Datasäkerhet och integritet

OH-3 v1

- Autentisering
- Host Autentisering
- Kerberos
- Katalogtjänster
- Active Directory
- Mer om PKI & certifikat
- WWW-exempel

Autentisering

- Autentiseringstekniker kan generellt sägas tillhöra någon av dessa metoder
  - Något du vet – lösenord
  - Något du har – elektrisk enhet
  - Något du är – fingeravtryck
- Består oftast av två steg
  - Identifieringsfas – presentera anv. för identifieringssystemet
  - Verifieringsfas – presentera och generera autentiseringsinformation
- Om användarnamnet är känt är det bara lösenordet kvar som kan skydda
- Enligt många experter så är det dags att avskaffa system som enbart använder lösenord för autentisering

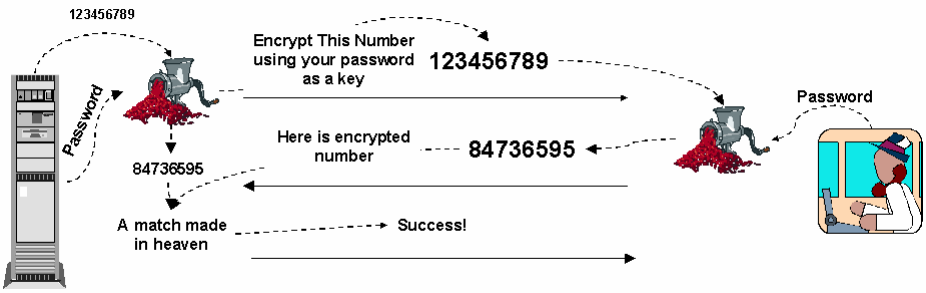
Autentisering

- Lösenord lagras vanligen som en en-vägs hash
  - Verifiering av lösenordet görs genom hashning av användarens input
- Fem huvudmetoder existerar för att knäcka lösenord
  1. ”Social engineering” – lura till sig det på nåt sätt
  2. Gissa lösenordet – kännedom om användaren kan underlätta, eller låta ett program använda ett speciellt uppslagsverk
  3. ”Cracka” lösenordet – om filen med hashade lösenord är tillgänglig och hashalgoritmen är känd kan man **mycket** snabbt gå igenom **många** lösenord, olika skydd mot detta är:
     - Skuggade lösenord (hashfilen är gömd)
     - Ett slumpmässigt ”frö” ingår i hashen
     - Engångslösenord
     - Tokeniserade lösenord (oftast genererade från elektrisk enhet)
     - Olika ”Challenge response” metoder

Autentisering

  4. Trojanska hästar – ett program som loggar lösenord eller helt enkelt har en falsk login prompt
  5. Spela upp (replay) använda lösenord
     - Via avlyssning eller annan elektronisk övervakningsteknik etc. har man kommit över lösenord (snooping), ett skydd mot detta är:
- Challenge – response scheman
  - Använder ett varierat delat hemligt autentiseringssystem utan att avslöja hemligheten
  - Responsen är bara giltig en gång och för en kort tid
  - Används på nätverksinloggningar
  - CHAP (Challenge Handshake Authentication Protocol)

Challenge - response



1) Klient gör login försök (ej med i bilden)
2) Servern genererar ett slumptal (challenge: 123456789 som exempel) och DES krypterar talet med användarens lösenord som nyckel (vilket ger 84736595, den förväntade responsen).
3) Servern sänder challenge till klienten enligt bilden.
4) Klienten skall kunna dekryptera challenge med giltigt lösenord och generera den giltiga responsen.
5) Klienten sänder responsen tillbaka till servern och om talen (ej lösenorden) matchar varandra så är klienten inloggad.

Skydda sig mot avslöjade lösenord?

