FFI RAPPORT

INFRASTRUKTUR FOR TILLITSHÅNDTERING I WINDOWS

WINDVIK Ronny, HALLINGSTAD Geir, VETLAND Stein Erik

FFI/RAPPORT-2002/01014

FFIE/780/113

Godkjent
Kjeller 13 March 2002

Torleiv Maseng
Forskningssjef

INFRASTRUKTUR FOR TILLITSHÅNDTERING I WINDOWS

WINDVIK Ronny, HALLINGSTAD Geir, VETLAND Stein Erik

FFI/RAPPORT-2002/01014

FORSVARETS FORSKNINGSINSTITUTT
Norwegian Defence Research Establishment
Postboks 25, 2027 Kjeller, Norge

FORSVARETS FORSKNINGSINSTITUTT (FFI)
Norwegian Defence Research Establishment

P O BOX 25
NO-2027 KJELLER, NORWAY

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE
(when data entered)

REPORT DOCUMENTATION PAGE

1) PUBL/REPORT NUMBER	2) SECURITY CLASSIFICATION	3) NUMBER OF PAGES
FFI/RAPPORT-2002/01014	UNCLASSIFIED	39
1a) PROJECT REFERENCE	**2a) DECLASSIFICATION/DOWNGRADING SCHEDULE**	
FFIE/780/113	-	

4) TITLE

INFRASTRUKTUR FOR TILLITSHÅNDTERING I WINDOWS

PUBLIC KEY INFRASTRUCTURE IN WINDOWS

5) NAMES OF AUTHOR(S) IN FULL (surname first)

WINDVIK Ronny, HALLINGSTAD Geir, VETLAND Stein Erik

6) DISTRIBUTION STATEMENT

Approved for public release. Distribution unlimited. (Offentlig tilgjengelig)

7) INDEXING TERMS

IN ENGLISH:	IN NORWEGIAN:
a) Windows 2000	a) Windows 2000
b) Public Key Infrastructure	b) Offentlig nøkkel-teknologi
c) Security	c) Sikkerhet
d) Trust management	d) Tillithåndtering
e) CA	e) CA

THESAURUS REFERENCE:

8) ABSTRACT

A PKI is viewed by many as a solution that satisfies the security requirements that need to be met by today's computer systems. The main task of a PKI system is to facilitate the establishment of trust between PKI users and other units or users, by verifying public keys stored in digital certificates. A PKI can, e.g., be used as a platform for e-commerce, since it provides support for signing and encrypting of files, email and other data.

Microsoft has implemented a PKI system in their operating systems Windows 2000 and Windows XP. This document describes the general PKI concept, the PKI functionality offered by Windows 2000 and how well these functions are implemented.

Windows 2000 PKI goes a long way towards fulfilling the requirements one expects a PKI system to meet, but some aspects, such as checking of revocation lists, are not satisfactorily implemented.

9) DATE	AUTHORIZED BY	POSITION
13 march 2002	This page only Torleiv Maseng	Director of Research

ISBN-82-464-0591-8

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE
(when data entered)

INNHOLD

INFRASTRUKTUR FOR TILLITSHÅNDTERING I WINDOWS

1 INTRODUKSJON

Offentlig-nøkkel-teknologi er av mange ansett som løsningen på mange av sikkerhets-problemene ved blant annet elektronisk handel. Offentlig-nøkkel-teknologi gir støtte for å kryptere og digitalt signere data. Dette fører til at kun utvalgte brukere kan lese data, og at mottaker av data kan være sikker på at avsender er den hun utgir seg for å være.

Et system består av et sett av enheter (brukere, applikasjoner, datamaskiner), hvor alle kan utveksle informasjon. En infrastruktur som ved hjelp av asymmetrisk kryptografi kan verifisere og autentisere gyldigheten til hver enhet i systemet, kalles Public Key Infrastructure (PKI). I et PKI-system kan A stole på B, hvis A stoler på en enhet som går god for at B er den B hevder å være. På denne måten vil et PKI-system inneholde relasjoner som angir hvem som går god for hvem, og PKI kalles derfor ofte et tillitshierarki.

Det eksisterer mange leverandører av PKI, og vi vil i dette dokumentet se på Microsoft sitt PKI-system. Microsoft har integrert PKI i operativsystemene Windows 2000 og Windows XP, men vi vil kun se på Windows 2000 PKI i dette dokumentet.

Windows 2000 PKI oppfyller langt på vei de kravene det er naturlig å stille til et PKI-system, men enkelte aspekter som sjekking av annulleringslister er ikke tilfredsstillende realisert.

1.1 Formålet med rapporten

Formålet med denne rapporten er å beskrive hva PKI er, hvordan og hvor godt PKI er realisert/implementert av Microsoft i Windows 2000, og hvilken funksjonalitet Windows 2000 PKI kan tilby. Rapporten er skrevet for lesere med middels kjennskap til IKT-systemer.

1.2 Begrensninger

Rapporten vil ikke sammenlikne Windows 2000 PKI og tilhørende løsninger med andre kommersielle PKI-produkter. Rapporten vil heller ikke gå i teknisk detalj for oppsett og vedlikehold av de skisserte egenskapene til Windows 2000 PKI, dette er beskrevet i et eget notat (28).

1.3 Arbeidet

Under vår evaluering av Windows 2000 PKI ble det opprettet en lab med opptil 10 datamaskiner, som skulle simulere nettverket til en liten bedrift med flere brukere. Her ble det satt opp to forskjellige Windows 2000 domener med Active Directory, flere arbeidsstasjoner, flere webtjenere, en e-posttjener (Exchange), flere nivåer av CA-er, nettverkssniffere, overvåkningsverktøy, to rutere, og en switch.

Under arbeidet har vi flere ganger vært i kontakt med Microsoft og andre aktører som tilbyr/benytter/tester Windows 2000 PKI.

1.4 Rapportens oppbygning

Kapittel 2 (Bakgrunn) gir en kort innføring i kryptografi, sertifikater og datasikkerhet.

Kapittel 3 (PKI-konseptet) presenterer hvordan et PKI-system bør være i teorien, og her gjennomgås basistjenestene et PKI-system bør/kan tilby.

Kapittel 4 (Windows 2000 PKI-Realisering) gjennomgår hvordan Windows 2000 PKI har realisert basistjenesten beskrevet i kapittel 3, og hvor god implementasjonen er.

Kapittel 5 (Windows 2000 PKI-Klienter) ser på hvordan operativsystemet Windows 2000 fungerer som en PKI-klient (bruker av PKI), mot et hvilket som helst PKI-produkt.

Kapittel 6 (Totalvurdering) trekker ut de viktigste positive og negative egenskapene til Windows 2000 PKI, og prøver å vurdere disse sett under ett.

Kapittel 7 (Videre arbeid) foreslår en evaluering av PKI i Windows XP, da enkelte ting fra Windows 2000 PKI er endret, og ny funksjonalitet er lagt til.

2 BAKGRUNN

I denne seksjonen gis det en kort innføring i kryptografi, og det beskrives hvordan forskjellige algoritmer, formater og standarder utgjør en plattform for den sikkerheten datasystemer ofte benytter seg av. Først betraktes to forskjellige typer krypteringsalgoritmer og deres egenskaper. Videre sees det på hvordan man kan signere data/meldinger, og hvordan slike signaturer verifiseres av en mottaker. Det beskrives så hva sertifikater er, og hvordan disse benyttes. Til slutt vises det hvordan asymmetrisk kryptografi kan implementere datasikkerhet i forhold til konfidensialitet, integritet, tilgjenglighet og autentisering i et PKI-system.

2.1 Kryptografi

Kunsten og vitenskapen som består i å holde en melding hemmelig kalles kryptografi. En kryptografisk algoritme er den matematiske funksjonen som brukes til kryptering og dekryptering av meldinger (26). En moderne kryptografisk algoritme benytter krypteringsnøkler for å kryptere og dekryptere, og sikkerheten i algoritmen baserer seg på bruken av nøklene. Dette betyr at algoritmen kan publiseres og analyseres, noe som gjerne gir mer tillit til algoritmen. Generelt sett eksisterer det to typer kryptografiske algoritmer. Dette er symmetrisk kryptografi og asymmetrisk kryptografi, som baserer seg henholdsvis på en hemmelig nøkkel og to nøkler med vidt forskjellige bruksområder. Asymmetrisk kryptografi kalles ofte offentlig-nøkkel-kryptografi eller ”public key”-kryptografi.

2.1.1 Symmetrisk kryptografi

Symmetrisk kryptografi benytter samme nøkkel for kryptering og dekryptering. Hvis A ønsker å sende en kryptert melding til B, må A og B på forhånd ha utvekslet nøkkelen på en sikker måte. A og B kan kommunisere sikkert så lenge den symmetriske nøkkelen holdes hemmelig for alle andre.

