Smartkort og Windows 2000

Hovedoppgave
ved
sivilingeniørutdanningen i
informasjons- og kommunikasjonsteknologi,
Høgskolen i Agder

Terje Landa

Våren 2000

Sammendrag

Sikkerhet er et viktig tema innenfor alle datasystemer, ikke minst i forbindelse med Internett. Internett åpner nye muligheter, men medfører også at datasystemene blir mer sårbare. Utfordringen for dagens datasystemer er å utnytte mulighetene et i globalt nettverk og samtidig beskytte mot eventuelle fiender. Sikkerhetsmekanismer basert på kryptografi er hjelpemiddelene som tas i bruk for hemmeligholding, autentisering og beskyttelse i datasystemer.

Microsoft har nylig lansert Windows 2000 som etterfølgeren til det populære operativsystemet NT 4.0. I følge Microsoft er det satset mye på sikkerhet i det nye operativsystemet, og nye sikkerhetsmekanismer er tatt i bruk. En av nyhetene er smartkortstøtte i viktige sikkerhetsoperasjoner. Hensikten med denne oppgaven er å undersøke hvilken smartkortstøtte som tilbys og hvilke sikkerhetsmekanismer som gjør bruk av smartkortfunksjonaliteten.

Sikkerhetsfunksjonene i Windows 2000 er basert på deres Public Key Infrastructure, offentlig-nøkkel infrastruktur. Dette systemer baseres seg på offentlig-nøkkel kryptografi og bruk av digitale sertifikater. Et digitalt sertifikat utstedes på bakgrunn av opplysninger om brukeren, og sammen med nøkkelpar garanteres brukerens identitet. Et system med sertifikater er velegnet til autentisering, som er en kritisk og viktig operasjon i alle datasystemer. En mengde standardiserte sikkerhetsmekanismer er basert på autentisering med sertifikater, spesielt på Internett som er et åpent nettverk der identitet ofte kan være et problem.

Windows 2000 kombinerer smartkort med PKI og digitale sertifikater. Smartkortet beskytter brukerens private nøkkel som korresponderer med sertifikatets offentlige nøkkel. Smartkortets egenskaper gjør det bedre egnet enn et vanlig passord til å beskytte personlige opplysninger, og styrker dermed autentiseringsmekanismenes svake punkt. I Windows 2000 benyttes smartkort til autentisering og digitale signaturer i sikkerhetsmekanismer på lokale maskiner, lokale nettverk og Internett.

Windows 2000 sikkerhetsmekanismer er basert på etablerte standarder som er med på å sikre interoperabilitet med ander systemer, ikke minst på Internett. Mange av disse mekanismene kan anvendes sammen med smartkort, og utnytter kortets styrke som er å beskytte private opplysninger i forbindelse med identitet. Smartkortfunksjonaliteten er tilpasset begrensningene til smartkort, som er liten prosesseringskraft og lav overføringskapasitet. For å ikke gå ut over systemets ytelse, er bruksområdet begrenset autentisering og digitale signaturer.

Forord

Denne rapporten inneholder resultater fra diplomarbeidet utført under vårsemesteret 2000 av Terje Landa, som er student ved sivilingeniørstudiet i informasjon og kommunikasjonsteknologi ved Høgskolen i Agder.

Oppgaven er gitt av Vladimir Oleshchuk i sammarbeid med Protective Technology i Mandal. Dette er et firma som arbeider med smartkortløsninger for datasystemer.

Min motivasjon for å velge denne oppgaven var først og fremst vilje til å lære mer om datasikkerhet. Dette var også interessant i kombinasjon med Windows 2000 som sannsynligvis kommer til å bli et svært utbredt operativsystem, og som jeg helt sikkert kommer til å bruke mye.

Jeg ønsker å takke min veileder Vladimir Oleshchuk og Ulf Carlsen som har vært min kontakt hos Protective Technology.

Grimstad, Juni 2000

Terje Landa

Innholdsfortegnelse

Figurliste

1 Innledning

Sikkerhet i datasystemer er et viktig tema. Ikke bare blir mer og mer informasjon digitalisert, men datasystemene blir også mer åpne. Internett og integrering mot kunder stiller helt andre krav til systemsikkerhet sammenliknet med et lukket system i en organisasjon. For å hindre at uvedkommende får tilgang til sensitive opplysninger er sikker adgangskontroll av brukere nødvendig. Et hjelpemiddel som styrker adgangskontroll er smartkort. Konvensjonelle passord blir erstattet med et smartkort og en PIN-kode. For å få adgang til systemet må man altså både være i besittelse av en fysisk gjenstang, og vite noe om den.

Interessen for smartkort har vært laber i PC miljøet og i forbindelse med organisasjoners datanettverk. Årsaken til dette kan være manglende behov, lite attraktive løsninger eller uvitenhet. Når Microsoft nå har lansert Windows 2000 har verdens største leverandør av operativsystem klargjort et av deres viktigste produkt for bruk av smartkort. Hensikten med denne hovedoppgaven er å se på hvilken støtte Windows 2000 gir for smartkort.

1.1 Oppgaveformulering

Formålet med dette prosjektet er å undersøke hvilken støtte for smartkort som ligger innebygd i operativsystemet Windows 2000, og hvordan disse brukes. Alle versjoner av Windows 2000 skal ha støtte for bruk av smartkort, blant annet for autentisering ved lokal- og nettverkslogon, kryptering og digital signering av e-post og kryptering av lagrede filer.

Første fase av prosjektet går ut på å samle informasjon og å sette seg inn i forskjellige sikkerhetsmekanismer, -protokoller og –standarder som benyttes av Windows 2000. Derav

- Secure Sockets Layer (SSL)
- X.509 v3
- Secure MIME (S/MIME)
- Kerberos v5/RFC-1510
- Windows 2000 Encrypting File System
- Smartkort for Windows 2000

Neste fase går ut på å ta i bruk disse mekanismene, ved å undersøke og demonstrere konfigurasjon og bruk av smartkort for Windows 2000:

- Konfigurering av Windows 2000 og smartkortet, herunder bruk av Microsoft Certificate Server for utstedelse av sertifikater.
- Bruk av smartkort for å utføre forskjellige smartkort-sikrede funksjoner som:
    - Autentisering/bruker logon
    - Sending/mottak av signert og kryptert e-post
    - Nøkkel for kryptert filsystem
- Lage en applikasjon for elektronisk handel over Internett med autentisering og kryptering vha. Smartkort og Windows 2000.

1.1.1 Videre spesifisering av oppgaven

Etter samtale med veileder ble det avtalt å utvide oppgaven til å se på smartkortfunksjonaliteten operativsystemet tilbyr, også for programmering av applikasjoner som bruker smartkort. Det ble også avtalt en sammenlikning med forgjengeren, NT 4.0, mhp. nyheter og forbedringer.

I oppgaveformuleringen er det uttrykt at det skal lages en webapplikasjon. Hensikten med dette var å bruke SSL til klientautentisering med smartkort. På tidspunktet da oppgaven ble formulert var det en felles oppfatning mellom min veileder og meg selv at SSL var applikasjonsavhengig. Dette har vist seg å ikke være tilfelle, og grunnlaget for en webapplikasjon er ikke tilstede.

1.2 Metode

Helt i begynnelsen av prosjektarbeidet gikk det med en del tid til grunnleggende forståelse av generell datasikkerhet og kryptografiske metoder. Parallelt med dette ble det utført litteratursøk for oppgavens første del. Litteratursøk og samling av informasjon utgjort en stor del av arbeidet i dette prosjektet.

Arbeidet ble etterhvert begrenset ned fra generelle smartkortløsninger til Windows 2000 spesifikke. Konfigurering av operativsystemets sikkerhetsmekanismer ble også en større del av oppgaven.

Gjennom hele prosessen har det vært nødvendig med informasjonssøk, og til det ble det brukt flere informasjonskanaler. For informasjon om tradisjonell kryptografi har jeg brukt skolens biblioteket, mens oppdaterte og nye standarder ble fremskaffet på Internett. Dette inkluderer Web steder, nyhetsgrupper og e-post lister. Windows 2000 Server Recource Kit og Windows 2000 Help har også vært til hjelp under arbeidet.

For diskusjon rundt oppgaven har jeg jevnlig hatt møter med min veileder.

Under arbeidet med prosjektet har jeg ikke hatt tilgang til smartkort, heller ikke under bruk og konfigurering av de forskjellige sikkerhetsmekanismene. Jeg tror likevel ikke prosjektet har lidd av denne mangelen.

1.3 Rapportens oppbygging

Rapporten er delt opp i fire hoveddeler. Første del gir en introduksjon til datasikkerhet og kryptografi før den tar for seg sikkerhetsmekanismene i Windows 2000. Videre ser jeg på smartkortrelaterte aspekter i systemet. Tredje del gir en sammenlikning av Windows 2000 med forgjengeren NT 4.0, og siste del viser konfigurasjon og bruk av sikkerhetsmekanismene fra første del.

For å gjøre det lettere for leseren å følge med har jeg valgt å gjøre drøftingen underveis i rapporten.

2 Introduksjon

Som en introduksjon til dette kapittelet vil jeg gi en generell oversikt over datasikkerhet, forskjellige kryptografiske systemer og deres bruksområder. Kryptografiske systemer er en grunnleggende del av sikkerhetsmekanismene i Windows 2000. Hvis du er kjent med kryptografiske systemer og bruk av de kan du hoppe til kapittel 3.

Behovet for sikring av informasjon har alltid vært til stede, både ved lagring og overføring. Med åpne, usikrede nettverk som Internett og med integrasjon utover organisasjonenes intranett for å møte kundenes behov, blir sikring av informasjon stadig viktigere. Når stadig mer informasjon behandles digitalt øker også risikoen for at uvedkommende skal snappe opp eller manipulere sensitiv informasjon.

2.1 Kryptografiske systemer

Begrepet kryptografi betyr læren om prinsipper og metoder for hemmeligholding av meldinger og data. Moderne kryptografi beskytter data som overføres over datanettverk og lagres digitalt. Slik sikring har tre prinsipielle målsetninger:

1. *Hemmeligholde* - Gjøre meldingsinnholdet uforståelig for uvedkommende.
2. *Autentisere* - Bevise identitet til den ene eller begge parter før utveksling av data/informasjon mellom dem.
3. *Beskytte* - Bevare dataenes integritet, dvs. skjerme innholdet mot manipulering.

2.1.1 Hemmeligholding

For at et kryptografisk system skal oppfylle det første punktet kreves det at dekrypteringsprosessen er fullverdig beskyttet. Krypteringsprosessen kan være kjent så lenge den ikke sier noe om dekrypteringsprosessen.

2.1.2 Autentitet

Formålet med autentitet er å sikre at en fiende ikke kan erstatte en original kryptert melding med en falsk uten at dette blir oppdaget av mottakeren. Krypteringsprosessen må derfor være fullverdig beskyttet slik at en fiende ikke kan generere en falsk melding. Dekrypteringsprosessen kan godt være kjent så lenge den ikke sier noe om krypteringsprosessen.

Vi ser at det er en motsetting mellom de krav som hemmeligholding og autentisering krever av krypterings- og dekrypteringsprosessen.

2.2 Symmetriske systemer

Et kryptografisk system er symetrisk hvis kryptering og dekryptering utføres med samme nøkkel. Ved slike systemer må man regne med at hvis krypteringsprosessen er kjent av en fiende er også dekrypteringsprosessen kjent, da disse lett kan avledes fra hverandre. Ved å hemmeligholde nøkkelen vil begge disse prosessene være

ukjente, og systemet oppfyller kravene til både hemmeligholding og autentitet. Symmetriske systemer kalles også hemmelig-nøkkel systemer.

Et symetrisk system er godt egnet for kryptering av en brukers private data. Systemet er også godt egnet for overføring av data over usikrede nettverk. For at kravene til hemmeligholding og autentitet skal være oppfylt må begge parter stole på hverandre. Dette er det klassiske kryptosystemet der to parter deler én hemmelig nøkkel.

Symmetriske systemer regnes for å være de raskeste krypteringssystemene, og egner seg for kryptering av store datamengder. Eksempler på vanlige symmetriske systemer er RC2, RC4 og DES.

2.2.1 DES

Dette kjente symmetriske systemet ble lansert på 70 tallet i USA, og er basert på IBM sitt Lucifer system. Data Encryption Standard (DES) ble vedtatt ved lov i USA som en standardisert krypteringsalgoritme. Virkemåten er svært kompleks, men bygger på flere runder med substitusjon og transposisjon slik at all data til slutt er sterkt påvirket. Virkemåten er velkjent, og sikkerheten er basert på hemmeligholding av nøkkelen.

DES har visse svakheter som stammer fra systemets sterke bit-orientering, og de såkalte S-blokkene. Disse svakhetene kan ungås ved å ikke velge noen få spesielle nøkler, såkalte svake og semisvake nøkler.

Siden sikkerheten i DES, og andre kjente symmetriske systemer, bygger på hemmeligholding av nøkkelen, er nøkkellengden viktig. DES originale nøkkellengde er 56 bit, som virket sikkert i 1977. Etterhvert som regnekraften i datamaskiner øker, minsker tiden det tar for å finne en krypteringsnøkkel ved hjelp av såkalt uttømmende søk. Et uttømmende søk sjekker alle mulige nøkler helt til den riktige er funnet. I dag regnes ikke 56 bit for en tilstrekkelig nøkkellengde for at krypterings- og dekrypteringsprosessen skal være fullverdig beskyttet. I begynnelsen av 1999 klarte en samling av over 100 000 PC'er og en spesiell DES "kode knekker" å finne en 56 bits nøkkel på under 22 timer. Nå er det ikke mange som har slike ressurser, men det vil være naivt å tro at ingen har det.

I dag regnes 128 bits nøkler i symmetriske systemer for å være tilstrekkelig. Det vil si at tiden det tar for å finne nøkkelen er *veldig* lang, selv med datakraft som blir tilgjengelig langt inn i fremtiden.

2.2.2 Amerikanske eksportregler

Den 14. januar 2000 annonserte Amerikanske myndigheter at eksportrestriksjonen av såkalt "Strong encryption" var opphevet. "Strong encryption" betegner nøkkellengder på 128 bit og lengre. Siden denne loven omfatter de fleste produsenter av programvare (også Microsoft) påvirker det svært mange internasjonale kunder. Tidligere har kryptografiske systemer med nøkkellengder på kun 40 og 56 bit vært tilgjengelig for internasjonale brukere.

2.3 Asymmetriske systemer

I et asymmetrisk system opereres det med to forskjellige nøkler. Det er her så stor forskjell mellom krypterings- og dekrypteringsprosessen at de ikke kan avledes fra hverandre. Det betyr at den ene prosessen godt kan være kjent uten at det svekker systemets sikkerhet. Systemet kalles ofte et offentlig-nøkkel system siden den ene nøkkelen kan være offentlig kjent.

I asymmetriske systemer oppnås hemmeligholding og autentitet gjennom forskjellen mellom de to prosessene. En oversending av en kryptert melding fra bruker A til B skjer på følgende måte. Bruker A fremskaffer bruker B sin offentlige nøkkel, og krypterer meldingen med denne. Deretter krypterer han den resulterende sifferteksten med sin egen private nøkkel, og sender resultatet til bruker B. Bruker B fremskaffer bruker A sin offentlige nøkkel, og dekrypterer meldingen. Så dekrypterer han resultatet med sin egen private nøkkel, og får klartekst meldingen. Dermed er hemmeligholding og autentitet oppnådd.

Hvis en melding dekrypteres med en bruker A sin offentlige nøkkel kan den kun være kryptert med bruker A sin private nøkkel. Siden det bare er bruker A som innehar denne nøkkelen er meldingen garantert kryptert av bruker A.

De spesielle egenskapene til offentlig-nøkkel systemene gir dem et bredt bruksområde. Foruten meldingsoverføring brukes ofte offentlig-nøkkel systemer til digitale signaturer og autentisering.

2.3.1 Digitale signaturer

En digital signatur er den elektroniske varianten av en skriftlig signatur. Den er et privat eierprivilegium som en bruker benytter til undertegning og dermed garantere sin delaktighet i en sak. En signatur må ha noen karakteristiske egenskaper:

- En motpart må kunne bekrefte at det virkelig er den oppgitte partens signatur.
- Det må ikke være mulig for noen å forfalske signaturen.
- En signatur må være juridisk bindende.

En digital signatur garanterer derfor at en bruker er den han utgir seg for å være.

Offentlig-nøkkel systemer muliggjør slike digitale signaturer. Når en bruker B mottar en melding med en bruker A sin digitale signatur, kan bruker B være helt sikker på at riktig bruker har signert meldingen siden kun bruker A innehar den private nøkkelen som genererer signaturen.

Digitale signaturer kan også genereres av symmetriske systemer, men det forutsetter en nøytral tredjepart som har begge brukernes hemmelige nøkler.

2.3.2 Autentisering

Autentisering er ofte et like stort problem som hemmeligholding, og noen ganger er man kun avhengig av en av delene. Autentisering baserer seg på digitale signaturer slik at en bruker signerer en melding med sin private nøkkel for å bevise sin identitet.

Til autentisering brukes ofte offentlig-nøkkel systemer sammen med digitale sertifikater. Digitale sertifikater er utstedt av en nøytral tredjepart, og binder en brukers identitet sammen med en offentlig nøkkel.

Asymmetriske systemer er mye tregere krypteringsmekanismer enn symmetriske systemer, og derfor anvendes de sjelden til kryptering av store datamengder. Systemets gode egenskaper til å autentisere to parter gjør at man ofte kombinerer symmetriske og asymmetriske systemer ved meldingsoverføring. Partene autentiserer seg ovenfor hverandre med et offentlig-nøkkel system, for deretter å overfører hemmelige nøkler for resten av kommunikasjonen.