- Engångslistor med fördefinierade lösenord
  - Efter första inloggningen sänds ett till lösenord tid dig via mobiltelefon
  - Skrapkort
- Upprepad hashning av lösenordet
  - Endast föregående hash - 1 sänds över nätet vid varje ny inloggning
  - S/key är den mest använda - http://www.surfnet.nl/innovatie/surf-ace/security/doc/skey.html
- Elektriska tokens
  - Vanligen ett smart card, USB-dongel, amulett, etc. med PIN-kod eller en dosa där engångslösenord genereras enligt ett visst tidsschema
  - RSA SecureID är den mest använda
- Algoritmiska lösenord
  - Om användaren innehar en privat nyckel som matchas av en känd publik nyckel på servern
  - Det krävs att användaren är registrerad av betrodd CA
- Biometriska lösningar (värdefullt som komplement)
  - Autentisering via fingeravtryck, ögon, röst, skrivstil etc.

Host (värd) Autentisering

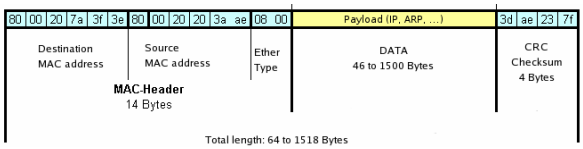
- Vanligaste hotet är att värden maskerar sig som en annan redan auktoriserad värd
  - Detta kallas spoofing
- IP (Internet Protocol) används för all kommunikation på Internet
  - IP-adresser är unika - dubbletter får inte förekomma!
- DNS (Domain Name System)
  - Håller reda på IP-nummer (adress) och DNS-namn (jmf. telefonkatalogen)
  - Innan en dator kan kommunicera måste den få en IP-adress av DNS-servern som matchas mot ett DNS-namn eller lokalt via egen konfiguration
- Innan detta sker så måste dock datorn få en MAC (Media Access Control) adress på LAN:et (Local Area Network)
  - Används inom IPv4 för att översätta Ethernet MAC hårdvaruadresser till IP-adresser
  - ARP protokollet är metoden (mellanhanden) som används för att hitta en värds hårdvaruadress när endast protokoll (t.ex. IP) -adressen är känd

ARP (Adress Resolution Protocol)

- Värdnamnet, ARP och IP identifierar värden men har ingen metod för att verifiera identiteten (att rätt MAC/IP adress är kopplad)
- ARP används i 4 scenarion när två värdar kommunicerar, När:
  - Två värdar finns på samma nätverk och en vill sända ett meddelande
  - Två värdar finns på olika nät och de måste använda en router/gateway för att nås
  - En router behöver forwarda ett meddelande från en värd genom annan router
  - En router behöver forwarda ett meddelande från en värd till destinationsvärden på samma nätverk
- Alla värdar har en ARP tabell
  - Är en slags cache där IP/MAC adress mappningen finns, förnyas periodiskt
  - I ett cmd shell: arp -a listar aktuella entrys i tabellen
- Referens - http://www.eventhelix.com/RealtimeMantra/Networking/Arp.pdf

Man In The Middle (MITM)

- En attack där attackeraren närsomhelst har möjlighet att läsa, infoga eller modifiera meddelanden mellan två värdar utan att dessa känner till det
- Benäms även ARP spoofing eller ARP poisoning



- Principen är att sända falska (spoofed) ARP meddelanden på LAN:et så att andra värdar får en felaktig ARP tabell
- Dessa Ethernetramar innehåller falska MAC adresser som förvirrar andra nätverksenheter att t.ex. sända ramarna till MITM istället
- Referenser
  - **http://www.oxid.it/downloads/apr-intro.swf**
  - **http://manugarg.blogspot.com/2005/06/sniffing-in-switched-network.html**
  - **http://www.grc.com/nat/arp.htm**

Skydda sig mot MITM/ARP-spoofing?