2.1.2 Asymmetrisk kryptografi

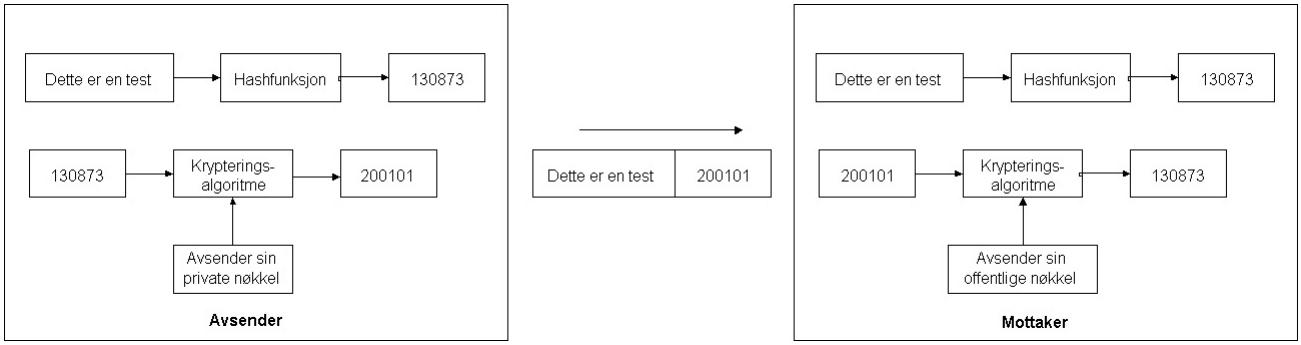
Asymmetrisk kryptografi benytter separate nøkler for kryptering og dekryptering. Disse nøklene kalles henholdsvis offentlig (public) og privat, hvor den offentlige kan publiseres til alle. Alle meldinger kryptert med en offentlige nøkkel kan kun dekrypteres med den tilhørende private nøkkelen og omvendt.

2.1.3 Digital signering

Den private nøkkelen kan også brukes til digitalt å signere en melding. Hvis A krypterer en melding med sin private nøkkel, vil alle med tilgang til den korresponderende offentlige nøkkelen og den krypterte meldingen kunne dekryptere meldingen. De vil samtidig være sikre på at det var A som utstedte meldingen, så sant A har holdt sin private nøkkel hemmelig. En digital signatur bør være en relativt lite plasskrevende komponent hektet til meldingen, som mottaker selv kan velge å verifisere. Den enkle signeringen med private nøkler beskrevet over krever at mottaker må verifisere signaturen (dekryptere) for å kunne lese meldingen.

Den kanskje mest brukte metoden for å digitalt signere meldinger er ved en kombinasjon av asymmetrisk kryptografi og enveis hashfunksjoner. En hashfunksjon konverterer variabel lengde data til en fast lengde data (en verdi). En enveis hashfunksjon har den egenskapen at den virker i en retning. Med dette menes det at det er enkelt å produsere en hashverdi av gitt data, men vanskelig å konstruere data som genererer/hasher til en gitt hashverdi.

Som vist i Figur 2.1, kan meldingen ”Dette er en test” konverteres til verdien 130873 ved hjelp av en hashfunksjon. Verdien 130873 kan nå krypteres med avsenderens private nøkkelen, og for eksempel bli 200101. Denne verdien hektes på meldingen. Mottaker vil i dette tilfelle motta meldingen ”Dette er en test200101”. Mottaker kan verifisere signaturen ved å kjøre meldingen ”Dette er en test” gjennom hashfunksjonen og få verdien 130873, og dekryptere 200101 med avsenders offentlige nøkkel, og få verdien 130873.



Figur 2.1: Digital signering

2.2 Sertifikater

Et sertifikat er i dette dokumentet en person sin offentlige nøkkel signert med en annen person eller organisasjon sin private nøkkel. Den som signerer informasjon går god for informasjonen, og det er vanlig å signere informasjon om personens identitet sammen med den offentlige nøkkelen. Dette betyr at den som signerer samtidig går god for/sertifiserer at informasjonen om personen er korrekt, og at den offentlige nøkkelen tilhører personen. Den som signerte har nå opprettet et sertifikat.

Strukturering og formatering av informasjonen i det signerte sertifikatet bør gjøres via åpne standarder. En mye brukt standard for sertifikater er ITU-T-anbefalingen X.509 (7). Standarden definerer blant annet som vist i Figur 2.2, sertifikatfelter for å angi X.509 versjonsnummer, serienummer, krypteringsalgoritmer, utsteder/signerer, gyldighet i tid, informasjon om eieren, den offentlige nøkkelen, og et felt for den digitale signaturen. Sertifikatstrukturen definert i X.509-standarden benyttes av protokoller som S/MIME (24), IPSec (12), SSL/TLS (25) og SET (27). PKCS #6 sertifikater, som beskrevet i appendiks, er et supersett av X.509-sertifikater, slik at et X.509-sertifikat kan ekstraheres ut fra et PKCS #6 sertifikat (26).

Figur 2.2: Utvalgte felter i et X.509 sertifikat

X.509 standarden er med i X.500 serien av ITU-T anbefalinger for katalogtjenester. En katalog er i denne sammenhengen en eller flere distribuerte datamaskiner som vedlikeholder en database med informasjon om blant annet brukere og datamaskiner, og en katalog vil derfor kunne være et egnet oppbevaringssted for sertifikater.

2.3 Datasikkerhet og asymmetrisk kryptografi

De tre viktigste egenskapene ved datasikkerhet er konfidensialitet, integritet og tilgjenglighet. Konfidensialitet er forhindring av uautorisert avsløring av informasjon, og integritet er forhindring av uautorisert modifikasjon av informasjon. Tilgjengelighet vil si at utstyr og data kan brukes av autoriserte enheter når disse har behov for det (6). Implementering av disse elementene i et system krever autentisering. Autentisering er prosessen for å bevise at en enhet (bruker, applikasjon eller datamaskin) er det som enheten utgir seg for å være.

Asymmetrisk kryptografi gir støtte for konfidensialitet ved hjelp av kryptering, integritet ved hjelp av signering, og baserer seg på at private nøkler er beskyttet og offentlige nøkler er tilgjengelige. Asymmetrisk kryptografi gir støtte for autentisering mellom en klient og en tjener, ved at først tjeneren krypterer tilfeldig valgt data (D) med egen privat nøkkel. Kryptert D sendes over til klienten, som dekrypterer med tjenerens offentlige nøkkel. Klienten krypterer så D med egen privat nøkkel, og sender kryptert D tilbake til tjeneren. Tjeneren dekrypterer med klientens offentlige nøkkel, og hvis den får D, har de autentisert hverandre.

Asymmetrisk kryptografi vil også kunne gi støtte for ikke-fornektelse, hvor en bruker i ettertid ikke kan nekte for at det var hun som utførte en transaksjon. Fornuftig håndtering av ikke-fornektelse krever ofte en tredjepart i systemet som både sender og mottaker stoler på. Tredjeparten kan signere en tidsstemplet transaksjon med egen privat nøkkel, og lagre transaksjonen sammen med tidsstempelet og signaturen. Tredjeparten bør lagre informasjon om transaksjonen.

3 PKI-KONSEPTET

I denne seksjonen presenteres teorien som ligger til grunn for et PKI-system. Hovedoppgaven til et PKI-system er å legge til rette for at PKI-brukere skal kunne etablere tillit til andre enheter eller brukere ved å verifisere offentlige nøkler innpakket i sertifikater. Dette krever en infrastruktur, eller et sett av komponenter, som i samspill kan utføre denne oppgaven på en skikkelig måte.

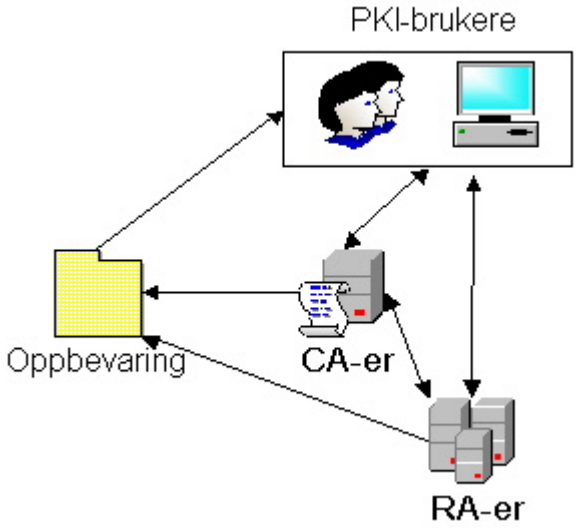
Først introduseres de forskjellige komponentene i et PKI-system, og deres samspill. Videre diskuteres hvordan forskjellige komponenter i systemet kan stole på hverandre ved bruk av sertifikater, og hvordan to brukere tilhørende vidt forskjellige lokasjoner/domener kan stole på hverandre. Deretter presenteres basistjenester som et PKI-system bør/kan implementere, og til slutt et konsept kalt kryssertifisering.

3.1 Public Key Infrastructure

En infrastruktur som legger til rette for at brukere, datamaskiner og applikasjoner skal kunne verifisere offentlige nøkler, refereres til som Public Key Infrastructure (PKI). Komponentene i et PKI-system inkluderer som vist i Figur 3.1 et oppbevaringssted for gyldige og annullerte sertifikater, forskjellige typer og nivåer av Certificate Authorities (CA), en eller flere Registration Authorities (RA), og et sett av PKI-brukere (3). Pilene i figuren illustrerer informasjonsflyten mellom komponentene. For eksempel vil PKI-brukere hente sertifikater og annulleringslister fra oppbevaringsstedet, men oppbevaringsstedet henter ingen informasjon direkte fra PKI-brukerne. Oppgaven til en CA er å utstede sertifikater og annulleringslister, og RA sin oppgave er å verifisere at PKI-brukerne kan få sertifikatene de har spurt om. Dersom man stoler på en CA, betyr det at man stoler på politikken til PKI-systemet, som CA-en er en del av. Politikken inneholder blant annet krav og regler for utstedelse og annullering av sertifikater.