Det er mange offentlig nøkkelsystemer i bruk, og de vanligste er RSA, DSS, DSA og Diffie Hellman.

2.3.3 RSA

RSA er kanskje det mest kjente offentlig-nøkkel systemet, og er utviklet av Rivest, Shamir og Adleman ved MIT. Som alle offentlig-nøkkel systemer baserer også RSA seg på de regnetekniske vanskeligheter som vi i dag mener eksisterer ved bestemmelse av faktorer i enormt lange og mangesifrede tall (100-150 sifre).

Et offentlig nøkkelsystems styrke baseres også på nøkkellengde, og vanlige nøkkellengder for et RSA system er fra 512, 1024 og 2048 bit. Lengere nøkkellengder er også i bruk. Grovt sett kan man si at en 64 bit lang symmetrisk nøkkel tilsvarer en 512 bit lang asymmetrisk nøkkel i styrke. En symetrisk nøkkel på 128 bit tilsvarer en asymmetrisk nøkkel på 2300 bit.

2.4 Message Digest / Hashing

Message Digest eller Hashing funksjoner benyttes når store mengder data skal signeres digitalt. Denne typen funksjoner komprimerer data på en sikker måte slik at det dannes en slags sjekksum på en fast lengde, f.eks. 128 bit. Algoritmen er ikke reversibel, og er distinkt for forskjellige data slik at det er svært liten sannsynlighet for at ulike data har samme hash verdi.

Ved signering av f.eks. en stor melding beregnes det ofte en hash verdi som signeres. Grunnen til dette er at det ofte benyttes asymmetriske systemer ved digital signatur, som ytelsesmessig ikke er egnet for store datamengder.

Vanlige hash algoritmer er SHA-1, MD4 og MD5.

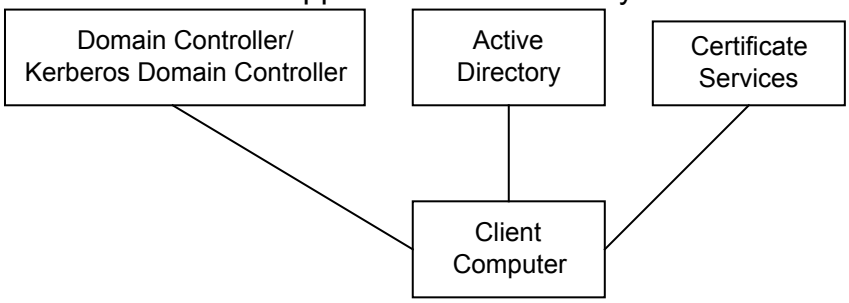
3 Sikkerhetsmekanismer i Windows 2000

Dette kapittelet behandler individuelle sikkerhetsmekanismer som benyttes i Windows 2000. Kapittelet tar også for seg sikkerhetsmekanismer som ikke er direkte bundet til operativsystemets primærfunksjoner, men anvender seg av smartkortstøtten som tilbys.

3.1 Public Key Infrastructure

I Windows 2000 har Microsoft integrert et offentlig nøkkelsystem som de kaller Public Key Infrastucture (PKI). PKI danner den grunnleggende strukturen for sikkerhetsmekanismene i Windows 2000.

PKI består av tre hoveddeler (figur 3-1): Active Directory katalogtjeneste, Kerberos autentiseringstjeneste og en sertifikattjeneste. Sistnevnte utsteder et sertifikat til brukeren basert på opplysninger i Active Directory. Ved pålogging til Windows 2000 kontrollerer Kerberos sertifikatet opp mot Active Directory.



Figur 3-1 Elementene i Public Key Infrastructure

Foruten autentisering på et lokalt nettverk, kan sertifikatet brukes til signering og kryptering av e-post (S/MIME) og til sikker kommunikasjon over Internett med SSL og TLS. Den siste tjenesten PKI tilbyr er kryptering av filer. Encrypting File System (EFS) krypterer filer et hemmelig nøkkel kryptosystem, og krypterer alle filenes nøkler med brukerens offentlige nøkkel.

3.1.1 Egenskaper

PKI er som de fleste sikkerhetsmekanismene til Microsoft, bygget på CryptoAPI. Dette betyr et standard grensesnitt for applikasjoner og tjenester som benytter seg av kryptografiske funksjoner. Det vil si at man kan velge mellom en rekke forskjellige kryptoalgoritmer og nøkkellengder. I stedet for at de kryptografiske operasjonene utføres i programvare, kan man også velge maskinvarebaserte løsninger. Et smartkort er et eksempel fra sistnevnte kategori.

CryptoAPI støtter også gjenvinning av nøkler. Siden dette kun er aktuelt der kryptert data skal ”leve” over lengre tid, er dette bare tilgjengelig for kryptert e-post og EFS filkrypteringssystem. Det skal legges til at det er svært risikabelt å lagre slike nøkler, og hvis det skal gjøres bør nøklene eksporteres til et transportabelt media og lagres i en safe eller et annet fysisk sikret sted.

For at PKI systemet skal være brukervennlig, må alle tjenester være tilgjengelig for en bruker over alt i nettverket. I PKI oppnås dette på to måter: Enten ved at Active Directory sørger for at sertifikat og nøkler er tilgjengelige ved pålogging, eller ved hjelp av et smartkort. Ved bruk av smartkort i Windows 2000 lagres et sertifikat med et nøkkelpar på kortet. Brukeren tar da fysisk med seg sertifikatet mellom de forskjellige stedene.

3.1.2 Standarder

Da flere av de PKI baserte mekanismene er beregnet for nettverk, er det viktig at de er mest mulig standardiserte. Microsoft har valgt å følge Internet Engineering Task Force (IETF) sin PKIX standard, som baserer seg på X.509 sertifikater. S/MIME og SSL/TLS er innarbeidede standarder som fungerer bra mellom produkter fra forskjellige produsenter. Microsoft sin implementasjon av Kerberos er utviklet for å kunne brukes sammen med offentlige nøkler og sertifikater, men er fortsatt kompatibel med IETF standarden. De komponenter som kommer i kontakt med omverdenen må derfor sies å være lagt til rette for interoperabilitet utover Windows 2000 og Microsoft sine produkter.

Siden offentlig nøkkelsystemer er egnet til signering av data, kan det også anvendes til signering av kode og signering av ”web-forms”. Dette er foreløpig ikke implementert i Windows 2000 PKI. Grunnen til dette er at det ikke er en innarbeidet standard for dette, som kan bety kompatibilitetsproblemer og at slike funksjonene dermed ikke har noen hensikt ennå.

3.1.3 Vurdering

Når Microsoft implementerer PKI i Windows 2000 er det for å best kunne tilfredsstille kunders behov for integrering utover egne nettverk, og kommunikasjon over åpne, usikrede nettverk som Internett. PKI muliggjør også en helhetlig sikkerhetspolitikk, med Active Directory som knutepunkt.

Praksisen med at hver bruker skal ha sitt personlige digitale sertifikat, er også et skritt fremover for digital kommunikasjon og digitale dokumenter. Etter hvert som vi går over til Internett banker og bort fra papirdokumenter, kan digitale sertifikater bli vår identifikasjon, og digitale signaturer bli vår underskrift.

3.2 Kerberos v5

Kerberos ble utviklet ved MIT (Massachusetts Institute of Technology) mot midten av 80-tallet, i et prosjekt ved navn Athena. Prosjektet var et samarbeid med bla. Digital Equipment Corporation og IBM. Hensikten med prosjektet var å konstruere et system for autentisering mellom entiteter i store distribuerte systemer. Kerberos ble første gang tatt i bruk i universitetsnettverket ved MIT, da i versjon 4.

Navnet Kerberos stammer fra Gresk mytologi, der Kerberos var den 3-hodede hunden som voktet inngangen til Hades. Hovedintensjonen med Kerberos er å sikre at en entitet som ønsker tilgang til en tjeneste i et nettverk blir autentisert korrekt og fullstendig, dvs. at entiteten virkelig er den han gir seg ut for å være. Dette oppnås ved å utveksle informasjon med autentiseringssystemet der det antas at

kommunikasjonen skjer over et usikret nettverk, og standard krypteringsmekanisme som benyttes er DES.

3.2.1 Kerberos protokollen

Når en entitet for første gang ønsker tilgang til en tjeneste må den autentiseres. Dette oppnås ved at informasjon om entiteten og eventuelle attributter krypteres med klientens hemmelige nøkkel og oversendes til Kerberos. Denne hemmelige nøkkelen er kjent av Kerberos, og er vanligvis basert på et passord. Etter å ha autentisert entiteten korrekt, sender Kerberos en billett som gir tilgang til den ønskede tjenesten, et par sesjonsnøkler for kryptering av informasjon som skal utveksles med tjenesten, samt et autentiseringsbevis som senere kan brukes til å motta nye billetter til andre tjenester. Denne informasjonen er også kryptert med entitetens nøkkel. Billetten som mottas inneholder informasjon om entiteten, og er kryptert med den ønskede tjenestens nøkkel, slik at det på denne måten garanteres at entiteten er korrekt autentisert. Kerberos autentiserer både brukere og tjenester.

Kerberos består av to deler; en autentiserings tjeneste og en billettutsteder. Autentiseringsdelen er kun i bruk når en entitet skal autentiseres, noe som skjer ved første gangs bruk, og så igjen etter en bestemt tid. Dette kan for eksempel skje ved arbeidsdagens begynnelse. Billettutstederen er i bruk hver gang en entitet ønsker tilgang til en tjeneste.

Når en entitet ønsker tilgang til en ny tjeneste og allerede er autentisert, sender den en forespørsel til Kerberos' billettutsteder. Forespørselen inneholder informasjon om ønsket tjeneste, det tidligere mottatte autentiseringsbeviset og den gamle billetten. Også denne gangen er informasjonen kryptert med entitetens nøkkel. Billettutstederen utsteder en ny billett til den ønskede tjeneste på bakgrunn av autentiseringsbeviset. Autentiseringsbeviset blir også endret, da det inneholder et tidsstempel som gjør at det kun er gyldig hos tjenesten en viss periode etter det er utstedet. Dette gjøres for å hindre misbruk. Som nevnt over blir det også utstedet en sesjonsnøkkel for kommunikasjon med den ønskede tjenesten.

3.2.2 Kerberos i Windows 2000

Implementasjonen av Kerberos i Windows 2000 skiller seg litt fra en standard versjon 5 implementasjon. Den største forskjellen Microsoft har lagt inn er muligheter til å benytte et offentlig-nøkkel system i stedet for et symmetrisk-nøkkel system. Dette er hovedsakelig gjort for å integrere Kerberos med andre offentlig nøkkel tjenester i Windows 2000, blant annet interaktiv logon ved hjelp av smartkort. Disse forandringer er basert på et forslag inn til høring i IETF (Public Key Cryptography for Initial Authentication in Kerberos).

Som det går frem av avsnittet ovenfor, er Kerberos systemet delt opp i en autentiseringstjeneste og en billettutsteder. I Windows 2000 er disse tjenestene en del av "Key Distribution Center" (KDC), og kjøres som en domene-tjeneste på domene-servere i nettverket.

Kerberos systemet kjenner alle klientenes nøkler, og disse er lagret sammen med annen brukerinformasjon i Active Directory. I Kerberos systemet genereres det også sesjonsnøkler og autentiseringsbevis. Hos klienten lagres disse i RAM så lenge de er

i bruk, og når klienten logger av nettverket tømmes denne delen av RAM. Dette utføres av Kerberos systemet etter beskjed fra den lokale sikkerhets autoritet (LSA). LSA er en tjeneste som kjøres på klientmaskinen sammen med Kerberos. Denne oppbevarer også brukerens passord når han er pålogget, i tilfelle tidsstempelet i autentiseringsbeviset skulle utgå. På denne måten kan LSA gi beskjed til Kerberos om å utstede et nytt bevis uten å måtte spørre brukeren om passordet på nytt.

3.2.3 Vurdering

Kerberos systemet har oppnådd mye oppmerksomhet i fagkretser, noe som hovedsakelig kan tilskrives store og viktige deltakere i prosjektet. I praksis har systemet vist seg effektivt og sikkert, men kritikken har hovedsakelig kommet på følgende 3 punkter:

1. En billett som brukes ved autentisering overføres kryptert med klientens nøkkel. Denne nøkkelen er generert med en enveis funksjon basert på brukerens passord, og sikkerheten er derfor avhengig av at brukere kan velge gode nøkler. Kjente navn og ord som passord kan lett finnes vha. søk med ordbok.
2. En klient kan motta en ubegrenset mengde billetter som alle er kodet med samme (klientens) nøkkel. Dette gjør det lettere for eventuelle fiender å finne nøkkelen.
3. Kerberos systemet gir ingen retningslinjer for bruk av klientmaskiner. Dermed kan f.eks. en Trojansk hest snappe opp passord og annen informasjon for misbruk.

I Windows 2000 sin implementasjon av Kerberos er som kjent utvidet for bruk med offentlig nøkkel system. Dette muliggjør også bruk av loggon med smartkort, som eliminerer menneskelig valgt passord som nøkkel. Punkt tre gjelder mer klientmaskinen enn protokollen, men er et kriterium Windows 2000 oppfyller. <Ctrl+Alt+Del> logon sekvensen aktiverer nemlig flere mekanismer som skal oppdage og ”forbikoble” eventuelle trojanske hester.

3.3 Active Directory

Active Directory er Microsofts versjon av en katalogtjeneste. En katalogtjeneste har ofte mange oppgaver, men hovedfunksjonen er å tilordne informasjon til entiteter. Et typisk anvendelsesområde for en katalogtjeneste som Active Directory er å holde orden på brukere i en organisasjons datanettverk. Katalogtjenesten kan da modellere organisasjonsstrukturen, noe som forenkler administrering av nettverket. Informasjonen som lagres for hver bruker (entitet) er typisk personopplysninger, brukerrettigheter, avdeling og sikkerhetsopplysninger. Active Directory er lokasjonstransparent.

3.3.1 Active Directory og sikkerhetsmekanismer i Windows 2000

Sikkerhetsaspektet ved Active Directory er å holde orden på sikkerhetsopplysninger om brukerne i domenet/nettverket. Det vil si at Active Directory har tatt over oppgaven som bla. Security Account Manager hadde i NT 4.0. Det er hovedsakelig to sikkerhetsmekanismer som er direkte knyttet opp mot Active Directory:

- Kerberos v5

- Certificate Server 2.0

Siden alle brukere i et nettverk har sin egen konto, og denne er registrert og administrert i Active Directory, vil man ved pålogging bli sjekket opp mot en slik konto. I Windows 2000 utføres denne funksjonen av Kerberos protokollen, og denne utsteder autentiseringsbevis på bakgrunn av informasjon den får fra Active Directory.

Som en del av PKI i Windows 2000 bruker mange av sikkerhetsmekanismene digitale sertifikat. Et slikt sertifikat utstedes til en entitet, og er et bevis for riktig identitet. I Windows 2000 er det en egen tjeneste som utsteder sertifikater, Microsoft Certificate Server. Denne utsteder X.509v3 sertifikater på bakgrunn av opplysninger om entiteten i Active Directory.

Active Directory er også integrert med Internet Information Server i Windows 2000. Dermed kan web- og filtjenester for alle brukere administreres på samme måte som for et LAN. En slik funksjon gjør det enklere og sikrere å gi bestemte brukere/-grupper utvidet tilgang til f.eks. spesielle web-sider.

3.4 X.509 v3

Internett er et distribuert system der det kan være vanskelig å fastslå identiteten til en kommunikasjonspartner. Det eksisterer heller ikke en fast fysisk forbindelse mellom partene, og dermed er muligheten god for å avlytte og manipulere meldinger. X.509 er et digitalt sertifikat som har til hensikt å garantere brukerens identitet ovenfor kommunikasjons partneren.

X.509 stammer fra X.500 katalogtjenesten som ble utviklet av IBM. Dette er en slags database der f.eks. en brukere er lagret hierarkisk og gjerne etter organisasjonsstrukturen i organisasjonen. Herfra stammer også navnegivningen, som derfor er tilpasset en kompleks, hierarkisk struktur med unike navn.

3.4.1 Prinsippet for digitale sertifikat

Et X.509 digitalt sertifikat anvendes sammen med et offentlig-nøkkel system. Digitale sertifikater utnytter egenskapen til slike systemer som gjør at data kryptert med en privat nøkkel kun kan dekrypteres med den korresponderende offentlige nøkkelen, og omvendt. For at et slikt system skal kunne brukes mellom to ukjente parter, må det være en tredje part i mellom som garanterer for en entitets identitet og binder denne til en bestemt offentlige nøkkel. Forholdet mellom de to ukjente partene går da gjennom en såkalt ”trusted third part”, som er sertifikatutstederen. Bindingen mellom hver entitet og den offentlige nøkkel garanteres således med en signatur av sertifikatet, generert med billettutstederens private nøkkel. Hovedfeltene i sertifikatet er entitetens unike navn, informasjon om entitetens offentlige nøkkel, sertifiseringsautoritetens unike navn og dennes digitale signatur av sertifikatet.

Når en entitet mottar et sertifikat kontrolleres det mot en liste over aksepterte sertifikater. Et sertifikat aksepteres hvis entiteten stoler på sertifikatets utsteder, hvis det ikke har gått ut på dato, ikke blitt inndratt og hvis sertifikatets signatur fra utstederen er gyldig. Signaturen kontrolleres med utstederens offentlige nøkkel, som entiteten innehar for sine aksepterte sertifikater.