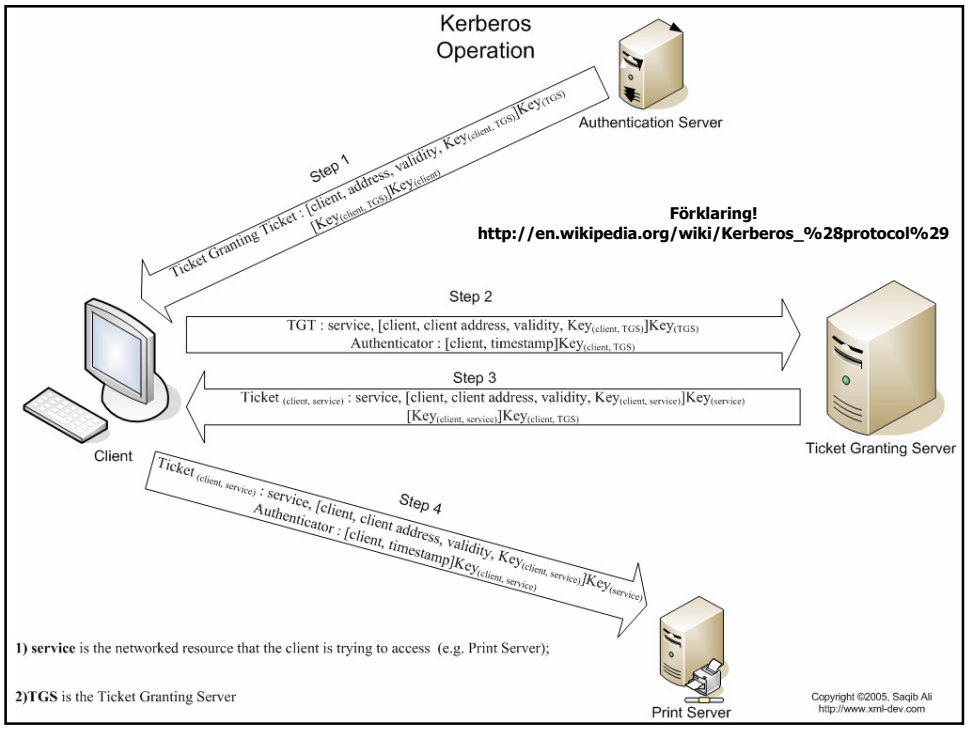
- Det finns i huvudsak fyra sätt att skydda sig
  - Spoof detektering (ARP-watch)
    - Protokoll detektering, DAD (Duplicate Adress Detection)
  - Statisk adressmappning
    - Man får själv upprätthålla en statisk lista och lägga in i arp-tabellen arp – s host_name mac_adress
  - Kontrollera ARP-mappningen med central ARP-server
  - Lita inte bara på en adress som autentisering, använd fler metoder
    - Bevisa ägandet av IP adressen (används av IPsec)
    - Bevisa identiteten av datorn (används av Kerberos)
    - Använd en token från tredje part (digitala certifikat/PKI)

Stark autentisering

- Det finns i huvudsak tre verktyg att autentisera användare, värdar och mjukvara för säker kommunikation
  - IPsec (IP security protcol), som ingår i de flesta moderna OS
    - är standard i IPv6, mer om detta senare
  - Kerberos
    - Är ett betrott tredje parts protokoll som kan göra det möjlig att säkert kommunicera och bevisa sin identitet över ett nätverk
  - Eller ett antal sätt baserade på publik kryptering
    - T.ex. enkel trevägs-handskakning, eller wireless 802.11x autentisering med ”shared secret”, mer om detta senare

Kerberos

- Datorn autentiserar sig själv mot Kerberos servern när den bootar upp
- Bygger på symmetriska nycklar och en betrodd tredje part KDC (Key Distribution Center), som består av en Authentication Server (AS) och en Ticket Granting Server (TGS)
- ”Tickets” representerar identiteten hos användare
- Kerberos hanterar en databas av hemliga nycklar där varje enhet på nätet delar en nyckel med sig själv och Kerberos vilket bevisar identiteten
- En sessionsnyckel för att säkra interaktionen skapas när enheter skall kommunicera med varandra
- Windows 2000/XP logon använder Kerberos