Ved siden av dette har et PKI-system en eller flere nøkkelgeneratorer hos for eksempel PKI-brukerne eller på CA-ene, som genererer nøkkelpar bestående av en offentlig og en privat nøkkel.

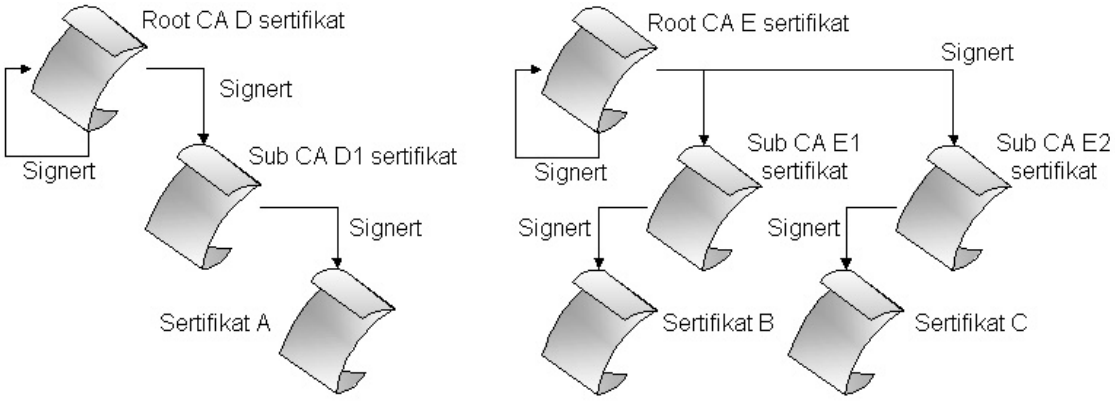
Et viktig krav til et PKI-system er at det håndterer sertifikater og nøkler på en mest mulig sikker, konsis og transparent måte. Hvis PKI-systemet er for vanskelig å bruke, vil det sannsynligvis ikke bli tatt i bruk verken av applikasjoner eller brukere.



Figur 3.1: PKI-arkitekturen

Når en PKI-bruker ønsker å få utstedt et sertifikat, må brukeren først autentisere seg ovenfor RA, som da kan gå god for identiteten til brukeren. RA sørger også for at det kun utstedes sertifikater for oppgaver brukeren er autorisert for. Nøkkelgeneratoren genererer, avhengig av en spesifikasjon, en offentlig og en privat nøkkel, og informasjon om identiteten til enheten, den offentlige nøkkelen og annen relevant informasjon signeres på CA-en med CA-en sin private nøkkel. Den signerte informasjonen og signaturen utgjør et sertifikat, og RA eller CA publiserer sertifikatet til et oppbevaringssted. Denne prosessen krever en sikkerhetsassosiasjon mellom RA og CA.

Valg av PKI-modell i forhold til hvem som stoler på hvem og hvor sertifikater publiseres, har sine fordeler og ulemper (23). En CA signerer et sertifikat som den utsteder med egen privat nøkkel. CA-en sin offentlige nøkkel er innpakket i eget sertifikat, signert av en annen CA eller CA-en selv. På denne måten opprettes kjeder av signerte sertifikater tilhørende forskjellige CA-er, som vist i Figur 3.2**.** En CA som signerer sitt eget sertifikat kalles en root CA, og en CA som har sitt sertifikat signert av en annen CA kalles en sub CA. På toppen av kjeden vil det altså befinne seg et root CA sertifikat, som root CA har signert selv.



Figur 3.2: Kjeder av signerte sertifikater

Når bruker A mottar et sertifikat fra bruker B vil det ikke alltid være slik at A lokalt har sertifikatet til CA-en som signerte sertifikatet til B (Sub CA E1 i Figur 3.2), og at A eksplisitt stoler på denne CA-en. For at A skal kunne stole på og verifisere gyldigheten til sertifikatet til B, må A hente inn en kjede av sertifikater tilhørende CA-er (Root CA-E sertifikatet og Sub CA E1-sertifikatet). Det holder at A stoler på root CA-en i kjeden, for å kunne stole på sertifikatet til B. Hvert sertifikat i kjeden verifiseres ved hjelp av overliggende CA i kjeden sin offentlige nøkkel (14).

Alle sertifikater bør inneholde en referanse til et oppbevaringssted over annullerte sertifikater utstedt av den gitte CA-en. Listen over annullerte sertifikater oppbevares stort sett elektronisk på en datamaskin, og kan hentes ved hjelp av forskjellige protokoller slik som HTTP, FTP og LDAP. Når en PKI-bruker mottar et sertifikat, bør annulleringslisten konsulteres. Det er vanlig å la PKI-systemet lagre/cache annulleringslister lokalt, og benytte disse basert på en gyldighetsperiode. Når gyldighetsperioden går ut, hentes annulleringslisten på nytt fra oppbevaringsstedet. Lokal caching av annulleringslister er fornuftig i forhold til den påkjenning det ville vært for nettverket og datamaskinen med annulleringslisten, hvis listen skulle konsulteres hver gang noen benyttet et sertifikat.

Mange av dagens nettbanker opererer med sertifikater uten referanser til annulleringslister. Det er sertifikatet nettbanken presenterer til din nettleser som ofte ikke innholder en referanse til en annulleringsliste. På denne måten får ikke brukeren sjekket om nettbankens sertifikat er annullert, og hver enkelt bruker må derfor stole på at banken ikke opererer med annullerte sertifikater.

Av frykt for ekstern kompromittering kan det velges å ikke koble root CA-er til nettverket. PKI-brukere vil da ikke kunne få lastet ned root CA-en sin annulleringsliste direkte fra root CA-en, og root CA-en må derfor manuelt publisere sin annulleringsliste i for eksempel en katalogtjeneste på nettverket. Uansett om man velger å koble root CA-en til nettverket eller ikke, må annulleringslisten til root CA alltid være tilgjengelig.

3.2 PKI-basistjenester

Ved siden av CA, RA, og oppbevaringssteder for sertifikater og nøkler, bør PKI-systemer gi støtte for sikkerhetskopiering og gjenoppretting av nøkler, eksportering av private nøkler og

sertifikater, ikke-fornektelse, automatisk oppdatering av nøkkelpar og sertifikater, nøkkelhistorikk, kryssertifisering, nedarvede applikasjoner, og åpne standarder (30).

Problemer kan oppstå når brukere mister sine private nøkler som en konsekvens av for eksempel et glemt passord. Det er i denne sammenhengen viktig med et system for sikkerhetskopiering og gjenoppretning av nøkler, men systemet bør ikke inkludere alle nøkler. Nøkler benyttet for digital signering bør aldri sikkerhetskopieres eller kunne gjenoppettes. Et viktig krav til digital signering er at det kun skal være brukeren som har tilgang til den private nøkkelen. En bedrift kan velge å ta sikkerhetskopier av ansattes private nøkler benyttet til for eksempel filkryptering (konfidensialitet), men bedriften har ingen grunn til å sikkerhetskopiere de private nøklene benyttet til digital signering. Bedriften burde aldri ha behov for å forfalske de ansattes digitale signaturer. Det vil av denne grunn være lurt å opprette sertifikater med forskjellige bruksområder. Et sertifikat vil da for eksempel kunne bli utstedt for å enten gi støtte for integritet (digitale signaturer), konfidensialitet (kryptering av data), ikke-fornektelse eller autentisering. En sikkerhetspolitikk bestemmer hvilke nøkler som skal sikkerhetskopieres, og dermed kunne gjenopprettes av for eksempel administratoren.

Sertifikater utstedes med en tidsbegrenset gyldighet, men det kan i fremtiden likevel oppstå behov for å dekryptere informasjon kryptert med den utgåtte offentlige nøkkelen tilknyttet sertifikatet. Det kan også i fremtiden oppstå behov for å verifisere en digital signatur laget ved hjelp av den utgåtte private nøkkelen. Et PKI-system burde derfor inkludere en oversikt over historien til utgåtte nøkkelpar og sertifikater, og knytte dette til nye/oppdaterte nøkkelpar og sertifikater. Den utgåtte private nøkkelen for digital signering må som nevnt på en sikker måte ødelegges/fjernes ved oppdatering, men den utgåtte private nøkkelen for konfidensialitet bør lagres på en sikker måte av PKI-systemet. Nøkler burde oppdateres automatisk og transparent før de går ut på dato, slik at det alltid er gyldige nøkkelpar og sertifikater tilgjengelig.

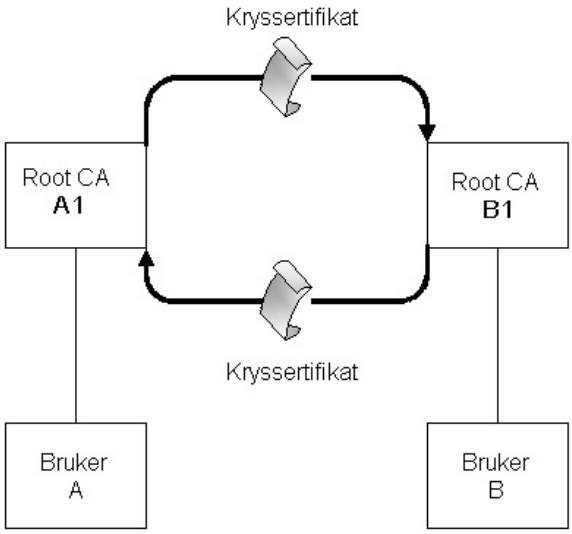
Brukere av et PKI-system bør kunne eksportere sine sertifikater og private nøkler til for eksempel en diskett. Hvis brukeren velger å eksportere sine private nøkler må disse beskyttes på lagringsstedet. Vanligvis krypteres de private nøklene med en symmetrisk krypteringsalgoritme hvor nøkkelen er basert på et valgt passord. Her er det vanlig å benytte PKCS #5, som beskrevet i appendiks C.