Et sertifikat er også utstedt til forskjellige formål. Det kan være autentisering av en entitet, kryptering av e-post, signering av programvare osv. Foruten ”trust” forholdet som entiteten har til utstederen, må også sertifikatet være utstedt til formålet det anvendes til. Hvis det ikke er samsvar her, vil ikke sertifikatet automatisk bli akseptert.

En viktig egenskap for X.509 er en liste over sertifikater som er inndratt (Certificate Revocation List). Hver sertifikatutsteder har en slik liste, der ugyldige sertifikater blir oppført. Grunnen til at et sertifikat havner på denne lista kan være misbruk eller at eieren ikke lenger eksisterer.

3.4.2 Bruksområder

Digitale sertifikater har etterhvert fått et bredt bruksområde, og hovedsakelig på Internett. Her er det hovedsakelig SSL som benytter sertifikater for autentisering av server og klient, og S/MIME for kryptering og digital signatur av e-post. Digital signatur av programvare er også begynt å bli vanlig, og spesielt ved nedlasting og installering av ”plugins” for web-klienter. Etterhvert vil nok signering av ”web-forms” også bli vanligere.

I Windows 2000 er bruken av digitale sertifikat utvidet gjennom PKI. Det vil si at de PKI relatere sikkerhetsmekanismene er basert på X.509v3 sertifikater og et offentlig nøkkel kryptosystem.

3.4.3 Sertifikater / X.509 v3 i Windows 2000

I Windows 2000 PKI benyttes sertifikater til autentisering av entiteter, både personer og tjenester. For eksempel må sertifikat tjenesten ha et spesielt sertifikat for å kunne utstede sertifikat til andre. Sertifikat tjenesten, MS Certificate Server 2.0, utsteder sertifikater på bakgrunn av brukerkontoer i Active Directory. Mange tjenester har også slike kontoer. Sertifikat tjenesten kan også utstede sertifikater som ikke er basert på Active Directory kontoer.

Flere forskjellige typer sertifikat er tilgjengelige for brukere, avhengig av bruksområde. De fleste personlige sertifikat er beregnet for interaktiv login, sikker kommunikasjon over Internett og kryptering og signering av e-post. Foruten disse funksjonene er også Encrypting File System (EFS) en mulighet. Sertifikat for smartkort, Smart Card User, inneholder ikke funksjonalitet for EFS (vedlegg D).

Tjenestene som anvender sertifikat i Windows 2000, er naturlig nok de samme som nevnt under Public Key Infrastructure (PKI).

3.4.4 Vurdering

Digitale sertifikat brukes i dag hovedsakelig på Internett. Grunnen til dette er at SSL bruker disse til autentisering av tjenere. Nå som bruken av banktjenester på Internett og e-handelen øker, tyder det på at digitale sertifikater er i ferd med å bli etablerte. Som med så mange mekanismer på Internett, er det også viktig med standardisering av sertifikater.

Slik som Internett er bygd opp, er det ingen kontroll av tjenestene som tilbys. Slik er det også med sertifikater. Sertifikatutstedere er kommersielle firmaer som er selvoppnevnte. Det vil si at det ikke er noe overordnet, uavhengig kontrollorgan som kontrollerer disse firmaenes virksomhet. Et sertifikat utstedes basert på opplysninger klienten selv gir, og for utstederen er det vanskelig å kontrollere disse. Dette er paradoksalt med tanke på den graden av tiltro som tillegges sertifikattjenester.

I Windows 2000 har man mulighet til å utstede sertifikater lokalt. Dette er en enkel metode for å gi alle brukerne personlige sertifikater. Slike sertifikater kan selvfølgelig benyttes i nettverkets tjenester, men når man beveger seg utenfor organisasjonens nettverk, kan man får problemer med sertifikatet. Sertifikatet er jo utstedt av organisasjonens egen tjeneste, som det er lite sannsynlig at entiteter utenfor organisasjonen har et ”trust” forhold til. Her kommer problemet med mange sertifikatutstedere og mangel på et organisert forhold mellom dem. Hvis to parter f.eks. skal kunne benytte seg av S/MIME til e-post er dette et problem.

Et annet problem med mangelen på et organisert forhold mellom sertifikatutstederne er navnerommet. Digitale sertifikat fordrer unike navn på entitetene, men det er ingenting som forhindrer to utstedere i å utstede sertifikater til to forskjellige entiteter med like navn. Begge sertifikatene vil i dette tilfellet være gyldige.

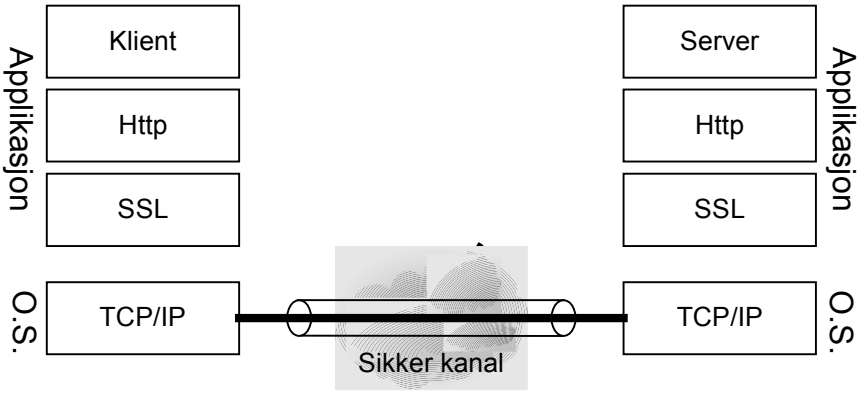
Etterhvert som elektroniske dokumenter tar over for papir dokumenter vil digitale signaturer bli likestilt med skriftlige signaturer. Digitale signaturer er langt vanskeligere å forfalske enn skriftlige, men som nevnt ovenfor er dette foreløpig ikke et feilfritt system.

3.5 Secure Socket Layer (SSLv3)

SSL ble utviklet av Netscape for å gi sikker kommunikasjon over Internett. I utgangspunktet var dette er proprietær løsning for Netscape sine Internett klienter og tjenere, men den ble senere sendt inn til IETF som et forslag til en standard sikkerhetsprotokoll på nettverk. SSL har nå kommet opp i versjon 3, men er ennå ikke selv blitt en offisiell Internett standard. TLS protokollen er derimot blitt en Internett standard, og bygger på og er veldig lik SSL. SSL er i utstrakt bruk på Internett, og støttes av de aller fleste web-klienter og -tjenere.

3.5.1 SSL Protokollen

Selv om SSL ble utviklet for typiske web-klienter og –tjenere, har den etterhvert blitt utviklet for sikring av all kommunikasjon over TCP/IP nettverk. I Internett stakken ligger SSL protokollen mellom applikasjonslaget og transportlaget (figur 3-2).

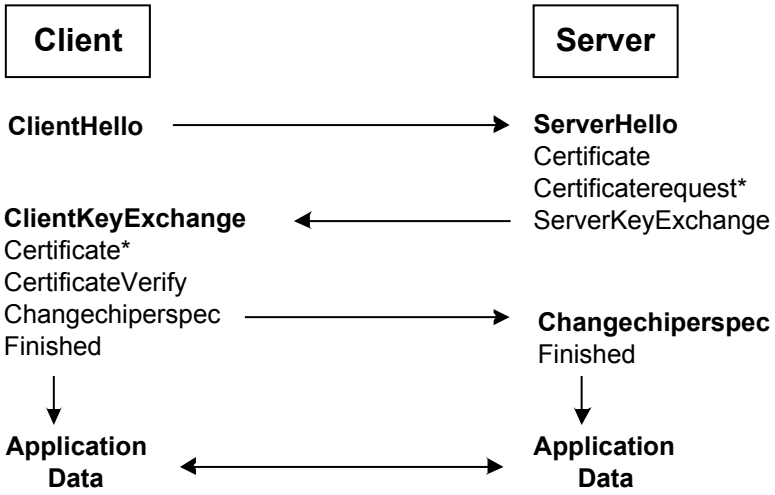


Figur 3-2 SSL protokollen

3.5.2 Virkemåte

SSL anvender seg av en kombinasjon av hemmelig- og offentlig nøkkel krypteringssystem sammen med X.509 digitale sertifikater. SSL autentiserer kan autentisere tjener og klient ovenfor hverandre og forhandle frem en hemmelig nøkkel for kryptering av oversendt data.

En klient som ønsker å utveksle data med en tjener sender en melding med opplysninger om SSL versjon, kryptografiske innstillinger, vilkårlig generert data og annen nødvendig informasjon til tjeneren. Tjeneren svarer med det samme, men sender også med sitt digitale sertifikat. Hvis påkrevet kan tjeneren kreve et sertifikat fra klienten. Ved hjelp av tjenerens svar kontrollerer klienten at sertifikatet er gyldig og utstedt av en kilde den stoler på (”trusted third part”). Ved hjelp av all data som til nå er generert lager klienten en meldingsom den krypterer med tjenerens offentlige nøkkel. Den krypterte meldingen sendes til tjeneren der den dekrypteres. Både klienten og tjeneren lager en ny melding ut i fra denne, og genererer sesjonsnøklene. Disse skal brukes til kryptering av data mellom partene, og til å verifisere dataenes integritet så lenge sesjonen pågår. Klient og tjener sender nå begge en melding om at meldinger fra nå vil være kryptert. SSL forbindelsen er nå klar til bruk.



Figur 3-3 Oppkopling med SSL Handshake

SSL kan benytte flere forskjellige krypteringsalgoritmer. De vanligste er DES, triple DES, RC2 eller RC4 for kryptering og SHA-1 eller MD5 generering av hash.

3.5.3 Bruksområde

SSL er som nevnt utviklet med tanke på sikker kommunikasjon mellom to (ukjente) parter over et usikret nettverk, slik som Internett. Anvendelsesområdet er naturlig nok Internett, der de fleste nettbanker og online butikker benytter seg av SSL.

SSL er en etablert standard de fleste web-klienter og –tjenere har implementert. At systemet fungerer mellom produkter fra forskjellige leverandører har også medvirket til protokollens popularitet.

3.5.4 SSL i Windows 2000

SSL er implementert i to Microsoft applikasjoner: Internet Information Server og Internet Explorer. SSL er også en del av Windows 2000 Public Key Infrastructure. Tjenere benytter seg av SSL må inneha et sertifikat, mens klienter kan bruke personlige sertifikat hvis klientautentisering er nødvendig. Smartkort kan benyttes sammen med klientautentisering i SSL.

3.5.5 Vurdering

SSL 3.0 regnes for en velutviklet og sikker protokoll. SSL benytter seg av en såkalt ”master secret” som sesjonsnøklene genereres ut i fra. Det benyttes forskjellige nøkler i hver retning under kommunikasjonen, og disse fornyes flere ganger under oppkoplingstiden. SSL 3.0 autentiserer også hver TCP/IP pakke med en 128 bit MAC. Både passive og aktive angrep på en ferdig oppkoplet SSL forbindelse vanskeliggjøres av dette.

Oppkoblingens prosedyren i SSL er relativt kompleks. Her er det enkelte situasjoner hvor informasjon om oppkoplingen sendes ukryptert. Dette er informasjon som gjennom aktive angrep i spesielle tilfeller kan brukes til å sabotere og/eller manipulere kommunikasjonen. Disse usikkerhetene stammer fra SSL 3.0 dokumentasjonen, men det er fult mulig at noen implementasjoner av SSL 3.0 er så robuste at de ikke lar seg lure.

På grunn av protokollens kompleksitet, oppdages det av og til nye feil i protokollen. Disse relateres gjerne til oppkoplingsprotokollen, mens transport delen av protokollen regnes for å være svært sikker, avhengig av nøkkellengden som benyttes.

3.6 Transport Layer Security (TLS)

At SSL aldri ble en offisiell Internett standard er ikke helt sant. I IETF utarbeides det Internett standarder ut i fra utkast, som vurderes av alle interesserte parter over lang tid, og blir kanskje en standard til slutt. SSL ble sendt inn som et utkast, og ble til slutt en Internett standard gjennom TLS (RFC2246). Når dette ble en IETF Internett standard var allerede SSL den etablerte standarden på Internett, og lever derfor side om side med TLS.

3.6.1 Endringer i forhold til SSL

Siden TLS er helt og holdent basert på SSL er det ikke mye som skiller i mellom dem. SSL svakeste ledd er autentisering, og TLS styrker blant annet denne delen. I tillegg er sertifikatbehandling og varsling om feil også forbedret. I fremtiden vil TLS støtte autentisering med Kerberos og elliptisk kurve kryptografi som et alternativ til RSA.

3.6.2 Bruksområder

TLS har ennå ikke tatt over for SSL i web-klienter, og er heller ikke særlig etablert standard. Et vanlig bruksområde er sikker kommunikasjon over nettverk i forbindelse med andre protokoller.

Extensible Authentication Protocol (EAP) er beregnet for autentisering mot Windows 2000 over Punkt-til-punkt protokollen (PPP). EAP lar tredjeparts sikkerhetsmoduler samvirke med Remote Access Service (RAS) i Windows 2000. Sammen med TLS kan EAP autentisere med digitale sertifikat, og også digitale sertifikat på smartkort.

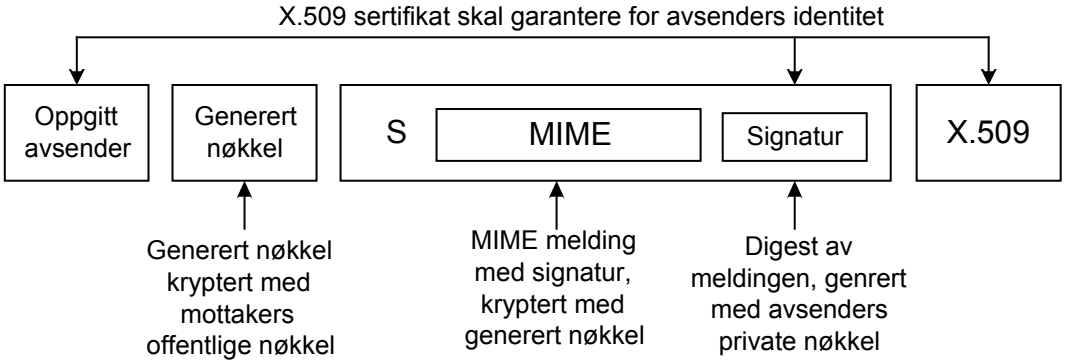
3.7 Secure Multipurpose Internet Mail Extensions (S/MIME v3)

Secure MIME (S/MIME) bygger på den etablerte Internett standarden Multipurpose Internet Mail Extensions (MIME). Dette formatet tillater bla. bruk av grafikk og lyd i e-post. S/MIME er en protokoll som legger til en digital signatur og krypterer innholdet i et slikt MIME format. Dette betyr at S/MIME ikke bare kan benyttes til e-post, men også annen data som html, grafikk, lyd osv.

Formålet med S/MIME formatet på e-post er å sikre autentisering, meldingintegritet og mot innsyn fra uvedkommende. Dette oppnås med bruk av et X.509 sertifikat og et offentlig nøkkel kryptosystem.

3.7.1 Protokollen

Fremgangsmåten som benyttes under sending og mottak av S/MIME e-post er som følger.



Figur 3-4 Meldingsformat i S/MIME

Senderen fremskaffer først mottakerens offentlige nøkkel. Denne får han ved å rekvirere mottakerens digitale sertifikat. Bruk av S/MIME forutsetter at begge parter har gyldige personlige sertifikater, med et ”thrust” forhold til de respektive

sertifikatutstederne. Avsenderen genererer en ny nøkkel som benyttes til kryptering av MIME meldingen. Denne nøkkelen må dermed også sendes til mottakeren, og krypteres derfor med mottakerens offentlige nøkkel før den sendes. Dette betyr at kun eieren av sertifikatet, altså mottakeren, kan dekryptere den genererte nøkkelen.

S/MIME anvender også såkalt digital signatur for å sikre meldingsintegritet. MIME meldingen kjøres gjennom en hash algoritme med den genererte nøkkelen og en digest/sjekksum fremkommer. Denne digest'en krypteres deretter med senderens private nøkkel, og sendes med meldingen sammen med avsenders digitale sertifikat.

Når en S/MIME melding mottas dekrypterer mottakeren den genererte nøkkelen med sin private nøkkel. Den genererte nøkkelen brukes deretter til å dekryptere innholdet i meldingen til klartekst. For å kontrollere at meldingen virkelig kom fra den oppgitte avsenderen dekrypterer mottakeren digest'en fra meldingen med avsenderens offentlige nøkkel. Så beregner mottakeren sin egen digest med den tidligere mottatte genererte nøkkelen. Stemmer den mottatte digest'en og den selv-utregnede overens, er meldingens integritet intakt og stammer fra den oppgitte avsenderen.

S/MIME følger PKCS #7 standard for digital signering og kryptering. Dermed bygger den på en etablert standard, som er en medvirkende årsaken til den relativt høye populariteten. S/MIME kan benytte flere kryptoalgoritmer, og de vanligste er DES, triple DES eller RC2 for kryptering og SHA-1 eller MD5 for autentisering.

3.7.2 S/MIME i Windows 2000

S/MIME brukes i sammenheng med e-post klienter og tjenere. Disse er ikke en del av Windows 2000, og leveres av en rekke forskjellige produsenter. Microsoft leverer Exchange Server, Outlook og Outlook Express som kan bruke S/MIME.

Windows 2000 Server leveres med en sertifikat tjeneste, Certificate server, som kan utstede X.509v3 sertifikater for bruk sammen med S/MIME.

