undersökning?

- Som en kriminell?
- Som en kollega?
- Känslokallt?
  - Tänk om det är en vän…?
  - Intressekonflikter kan uppstå
- **Objektivitet är nyckeln till att bli en framgångsrik utredare!!**
- Kom ihåg!
  - Personen kan vara oskyldig, vederbörandes maskin kan ha använts utan personens vetskap eller tillstånd!
- Det kan under undersökningen komma fram bevis som är till personens fördel, vilket kan frigöra denne helt från misstanke!

Hantering av ifrågasättanden och undersökt hårdvara

- Hur hanterar vi närgångna/nyfikna personer?
  - Andra på avdelningen kan ha frågor och synpunkter på tillvägagångssättet hos den forensiska utredaren
    - Närliggande kontorsrum
    - Förbipasserande
    - Andra chefer
  - Om detta händer så försök att avleda intresset till något annat…
    - Rolig historia etc. (”social kompetens” är en viktig förmåga)
- Se till att all undersökt hårdvara är inventerad
  - Modellbeteckning, tillverkare, firmware, serienummer etc.
  - Anti-statiska påsar, förpackningsskydd
  - Använd identifierings-id klisterlappar – matchas mot rapportloggen
  - Intresse för detaljer och att snabbt identifiera och matcha bevis mot dokumentation är en stor del av jobbet

Hur man dokumenterar och loggar bevis

- Bärbar dator eller surfplatta fungerar ok
  - Datum/tidsstämpel på varje bevisföremål, ett kalkylblad kan vara tillräckligt för detta – kamerabild!
- Använda tredjeparts programvara
  - Ger formulär för att logga bevis
  - Säkerställer att alla detaljer loggas och inget missas
  - Exempel
    - NetForensics - www.netforensics.com
    - ArcSight - www.arcsight.com
- Verktygen bör definiera nyckelaspekter hos bevisen
  - Detaljer om påverkade inventarier
  - Beskrivning av incidenten och stödjande bevis
  - Påverkas system/business? Åtgärder för att reducera negativa effekter? Finns det andra följdåtgärder?

Logga bevis med forensiska verktyg

- AccessData FTK (Forensic Tool Kit) och de flesta andra forensiska tool kit har funktionalitet för
  - Rapport av undersökningen och loggning av information
  - Återskapa raderade filer och inbäddade filer i filer
  - Hitta data/filer i slack-space och free-space
  - Carving för att hitta data och filer
  - Olika typer av filsystem
  - Rapporter om funna filer på disken och deras hash
  - Filtypsanalyser av header (filer med fel filsuffix)
  - Time-lines för filer i systemet
  - Mycket mera…
- Verktygens kostnad är från fria -> mycket dyra