Samarbeid mellom forskjellige PKI-systemer og bruken av forskjellige PKI-implementasjoner/ produkter forutsetter bruk av åpne standarder. En annen viktig egenskap er at PKI-systemet bør enkelt kunne integreres i nedarvede/eldre applikasjoner, slik at alle nivåer i datasystemet kan benytte PKI. Disse egenskapene er ofte nødvendige for at PKI-systemet skal være brukbart.

3.3 Kryssertifisering

Kryssertifisering er et konsept benyttet i en tillitsmodell (hvem stoler på hvem og hvordan) kalt Network Trust Model (NTM). I NTM er alle CA-er root CA-er, og de forskjellige root CA-ene stoler på hverandre ved å kryssertifisere. Root CA A1 kan kryssertifisere root CA B1 ved å utstede et kryssertifikat til B1. Alle brukere som stoler på A1 vil etter dette stole på alle brukere og CA-er under B1, men ikke omvendt. Dette kalles en unilateral kryssertifisering, og denne kan settes opp uten at B1 vet noe om den. Det eneste A1 trenger for å kryssertifisere B1 er B1

sitt sertifikat. Det mest vanlige er kanskje bilateral kryssertifisering, hvor også B1 utsteder et kryssertifikat til A1, som vist i Figur 3.3. Hvis root CA C1 tidligere hadde kryssertifisert A1, vil nå brukere under C1 stole på brukere under B1. Et problem med NTM er kjennskapet til hvem som har kryssertifisert hvem. Dette krever en global katalog med oversikt over kryss-sertifiseringene. Hvis realiseringen av en slik global katalog er vanskelig, må eventuelt hver datamaskin/bruker lokalt ha lagret listen over kryssertifiseringer.



Figur 3.3: Bilateral kryssertifisering

4 WINDOWS 2000 PKI-REALISERING

I denne seksjonen blir det presentert hvordan Microsoft har valgt å realisere sitt PKI-system i Windows 2000. Klientdelen av PKI-systemet vurderes i neste seksjon.

Først gis en presentasjon av Windows 2000 sin realisering av katalogtjenere og domenekontrollere i et domene. Videre presenteres de forskjellige typene Windows 2000 CA-er, og Microsofts realisering av RA-rollen. Windows 2000 PKI opererer som de fleste andre PKI-systemer med sertifikater, så den påfølgende seksjonen ser på utstedelse og publisering av sertifikater og annulleringslister. Det sees så på hvordan en administrator kan sikkerhetskopiere Windows 2000 CA-er, mangelen av tjenesten ikke-fornektelse, håndteringen av kryssertifisering, og til slutt tilleggskomponenten Key Management Service (KMS). KMS støtter blant annet sentral generering av nøkler og automatisk utstedelse av sertifikater til brukere, men kun for e-post.

4.1 Katalogtjenere og domenekontrollere

Windows 2000 PKI er sterkt knyttet til Windows 2000 domener, som inneholder en eller flere katalogtjenere. En katalogtjener har som oppgave å oppbevare informasjon om brukere, tjenester, applikasjoner og datamaskiner i domenet på en strukturert måte. Katalogtjenesten i Windows 2000 er X.500-basert (ITU-T anbefalinger for katalogtjenester) og kalles Active

Directory (AD). AD brukes blant annet av CA-er i domenet til å oppbevare sertifikater.

Microsoft har i Windows 2000 delvis gått bort fra begrepet domenekontroller, som ble brukt i Windows NT domener. I Windows 2000 domener benyttes AD, som inneholder en finkornet politikk for hvem som kan gjøre hva i domenet. Datamaskinen med AD inneholder også funksjonalitet for å opprettholde politikken og utføre oppgavene Windows NT domene-kontrollere utfører. Oppgavene Windows NT domenkontrollere utfører er beskrevet i (29). For dette dokumentet antar vi at oppgavene til Windows NT domenekontrollere er blitt migrert inn i AD-serveren i Windows 2000 domener.

4.2 Windows 2000 CA-er og RA-er

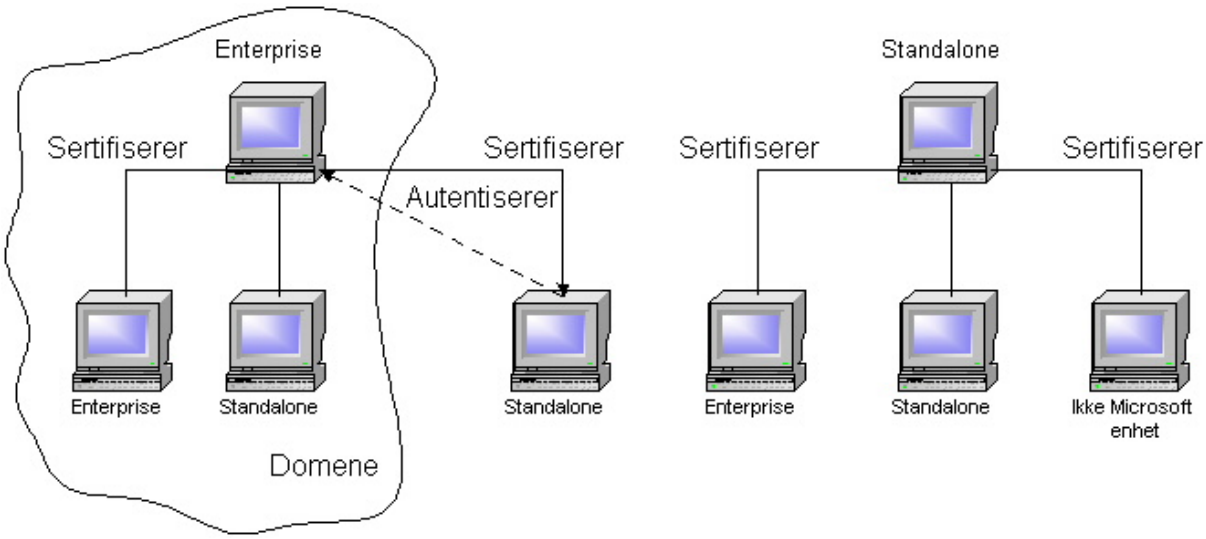
I denne seksjonen blir det presentert hvordan Windows 2000 realiserer CA- og RA-rollene, som beskrevet tidligere i dokumentet. Seksjonen beskriver også hvordan de forskjellige CA-ene håndterer sertifikater og annulleringslister, samt hvordan en administrator kan sikkerhetskopiere en CA.

4.2.1 Windows 2000 Enterprise CA-er og Standalone CA-er

Windows 2000 PKI opererer med to forskjellige klasser av CA-er, kalt Enterprise og Standalone CA-er. En Enterprise CA har som oppgave å automatisk utstede sertifikater til brukere og datamaskiner som tilhører et Windows 2000 domene, og baserer utstedelsene av sertifikater på politikken i domenet. For eksempel kan domeneadministratoren angi i politikken at alle brukere i domenet skal kunne få utstedt sertifikater for kryptering av e-post.

En Standalone CA har som oppgave å utstede sertifikater til brukere og datamaskiner uten å være styrt av en politikk i et domene. For eksempel vil en Standalone CA kunne utstede sertifikater til kunder tilhørende andre domener.

Enterprise og Standalone CA-er kan i Windows 2000 PKI være av typen root eller subordinate. En root CA signerer sitt eget sertifikat, mens en subordinate CA har sitt sertifikat signert av en annen CA, og da enten en root CA eller en subordinate CA. Det at A sertifiserer B, betyr i dette dokumentet at A usteder et sertifikat til B. Som vist i Figur 4.1, kan en Enterprise CA sertifisere både andre Enterprise CA-er og Standalone CA-er. En Standalone CA kan også sertifisere andre Enterprise CA-er og andre Standalone CA-er. En Standalone CA må kunne autentisere seg ovenfor en Enterprise CA, for å kunne bli sertifisert av Enterprise CA-en. Hvis datamaskinen Standalone CA-en kjøres på er medlem i domenet er den allerede autentisert, og vil automatisk kunne bli sertifisert av Enterprise CA-en. Siden Enterprise CA-er kun kan utstede sertifikater automatisk, vil ikke Standalone CA-er, uten mulighet for å bli automatisk autentisert (ikke medlem i domenet), kunne bli sertifisert av Enterprise CA-er.



Figur 4.1: Sertifisering av CA-er

Siden Standalone CA-er kan utstede sertifikater til alle enheter, selv til ikke-Microsoft enheter, slik som CA-er fra andre leverandører, er disse kanskje mer passende som root CA-er (5). Siden en Enterprise CA alltid må være tilkoblet nettverket på grunn av den tette integrasjonen med AD, må det benyttes en Standalone root CA hvis man ønsker en root CA frakoblet (offline) nettverket. En Standalone CA har ikke behov for å direkte autentisere over nettverket når noen ønsker å få utstedt et sertifikat.