3.7.3 Vurdering

I likhet med SSL regnes S/MIME for å være en relativt sikker protokoll, men også her dukker det av og til opp små problemer. Forhandling og utveksling av nøkler har vært hoved problemet til S/MIME. I tidlige versjoner falt partene ofte ned på laveste nivå av sikkerhetsmekanismer, som begrenset seg til 40 bits nøkkellengder.

I den senere tid har det også vært svaketer ved angrep på S/MIME meldinger som bruker Diffie-Helleman Key Agreement Method for generering og utveksling av hemmelige nøkler. Disse problemene er tatt opp i en egen IETF rfc (rfc2785, Methods for Avoiding the "Small-Subgroup" Attacks on the Diffie-Helleman Key Agreement Method for S/MIME).

Et annet problem med S/MIME er liten utbredelse av digitale sertifikater. For å bruke S/MIME må som kjent begge parter ha personlige sertifikater. Svært få har dette, og selv om en organisasjon utsteder sertifikater til sine ansatte/medlemmer, mangler sannsynligvis det nødvendige "thrust" forholdet utenfor organisasjonen.

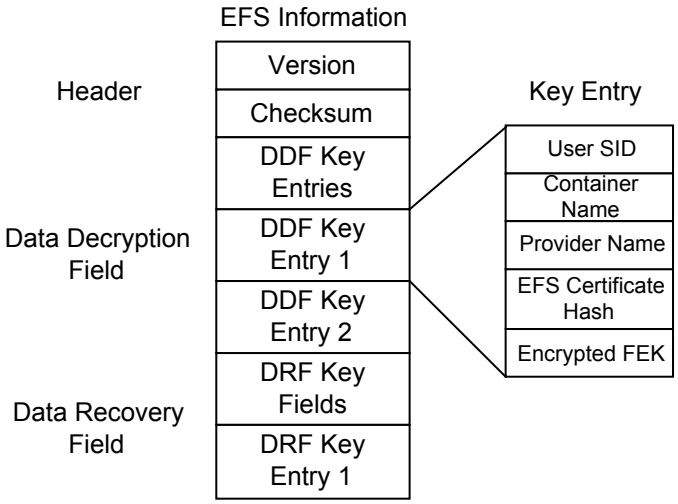
3.8 Encrypting File System (EFS)

Windows 2000 kommer med et eget system for å sikre filer og kataloger som er lagret på harddisk. Formålet med en slik sikring, ved hjelp av kryptering, er å hindre at uvedkommende får tilgang til den lagrede informasjonen. En slik funksjon er mest interessant der tilgang til maskinen ikke er fysisk sikret, for eksempel en bærbar PC. Filkryptering er en del av operativsystemet, og deler av programkoden kjøres i beskyttet modus i operativsystemkjernen. Dette sikrer høyere sikkerhet en i tredjeparts løsninger. Sømløshet er også viktig i denne sammenheng. En bruker med riktig nøkkel skal kunne bruke de krypterte filene på samme måte som ukrypterte filer. Operativsystemet har selvfølgelig også tilgang til krypterte filer.

3.8.1 Kryptering

Første gang man tar i bruk EFS blir systemet nødt til å fremskaffe brukerens private og offentlige nøkkel par. Dette paret må enten genereres eller fremskaffes fra brukerens sertifikat område, der operativsystemet lagrer nøkkelparene.

For å kryptere filer og kataloger i EFS benyttes det både hemmelig- og offentlig nøkkel krypteringssystemer. Når en bruker velger å kryptere en fil, genereres det et tilfeldig tall (128bit) som blir en hemmelig nøkkel til den krypterte filen. Denne nøkkelen kalles File Encryption Key (FEK), og krypteringsmekanismen som benyttes er en versjon av DES, kalt DESX. Hver fils FEK lagres sammen med filen, men kryptert med (brukerens) EFS' offentlig nøkkel gjennom en RSA krypteringsmekanisme.



Figur 3-5 Nøkkelfelt i en kryptert fil

3.8.2 Deling av filer

Et problem med krypterte data er når flere parter skal ha tilgang til samme informasjon. Å distribuere en felles hemmelig nøkkel til alle partene regnes for å være lite sikkert. EFS' offentlig nøkkel kryptering av filenes FEK løser dette problemet. Når en fil skal deles til flere brukere blir filens FEK kryptert med hver brukers offentlig nøkkel. For å kunne lese filen i klartekst må man være i besittelse av en av disse brukernes private nøkkel.

En slik samling av offentlige nøkler kalles en nøkkelring (key ring), og i tillegg til brukerenes ring, er det også en ring for gjenoppretting av data. Dette er spesielle brukere, såkalte recovery agenter , som kan trenge adgang til den krypterte informasjonen.

3.8.3 Dekryptering

For å lese innholdet i en kryptert fil eller katalog må brukeren fremskaffe filens FEK som kan dekryptere filen. Som nevn er filens FEK kryptert med brukerens offentlige nøkkel, og når EFS får beskjed om å dekryptere en fil med en gitt privat nøkkel vet den ikke hvilken FEK som har den korresponderende nøkkelen. Det vil si at EFS søkker gjennom de to nøkleringene, Data Decryption Field (DDF) og Data Recovery Field (DRF) for å finne riktig FEK. For hvert felt den søker i er det en sertifikat hash som sammenliknes med brukerens sertifikat. Stemmer sertifikatene overens er det riktige feltet funnet og dermed også det riktige nøkkel parret som dekrypterer filen.

3.8.4 Recovery Agent

Som en del av sikkerhetssystemene i Windows 2000 er det laget en mulighet for å spesielt utvalgte brukere i et domene skal kunne dekryptere filer i EFS. Dette er nødvendig hvis for eksempel en bruker slutter i organisasjonen, med viktig informasjon som kryptert med brukerens private nøkkel. Virkemåten for krypteringen er den samme som for en vanlig bruker, bortsett fra at brukeren legges inn i DRF-nøkkelringen. Denne brukeren kalles en recovery agent og er typisk en administrator i domenet. På samme måte som for vanlige brukere, har også recovery agenten et sertifikat som brukes til å finne filens FEK. I dette tilfellet gir sertifikatet tilgang til alle krypterte filer i hele domenet, og det er derfor viktig at dette sertifikatet lagres trygt. Microsoft anbefaler at recovery sertifikatet fjernes helt fra domene serveren og lagres på et fysisk sikret sted. På denne måten kan ingen som tilegner seg recovery agentens passord få tilgang til domenets krypterte filer.

3.8.5 Smartkort

Som nevnt er smartkort login en del av Microsofts Public key Infrastructure (PKI), noe Encrypting File System også er. PKI er også sterkt knyttet til smartkort, og deres evner til å håndtere offentlig nøkkel kryptosystemer isolert på kortet. Umiddelbart skulle man derfor tro at EFS og smartkort var knyttet sammen på den måten at brukerens sertifikat og nøkkel var lagret på smartkortet i stedet for på brukerens sertifikat-lagringsområde (eks. C:\Documents and Settings\<bruker>\Application Data\Microsoft\SystemCertificates\My\Certificates\<kryptert sertifikat>). Grunnen til at EFS ikke støtter smartkort skyldes begrensninger i smartkort. Med lite prosessorkraft og lav overføringskapasitet ville en slik løsning vært for treg til å nødvendig sømløshet. Et tregt system er heller ikke særlig brukervennlig.

3.8.6 Vurdering

Et krypterings system for filer lagret på en harddisk er i utgangspunktet ikke utsatt for samme risikoer som f.eks. systemer som skal fungere mellom to ukjente parter over et åpent nettverk. Måten EFS er integrert i operativsystemet skulle tilsi at det er svært vanskelig for en fiende å få tilgang til de krypterte filene i klartekst uten riktig nøkkel. I

EFS er det minst 2 par nøkler som kan dekryptere filene: brukerens og Recovery Agentens. Microsoft presiserer klart og tydelig at Recovery Agentens nøkkelfil må eksporteres bort fra maskinen med de krypterte dataene, og lagres på et fysisk sikret sted. Hvis dette er gjort er det bare brukerens private nøkkel som ligger igjen på maskinen på samme sted som brukerens sertifikat. Klarer man å fremskaffe denne nøkkelen kan man dekryptere filene. Brukerens private nøkkel er beskyttet av brukerens passord.

En annen mulighet er selvfølgelig et uttømmende søk i filene for å enten finne den enkelte filens symmetriske nøkkel, eller å finne brukerens private nøkkel.

3.9 Andre sikkerhetsmekanismer

Windows 2000 benytter seg også av en rekke andre sikkerhetsmekanismer. Siden oppgavens fokus er smartkort og Windows 2000, legger jeg ikke særlig stor vekt på de sikkerhetsmekanismene som ikke er forberedt for smartkort.

3.9.1 IP Security (IPSec)

Er en protokoll som beskytter IP-trafikk. Protokollen er utviklet av IETF for neste generasjons IP (versjon 6), men kan også brukes i dagens versjon. IPSec består av to protokoller:

- Authentication Header (AH)
- Encapsulating Security Payload (ESP)

AH sikrer data integritet ved autentisering av hver IP pakke og payload (pakkens innhold). AH varsler motparten hvis noen av pakkene skulle bli forandret underveis. ESP krypterer IP-pakkene for å sikre mot innsyn fra uvedkommende. ESP kan også sikre IP-pakkenes integritet, men kan ikke autentisere pakke hodene slik som AH kan. IPSec beskytter interne nettverk mot flere typer angrep utenfra, bla. DoS, main-in-the-middle og spoofing.

IPSec er en del av PKI i Windows 2000, og kan bruke både Kerberos v5 og digitale sertifikater for autentisering. IPSec opererer på nettverkslaget, og autentiserer ikke brukere, men maskiner. Windows 2000 benytter IPSec når det skal kommunisere med en part det ikke har et ”thrust” forhold til.

4 Smartkort og Windows 2000

Et smartkort er noe de fleste har vært i kontakt med. Bankkort, bensinkort, telekort og Sim-kortene i GSM mobiltelefonene går alle inn under kategorien smartkort. Avhengig av anvendelsesområde varierer smartheten på kortene, dvs. lagringskapasitet og eventuelt mikroprosessor. Mens noen kort kun inneholder en kryptert nøkkel, kan andre inneholde en mikroprosessor som muliggjør at for eksempel kryptografiske operasjoner utføres på kortet. I forbindelse med denne oppgaven er der kun de sistnevnte kortene som er aktuelle. Det fysiske grensesnittet til smartkortene varierer også, men den fysiske størrelsen er den samme. Med smartkort i denne oppgaven mener jeg kort med mikroprosessor.

4.1 Standarder for Smartkort

De fleste betalingskort og kredittkort som brukes i dag er av typen med magnetstripe. Denne typen kort er hverken spesielt avanserte eller sikre, og krever omfattende autentisering mot en tjener. Etterhvert som kryptografien gjorde fremskritt og behov for smartkort med klientside applikasjoner dukket opp, kom mikroprosessorkortene. For å kommunisere med denne typen mer fleksible og avanserte kort, ble det utviklet forskjellige industri standarder. Først ut var The International Organization for Standardization (ISO), som definerte bla. Fysisk- og elektronisk grensesnitt, protokoller og instruksjonssett. De fleste videre standardiseringer bygger på hele eller deler av denne ISO 7816 standarden.

Europay, MasterCard International og Visa (EMV'96) bygger på ISO 7816, og definerer et grensesnitt for betalingskort. Deres mål er å sikre interoperabilitet mellom forskjellige typer smartkort, og å definerte en minimum funksjonalitet for kort og kortleser.

4.1.1 PC/SC Workgroup

Sammen med store aktører, som bla. Gemplus, IBM og Sun Microsystems, er Microsoft en del av en arbeidsgruppe som kaller seg Personal Computer Smart Card (PC/SC) Workgroup. Denne gruppen har utarbeidet en åpen spesifikasjon ('97) rettet mot integrasjon av smartkort og smartkortlesere mot PC'en. Spesifikasjonen dekker også begrensninger i tidligere standarder mht. interoperabilitet mot applikasjoner på en PC. Interoperability Specification for ICCs and Personal Computer Systems 1.0 omfatter blant annet:

- Høynivå API for lettere å kunne utvikle og vedlikeholde smartkort applikasjoner.
- Programvare (drivere) for smartkortlesere.
- Spesifikasjoner for kryptografisk funksjonalitet og sikker lagring innebygget i smartkortet

PC/SC standarden bygger på og er kompatibel med ISO 7816 for fysisk og elektronisk grensesnitt.

4.1.2 OpenCard

En annen stor gruppering er Network Computer Reference Profile med deres OpenCard Framework (OCF). OpenCard er en åpen standard for interoperabilitet for smartkort på flere program- og maskinvare plattformer. OCF gir applikasjonsutviklere en objektorientert plattform og et sett med API gir uavhengighet fra de andre delene i smartkort løsningen (smartkort operativsystem, kortlesere). Referanse implementasjonen av OCF er utviklet som et sett Java pakker og –klasser, har kommet i en rekke oppdaterte versjoner. Disse følger ofte Sun sitt JDK.

4.1.3 PC/SC Workgroup og OpenCard

OpenCard ble utviklet etter PC/SC's standard, og et av målene var at de skulle være kompatible. Det er de også blitt, og som en del av referanse implementasjonen av OpenCard Framework er det en egen Java klasse for å kommunisere med en PC/SC kort terminaler. De to standardene dekker ikke de samme områdene, men kan sies å være overlappende og komplementære.

4.2 Smartkort grensesnitt

Microsoft sin støtte for smartkort er basert på PC/SC standarden. Det innebærer et standard grensesnitt mellom applikasjon og maskinvare. Alle PS/SC standardiserte kortleser og smartkort skal derfor fungere med applikasjoner utviklet for Microsoft sin win32 plattform.

4.2.1 Windows 2000 og Smart Card Base Components

Selv om det er først med Windows 2000 at Microsoft fremhever smartkort støtte, finnes dette også i Windows 9x og NT4.0 (win32 plattformen). Ved hjelp av Microsoft Smart Card Base Components kan også disse eldre operativsystemene utnytte PC/SC standarden for smartkort. Dette er en slags driver som lar applikasjoner kommunisere med smartkort gjennom en smartkortleser og driver. I Windows 2000 er smartkortstøtten mer integrert enn hva den er i Windows 9x og NT4.0 med Smart Card Base Components, og man kan benytte Windows 2000 offentlig nøkkel infrastruktur (PKI) sammen med smartkort. Dette innebærer at tjenester som er integrert i operativsystemet kan anvendes sammen med smartkort. Den viktigste tjenesten er interaktiv logon og nettverksautentisering med Kerberos.

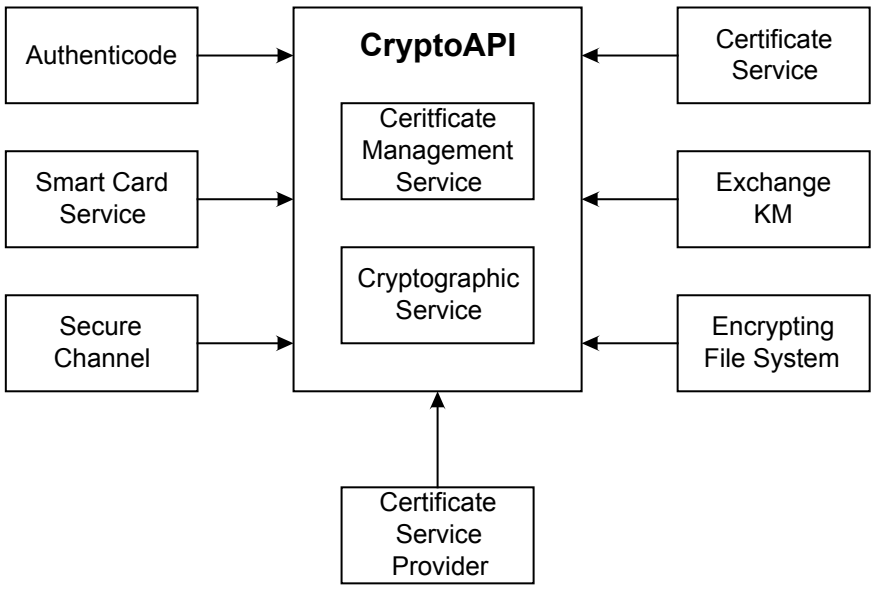
Utover Windows 2000 sine innebygde funksjoner, er det spesielle applikasjoner som gjør bruk av smartkort. Applikasjoner fra Microsoft som støtter smartkort interaksjon på win32 plattformen er Internet Explorer, Outlook Express og Outlook.

For utvikling av applikasjoner med smartkortstøtte tilbyr Windows 2000 tre forskjellige applikasjon programmerings grensesnitt (API).

4.2.2 CryptoAPI

CryptoAPI er et grensesnitt som gir utvikleren tilgang til kryptografiske funksjoner og algoritmer som er innebygget i Windows. Utvikleren trenger ikke ha kjennskap til kryptografi for å bruke disse tjenestene.

CryptoAPI har en sentral rolle i Windows, siden alle sikkerhetsmekanismene er bygget rundt det (figur 4-1). CryptoAPI bygger på tjenester fra forskjellige installerbare Cryptographic Service Providers (CSPs), og leverer et standard grensesnitt for disse. En CSP kan være program- eller maskinvarebasert, og kan støtte en mengde kryptografiske algoritmer og nøkkellengder. Gjennom CryptoAPI kan man også får tilgang til sertifikat tjenester i Windows 2000, som er en del av PKI.



Figur 4-1 Komponenter knyttet til CryptoAPI

Microsoft sitt eget Windows Powered Smart Card benytter dette API'et, og kommer med en installerbar CSP (maskinvarebasert). Sikkerhetsmekanismene som er knyttet til CryptoAPI får dermed automatisk tilgang til denne CSP'en. Det betyr blant annet at denne typen smartkort kan brukes sammen med Windows 2000 PKI.