Stark Autentisering, enkel trevägs-handskakning (hemlig nyckel finns redan)

- En klient skickar krypterat meddelande E(x, CHK) där x=slumptal och CHK Client handshake key samt ett ClientId till servern
- Servern dekrypterar med SHK (Server Handshake Key) och skickar krypterat E(x+1, y) där y=slumptal tillbaka till klienten
- Om klienten erhåller önskat värde (x+1) efter dekryptering är servern autentiserad
- Klienten svarar med att skicka y+1 krypterat tillbaka till servern
- Om servern erhåller önskat värde (y+1) efter dekryptering är även klienten autentiserad

Behörighetsadministration

- Effektiv hantering av behörigheter är nyckeln till god IT-säkerhet.
- ”Digital identitet”
  - Unik identifierare – principal
  - Kontaktinformation etc.
- Identitetsnätverk
  - B2B (bussiness to bussiness), B2C… (to client)
  - Standardprotokoll mellan säkerhetsdomäner
  - PKI, Kerberos, .NET passport, WS-trust, SAML, Liberty

MS .NET Passport

- Beskrivning
  - Katalogtjänst
  - Försörjning
  - Autentisering
  - Auktorisation
  - Privacy
  - Applikationer

1. Uppkoppling www-server
2. Verifiering mot passport
3. www verifierar puid mot AD
4. Auktoriseras i katalogtjänst

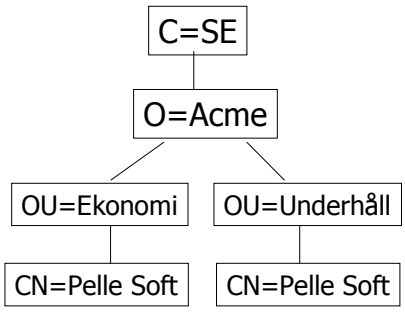
- Autentiseringstjänst för Internet
- Vid registrering skapas ett 64 bitars PUID

Katalogtjänstteknik

- Hierarkisk databas av objekt enligt ett schema
  - Användare, persondatorer, mobiltelefon etc.
- Har attribut som:
  - AnvändarNamn, ModellNamn, TelefonNummer etc.
- Central eller distribuerad
- Hierarkisk för enkelhet och skalbarhet
  - Liknar upp och nervänt träd
  - Medger lagring av likadant AnvändarNamn om det lagras i olika löv (där själva datat lagras)

X.500

- ISO och CCITT skapade i slutet av -80 talet en global distribuerbar katalogtjänst för telekomindustrins ”vita sidorna”
- Katalogträdets underliggande nivåer består av containerobjekt som i sin tur består av andra containerobjekt (OU, O, C) innan löven (CN)



Katalogtjänstprotokoll

- DUA (Directory User Agents) behövs för att användare och tillämningar skall kunna nå information i trädet
- DUA kommunicerar med DSA (Directory System Agent) via ett DAP (Directory Access Protocol)
- DAP använder OSI-protokollet och därmed resurskrävande, därför har Lightweight DAP blivit populärt, det använder TCP/IP och numera även SSL (Socket Secure Layer)
- Om man loggar in som användare på vissa av högskolans tjänster så används LDAP som informationsbärare för autentisering i katalogtjänsten
- En global katalogtjänst är att föredra, kan vara dyr att sätta upp
  - Lägre administrativ kostnad och effektivare rutiner
  - Säkrare behörighetsadminstration
- Motsatsen - en katalogtjänst för varje tjänst ger det motsatta