Enterprise CA-er gir ikke støtte for manuell godkjenning av sertifikatforespørsler. Dette betyr at sertifikater alltid utstedes automatisk av Enterprise CA-er, så sant politikken tillater dette, og det ikke er mulig å skru av den automatiske utstedelsesprosessen. For Standalone CA-er legges alle forespørsler om utstedelse av sertifikater i en såkalt pending/venteliste (1). En autorisert bruker vil manuelt måtte godkjenne utstedelsene av sertifikatene fra en Standalone CA.

Windows 2000 støtter automatisk utstedelse av sertifikater til nye datamaskiner i domenet, men det støtter ikke automatisk utstedelse av sertifikater til nye brukere i domenet. Dette fører til at hver bruker i domenet eksplisitt må spørre om å få et sertifikat utstedt manuelt. For automatisk utstedelse av sertifikater til brukere for sikker e-post, kan eventuelt tilleggskomponenten Key Management Service (KMS) installeres. Se kapittel 4.5 for mer om KMS.

4.2.2 Windows 2000 RA-er

En Enterprise CA vil ved forespørsel om utstedelse av et sertifikat sjekke politikken i domenet, for å finne ut om brukeren eller datamaskinen har rettigheter til å få utstedt et slikt sertifikat. Hver bruker og datamaskin er på forhånd autentisert i domenet, og på denne måten er RA-rollen dekket av samarbeidet mellom Enterprise CA-en, domenepolitikken lagret i AD og funksjonaliteten rundt autentisering i domenet. Microsoft har med dette som bakgrunn valgt å ikke eksplisitt skille CA- og RA-rollene i sin realisering av PKI.

4.2.3 Håndtering av sertifikater og annulleringslister

Windows 2000 CA-er utsteder forskjellige sertifikater med et sett av forskjellige bruksområder.

De forskjellige bruksområdene inkluderer blant annet signering og kryptering av e-post (sikker e-post), kryptering av filer, gjenvinning av krypterte filer, autentisering av klienter og tjenere, utstedelse av sertifikater, signering av filer og nettverksnivåsikkerhet (IPSec). Windows 2000 kommer med et sett av forhåndsdefinerte sertifikatmaler, med forskjellige sett av bruksområder. Et eksempel er sertifikatmalen User som inkluderer bruksområdene kryptering av filer, kryptering og signering av e-post og autentisering av klienter. En innehaver av et sertifikat basert på sertifikatmalen User, vil dermed kunne bruke sertifikatet for de gitte bruksområdene.

Det er ikke mulig å opprette egne sertifikatmaler, og bruksområdene til de forhåndsdefinerte sertifikatmalene kan heller ikke reduseres. Det kunne for eksempel vært nyttig å kunne redusere bruksområdene for User sertifikatmalen til kun signering for alle brukere i domenet, unntatt de som er medlem i administratorgruppen.

Domeneadministratoren kan i domenepolitikken angi hvilke brukere som skal få utstedt hvilke sertifikater basert på de gitte sertifikatmalene. På hver CA angis det hvilke sertifikatmaler CA-en skal få utstede sertifikater etter, og på denne måten vil domeneadministratoren kunne ha finkornet kontroll med bruken av sertifikater i domenet.

Utstedte sertifikater publiseres automatisk i AD av Enterprise CA-er. Hvert sertifikat følger X.509 standarden, og har en referanse til publiseringsstedet for annulleringslisten for sertifikater utstedt av den gitte CA-en. Annulleringslisten kalles Certificate Revocation List (CRL), og publiseringsstedet for CRL-en kalles CRL Distribution Point (CDP). Sertifikatene inneholder også en referanse til informasjon om CA-en (CA sertifikatet) som kalles Authority Information Access (AIA). CDP og AIA vil for Windows 2000 PKI typisk være i AD og på en webside.

En CA sin CRL kan lastes ned fra CDP ved hjelp av protokollene FTP, HTTP eller LDAP. CRL-er inneholder en liste over serienummerene på alle annullerte sertifikater utstedt av den gitte CA-en, og listen er digitalt signert med CA-en sin private nøkkel. Enterprise CA-er kan hyppigst settes til å automatisk publisere sin CRL en gang per time, og utenom dette kan administratoren eksplisitt publisere CRL-en når som helst. En CRL inneholder også informasjon om neste automatiske publisering. En Standalone CA kan publisere sin CRL lokalt eller i AD, sistnevnte er det mest fornuftige hvis Standalone CA-en ikke er tilknyttet nettverket. En CRL fra en offline CA må periodisk eksporteres til for eksempel en diskett, og manuelt importeres inn i korresponderende CDP. CDP-en kan for eksempel være et objekt i AD.

Når en Windows 2000 CA utsteder et sertifikat, vil gyldighetsperioden for det utstedte sertifikatet alltid være kortere enn sertifikatet den utstedende CA-en benyttet i utstedelsen (signeringen). For eksempel vil sertifikater utstedt til brukere (brukersertifikater) vanligvis ha en gyldighet på ett år, men dersom CA-en sitt sertifikat utgår før dette, vil brukersertifikatene bli utstedt med en gyldighetsperiode som er tilsvarende redusert. På denne måten vil man aldri komme opp i en situasjon hvor et sertifikat ikke kan verifiseres på grunn av at root CA-sertifikatet har utgått på dato. CA-er må derfor fornye sine sertifikater, og det nye sertifikatet vil få de samme egenskapene som det gamle sertifikatet, men da selvsagt med en ny gyldighetsperiode. Windows 2000 CA-er tillater fornying av sertifikater med nytt eller gammelt nøkkelpar.

4.2.4 Sikkerhetskopiering av Windows 2000 CA-er

Enhver Windows 2000 CA kan sikkerhetskopieres til for eksempel en diskett, og informasjonen kan på et senere tidspunkt importeres tilbake i CA-en. En sikkerhetskopi kan inkludere CA-en sine private nøkler, CA-en sine egne sertifikater, konfigurasjonsinformasjon, logg over utstedte sertifikater og sertifikater som er under behandling for utstedelse (Standalone CA-er). Sensitiv data i sikkerhetskopien krypteres basert på et valgt passord, og det gis støtte for inkrementell sikkerhetskopiering.

Ved siden av dette kan en administrator når som helst velge å eksportere en CA sine egne sertifikater (har den private nøkkelen) og alle utstedte sertifikater. Den korresponderende private nøkkelen til egne sertifikater, kan også eksporteres.

4.3 Ikke-fornektelse

Standard Windows 2000 PKI gir ikke støtte for ikke-fornektelse annet enn ved at avsender digitalt signerer data. Det er ikke implementert automatisk støtte for en tredjepart som kan signere tidsstemplede transaksjoner mellom en sender og mottaker.

4.4 Kryssertifisering

Kryssertifisering er noe som utføres mellom root CA-er, slik at det kan opprettes et nettverk av root CA-er som direkte eller indirekte stoler på hverandre. Et av problemene med kryssertifisering er at kryssertifikater må oppbevares globalt tilgjengelig for alle brukere. Når bruker A under root CA A1 mottar et sertifikat fra bruker B under root CA B1, vil A kunne stole på dette sertifikatet hvis root CA A1 har kryssertifisert root CA B1, som vist tidligere i Figur 3.3. Bruker A må i dette tilfellet kunne laste ned kryssertifikatet fra for eksempel root CA A1.

Windows 2000 gir støtte for å etablere tillit mellom flere hierarkier av CA-er, men benytter ikke kryssertifisering. Operativsystemet Windows 2000 opererer for hver bruker og datamaskin med en liste over root CA-sertifikater man stoler på, kalt Trusted Root Certification Authorities Store. Denne listen er sammensatt av root CA-sertifikater som brukeren, datamaskinen og domenet stoler på. Når et gitt root CA-sertifikat legges inn i listen på domenenivå, vil dette være ekvivalent med at eget domene kryssertifiserer den aktuelle root CA-en, men det utstedes ikke noe kryssertifikat.

Den sammensatte listen med root CA-sertifkater er Microsoft sitt alternativ til kryssertifisering (19). Windows 2000 kan prosessere kryssertifikater, og benytte dem i avgjørelsen om man kan stole på mottatt sertifikat. Microsoft mener selv at kryssertifikater er unødvendige i deres tillitsmodell, og har bevisst unngått bruken av kryssertifisering grunnet blant annet mye administrativt arbeid med utstedelse og vedlikehold av kryssertifikatene.

4.5 Key Management Service

Med Microsoft Exchange 2000 (e-posttjener) kommer det en komponent som heter Key Management Service (KMS). Når tjenesten installeres, inntar den en rolle som RA (verifiserer

at PKI-brukerne kan få sertifikatene de har spurt om) for en CA, men kun for forespørsler som har med e-post i domenet å gjøre.

Med KMS er det mulig å automatisk utstede sertifikater til mange brukere samtidig, noe som gjøres med sentral nøkkelgenerering. Ved en slik utstedelse vil KMS generere to nøkkelpar, ett for signering og ett for kryptering, og det utstedes to sertifikater med tilsvarende bruksområder. KMS vil deretter ta en sikkerhetskopi av nøkkelparet for kryptering før begge nøkkelpar blir overført til klienten. KMS-administratorene kan med andre ord gjenvinne kryptert e-post dersom KMS brukes.

Når brukere er lagt inn i KMS, vil man ved verifisering av en signatur eller ved kryptering av e-post, ta kontakt med KMS for å få det riktige sertifikatet. KMS vil med andre ord også fungere som en katalogtjener (AD) i dette tilfellet.