4.2.3 SCard COM

SCard COM er et grensesnitt som er uten kryptografiske funksjoner. Dette er beregnet for å få tilgang til smartkort tjenester i egenutviklede applikasjoner. API'et bygger på Microsoft sitt Component Object Model (COM) grensesnitt, som er kjent for de fleste utviklere på win32 plattformen.

4.2.4 Win32

Win32 er et grunnleggende API for å aksessere smartkort, og krever en dypere forståelse av både Windows operativsystemet og smartkort for å kunne brukes effektivt. På den annen side gir dette API'et størst fleksibilitet og kontroll over smartkort, -lesere og tilhørende komponenter.

4.2.5 OpenCard

De nevnte API'ene er de Microsoft tilbyr applikasjonsutviklere på deres Windows plattform. Her kan det også være interessant å nevne en fjerde måte applikasjonsutviklere kan bruke smartkort og –leser under Windows. PC/SC

Workgroup og OpenCard er de to ledende standarder for smartkort til PC. Av disse er Microsoft kun medlem i førstnevnte, og har derfor ingen direkte støtte for OpenCard applikasjoner og kort. Ettersom OpenCard har en hvis støtte for PC/SC standardisert utstyr, er det relativt enkelt å bruke OpenCard under Windows. Som navnet antyder er OpenCard en plattformuavhengig åpen standard, og består bla. av et klassebibliotek for Java (1.2), OpenCard Framework. Dette inneholder klasser for programmering av applikasjoner som bruker smartkort og klasser for programmering av OpenCard smartkort. OCF inneholder også en klasse som kommuniserer med PC/SC kortlesere og –smartkort. Sammen med JavaX.Com kan man dermed kommunisere med smartkort og –leser fra en Java applikasjon/-applet. Siden Windows tilbyr et grensesnitt mot Java tilbyr det også et grensesnitt mot OpenCard.

4.3 Applikasjonsutvikling

Basert på forrige avsnitt vil jeg her se på hvilken funksjonalitet som tilbys utviklere av applikasjoner som bruker smartkort under Windows 2000. Siden MS leverer et eget utviklingsverktøy for slike applikasjoner vil jeg se nærmere på dette.

4.3.1.1 Windows Smart Card Toolkit

Microsoft sitt verktøy er basert på deres Visual Studio, herunder Visual C++, Visual J++ og Visual Basic, og man kan dermed velge mellom de vanligste programmeringsspråkene. Til disse språkene følger det med klasser som gjør det mulig å benytte smartkort API'ene i Windows 2000, avhengig av hvilke funksjoner på smartkortet man ønsker tilgang til. CryptoAPI leverer kryptografiske funksjoner basert på en (eller flere) CSP'er. Dette kan være en av Microsoft sine, dine egenutviklede eller tredjeparts løsninger. Typisk vil en leverandør av smartkort ha sin egen CSP, og Windows 2000 leveres med CSP fra Gemplus og Schlumberger. Ønsker man å utvikle sin egen CSP, følger det med et utviklingssett sammen med Windows Smart Card Toolkit.

For webapplikasjoner som benytter smartkort er det en ActiveX komponent for bruk på Microsoft sin webserver, Internet Information Server (IIS). Gjennom denne kan man aksessere smartkort og –leser ved hjelp av ASP (Active Server Pages).

Microsoft sin løsning er egentlig to deler, et operativsystem for smartkort, Windows for Smart Cards, og Visual Basic for Smart Cards. Windows Smart Card Toolkit inkluderer utviklingsverktøy både for applikasjoner på selve smartkortet og for applikasjoner på win32 plattformen som skal implementeres med smartkortstøtte.

4.4 Smartkortfunksjonalitet

Smartkort i Windows 2000 brukes sammen med digitale sertifikater, og foruten å tilby sikker lagring av brukerens private nøkkel, har kortet innebygd flere kryptografiske algoritmer.

4.4.1 Kryptofunksjoner

I Windows er det de såkalte CSP'ene som leverer de kryptografiske algoritmene, og et smartkort defineres som en maskinvare CSP. Ved bruk at smartkort er det derfor et begrenset utvalg algoritmer som kan brukes:

- RSA kan benyttes til autentisering på kortet mot vertsmaskinen, for å generere digital signatur og for å generere RSA nøkkelpar.
- SHA-1 kan benyttes for å beregne hash/Message Digest av data.
- DES og Triple DES benyttes for autentisering fra kort til vertsmaskin og omvendt.

Ut i fra dette ser vi at smartkort kun benyttes i forbindelse med autentisering og digital signatur. Kortene kan brukes til å generere asymmetriske nøkkelpar (RSA), mens generering av symmetriske nøkler (DES) overlates til vertsmaskinen. Symetrisk kryptering/dekryptering utføres også på vertsmaskinen, fordi smartkort har begrenset regne- og overføringskapasitet.

For de enkelte sikkerhetsmekanismene i Windows 2000 betyr dette protokollenes kryptografiske krav ofte deles mellom vertsmaskinen og smartkortet.

I *S/MIME* benyttes RSA for autentisering med X.509v3 digitalt sertifikat og digital signatur av SHA-1 generert hash av meldingen. Generering av felles DES nøkkel for kryptering av meldingen gjøres på vertsmaskinen, som også vil stå for selve krypteringen. Generering av hash av en hel melding vil være svært tidkrevende for et smartkort, så også dette gjøres av vertsmaskinen. Smartkortets funksjon er å signere denne meldingens hash med brukerens private nøkkel.

SSL og *TLS* benyttes hovedsakelig til autentisering av tjenere, og ikke så ofte til klientautentisering med personlige sertifikat. Når klientautentisering derimot kreves benyttes brukerens personlige sertifikat og private nøkkel som er lagret på smartkortet som benyttes. Ved autentisering av brukeren brukes smartkortet til å signere generert data med sin private nøkkel (RSA). Resultatet ender etterhvert opp som en "master secret", Vertsmaskinen bruker denne til å generere symmetriske nøkler gjennom sesjonen og tar seg også av kryptering/dekryptering av data. Smartkortet brukes altså kun til klientautentisering under SSL Handshake.

Noen smartkort tilbyr mer funksjonalitet i forbindelse med SSL protokollen, men Windows 2000 vil i utgangspunktet ikke kunne benytte seg av dem.

Microsoft sin utvidelse av *Kerberos* bruker også sertifikater, og benyttes sammen med Smart Card Logon. Smartkortet brukes også her til autentisering med RSA algoritmen.

I standardiserte sikkerhetsmekanismer er det ofte oppgitt flere forskjellige kryptografiske algoritmer for de samme funksjonene. Dette sikrer fleksibilitet, men kan i tilfeller føre til inkompatibilitet. Siden et smartkort kun kan støtte en begrenset mengde kryptografiske algoritmer, implementeres ofte de som er anbefalt. Dette begrenser velgmulighetene når man bruker smartkort.

4.4.2 Nøkkelbehandling og sertifikater

Smartkort i Windows 2000 er basert på sertifikater og offentlig nøkkelsystemer. Styrken ved et slikt system er at brukerens private nøkkel kun er lagret på kortet, og er ikke kjent av noen. Ved bruk av smartkortet for første gang blir sertifikatet kopiert over på vertsmaskinen og registrert for bruk på den. Sertifikatets korresponderende private nøkkel forblir på kortet.

Moderne smartkort er ofte såkalte multiapplikasjonskort, som betyr at de kan brukes sammen med flere applikasjoner. Ofte kan slike kort også lagre flere sertifikater. Dette er ikke støttet i Windows 2000, selv om korttypene støtter det. I praksis innebærer dette at en bruker med et sertifikat som er utstedet av organisasjonen, ikke vil ha noe nytte av smartkortet mot parter organisasjonen ikke har et ”thrust” forhold til. For å bruke smartkortet mot en ukjent part kan det derfor være nødvendig med et sertifikat som er utstedet av en (kommersiell) global sertifikat utsteder med ”thrust” forholdt til langt flere brukere.

Av sikkerhetsgrunner ønsker man gjerne å holde alle krypteringsnøkler best mulig skjult. Det kunne derfor vært ønskelig at smartkortet tilbød mer funksjonalitet, slik at flere av nøklene ble anvendt kortet i stedet for på vertsmaskinen. Igjen er det smartkortets regne- og overføringskapasitet som reduserer bruksområdet. I Windows 2000 kunne det f.eks. være ønskelig at Encrypting File System kunne benyttes sammen med smartkort. Dette er ikke implementert da smartkortet ville begrense systemets ytelse betraktelig.

4.4.3 Vurdering

Smartkort i Windows 2000 benyttes kun til autentisering og digitale signaturer med brukerens private nøkkel. Andre aktuelle bruksområder elimineres av smartkortets ytelse. Hvis smartkort også følger More’s lov om fordobling av prosessorkraft og en halvering av pris i løpet av 18 måneder, vil det fortsatt gå noen år før smartkortets bruksområder er nevneverdig utvidet.

4.5 Smartkorttyper

Måten Microsoft har laget smartkortstøtte i Windows 2000 innebærer såkalt kryptografiske tjenester i maskinvare (Hardware CSP). Som nevnt har Windows 2000 flere kryptografiske tjeneste leverandører i programvare (Software CSP), og ved hjelp av CryptoAPI kan man også lage sin egen. Et smartkort regnes for en hardware CSP og forskjellige leverandører av smartkort leverer hver sin CSP tilpasset sin egen smartkort type. Fra Microsoft leveres Windows 2000 med støtte for to forskjellige smartkort, Gemplus GemSAFE og Schlumberger Cryptoflex. På grunn av amerikanske eksportlover mhp. sterke kryptografiske operasjoner er ikke Microsoft sin CSP for Windows Powered Smart Card inkludert i Windows 2000. Nå er for øvrig disse reglene oppmyket slik at denne CSP’en er tilgjengelig på Internett for de fleste.

4.5.1 Gemplus GemSAFE Enterprise

Gemplus var første leverandør av smartkort beregnet for Windows 2000. Deres GemSAFE kort leveres både for bruk i Windows 2000 og NT 4.0. Kortet er basert på GPK8000, som er et kort beregnet for offentlig-nøkkel systemer, og mangler DES funksjonalitet.

Siden GemSAFE er utviklet for et større marked enn kun Windows 2000, har kortet funksjoner som ikke anvendes i Windows 2000. Kortet har f.eks. en såkalt Unwrap funksjon, i forbindelse med RSA dekryptering, som ikke benyttes. Gemplus leverer både et utviklingsverktøy og administrasjonsverktøy for GemSAFE.

4.5.2 Sclumberger Cryptoflex

Sclumberger er den andre leverandøren av smartkort til Windows 2000. Deres Cryptoflex er basert på et eksisterende kort, Multiflex. Dette er en hel serie med kort med et stort bruksområde.

Også Schlumberger leverer administrasjonsverktøy og utviklingsverktøy for deres smartkort.

4.5.3 Windows Powered Smart Cards

Denne typen smartkort er egentlig en del av Microsoft sitt Windows Smart Cards Toolkit for Visual Basic 6.0, og er beregnet for utviklere av smartkort applikasjoner for Windows. Utover mulighetene til å integrere smartkort i egenutviklede applikasjoner, er det også mange forskjellige konfigureringsmuligheter for kortet (tabell 4-1).

Filsystem	Microsoft FAT-filsystem, variabel partisjonsstørrelse, flere partisjoner
Lagringskapasitet	EEProm for kortet låses på en gunstig størrelse, opp til 40kb
Instruksjonssett	Min./Utvidet ISO 7816-4, EMV. (GSM i egen versjon)
Kryptoalgoritmer	DES, Trippel-DES, RSA, SH5
Brukerinformasjon	Navn, PIN kodens lengde
Runtime Environment	Første versjon tolker Visual Basic
API	Nøytralt ovenfor språk. Avhengig av RunTime Engine

Tabell 4-1 Konfigureringsmuligheter i Windows for Smart Cards

Kortet kan selvfølgelig også konfigureres til å brukes sammen med Windows 2000, se vedlegg C for informasjon.

Microsofts eget alternativ for smartkort og applikasjonsutvikling virker som et meget godt alternativ. Utviklingsmiljøet er kjent for de fleste og er et kraftfullt verktøy og perfekt for sømløs integrasjon med Windows operativsystemet. Ettersom kortet er PC/SC kompatibelt og anvender et standardisert instruksjonssett er ikke kortets bruksområde begrenset til windows plattformen, selv om utviklingsverktøyet er det.

Windows Powered Smart Cards er et utviklingskort, som ikke er beregnet for direkte bruk i Windows 2000. Et administrasjonsverktøy levers derfor heller ikke av Microsoft.

4.5.4 Vurdering

De forskjellige smartkorttypene beregnet for Windows 2000, tilbyr samme funksjonalitet.

Egenskaper	GemSAFE	Cryptoflex	WPSC
Kryptografisk coprosessor	Ja	Ja	Ja
RSA (bit)	512,768, 1024	512, 768, 1024	512, 1024
DES (bit)	40, 56, 128	64 (56), 128	40, 56, 128
Triple DES (bit)	168	168	168

Tabell 4-2 Egenskaper ved forskjellige smartkort

GemSAFE og Cryptoflex er en ferdigutviklet løsning med videreutviklings potensiale, mens Windows Powered Smart Cards i utgangspunktet er beregnet for utviklere, og ikke for direkte bruk i Windows 2000. Det sistnevnte kortet har derimot et bra og velkjent utviklingsverktøy, og det er stor satsing på WPSC fra mange områder, bla. fra Gemplus med deres GemShield kort.

4.6 Sikkerhetsaspekter ved bruk av smartkort

Smartkort blir ofte fremstilt som et vidundermiddel for beskyttelse av sensitiv informasjon. Som ved alle systemer er heller ikke smartkort uten trusler, men de har ofte et positivt forhold mellom fordeler og ulemper.

4.6.1 Smartkort vs. passord

I et vanlig nettverksmiljø er det brukernavn og passord som autentiserer brukeren. Dette gjøres ved at det genereres en enveis hash streng på en viss lengde første gang brukerens passord velges. Nøkkelen til denne strengen er dermed brukerens passord. Problemet er at et menneskelig valgt passord ikke er særlig egnet som kryptografisk nøkkel. Mennesker har en tendens til å velge navn, ord, datoer eller kombinasjoner som er lette å huske. Det gjør det også enklere for en fiende å finne passordet.

Ved bruk av et smartkort erstattes passordet med to ting: selve smartkortet og en PIN-kode; du har noe og du vet noe om det. PIN-koden autentiserer brukeren til

kortet og kortet autentiserer brukeren til nettverket/datamaskinen. For å starte sist, så autentiserer smartkortet brukeren ved hjelp av et personlig digitalt sertifikat. Sertifikatet lagres på smartkortet sammen med sertifikatets korresponderende private nøkkel. Selv om sertifikatet leses ut av kortet, vil aldri den private nøkkelen forlate kortet. Dermed vil ingen kunne vite hva nøkkelen er, heller ikke innehaveren av smartkortet eller utstederen av sertifikatet. Den private nøkkelen har en lengde på mellom 512 og 1024 bit og er atskillig vanskeligere for en fiende å fremskaffe/knekke.

I likhet med passord er PIN-kode noe brukeren kan velge selv. Her gjelder derfor noen av de samme betenkelighetene som med passord. Brukeren velger kanskje en fødselsdato eller lignende, som en fiende kan klare å finne fram til på tre forsøk. Ofte velger man kanskje en PIN-kode man har fra før, for å slippe å huske for mange tallkombinasjoner. En fiende kan derfor ha andre hensikter enn å få tilgang til nettverket/datamaskinen, som f.eks. husalarm, minibankkort osv.

Det har vist seg at folk har et annet forhold til PIN-koder enn passord, gjennom bruk av minibankkort. Slepphendt oppbevaring og bruk av koden har direkte økonomiske følger og man passer derfor ekstra godt på å holde denne koden skjult.

Smartkort som erstatning for passord har flere sikkerhetsmessige fordeler. I Windows 2000 lagres passord i Security Accounts Manager (SAM). Dette er en fil som lagres lokalt på datamaskinen etter første logon. Hvis en fiende får tak i denne filen kan han i løpet av veldig kort tid klare å finne en brukers passord. Dette er en generell svakhet når passord lagres på en eller annen form på maskinens harddisk. Ved bruk av smartkort og digitale sertifikat vil brukerens private nøkkel alltid ligge beskyttet på kortet. Den private nøkkelen vil være ukjent for alle i og med den aldri forlater kortet, og gir heller ingen snarveier for å finne nøkkelen.

4.6.2 Fysiske angrep på smartkortet

Fysisk angrep på et smartkort er en omfattende og ressurskrevende operasjon. De grundigste metodene går ut på å analysere arkitekturen til smartkortets mikroprosessor. Hensikten er å få oversikt over kommunikasjonslinjene mellom prosessorens forskjellige deler og dermed forbikoble eller simulere kritiske operasjoner som f.eks. autentisering av PIN-kode eller kryptografiske instruksjonskal. En slik analyse kan gjøres ved å fysisk demontere mikroprosessoren for å bygge opp en ny erstatning, frekvensanalyse av prosessorens (transistorer) forskjellige tilstander i sanntid eller å avlytte kommunikasjonslinjene elektronisk med prober. Felles for alle metodene er at de krever svært gode kunnskaper om CMOS VLSI designteknikk og tilgang til avansert utstyr.