Metakatalogtjänster

- Erbjuder användning av hjälpmetoder för att efterlikna en global katalogtjänst när man i verkligheten har ett antal olika katalogtjänster
- Connectivity
  - Ett sätt att dela information mellan olika katalogtjänster, databaser och applikationer
- Brokeringfunktionalitet
  - Metoder att distribuera en förändring till samtliga repositories (DB, katalogtjänst, applikationer)
- Integritetsmekanismer
  - Transaktionshanterare som tillser att besläktade data behåller sin konsistens rakt igenom
  - En slags vakt som tillser att brokern sköter sig kan man säga

MMS (Microsoft Metadirectory Services)

- MS Active Directory (AD) som exempel för metakatalogtjänst
- Active Directory Services Interface (ADSI)
  - Programmeringsgränssnitt baserade på COM (Common Object Model), t.ex.
  - SAM-databasen (Security Account Manager) i Windows NT 4.0
  - Katalogtjänster baserade på Active Directory
  - NDS (Novell Directory Services)
  - Valfri LDAP-kompatibel tjänst
  - Hanterar även MS databas ramverk för åtkomst till databaser OLE DB, innebär att SQL ävan kan användas

MMS (Microsoft Metadirectory Services)

- Active Directory Connector (ADC) och DirSynch
  - Synkroniseringstjänster mellan AD och Exchange samt åtkomst till andra LDAP kompatibla katalogtjänster
  - Dirsynch används för att bygga egna synkroniseringstjänster till AD
- Metakatalogteknik
  - MMS, köptes in -99 för att skapa plattform för metakatalogtjänster med AD i botten
- Katalogtjänstkonsolidering
  - Gradvis anpassning av produkter för att använda AD

MMS -> MIIS 2003

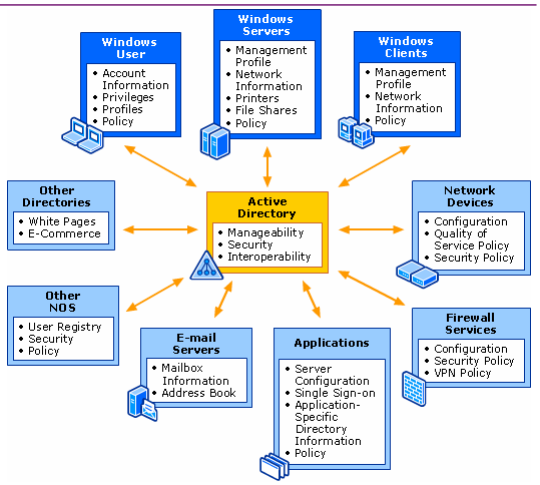
- Microsoft Identity Integration Server 2003 är nya MMS
  - En servertjänst som hanterar all identitesinformation
  - Ett datalager för lagring av identitetsdata med SQL server 2000
  - Anpassninsbart gränssnitt för att utöka funktionalitet mot andra plattformar
- Följande funktioner och förbättringar
  - Synkronisering av datakällor
  - Synkronisering av globala adresslistan i AD
  - Förbättrad lösenordhantering, förändringar kan synkroniseras till alla anslutna system
  - Automatiserad kontohantering
  - Gruppadminstration och certifikatpublicering

Active Directory (AD) på djupet

- Det finns andra katalogtjänster som följer X.500 standarden och hanterar LDAP, t.ex. Novell med sitt NDS långt före AD
  - Läs historia: http://www.nss.co.uk/Articles/Jul97.htm
- AD kom med Windows 2000, läs mera:
  - http://www.microsoft.com/technet/prodtechnol/windows2000serv/technologies/activedirectory/deploy/projplan/adarch.mspx
- Arkitektur, se bild 5.20 sid. 82
- Active Directory Server baseras på en Directory System Agent (DSA) som svarar på LDAP- och DNS-anrop
- DSA-agenter använder Kerberos Key Distribution Center (KDC) för att höja säkerheten (se bild 5.21 sid. 83)
- Kombinerar det bästa ur DNS (Domain Name Service) och LDAP
  - Kan därmed bilda domäner träd och skogar (se bild 5.22/5.22 sid. 84/85), sökningar kan utföras (se bild 5.24 sid. 86)

Active Directory i Windows 2003

- Hanterar i stort sett alla behörigheter från en central plats!