5 WINDOWS 2000 PKI-KLIENTER

Denne seksjonen ser kun på klientdelen av Windows 2000 PKI. En Windows 2000 klient betyr her en bruker, applikasjon eller datamaskin på/med et Windows 2000 operativsystem. En Windows 2000 klient kan benytte andre CA-er enn Windows 2000, da Windows 2000 PKI støtter de fleste standarder som vanligvis blir benyttet i andre PKI-systemer (20).

En Windows 2000 klient kan generelt sett be en CA om å få utstedt et nytt sertifikat, fornye et eksisterende sertifikat, beskytte sine private nøkler mot lokale applikasjoner, modifisere bruksområdet på sertifikater, kontrollere hvilke sertifikater brukeren stoler på, eksportere og importere sertifikater, og laste ned annulleringslister tilhørende sertifikater.

I denne seksjonen sees det først på de kryptografiske tjenestene på Windows 2000 klienter, og hvordan klienten utfører sertifikatforespørsler. Det presenteres så hvordan klienten håndterer nøkler og sertifikater, med henblikk på lagring og oppdatering. Videre sees det på hvordan klienten håndterer annulleringslister tilhørende sertifikater, noe som kanskje er det som er mest kritikkverdig med Windows 2000 PKI. Det gis til slutt en presentasjon over hvordan klientene kan benytte sikker e-post, sikker webtrafikk, beskytte nettverkstrafikk, kryptere filer, og signere kode.

5.1 Kryptografiske tjenester

Windows 2000 opererer med såkalte Cryptographic Service Providers (CSP), som er moduler/software som utfører kryptografiske oppgaver. De kryptografiske oppgavene inkluderer blant annet å generere nøkkelpar, lagre nøklene, beskytte den private nøkkelen ved eksportering, kryptere og dekryptere. Disse modulene er i utgangspunktet software men kan også benytte seg av hardwarebaserte krypteringsenheter som smartkort. Windows 2000 klienter kan fritt fjerne eller installere nye CSP-er. En gitt CSP kan for eksempel gi støtte for andre krypteringsalgoritmer enn en annen CSP, og kanskje tilby lengre krypteringsnøkler.

Applikasjoner vil ha tilgang til CSP-ene via et grensesnitt kalt CryptoAPI. Egenutviklede applikasjoner kan også benytte CryptoAPI, og kryptografiske tjenester kan integreres på denne

måten inn i nye og eldre applikasjoner.

5.2 Sertifikatforespørsler

Når en bruker på en Windows 2000 datamaskin (uten bruk av KMS) ønsker å få utstedt et sertifikat, vil lokal valgt kryptografisk tjener (CSP) generere et nøkkelpar. Den offentlige nøkkelen pakkes etter PKCS #10-formatet sammen med annen informasjon, slik som for eksempel ønsket publiseringssted, og sendes til angitt CA. Etter en stund vil brukeren motta et signert sertifikat, eller en feilmelding om at utstedelsen ikke lot seg gjøre.

Ved bruk av Key Management Service (kun for e-post) genereres nøklene sentralt hos KMS, og utvalgte brukere får tildelt sertifikater automatisk.

5.3 Håndtering av nøkler og sertifikater

I denne seksjonen beskrives det hvordan Windows 2000 klienter håndterer nøkler og sertifikater. Først sees det på hvordan offentlige og private nøkler lagres, etterfulgt av hvordan sertifikater tilhørende forskjellige enheter oppbevares i forskjellige lister. Til slutt i seksjonen beskrives hvordan personlige sertifikater og nøkler oppdateres.

5.3.1 Lagring av nøkler

Mekanismene for å lagre en brukers og datamaskins nøkler, avhenger av valgt kryptografisk tjeneste (CSP). Basis-CSP-ene som kommer med Windows 2000 lagrer nøklene i en kryptert form i software (16) (2). Vanligvis er en privat nøkkel tilhørende en bruker lagret kryptert i en fil i brukerens profil, og filen vil være beskyttet (lese/skrive) av filsystemet i Windows 2000 (5). Andre CSP-er kan lagre de private nøklene på andre måter, for eksempel vil CSP-ene for smartkort kunne lagre nøklene på smartkortet.

Når en applikasjon ønsker å benytte en privat nøkkel, vil CSP-en returnere denne i klartekst. CSP-ene gjør i utgangspunktet ingenting for å beskytte den returnerte private nøkkelen, slik at applikasjonene må selv sørge for at den private nøkkelen ikke blir lagret ukryptert (18).

CSP-ene kontrollerer også om den private nøkkelen kan eksporteres, og den kan settes opp til å varsle brukeren når en applikasjon ønsker å benytte den private nøkkelen. Disse beskyttelsesmekanismene er transparent for applikasjonene, som kun refererer til nøkkelpar med en referanse som er unik i forhold til gitt CSP.

Når en applikasjon benytter en CSP til å generere et nøkkelpar, kan brukeren/applikasjonen velge å ekstrabeskytte den private nøkkelen. En privat nøkkel kan krypteres basert på en nøkkel (K), derivert ut i fra en hovednøkkel (HK). Hver bruker har sin HK lagret i egen profil, og HK byttes hver tredje måned. HK er kryptert av en nøkkel (B) basert på blant annet brukerens innloggingspassord (22). Når Windows 2000 bytter en brukers HK, vil Windows 2000 ta vare på den gamle HK-en, ved å kryptere den gamle HK-en med den nye HK-en. Denne ekstrabeskyttelsen kan settes opp i to nivåer, medium og sterk.

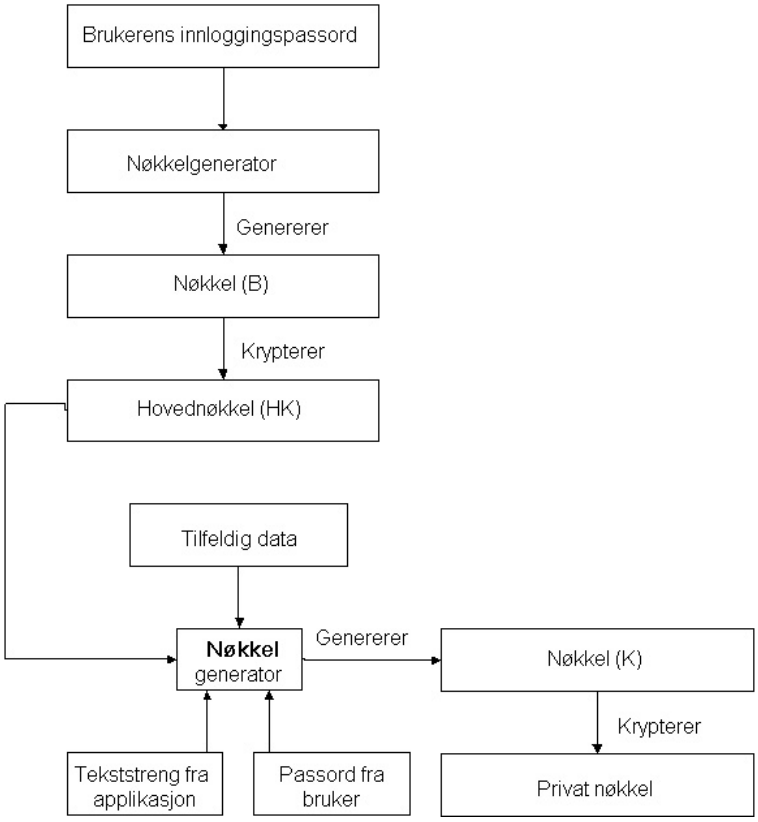
Medium ekstrabeskyttelse av en privat nøkkel, innebærer at brukeren får beskjed (dialogboks)

hver gang en applikasjon ønsker å benytte den private nøkkelen. Som nevnt over vil også CSP-er tilby dette, men da er ikke den private nøkkelen ekstrabeskyttet. Varslingen beskytter en bruker sine private nøkler fra ondsinnede applikasjoner (for eksempel virus). Nøkkelen K benyttet til å kryptere den private nøkkelen er her basert på HK.

Sterk ekstrabeskyttelse av en privat nøkkel innebærer at den private nøkkelen i tillegg krypteres basert på et brukervalgt passord per private nøkkel. Dette fører til at brukeren må taste inn et passord hver gang en applikasjon har behov for den gitte private nøkkelen. Dette gir også god kontroll for når applikasjoner ønsker å benytte de private nøklene. Nøkkelen K er her basert på HK og brukervalgt passord.

Applikasjoner kan beskytte sine private nøkler fra andre applikasjoner brukeren kjører. Dette gjøres ved å i tillegg basere nøkkelen K på en tekststreng (22). Denne tekststrengen skal da kun applikasjonen vite om, og den sendes med ved kryptering og dekryptering.

Nøkkelen K benyttet til å kryptere en privat nøkkel baseres derfor på brukerens HK, et brukervalgt passord (valgfritt), og en applikasjonsvalgt tekststreng (valgfritt), som vist i Figur 5.1. I tillegg baseres K på tilfeldig data, som lagres i klartekst ved siden av den krypterte private nøkkelen (brukes til salt).