Den andre strategien for å knekke et smartkort skjer fra utsiden. Den ene metoden er å monitorere strømforbruket i kortet i sanntid. Forskjellige aktiviteter i prosessoren kan ofte skilles ut, og brukes til og rekonstruere deler av algoritmene. Den andre metoden, og kanskje mest vellykkede, er å påføre smartkortets mikroprosessor en spenningspuls for å fremprovosere en feil. Ved å gjøre dette på riktig tidspunkt kan man får prosessoren til å hoppe over kritiske operasjoner, f.eks. til en tilstand der PIN-kode allerede er autentisert. Denne metoden er blant annet benyttet med hell på betal-TV kort.

Når man har klart å trenge tilstrekkelig dypt inn i et kort, vil man også kunne manipulere mikroprosessoren til å lese ut eventuelle krypteringsnøkler. Det skal legges til at designere av smartkort stadig legger inn flere og bedre sikkerhetsmekanismer, som gjør det vanskeligere for en fiende å hente ut nyttig informasjon.

4.6.3 Logiske angrep på smartkortet

Denne typen angrep er langt i fra like kompliserte som fysiske angrep. Angrepet går ut på bruke smartkortet til å kryptere kjent data. Ved å analysere resultatet kan man finne den private nøkkelen/krypteringsnøkkelen. Det er som kjent mulig å finne en kryptografisk nøkkel i tilfeller der både kryptert- og klartekst data er kjent, og spesielt når man har mye data. Angrepet krever kjennskap til kortets PIN-kode.

4.6.4 Angrep gjennom vertsmaskinen/kortterminalen

Angrepet baseres på at fiendtlig programvare kjøres på datamaskinen, som en slags trojansk hest. Dette kan skje ved at en fiende rett og slett benytter seg av smartkortet etter at riktig bruker har tastet inn sin PIN-kode. Fienden aksesserer smartkortet over et nettverk og kan bruke den private nøkkelen til f.eks. digitale signaturer.

4.6.5 Vurdering

Smartkort er velegnet til å beskytte sensitive opplysninger. I denne sammenheng er dette kryptografiske nøkler. Kombinert med et offentlig-nøkkel system benyttes smartkort til autentisering, og er i det henseende overlegent vanlige passord.

Selvom smartkort regnes som en sikker måte å lagre opplysninger på, fins det også metoder som kan knekke et smartkort. Disse metodene er svært ressurskrevende, både tids- og kostnadsmessig, og krever også grundige kunnskaper.

Alle sikkerhetsmekanismer kan brytes, det bare et spørsmål om ressurser. Som grunn regel bør kostnaden må være større enn verdien av dataene. Og man bør også tenke på hvem vil man beskytte seg mot, og hvilke ressurser de kan tenkes å inneha.

5 Windows 2000 og NT 4.0

Forgjengeren til Windows 2000, NT 4.0, har i sin levetid måttet tåle skarp kritikk for dårlig sikkerhet. Hovedgrunnen til dette er at operativsystemet ble utviklet på et tidspunkt da sikkerhetskravene var mindre. Etter hvert som mer åpne nettverk som Inter-, intra- og ekstranett har blitt vanlig, har også sikkerhetstrusselen mot nettverk og enkeltmaskinene i nettverkene økt. I tillegg til dette har uheldige programmeringsfeil, ”bugs”, i blant annet TCP/IP implementasjonen fått mye oppmerksomhet. Etterhvert som Microsoft har fått orden på slike feil, og tilført ekstra sikkerhetsfunksjoner i såkalte ”service packs”, har kritikken også stilnet en hel del.

5.1 Hva er nytt?

Windows 2000 inneholder flere nye sikkerhetsmekanismer i forhold til NT 4.0. Noen av mekanismene gir helt nye funksjoner, mens andre erstatter funksjoner i NT 4.0.

5.1.1 Kerberos v5

En av de største forandringene i Windows 2000 er autentiseringsprotokollen for LAN. Frem til nå har Microsoft benyttet seg av NT LAN Manager i både Windows NT og 9x. Denne proprietære protokollen er nå byttet ut med den standardiserte Kerberos v5 protokollen, som også betyr høyere grad av kompatibilitet med andre ikke-Microsoft operativsystemer. Denne protokollen har en rekke fordeler fremfor NTLM:

- Autentisering av brukere fra flere domener. Kerberos “trust relationship” eksisterer også mellom forskjellige domener. Dvs. stoler domene A på bruker X og domene B stoler på A, så stoler også B på X. NTLM tilbyr ikke automatisk autentisering mellom domener. Dette betyr raskere og sikrere autentisering mellom domener med Windows 2000, samt høyere grad av sømløshet ovenfor brukerne.
- NTLM autentiserer kun klient mot server, og ikke server mot klient. Klienten vet derfor ikke sikkert hvem den kommuniserer med. I Kerberos er det gjensidig autentisering av server og klient. Begge parter kan dermed være sikre på hvem de snakker med.
- Kerberos regnes også for å være raskere enn NTLM, fordi klienten selv innehar sitt autentiseringsbevis som inneholder tilgangsrettigheter. NTLMs oppslag i SAM databasen er derfor vanligvis ikke nødvendig.
- Public Key Infrastructure(PKI) utvidelsen i Kerberos implementasjonen i Windows 2000 har åpnet for autentisering med smartkort. NTLM kan hverken bruke PKI eller påloging med smartkort.
- Kerberos autentiseringsprotokollen er i utgangspunktet beregnet for å brukes å et usikret nettverk. Dette oppnås ved kryptering av all data. NTLM har ikke denne egenskapen.

5.1.2 Public Key Infrastructure

Store deler av sikkerhetsmekanismene i Windows 2000 er basert på såkalt Public Key Infrastructure (PKI). Dette systemet autentiserer entitetene med et personlig digitalt sertifikat. Sertifikatet er utstedt av en ”thrusted part”, og binder en entitet til en offentlige nøkkel. En entitet kan dermed bevise sin identitet med den

korresponderende private nøkkelen. Et sertifikat kan benyttes til autentisering på LAN (Kerberos v5), over Internett (SSLv3), i forbindelse med e-post(S/MIMEv3) og til filkryptering.

I NT 4.0 var ikke PKI en del av operativsystemet, men diverse sikkerhetsprotokoller benytter seg av sertifikater. Naturlig nok støtter også Internett tjeneren og klienten for NT 4.0 disse protokollene. Diverse e-post klienter bruker også sertifikater i NT 4.0.

5.1.3 Smart Card logon

Nytt i Windows 2000 er også muligheten til pålogging med smartkort. Dette er naturlig nok nært knyttet til Kerberos v5 autentiseringsprotokollen, men også Public Key Infrastructure (PKI). Bruk av smartkort logon medfører en overgang til PKI og dermed må alle smartkort brukere ha sitt personlige digitale sertifikat. Et sertifikat av X.509 v3 format lagres på brukerens smartkort, og offentlig nøkkelparet i sertifikatet brukes til å autentisere brukeren mot Kerberos. Fordelen med å bruke smartkort er at brukerens private nøkkel ikke er et resultat av et valgt passord, og at nøkkelen heller aldri forlater smartkortet. I Windows 2000 vil sertifikatet bli lest ut av smartkortet ved første gangs bruk, og ligge lagret på datamaskinens harddisk. Man vil ikke kunne bruke dette sertifikatet uten den korresponderende private nøkkelen, som fortsatt ligger lagret på smartkortet.

Ved logon på en lokal maskin, dvs. ikke på nettverk, autentiserer ikke brukeren seg med Kerberos tjenesten. Local Security Authority Sub System (LSASS) brukes til autentisering mot den lokale maskinen. For øvrig vil man også ved nettverkslogon først autentisere seg mot maskinen lokalt før autentisering mot nettverket.

Nå er heller ikke NT 4.0 helt ukjent med smartkort. Smart Card Base Components (SCBC) 1.0 er en del av Service Pack 4, og gjør at også NT 4.0 kan brukes sammen med PC/SC smartkort utstyr. SCBC gjør at applikasjoner som bruker smartkort også fungerer under NT 4.0. Det derimot ikke snakk om funksjoner som er integrert med operativsystemet slik som autentisering i Windows 2000.

5.1.4 Encrypting File System

Encrypting File System (EFS) er en ny sikkerhets funksjon i NT File System (NTFS). NTFS i NT 4.0 skulle gi en hvis grad av beskyttelse av filer. Det var ikke snakk om kryptering av filer i dette systemet, men mere brukertilgang under NT4. I andre operativsystem fikk man derimot programvare som kunne lese all lagret data på NTFS uavhengig av brukertilgang. I Windows 2000 lanserer Microsoft EFS, som er et verktøy for kryptering av filer. Sikkerheten for lagrede data økes dermed betraktelig. EFS er en del av Publik Key Infrastructure (PKI) som betyr at hvis du har riktig nøkkel kan du lese de krypterte dataene. Dette skjer uten at brukeren må taste inn passord, og operativsystemet prøver automatisk brukerens sertifikat for EFS når man ønsker å lese kryptert data. EFS gir en langt større grad av sømløshet enn tredje part systemer til NT 4.0, der brukeren må dekryptere dataene før bruk, og dekryptere de igjen når han er ferdig.

5.1.5 Active Directory

Sammen med Kerberos er kanskje Active Directory (AD) den største nyheten i Windows 2000. AD er en katalogtjeneste som er hierarkisk og objektorientert for lettere å kunne modellere organisasjonsstrukturer. I AD er all brukerinformasjon lagret og administrert, også sikkerhetsinformasjon. Administrasjon av systemet blir forenklet ved at bruker- og sikkerhetsnivåene er knyttet opp til en modell av organisasjonen. I NT 4.0 blir denne jobben gjort av Security Accounts Manager (SAM). SAM og egenskapene til NTLM "trust forholdet" begrenser sikkerheten til tre nivåer: globale og lokale grupper, og individuelle brukere. Dette resulterer i en flat struktur der det er vanskeligere å holde oversikt over brukerne.

5.2 Generelt sikkerhetsnivå i Windows 2000

Windows 2000 er et veldig nytt operativsystem, og få organisasjoner har tatt det i regulært bruk. Operativsystemet er bygget på NT 4.0 og erfaringer som er gjort med det over flere år. I tillegg har Windows 2000 vært gjennom en lang periode med betatesting, blant annet under navnet NT 5.0. En vurdering av sikkerheten i Windows 2000 vil derfor være basert på rapporter om NT 4.0 og om de nye sikkerhetsmekanismene som er lagt til.

En grundig analyse av et operativsystem er en tidkrevende og omfattende jobb, og for at den skal være troverdig bør den være utført av et uavhengig organ. En programvareutvikler som Microsoft kan få sine produkter verifisert av nasjonale myndigheter i forskjellige land. Microsoft har bla. fått NT 4.0 godkjent av myndighetene i USA, Canada og Storbritannia.

5.2.1 C2 og E3/F-C2 sikkerhetsgrader

C2 og E3/F-C2 er to sikkerhetsgrader som tildeles av henholdsvis National Computer Security Center (NSCS) i USA og UK IT Security Evaluation and Certification Scheme (ITSEC) i Storbritannia. De to gradene regnes som likestilte, og begge evalueringene bygger på granskning av kildekode, dokumentasjon, testing og kontroll av at eventuelle feil og mangler blir rettet opp.

Sikkerhetsgradene omfatter følgende funksjoner:

- Adgangskontroll – Kun autoriserte brukere får tilgang til ressurser.
- Diskresjon – Brukerne kan beskyte data hvis ønskelig
- System kontroll – Systemet kan kontrollerer bruker og system oppgaver.
- Gjenbruk – Systemet hindrer brukere å få tilgang til ressurser som er brukt av en tidligere bruker, f.eks. deallokert minne eller filer som er slettet.

NT oppfyller også noen av kravene til NSCS B1 graden.

C2 og E3/F-C2 regnes for høyeste sikkerhetsgraden et operativsystem for generelt bruk kan oppnå i de respektive graderingene. C2 graden ble oppnådd med Service Pack 6a og C2 i desember 99, mens E3/F-C2 graden ble oppnådd med Service Pack 3 i april 99. Evalueringen er foretatt på enkeltstående maskiner og ikke i forbindelse med nettverk.

Både NT 3.5 og 4.0 har oppnådd de nevnte sikkerhetsgradene, og det forventes at også Windows 2000 vil nå minst tilsvarende nivå.

Rapportene fra NSCS og ITSEC finnes på henholdsvis http://www.radium.ncsc.mil og http://www.itsec.gov.uk .

5.2.2 FIPS 140-1 sikkerhetsgrad

Federal Information Processing Standard (FIPS) 140-1 sikkerhetsgraden utstedes av National Institute of Standards and Technology (NIST), og er en evaluering av Microsoft CryptoAPI. Dette er en viktig byggesten i alle sikkerhetsmekanismene i Windows 9x, NT 4.0 og 2000. CryptoAPI tilbyr kryptografiske tjenester for alle applikasjoner for operativsystemet, og kan utvides ved å installere CSP'er (Cryptographic Service Provider).

Evalueringensprosessen starter med å fastslå om produktet implementerer de kryptografiske funksjonene korrekt. Dette er f.eks. sammenlikning mot referanse implementasjonen og nøkkelbehandling. Når disse er verifisert korrekt settes det en karakter på hvilken grad av sikkerhet systemet tilbyr, avhengig av omgivelsene rundt maskinen. De kryptografiske funksjonene som ble verifisert er de som er inkludert i standard CSP'ene i Windows 9x, NT 4.0 og 2000:

- Data Encryption Standard (DES)
- Digital Signature Algorithm (DSA)
- Secure Hash Algorithm (SHA-1)

CryptoAPI oppnådde karakteren 1 (Level 1), dvs. at de benyttes i generelle PC omgivelser der det ikke er gjort tiltak for å hindre sabotasje. I forbindelse med C2 godkjennelsen av NT 4.0 blir karakteren hevet til Level 2, der systemet opererer i omgivelser som er sikret mot sabotasje. Det er fire sikkerhetsnivåer i FIPS 140.

Microsoft regner med at også Windows 2000 vil oppnå C2 godkjenning slik at CryptoAPI også her vil nå opp til en FIPS 140-2 sikkerhetsgrad.

Windows 2000 leveres med CSP'er for smartkort, noe som ikke er tilfelle tidligere i CryptoAPI. FIPS 140-3 fordrer at kryptosystemet opererer i omgivelser der det er gjort betydelige anstrengelser mot sabotasje. For å oppnå Level 3 vil det kreves spesiell maskinvare eller programvare sammen med fysisk sikring. Et smartkort vil delvis kunne oppfylle disse kravene, men det gjenstår å se om et kort er nok for å fysisk sikring.

5.2.3 Rapporterte sikkerhetshull

På grunn av liten fartstid i den virkelige verden er det foreløpig få sikkerhetshull som har kommet frem. Ettersom Windows 2000 bygger svært mye på NT 4.0 er trolig de fleste kjent hull tettet fra fødselen av. Usikkerhetsmomentene er eventuelt de nye mekanismene og funksjonene som er implementert for første gang i Windows 2000. To av nyhetene i Windows 2000 er Active Directory og Encrypting File System, og i disse har det kommet rapporter om sikkerhetshull. I begge tilfeller har Microsoft vært raske til å tilbakevise disse påstandene.

Encrypting File System er et filkrypteringssystem som er helt nytt i Windows 2000. Når en fil krypteres med dette systemet lagres den krypterte filen med to nøkler; en for brukeren og en EFS Recovery Key, som en administrator har tilgang til. Klarer en fiende å få tilgang til en administrators brukerkonto vil han også kunne dekryptere alle filene på systemet. I det rapporterte vellykkede angrepet klarte fienden å tilegne seg administrator rettigheter på maskinen der EFS Recovery Key lå på maskinen. Tilgang til administrator brukerkontoen kan man få ved å dekryptere maskinens SAM-fil (System Account Manager).

Microsoft advarer mot å la EFS Recovery Key bli liggende på en usikret maskin, og anbefaler at den eksporteres til en diskett og plasseres på et fysisk sikret sted. En fiende vil dermed ikke få dekryptert filene selv med tilgang til administratorens brukerkonto. Microsoft anbefaler også at maskinens SAM-fil beskyttes med SYSKEY.

Den andre rapporten om sikkerhetshull i Windows 2000 gjelder Active Directory. Novell, som leverer en konkurrerende tjeneste, rapporterte om en feil som gjaldt eierskap og adgangsrettigheter til objekter. I AD kan en administrator tilegne seg rettigheter til alle objekter, men eieren av objektet vil bli varslet om dette. Hvis en bruker har full kontroll over et objekt og nekter alle andre enn seg selv adgang, kan fortsatt en administrator altså tilegne seg selv rettigheter. Novell mener dette er et sikkerhetshull, mens Microsoft mener det bygger på en misforståelse rundt Windows 2000/NT sin sikkerhetsmodell. Microsoft går ut i fra at i en organisasjon må noen ha mulighet til å ”åpne” opp en sperret konto, hvis f.eks. brukeren slutter i organisasjonen eller av andre årsaker ikke kan åpne kontoen.

En annen misforståelse som ble påpekt i rapporten til Novell, var at eieren av et objekt må være den primære brukeren, og ikke administratoren. Objektets eier kan nemlig ikke endres, selv ikke av en administrator. Dermed kan ikke en administrator tilegne seg adgangsrettigheter til et objekt bak ryggen på objektets eier.

5.2.4 Andre egenskaper

De andre store nyhetene i Windows 2000 er PKI og Kerberos. Spesielt Kerberos regnes som en kraftig forbedring fra det gamle NTLM. Kerberos v5 er en annerkjent protokoll som har vært i bruk i diverse Unix miljøer over lengre tid. For bakover kompatibilitet støtter Windows 2000 også NTLM. Dette må regnes som en svakhet fordi et nettverk dermed kan være åpent for autentisering med denne langt svakere protokollen. Dette gjelder enten hvis Windows NT 4.0 eller 9x operativsystemer benyttes i et Windows 2000 domene, eller at protokollen av andre grunner ikke er slått av. Hvis domene tjeneren(e) ikke er Windows 2000, vil også NTLM bli benyttet fremfor Kerberos.