AD 2003 förbättringar

http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx

- Införande och administration
  - Kan hantera riktigt stora och distribuerade miljöer
  - Migrationer från äldre installationer
  - Namnbyten och omdefiniering av scheman m.m.
- Säkerhet
  - Autentisering och auktorisation mellan skogar
  - Begränsningspolicy för programvara
  - Korscertifiering och säkrare lager för lagring av inloggningsdata och X.509 V.3 certifikat m.m.
- Prestanda
  - Snabbare fjärrinloggning och replikeringar m.m.

PKI (Public Key Infrastructure) i Windows 2000/2003 **server** versioner

- Standardtillämpningar i ”paketet”
  - Klientautentisering (SSL/TLS)
  - Webbserverautentisering och kryptering
  - Krypterad och signerad e-post (S/MIME)
  - Digitalt signerat innehåll
    - Dokument
    - Programkod
  - Filsystemkryptering via EFS (Encrypted File System)
  - Inloggning med aktiva kort
  - Nätverksautentisering av användare/enheter och kryptering via IPSec
  - Katalogtjänstautentisering via LDAP/SSL
  - Ramverk (API) för utveckling av egna tillämpningar

PKI (Public Key Infrastructure)

- Grundläggande funktion för all certifikathantering är att rätt objekt (användare, nätverksenheter eller programvaror) har ett korrekt utfärdat certifikat för en viss funktion
- Utfärdandeprocessen handhas av en CA (Certificate Authority) som är betrodd
  - För egna tillämpningar kan man låta egna företaget vara det
- Certifikat typer
  - Mjuka – lagringen sker i en fil på datorn
  - Hårda – lagringen sker på ett aktivt kort (smartcard etc.)
- Exempel på CA i Sverige: Posten, Telia (hårda och mjuka), banker mfl.

Certifikat

- CA-rollen - certifikatadministration
  - Egen regi eller extern leverantör?
- Certifikatprocessen
  - Efter ett certifikat utfärdats så måste det distribueras till samtliga distributionspunkter i hierarkin (katalogtjänsten)
  - Certifikat som finns i revokeringslistan (CRL) anses ogiltiga
  - Detsamma gäller certifikatets bäst före datum gått ut
- Lagring av utfärdade certifikat
  - I Windows sköts det av ett subsystem CryptoAPI

Användning av aktiva kort (Win 2000/2003)
(egen processor och minne)

- Manipuleringssäkert
- Ansluts via kortläsare, USB etc.
- Interaktivt login
  - Använder Active Directory, Kerberos v5 (Windows logon) och PKI-certifikat
  - Användare loggar in på kortet…
  - Se flöde sid 93 bild 5.25
- Klientautentisering
  - Kortet sänder digital signatur och jämför den tillbakasända publika nyckeln mot kortets privata nyckel
- Fjärrlogin
  - Publik nyckel, EAP, TLS…

PKI (Public Key Infrastructure) exempel: Java WWW on-line auktion

http://www.enges.org/anders.enges/html/ecomm4.html

Klient med Java applet

Server med Java servlet

- All kommunikation sker via webbsidor
- HTTP används för att servern skall få input från och sända output till klienten
- Klientdata sänds till servern genom att använda HTML formulär vilket kan inkludera såväl gömda som synliga data fält
- Varje sida som webbservern genererar i respons är beroende av användares indata hos klienten

PKI (Public Key Infrastructure) exempel: Java WWW on-line auktion

- Klienten har investerat i Baltimore UniCERT och har en global PKI
- Säkerhet på denna nivå
  - Autentisering
    - Det var klienten som klickade på SIGNERA
  - Integritet
    - On-line budet var klientens
  - Icke-förnekande
    - Klienten kan inte vägra erkänna gjort bud