Figur 5.1: Ekstrabeskyttelse av private nøkler

Selv om HK-en er kryptert med B, som er derivert av brukerens innloggingspassord, betyr ikke dette at en bruker mister de ekstrabeskyttede private nøklene, hvis et nytt innloggingspassord settes av lokal- eller domeneadministrator. Windows 2000 sin rutine for endring av passord sørger for at HK-en blir kryptert med den nye nøkkelen B, basert på det nye passordet. Våre tester viser at en lokal bruker vil miste de ekstrabeskyttede nøklene hvis brukerens passord

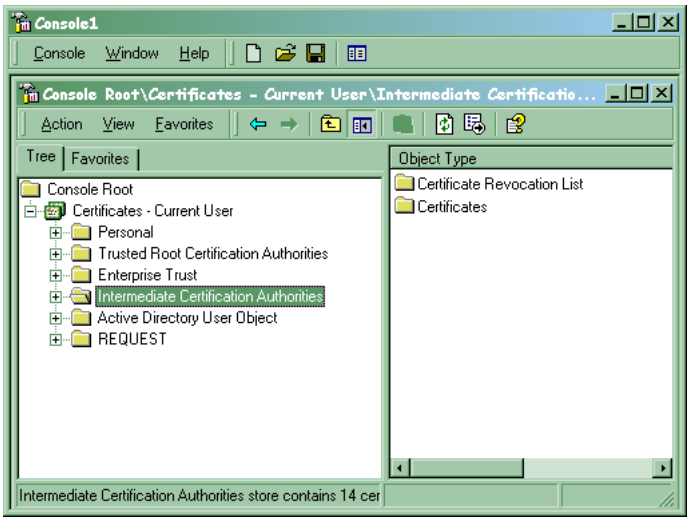
endres på lokal datamaskin utenfor Windows 2000 (passordfilen til Windows 2000 overskrives av et annet operativsystem (8)). I et domene er brukerens HK kryptert med AD sin offentlige nøkkel, slik at AD kan gjenvinne HK-en (22).

En brukers profil ligger lagret på hver enkelt datamaskin, noe som betyr at de private nøklene ikke er tilgjengelige hvis brukeren bytter datamaskin. En bruker sine offentlige nøkler er pakket inn i sertifikater som blant annet også er lagret i brukerens profil. Funksjonelt sett vil det derfor lønne seg å lagre brukeres profiler på en filtjener, og laste den enkelte brukers profil med private og offentlige nøkler ned på den gitte datamaskinen etter godkjent autentisering (roaming profiles). På denne måten vil man også kunne sikkerhetskopiere hver bruker sine krypterte private og offentlige nøkler.

For å redusere sannsynligheten for tap av private nøkler, kan det lønne seg å eksportere sine private nøkler til for eksempel en diskett, og kryptert med en nøkkel basert på et brukervalgt passord. Dette er nyttig hvis for eksempel brukerens profil går tapt.

5.3.2 Lokal lagring av sertifikater

Operativsystemet Windows 2000 opererer for hver bruker og datamaskin med flere oppbevaringssteder/lister for sertifikater lokalt, kalt stores. De forskjellige stores er Personal, Trusted Root Certification Authorities, Enterprise Trust, Intermediate Certification Authorities, Active Directory User Object og Request, som vist i Figur 5.2.



Figur 5.2: Lokal lagring av sertifikater

Sertifikater plassert i Personal-listen er sertifikater man har korresponderende private nøkler for, og både brukere og datamaskiner oppbevarer sine personlige sertifikater her.

Listen Trusted Root Certification Authorities lagrer sertifikater til root CA-er man eksplisitt velger å stole på. I utgangspunktet inneholder denne omtrent 100 sertifikater til eksterne CA-er, og utvides med root CA-er i domenet når disse tas i bruk av brukeren.

I listen Enterprise Trust kan brukeren velge å opprette såkalte Certificate Trust Lists (CTL). En CTL inneholder root CA-sertifikater med egendefinerte restriksjoner for bruk. En bruker kan for eksempel velge å stole på root CA A, B og C sine sertifikater for kun signering, selv om de i

utgangspunktet var utstedt for signering, kryptering og autentisering.

Listen Intermediate Certification Authorities inneholder sertifikater utstedt til andre mennesker/brukere og andre CA-er enn de i listen Trusted Root Certification Authorities. Denne inneholder i utgangspunktet 12 sertifikater, hvor noen er root CA-sertifikater og andre er subordinate CA-sertifikater. Listen inneholder blant annet et sertifikat fra Microsoft, som skal benyttes av Windows 2000 til å verifisere signerte drivere. Dette sertifikatet er signert av en root CA hos Microsoft, og root CA-en sitt sertifikat ligger i listen Trusted Root Certification Authorities. Når det opprettes en subordinate Enterprise CA i domenet, legges sertifikatet dens automatisk inn via AD i listen Intermediate Certification Authorities på alle datamaskiner i domenet. Når en bruker i domenet blir utpekt som en gjenvinningsagent for kryptert data, blir dette sertifikatet også lagt inn i listen Intermediate Certification Authorities. Intermediate Certification Authorities store inneholder også en katalog med annulleringslister, kalt Certificate Revocation List. Når en bruker manuelt installerer en annulleringsliste, blir den automatisk lagt inn i denne katalogen.

Sertifikater assosiert med brukere og datamaskiner kan automatisk publiseres i AD. Listen Active Directory User Object inneholder sertifikatene assosiert med brukeren eller datamaskinen, som er publisert i AD.

Den siste listen for sertifikater lokalt er Request. Her lagres forespørsler om utstedelse av sertifikater som er under behandling eller som har blitt avslått.

Listen Trusted Root Certification Authorities er sammensatt av en liste over root CA-sertifikater definert på domenenivå (lagret i AD), på lokal datamaskin og av brukeren selv. Trusted Root CA-sertifikater kan derfor legges inn i listen av bruker, administrator på den gitte datamaskin eller domeneadministrator på domenenivå. Når domeneadministratoren legger inn et nytt root CA-sertifikat på domenenivå legges dette inn i AD, og sertifikatene i AD lastes inn på datamaskinene i domenet ved hver boot av Windows 2000 operativsystemet, auto-enrollment (hver 8.time), og ved oppdatering av politikken i domenet (1). Listen Intermediate Certification Authorities er sammensatt på tilsvarende måte.

Bruksområdene til sertifikater som brukeren selv har lagt inn kan modifiseres. Brukeren kan for eksempel velge å ikke stole på root CA A sitt sertifikat for signering av kode, selv om sertifikatet var utstedt med dette bruksområdet. Lokal- og domeneadministratoren kan modifisere på bruksområdene til alle sertifikater som lastes inn i brukerne sine lister. Dette gjelder for sertifikater i listen Trusted Root Certification Authorities og sertifikater i listen Intermediate Certification Authorities, lagt inn på domenenivå eller på datamaskinnivå.

En bruker kan velge å fjerne/flytte et sertifikat hun har lagt inn i de forskjellige listene, noe som kan markere at hun ikke lenger stoler på dette sertifikatet. Lokal og domeneadministratoren kan også fjerne/flytte alle sertifikater på lokal datamaskin, noe som vil påvirke alle brukere sine lister over sertifikater på den gitte datamaskinen. Domeneadministratoren kan også på domenenivå modifisere listene over sertifikater det stoles på i domenet, noe som vil påvirke alle brukere i domenet.

5.3.3 Oppdatering av sertifikater og nøkler

Nøkkelpar og sertifikater utstedt til datamaskiner kan oppdateres både manuelt og automatisk. Når en datamaskins sertifikat utgår skjer en oppdatering av sertifikatet automatisk. Brukere får automatisk et nytt sertifikat når de forsøker å utføre en operasjonen med et utgått sertifikat. Sertifikater utstedt for konfidensialitet (kryptering av data) vil beholde det gamle nøkkelparet, men sertifikater utstedt for integritet (digital signering) vil opprette et nytt nøkkelpar.

Når brukere ønsker å manuelt oppdatere eller få et nytt sertifikat, kan de velge å benytte et nøkkelpar knyttet til et allerede eksisterende sertifikat eller få generert et nytt. Ved forespørsel om nytt sertifikat som skal benytte allerede eksisterende nøkkelpar, velger brukeren fra en liste over sertifikatmaler det nye sertifikatet skal utstedes for. Ved forespørsel om en oppdatering av et sertifikat, kan brukeren velge å benytte eksisterende nøkkelpar, eller opprette et nytt. Et nytt sertifikat med allerede eksisterende nøkkelpar vil redusere antall nøkkelpar per bruker, men det er viktig å ikke blande bruksområdene til et nøkkelpar. Det er for eksempel ikke lurt å benytte samme nøkkelpar for konfidensialitet og integritet, og det sikreste vil alltid være å benytte et nytt nøkkelpar (1).

Våre tester viser at private nøkler for både konfidensialitet og integritet blir tatt vare på i brukeren sin profil, når tilhørende sertifikater blir annullert. Det beste her var om de private nøklene for integritet ble slettet.

5.4 Håndtering av annulleringslister

Ved verifikasjon av sertifikater, laster automatisk Windows 2000 PKI-klienter ned og oppbevarer annulleringslister (CRL-er) tilhørende CA-er i en lokal cache (automatisk CRL-håndtering). Basert på publiseringsperioden i en CRL regner PKI-klientene ut en gyldighetsperiode for CRL-en. Gyldighetsperioden angir hvor lenge i tid CRL-en kan anses som autoritativ for verifikasjon av sertifikater fra den gitte CA-en. Gyldighetsperioden settes i utgangspunktet til 10% lenger enn publiseringsperioden av CRL-en, men aldri lenger enn 12 timer mer enn publiseringsperioden. For eksempel kan publiseringsperioden være satt til 24 timer, noe som betyr at gyldighetsperioden da blir 1.1*24 timer = 26,4 timer (1). PKI-klienten laster ikke ned en ny CRL, så lenge den har en gyldig CRL lagret lokalt i cachen.