PKI sin styrke er de digitale sertifikatene, og spesielt sammen med smartkort. Smartkort erstatter et passord med et kort og en PIN-kode. Det betyr at en bruker både må ha en ting og vite noe får å få tilgang til en ressurs. Smartkortet sikrer at uvedkommende ikke får tilgang til brukerens konto ved å beskytte nøkkelen med en PIN-kode, og å fjerne nøkkelen fra maskinen når den ikke er i bruk. Ved kun å tillate smartkort logon på en brukerkonto, er bruk av passord ikke mulig. Autentisering er dermed også den funksjonen som har størst utbytte av smartkort.

5.2.5 Konklusjon

Uavhengige rapporter og offentlige godkjenninger av NT 4.0 og de forbedringene som er gjort i Windows 2000 tyder det på at operativsystemets sikkerhet vil være i toppsjiktet innen sitt bruksområde. Et operativsystem av denne typen stiller krav til brukervennlighet og kostnader, faktorer som ikke alltid lar seg forene med svært høye krav til sikkerhet. Jeg tenker i første omgang på fysisk sikring av selve PC'en og mer avanserte maskinvarebaserte autentiseringsmekanismer som kontrollerer f.eks. øyets iris-mønster.

Kommunikasjon mot Internett betyr også alle som ønsker, kan prøve å knekke systemet. Dette medfører alltid en hvis risiko for at noen skal klare det.

Microsoft har i de senere årene, og under lanseringen av Windows 2000, gitt uttrykk for at de ønsker å satse på sikkerhet. De hevder også at de vil reagere raskt når det oppdages sikkerhetshull eller svakheter i deres produkter.

6 Demonstrasjon av smartkort i Windows 2000

De fleste sikkerhetsmekanismene som er omtalt i kapittel to konfigureres av en administrator eller bruker. I dette kapittelet har jeg sett på hvordan de skal konfigureres for å brukes med sertifikater, og fortrinnsvis med sertifikatet på smartkortet.

Første punkt er selvfølgelig å få tilgang til en Server versjon av Windows 2000. Jeg har valgt å bruke en Advanced Server. Installasjonen må inkludere Internet Information Services og Certificate Services. Administrator rettigheter på maskinen er også nødvendig. Jeg disponerte også en klient, Windows 2000 Professional, for å bruke nettverkstjenesten i et domene.

6.1 Hvordan fungerer det i praksis

Smartkort funksjonene i Windows 2000 bygger på PKI og bruk av digitale sertifikater. Et personlig sertifikat av X.509v3 formatet lagres på et smartkort sammen med sertifikatets korresponderende private nøkkel. Kombinasjonen av disse to autentiserer brukeren ovenfor de forskjellige sikkerhetsmekanismene Windows 2000. Informasjonen i sertifikatet er basert på brukerprofilen i Active Directory.

Mekanismene som benytter seg av personlige sertifikat er:

- Smart Card logon/Kerberos v5
- SSL
- S/MIME
- EFS

I tillegg leveres Windows 2000 med Certificate Server som utsteder sertifikater.

6.2 Bruk av sertifikater

Som nevnt er digitale sertifikater en del av PKI som er den grunnleggende infrastrukturen for sikkerhetsmekanismene i Windows 2000. For å utnytte PKI fullt ut kreves det at alle entiteter i infrastrukturen innehar hvert sitt sertifikat som er gyldig for alle tjenester de måtte tilby og gjøre bruk av. Gjennom Certificate Services vil de nødvendige tjenestene i operativsystemet få riktig sertifikat. Personlige sertifikat til alle brukerne av systemet rekvireres gjennom en spesiell web tjener, eks. http://<domenetjener>/certserv.

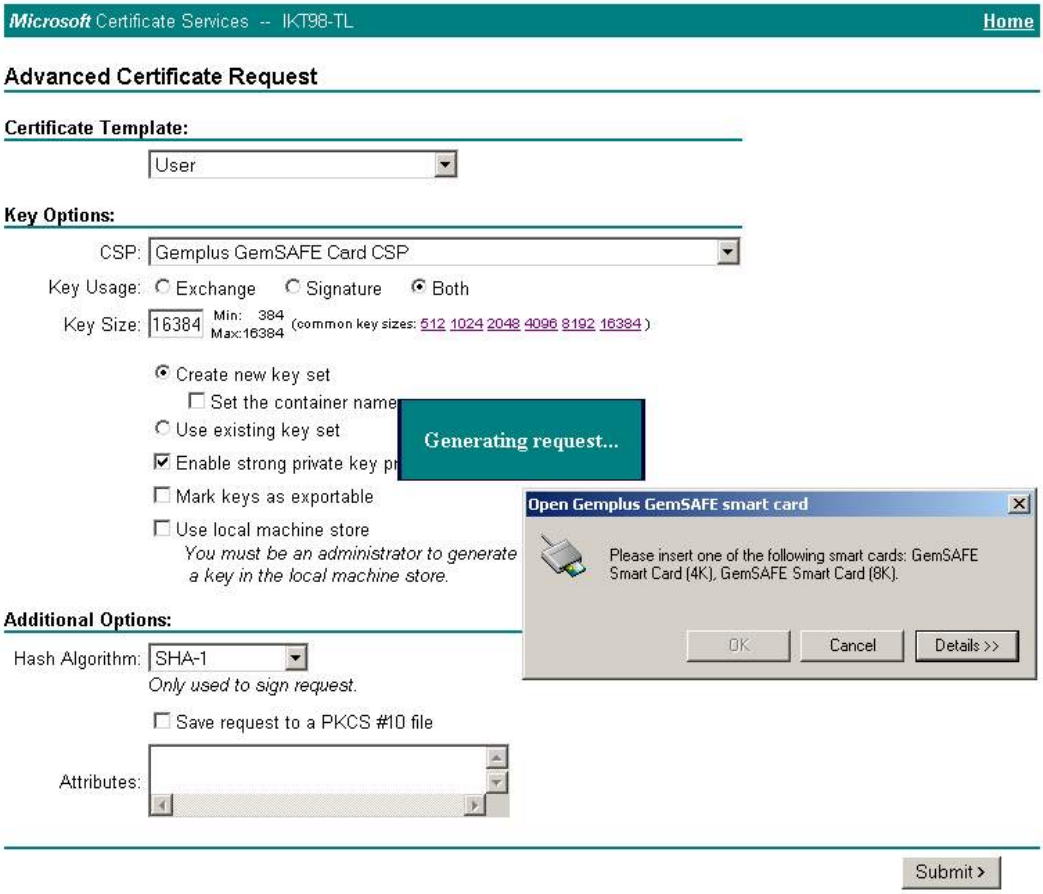
Domenetjeneren har selvfølgelig også et sertifikat, for bla. Utstedelse av sertifikater. Domenetjeneren er en såkalt ”thrusted part”, og dens sertifikat er derfor i enhver brukers liste over sertifiseringsautoriteter. Man kan selvfølgelig også benytte seg av en utenforstående sertifiseringstjeneste, eller en kombinasjon av intern og utenforstående.

6.2.1 Certificate Server og Smartkort?

Ved bruk av smartkort i Windows 2000 må brukerens personlige sertifikat utstedes til et smartkort. Et sertifikat er basert på en mal viss type avhenger av bruksområde. For en vanlig bruker er hovedtypen User, og for smartkort brukere er det Smart Card

Logon og Smart Card User. Alle sertifikat typene er utstedet for klient autentisering, Smart Card User har i tillegg sikker e-post, og User har sikker e-post og EFS i tillegg. I brukermanualen til Gemplus GemSAFE presiseres det at kun sertifikat av typen Smart Card User eller Smart Card Logon kan brukes med smartkort (vedlegg D).

Som diskutert tidligere i rapporten er det litt usikkerhet rundt hvorvidt et smartkort kan brukes sammen med Encrypting File System (EFS). På figur 5-1 ser vi at det lang på vei er mulig å utstede et sertifikat av typen User til et smartkort. Denne typen sertifikat kan brukes sammen med EFS. Det var dessverre ikke mulig for meg å verifisere om dette fungerer, da jeg ikke hadde tilgang til riktig type smartkort i prosjektperioden.

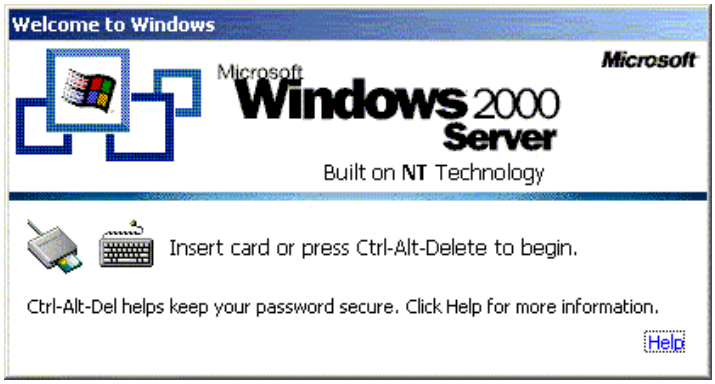


Figur 6-1 Utstedelse av "User" sertifikat til smartkort

6.3 Smart Card Logon

Dette er sannsynligvis den viktigste smartkortfunksjonen i Windows 2000. Smartkortets primæroppgave er å beskytte brukerens private nøkkel, som benyttes til å autentisere brukeren ovenfor Windows 2000, og Kerberos hvis maskinen står i et nettverk. Autentisering ar en svært viktig oppgave fordi det avgjør om en bruker skal få tilgang til systemets ressurser. En annen styrke ved smartkort er at brukeren kan fjerne den private nøkkelen når han ikke lenger bruker maskinen/ressursene.

Smart Card Logon tjenesten starter når en smartkort leser blir installert, og bytter ut den vanlige <Ctrl+Alt+Delete> GINA (Graphical Identification and Authentication) med en for smartkort (figur 5-2).



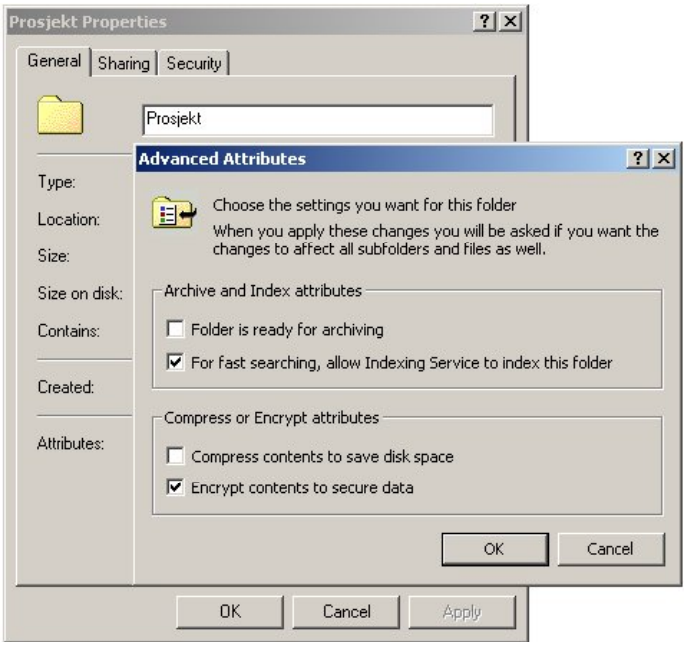
Figur 6-2 Smart Card Logon

Introduksjon av smartkort i Windows 2000, medfører også en overgang til PKI. Dette blir ofte sett på som en stor overgang, og en stor oppgave for systemadministratorene. Microsoft hevder selv at Windows 2000 PKI ikke krever mer vedlikehold, og at administrering vil være svært likt et tilsvarende system uten PKI.

I sammenheng med Smart Card Logon kan det være verdt å nevne hvordan svakhetene til smartkort av og til kommer frem. Windows 2000 kan på samme måte som bla. NT 4.0 låses når maskinen ikke er i bruk. Med smartkort gjøres dette ved å fjerne kortet fra kortleseren. Når man ønsker å låse opp maskinen igjen må brukeren autentiseres på nytt, en operasjon som sjelden tar over et sekund ved bruk av brukernavn og passord. Med smartkort tar denne operasjonen 10-15 sekunder. Liten regne- og overføringskapasitet er årsaken til den lange ventetiden.

6.4 Encrypting File System

Encrypting File System (EFS) er også en del av Windows 2000 PKI, men er ikke implementert med smartkortstøtte i første versjon. Systemets oppbygning tyder på at det er lagt til rette for smartkort, og at det derfor kanskje vil bli implementert i senere versjoner.



Figur 6-3 Kryptering av filer

6.4.1 Eksport av EFS nøkler

Microsoft anbefaler systemadministratorer å fjerne EFS Recovery Agent'ens nøkler fra systemet som har tilgang til de krypterte filene. Nøklene bør helst plasseres på et fysisk sikret sted, da uvedkommende som innehar disse nøklene kan dekryptere alle krypterte filer på systemet.

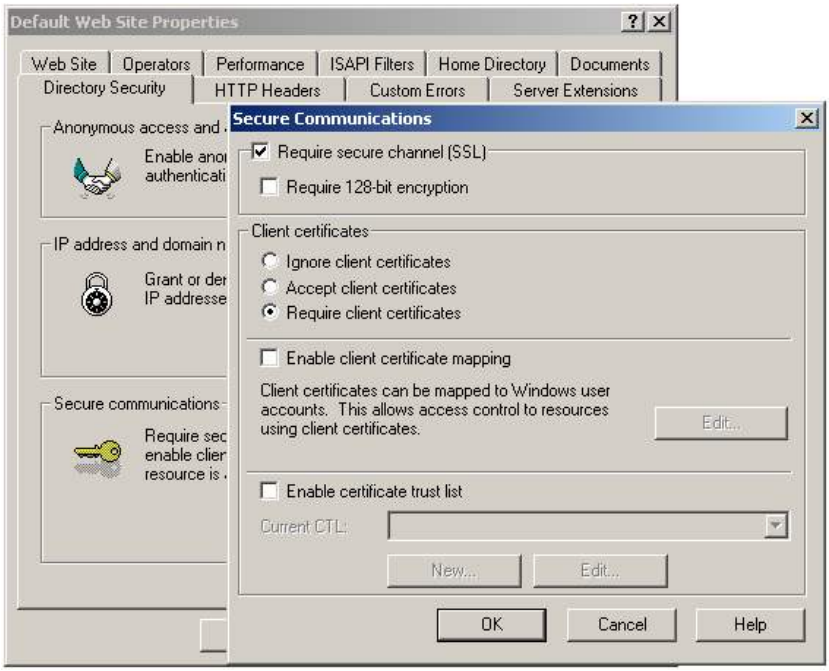
6.5 Internet Information Server og Internet Explorer

For autentisering og sikker overføring av data på Internett benyttes SSL. Denne protokollen er implementert i web-tjener og -klient, som i Windows 2000 er henholdsvis Internet Information Server og Internet Explorer.

6.5.1 Internet Information Server (IIS)

SSL i IIS konfigureres for hver webtjener, f.eks. for websider på port 80 eller alle sider på port 81. Hvilke av sidene som skal bruke SSL konfigureres individuelt. SSL er basert på bruk av sertifikater for autentisering, og vanligvis er det kun webtjeneren som autentiseres. I mitt tilfelle benyttet jeg webtjeneren på domenetjeneren, og denne hadde allerede et sertifikat for autentisering.

Ved konfigurasjon av SSL funksjonene for en webside kan man velge om klienten skal autentiseres, og om den skal koples mot en brukerkonto i Windows 2000 (figur 5-4). Også klienten autentiseres med sertifikat.



Figur 6-4 Konfigurasjon av SSL i IIS

6.5.2 Internet Explorer

Internet Explorer støtter både tjener- og klientautentisering med SSL. Tjeneren vil typisk autentisere seg først, og klienten kontrollerer at tjenerens sertifikat er gyldig og utstedt av en ”thrusted part”. Hvis dette ikke er tilfelle vil brukerne få beskjed om eventuelle feil, og med valg om å fortsette (figur 5-5).

Figur 6-5 Advarsel om ugyldig sertifikat

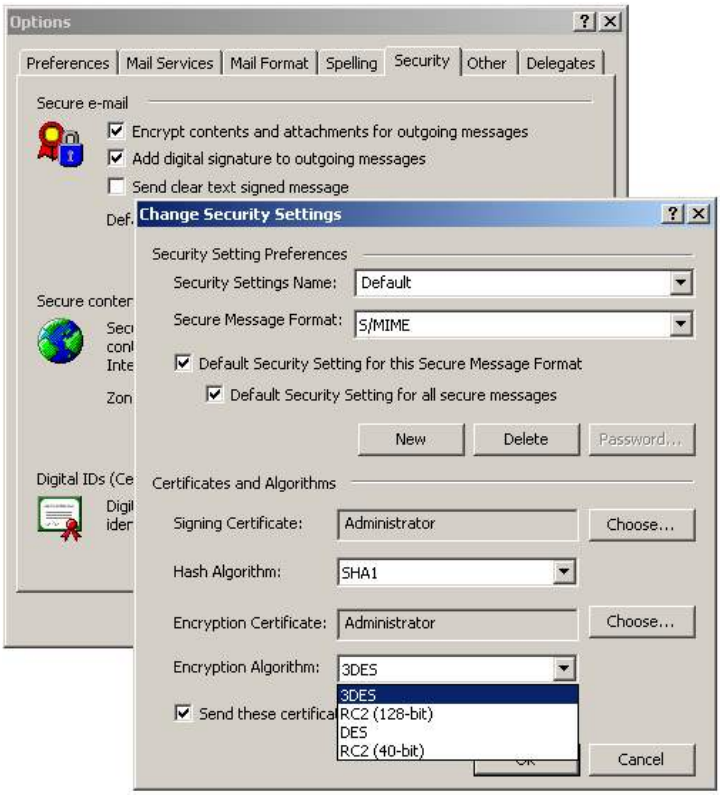
Autentisering av en klient skjer med brukerens personlige sertifikat (figur 5-5), som må være utstedt med funksjon for klientautentisering. En bruker kan ha sitt sertifikat på et smartkort.