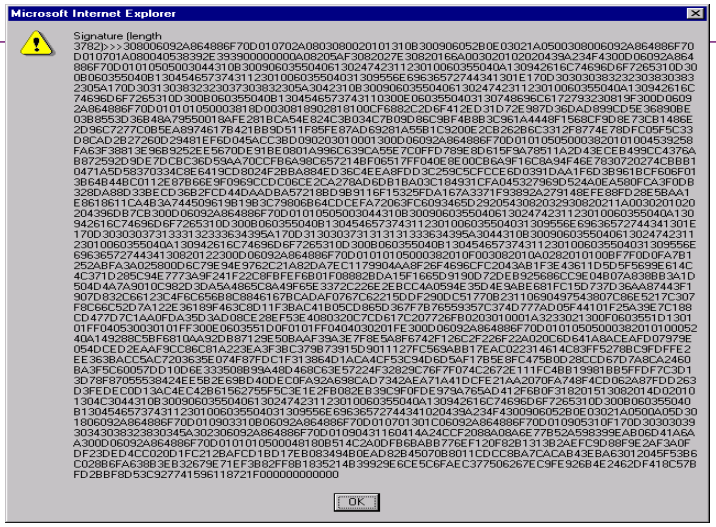
Klient processen

- Klienten hämtar webbsidan och beräknar digital signatur när användaren klickar på SIGNERA
- Sänder formulär med budet till servern med den digitala signaturen i ett gömt fält
- Vad behöver klienten för att beräkna den digitala signaturen?
  - Signerings mjukvara
    - Måste vara "trusted" för att få åtkomst till klientens "token" med den privata nyckeln
    - Måste finnas med i Java appleten som laddats tillsammans med webbsidan
  - Åtkomsten till signerarens privata nyckel
    - Lagras i en säker "enhet" (token)
    - Kan vara en hårdvaru eller mjukvaru token
    - Token innehåller även det digitala certifikatet utgivet av CA

Klientens säkerhetsaktiviteter

- Signerings mjukvaran/appleten:
  - Kan behöva ladda ner den mjukvara (.class filer) den behöver för att beräkna signaturen, för att implementera t.ex. RSA eller SHA-1
  - Visa en lösenordsdialogruta för användaren som behövs för att få åtkomst till användarens privata signeringsnyckel (mjuk eller hård)
  - Måste vara "trusted" för att få åtkomst till användarfiler: en signerad CAB fil används
  - Budet, den beräknade signaturen och användarens digitala certifikat (läst från säkerhets token) paketeras av den signerande mjukaran/appleten till ett PKCS#7 objekt
  - Public-Key Cryptography Standards (PKCS) är företaget RSA Data Security de-facto standard format för public-key cryptography.
  - Detta objekt sänds till servern som en (dold) hex-encoded sträng inuti SIGNERA formuläret

Public-Key Cryptography Standards (PKCS)#7 objekt



Server processen

- Kör servlet när klienten sänder in formulär
- Servlet extraherar data från formuläret och processar det inklusive den digitala signaturen
- Servlet genererar HTML respons webbsida om signaturen är giltig och utifall budet är accepterat
- Vad behöver servern för att verifiera den digitala signaturen?
  - Signaturens publika nyckel och digitala certifikat
  - Funktion att traversera en certifikatskedja
  - Åtkomst till CRL (Certificate Revocation Lists)
    - http://java.sun.com/j2se/1.4.2/docs/guide/security/CryptoSpec.html

Serverns säkerhetsaktiviteter

- När servletet som aktiverats av SIGNERA webbsidan mottar PKCS#7 objektet måste det packa upp och verifiera signaturen som använder det digitala certifikatet
- Servern måste ha åtkomst till verifierings mjukvara och online bibliotek (foldrar), i praktiken så traverseras en certifikats-kedja tills ett *trusted* CA påträffas
- On-line CRL:er måste kontrolleras som en del i processen