Figur 6-6 Klientautentisering med SSL og Internet Explorer

6.6 E-post

E-post klienten som følger med Windows 2000 heter Outlook Express. Jeg har valgt å ikke bruke denne gratis klienten, men heller Microsoft Outlook 2000 som er en del av Office 2000. Begge klientene støtter S/MIME og smartkort.

Bruk av S/MIME til å sende e-post som er kryptert og/eller signert krever et personlig sertifikat. Ved bruk av smartkort blir den digitale signaturen foretatt på kortet, men ikke krypteringen av meldingen. S/MIME kan benytte flere typer signatur, men ved bruk av smartkort i Windows 2000 er det foreløpig kun SHA-1 som er støttet.



Figur 6-7 Konfigurasjon av S/MIME

6.7 Problemer

Ved konfigurasjon av de nevnte mekanismene opplevde jeg lite problemer. Det meste gikk som det skulle bortsett fra noen får ting.

Ved installasjon og konfigurasjon av sertifiseringstjenesten må man oppgi navnet til maskinen tjenesten kjører på, og det ble opplyst om at dette ikke kunne forandres etter at tjenesten var installert. Navnet som skal oppgis er det lokale navnet, og ikke DNS navnet (eks. <tjenernavn>.grm.hia.no). Senere fikk jeg derfor problemer med at ved bruk av noen sertifikater ble det opplyst om at navnet på tjeneren ikke stemte med navnet på sertifikatet. Det var også problemer med å finne utstederen av sertifikatet når navnene ikke stemte overens.

6.8 Manglende funksjonalitet / Konklusjon

Mangelen på smartkort støtte i EFS må regnes som en svakhet. EFS er en kjærkommen funksjon for brukere av bærbare datamaskiner, og da kunne det vært ønskelig at uvedkommende skulle ha størst mulig problemer med å dekryptere data på maskinen. Årsaken til at EFS ikke benyttes sammen med smartkort er i følge Microsoft krav til sømløs behandling av krypterte filer. Et smartkort ville brukt 10-15 sekunder til å dekryptere DESX nøkkelen for hver fil brukeren ønsker å åpne. Slike forsinkelser ville trolig føre til at de aller fleste hadde valgt å ikke kryptere filer utenom i spesielle tilfeller. Noen kunne nok likevel ønske seg en mulighet til å sikre krypterte filer med en nøkkel beskyttet av smartkortet.

7 Konklusjon

Et operativsystem inneholder en mengde sikkerhetsmekanismer. Disse skal dekke typiske operativsystemfunksjoner, og funksjoner som tilbys applikasjonene på operativsystemet. I Windows 2000 er de fleste sikkerhetsmekanismene integrert i en offentlig-nøkkel infrastruktur, Public Key Infrastructure (PKI). Windows 2000 PKI bygger på Internett standarden PKIX, som er basert på digitale sertifikater. I Windows 2000 kombineres PKI, digitale sertifikater og smartkort for å styrke sikkerhetsmekanismene.

Mange av de nye sikkerhetsmekanismene i Windows 2000 brukes til kommunikasjon mot omverdenen. I større grad enn tidligere har Microsoft satset på etablerte standarder fremfor proprietære løsninger. Det sikrer integrering mot produkter fra andre leverandører. Selv om sikkerhetsmekanismene er standardiserte, garanterer heller ikke de total sikkerhet, og de fleste har mindre svakheter.

Smartkortstøtten i Windows 2000 er bygget rundt smartkortets styrker og svakheter. Et smartkortet er velegnet til å beskytte sensitive opplysninger. I Windows 2000 brukes det til å beskytte brukerens personlige kryptografiske nøkkel, som sammen med et digitalt sertifikat autentiserer brukeren mot systemet, i henhold til PKI. Autentisering er en kritisk operasjon i ethvert datasystem, og smartkort styrker denne funksjonen i forhold til bruk av konvensjonelle passord. Smartkortets begrensninger grunner i liten regnekapasitet og lav overføringskapasitet. Det betyr at kortet er uegnet til behandling av store mengder data. I Windows 2000 benyttes smartkort kun til autentisering og digitale signaturer.

Kombinasjonen av nye, forbedrede sikkerhetsmekanismer og erfaringer fra forgjengeren, NT 4.0, borger for at sikkerheten i Windows 2000 er høy. I kombinasjon med smartkort vil den heves ytterligere. Konfigurering og bruk av sikkerhetsmekanismene er gjort brukervennlig slik at selv brukere uten erfaring med sikkerhet kan utnytte sikkerhetspotensialet i operativsystemet.

Selv om Windows 2000 har et generelt høyt sikkerhetsnivå, stilles det krav til brukervennlighet og ytelse i denne typen operativsystem. Og det hører med at alle sikkerhetsmekanismer kan brytes med tilgang på tilstrekkelige ressurser. Man må ha klart for seg hvem man ønsker å beskytte seg mot, og at verdien av beskyttet data er mye mindre en ressursene som kreves for å trenge igjennom sikkerhetsmekanismene.

Når Windows 2000 kommer ut i generelt bruk gjenstår det å se hvor mange som implementerer PKI og smartkort i sin organisasjon. Noen hevder nemlig at smartkortlesere i PC'er snart blir like vanlig som cd-rom spillere.

Litteraturoversikt

T.W. Shinder, D. L. Shinder, D. L. White: Configuring Windows 2000 Server Security. Syngress Media, 2000.

P. A. Holst: Datasikring - Metoder og Prinsipper, Per A. Holst Forlag, 1997, 2. utgave.

U. Hansmann, M. S. Nicklous, T. Schäck, F. Seliger: Smart Card Appøication Development Using Java. Springer-Verlag Berlin Heidelberg, 2000.

Ukjent: Microsoft Windows 2000 Server, Smart Card Logon White Paper, Microsoft. http://www.microsoft.com/security/resources/whitepapers.asp

Ukjent: Microsoft Windows NT Server, Smart Cards White Paper, Microsoft. http://www.microsoft.com/security/resources/whitepapers.asp

Donlund(?): Microsoft Windows NT Server, Windows 2000 Kerberos Authentication White Paper, Microsoft. http://www.microsoft.com/security/resources/whitepapers.asp

Ukjent: Microsoft Windows 2000 Server, An Introduction to the Windows 2000 Public-Key Infrastructure White Paper, Microsoft. http://www.microsoft.com/security/resources/whitepapers.asp

Ukjent: Microsoft Windows 2000 Server, Microsoft Windows 2000 Public-Key Infrastructure White Paper, Microsoft. http://www.microsoft.com/security/resources/whitepapers.asp

Ukjent: Microsoft Windows 2000 Server, Encrypting File system for Windows 2000 White Paper, Microsoft. http://www.microsoft.com/security/resources/whitepapers.asp

Ukjent: Microsoft Windows 2000 Server, SecureNetworking Using Windows 2000 Distributed Security Services White Paper, Microsoft. http://www.microsoft.com/security/resources/whitepapers.asp

M. Russinovich: Inside Encrypting File System. NT Internals, Juni 1999. http://www.winntmag.com

M. Russinovich: Windows NT Security. NT Internals, Mai 1998. http://www.winntmag.com

M. Russinovich: Logon to NT 5.0. Windows 2000 Magazine Online, Mai 1998. http://www.winntmag.com

R. F. Smith: Secure E-Commerce with SmartCards, Windows 2000 Magazine, Oktober 1999. http://www.winntmag.com

T. Zhou: IP Security in Windows 2000. Windows 2000 Magazine Online, Mars 2000. http://www.winntmag.com

J. Lewis, S. Morse: Windows NT Security. http://www.tbg.com , Mars 1998

Z. Ahmad: Kerberos Security in Windows 2000. Windows 2000 Magazine Online, Januar 2000. http://www.winntmag.com

S. Petri, An Introduction to Smartcards. http://www.litronic.com/whitepaper

B. Schneider, A. Shostack: Breaking Up Is Hard to Do: Modeling Security Threats for Smart Cards. Counterpane Internet Security, 2000. http://www.counterpane.com/smart-cars-threats.html

O. Kömmerling, M. G. Kuhn: Design Principles for Tamper-Resistant Smartcard Processor. http://www.cl.cam.ac.uk/~mgl25/sc99-tamper.pdf

D. Wagner, B Schnider: Analysis of the SSL 3.0 protocol. http://counterpane.com/ssl.html

S/MIME and Open PGP, Internet mail consortium. http://www.imc.org/smime-pgpmime.html

Introduction to SSL, Netscape. http://developer.netscape.com/manuals/security/sslin/contents.htm

NIST, CryptoAPI FIPS 140-1 Validation. http://csrc.nist.gov/cryptval/140-1/1401val1999.htm

NSCS, Windows NT C2 Evaluations, http://radium.ncsc.mil

ITSEC, Windows NT E3/F-C2 Evaluations, http://www.itsec.gov.uk

RSA Security. http://www.rsasecurity.com

Microsoft Security Advisor. http://www.microsoft.com/security/tech

Microsoft, http://www.microsoft.com

Schlumberger Cryptoflex. http://cryptoflex.slb.com

Gemplus GemSAFE. http://www.gemsafe.com

Windows for Smart Cards/Windows Powered Smart Cards. http://www.microsoft.com/smartcard

PC/SC Workgroup, http://www.pcscworkgroup.com

OpenCard, http://www.opencard.org

Vedlegg

A Liste over Akronymer

API	Application Programming Interface
ASP	Active Server Pages
CA	Certificate Authority
COM	Component Object Model
CSP	Cryptographic Service Provider
DDF	Data Decryption Field
DNS	Domain Name Server
DRF	Data Recovery Field
EAP	Extensible Authentication Protocol
EFS	Encrypting File System
FEK	File Encryption Key
GINA	Graphical Identification and Authentication
IE	Internet Explorer
IETF	Internett Engineering Task Force
IIS	Internet Information Server
IPSec, IP Security	Internet Protocol Security
KDC	Key Distribution Center
LSASS	Local Security Authority Sub System
MIT	Massachusetts Institute of Technology
MS	Microsoft
OSI	Open Systems Interconnection
PKI	Public Key Infrastructure
PPP	Punkt-til-Punkt Protokoll
RAS	Remote Access Service
RFC	Request For Comments
SAM	Security Accounts Manager
SSL	Secure Socket Layer
S/MIME	Secure Multi
TLS	Transport Layer Security
v3, v5	Versjon 3, versjon 5
Win2k, w2k	Windows 2000
Windows 9x	Windows 95 og 98

B Public Key Infrastructure

Public Key Infrastructure i Windows 2000 støtter standarder (tabell B-1). Hentet fra "An Introduction to the Windows 2000 Public-Key Infrastructure White Paper"

Standard	What it defines	Why it matters
X.509 version 3	Format and content of digital certificates	Without a standard for certificate formats, there's no way to exchange certificates between vendors
CRL version 2	Format and content of certificate revocation lists	Sites need to have a way to interchange revocation information
PKCS family	Format and behavior for public-key exchange and distribution	Allows different vendors' implementations to request and move certificates in a way that all understand.
PKIX	Format and behavior for public-key exchange and distribution	PKIX is an emerging PKI standard that many major vendors and enterprises are adopting in place of the PKCS standards.
SSL version 3	Encryption for web sessions.	SSL is the best-known and most widely used security protocol on the Internet, but it's subject to export controls.
SGC	Provides SSL-like security without export complications	SGC allows full 128-bit security and is exportable for certain uses
IPSec	Encryption for network sessions using the Internet Protocol (IP)	IPSec promises to offer transparent and automatic encryption of network connections.
PKINIT	Emerging standard for using public keys to log on to networks that use the Kerberos authentication protocol	Kerberos identifies users on the network; PKINIT allows Kerberos to use digital certificates on smart cards as credentials.
PC/SC	Standard for interfacing computers to smart cards.	Any vendor's smart cards that adhere to this standard can be used under Windows 2000 without the need for proprietary software

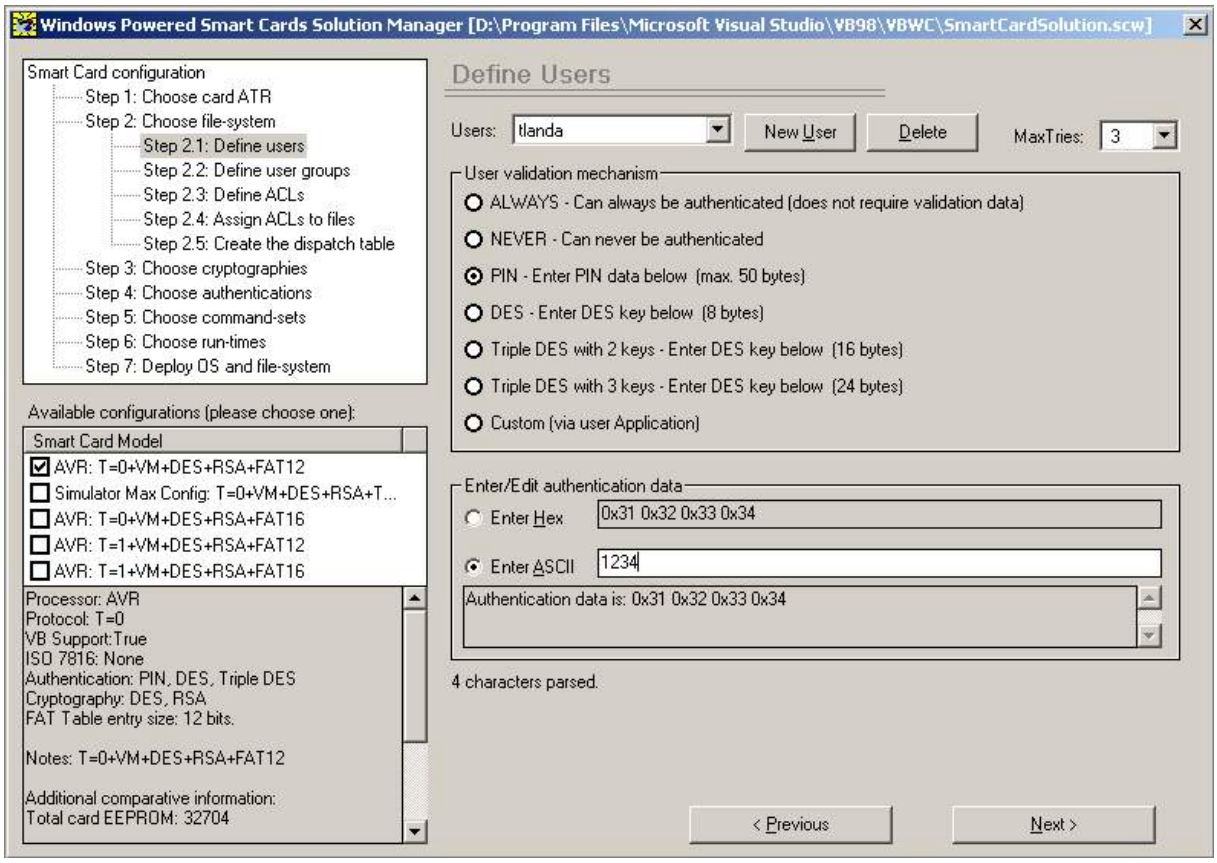
Tabell B-1 Public Key Infrastructure i Windows 2000

C Konfigurasjon av Windows for Smart Cards

Parametere for å bruke Windows Powered Smart Cards i Windows 2000.

- Processor: AVR
- Protocol: T=0
- VB Support:True
- ISO 7816: None
- Authentication: PIN, DES, Triple DES
- Cryptography: DES, RSA
- FAT Table entry size: 12 bits.
- File system size: 27kB

Dvs. velg innstillingen T=0+VM+DES+RSA+FAT12, og forandre fil system størrelsen. Innstillingene gjøres I Solution Manageren (Figur C-1).



Figur C-1 Konfigurasjon av Windows for Smart Cards

D Certificate templates

Følgende maler for sertifikat eksisterer i Windows 2000 (tabell D-1). Tabellen er hentet fra Windows 2000 Server Help.

Certificate Template Name	Certificate Purposes	Issued To People or Computers
Administrator	Code signing, certificate trust list (CTL) signing, encrypting file system (EFS), Secure E-mail, Client Authentication	People
Authenticated session	Client authentication	People
Basic EFS	Encrypting File System	People
Computer	Client authentication, server authentication	Computers
Code Signing	Code signing	People
Domain Controller	Client authentication, server authentication	Computers
EFS Recovery Agent	File recovery	People
Enrollment Agent	Certificate request agent	People
Enrollment Agent (Offline request)	Certificate request agent	People
IPSec (Offline request)	Internet Protocol security	Computers
IPSec	Internet Protocol security	Computers
Router (Offline request)	Client authentication	Computers/routers
Smart Card Logon	Client authentication	People
Smart Card User	Client authentication, secure e-mail	People
Subordinate certification authority	All	Computers
Trust List Signing	Certificate trust list signing	People
User	Encrypting File System, secure e-mail, client authentication	People
User Signature Only	Secure e-mail, client authentication	People
Web Server	Server authentication	Computers

Tabell D-1 Certificate Templates