Brukere kan når som helst laste ned og installere CRL-er. CRL-ene blir da ikke lagt inn i den lokale cachen, men i en liste over CRL-er tilhørende den gitte brukeren. Sett fra brukerens perspektiv oppbevares derfor CRL-er på to steder på PKI-klienten.

Et problem med den automatiske CRL-håndteringen på Windows 2000 klienter, er at den ikke sjekker brukerens lokalt lagrede og installerte CRL-er. Dette ble identifisert som et problem da noen utga seg for å være ansatt i Microsoft, og fikk utstedt to sertifikater for kodesignering fra Verisign. Microsoft har derfor publisert en fiks, som inneholder en CRL med disse sertifikatene, og en annulleringshåndterer som konsulterer også lokalt installerte CRL-er, hvis sertifikatet mangler CDP, eller at CDP-en er ugyldig.

Det viser seg at verifikasjon av CRL-er håndteres av den enkelte applikasjon, for eksempel Internet Explorer og Outlook. Den enkelte bruker kan derfor ikke være sikker på at disse

applikasjonene utfører denne oppgaven på en skikkelig måte. For eksempel vil Internet Explorer med standard oppsett ikke sjekke CRL-er for sertifikater til webtjenere den kommuniserer med.

5.5 Sikker e-post

Ved å bruke PKI-funksjonaliteten i Windows 2000, vil man ha mulighet til å signere og/eller kryptere e-post i Outlook. Signering og kryptering kan gjøres basert på ett sertifikat med begge bruksområder, eller med to separate sertifikater, ett for hvert bruksområde. Brukere får utstedt sertifikater til bruk for sikker e-post, ved på vanlig måte å sende en forespørsel til en CA.

Etter å ha konfigurert sikker e-post i Outlook er det mulig å sende signert e-post. Ved mottak av en signert e-post, vil mottaker bruke sertifikatet til avsender for å verifisere at signaturen er riktig. Dersom signaturen er riktig og mottaker stoler på utsteder av sertifikatet (sjekker signaturkjeden og stoler på root CA), er e-posten å anse som gyldig. I Windows 2000 og Outlook legges vanligvis sertifikatet til avsender med som et vedlegg til e-posten, slik at mottaker slipper å lete opp sertifikatet.

For å kryptere e-post brukes den offentlige nøkkelen (inkludert i sertifikatet) til mottaker. Avsender må derfor ha tilgang til denne, og kan deretter kryptere (og eventuelt signere) e-posten. I et domene vil Outlook hente sertifikatet til andre domenebrukere fra AD dersom det er nødvendig[1].

Et program for deteksjon og fjerning av virus (virusprogram) kan ikke sjekke kryptert e-post for virus, så sant virusprogrammet ikke har den private nøkkelen. Dette vil være en ulempe, da en kryptert e-post ikke kan virussjekkes før e-posten er dekryptert. I Windows 2000 PKI utføres dekryptering av e-post på klientene, og all virussjekk må dermed gjøres på her. Dette gjelder ikke for kun signering av e-post.

Alternativt kan komponenten Key Management Service (KMS) brukes til automatisk å utstede sertifikater med sentralt genererte nøkkelpar, for brukere av sikker e-post i domenet. Ved bruk av KMS vil Outlook ta kontakt med KMS, for å laste ned riktige sertifikater ved verifikasjon av signaturer og sending av kryptert e-post.

5.6 Sikker webtrafikk

Når man bruker web kan det ofte være nyttig at webtjeneren beviser at webtjeneren faktisk er den webtjeneren den utgir seg for å være. Dersom det er ønskelig fra webtjeneren sin side kan også klienten bli bedt om å presentere et sertifikat. Dette gjøres ofte med protokollen Secure Sockets Layer (SSL). Tjeneren presenterer da først et sertifikat til klienten, og klienten verifiserer sertifikatet på vanlig måte. Dersom tjeneren har bedt om gjensidig autentisering presenterer deretter klienten sitt sertifikat til tjeneren som verifiserer dette.

Når sertifikater er utvekslet og verifisert, kan klient og tjener autentisere hverandre basert på at motparten innehar den private nøkkelen korresponderende til utvekslet sertifikat. Vanligvis

[1] Dette gjelder kun Outlook 2000 SR-1 og nyere

oversender motparten en sesjonsnøkkel kryptert med mottakers offentlige nøkkel, og mottaker må inneha den korresponderende private nøkkelen for å kunne dekryptere sesjonsnøkkelen, og kommunisere sikkert med avsender. På denne måten kan klient og tjener gjøre en enveis autentisering (kun den ene parten autentiserer seg ovenfor den andre), eller gjensidig autentisering (begge autentiserer seg ovenfor hverandre).

Microsoft sin webtjener, Internet Information Services (IIS) gir støtte for mapping av sertifikater til brukerkontoer. Sertifikatmapping kan brukes i tre forskjellige modi. Man kan mappe ett spesifikt sertifikat til en spesifikk bruker i domenet, en såkalt en-til-en mapping. I denne modusen vil en brukers sertifikat bli lagt inn i webtjeneren, og dersom en bruker presenterer det eksakt samme sertifikatet i SSL vil han få aksessrettighetene som den kontoen han blir mappet til, så sant han innehar den korresponderende private nøkkelen (autentiserer seg ovenfor tjeneren).

Det er også et alternativ å bruke en mange-til-en mapping. I dette oppsettet vil for eksempel alle som har et sertifikat utstedt av en gitt CA, eller alle sertifikater som er utstedt til en gitt bruker, bli mappet til en gitt konto, så sant brukeren har den korresponderende private nøkkelen (autentiserer seg ovenfor tjeneren).

Det tredje alternativet/modusen er kun mulig å slå på for hele webtjeneren, og kalles directory mapping. Dersom den er slått på vil alle brukere som kommer inn med et SSL sertifikat bli mappet til en korresponderende konto, så sant brukeren innehar den korresponderende private nøkkelen (autentiserer seg ovenfor tjeneren). Til forskjell fra en-til-en mappingen på webtjeneren, er denne mappingen styrt av en mapping satt opp i AD, og webtjeneren henter de forskjellige mappingene fra AD.

5.7 Beskyttelse av nettverkspakker

Med beskyttelse av nettverkspakker/nettverksnivåsikkerhet menes implementering av konfidensialitet, integritet og autentisering på nettverksnivå, hvor det her kun sees på TCP/IP-baserte nettverk som Internett. IP er nettverkslaget i TCP/IP, og har som oppgave å rute datapakker fra avsender til mottaker.

En fordel med å implementere sikkerhetsmekanismer på nettverksnivå er at dette blir transparent for/påvirker ikke overliggende applikasjoner, som dermed ikke må endres. En annen fordel er at nettverkskomponenter som switcher, rutere og broer ikke påvirkes, som de ofte blir hvis sikkerhetsmekanismene blir implementert på et lavere nivå.

Det kanskje mest brukte settet av protokoller for sikkerhet på IP-nivå er IP Security (IPSec). IPSec dokumenteres av et sett av RFC-dokumenter (12), der forskjellige sikkerhetsprotokoller beskrives, deriblant Authentication Header (11) og Encapsulating Security Payload (10). IPSec gir støtte for integritet, autentisering og konfidensialitet, og krypterte IP-datapakker er beskyttet mot gjenspilling (replay) (15).

Operativsystemet Windows 2000 har innebygd støtte for IPSec. Microsoft hevder å følge de RFC-dokumentene som omhandler IPSec, og Windows 2000 datamaskiner vil dermed kunne kommunisere sikkert med andre datamaskiner, gjerne med et annet operativsystem enn

Windows 2000 (5).

I utgangspunktet er IPSec på en Windows 2000 datamaskin skrudd av, men kan enkelt startes i en av tre forhåndsdefinerte nivåer/politikker. Nivåene er henholdsvis klient (kun svar), sikker tjener (krev IPSec), og tjener (forespør IPSec). Datamaskiner satt opp med IPSec klient (kun svar) vil kun benytte IPSec hvis kommuniserende part ber om det. Datamaskiner satt opp med IPSec sikker tjener (krev IPSec) vil kreve at all kommunikasjon benytter IPSec, eller så avslås egne og andres initiativ til kommunikasjon. Datamaskiner satt opp med IPSec tjener (forespør IPSec) vil spørre om den andre datamaskinen støtter IPSec, men til forskjell fra IPSec sikker tjener vil den fortsette kommunikasjonen hvis motparten ikke støtter IPSec.

Windows 2000 gir en administrator mulighet til å opprette en ny IPSec-politikk for den gitte datamaskinen eller gjeldene for hele domenet. En IPSec-politikk består av et sett av regler og hvilke datamaskiner basert på IP-adresse, portnummer og protokoller (FTP, HTTP, LDAP, Telnet ...), reglene gjelder for. IPSec er datamaskinspesifikt, noe som betyr at IPSec-politikken på datamaskinen gjelder for alle brukere på den.

De forhåndsdefinerte IPSec-nivåene gjelder i utgangspunktet for alle datamaskiner den kommuniserer med, men dette kan også enkelt endres til å gjelde bare for et sett utvalgte datamaskiner med gitte tjenester/protokoller. Politikken kan for eksempel angi at alle datamaskiner skal kommunisere med IPSec, at all kommunikasjon med AD skal være med IPSec, eller at all kommunikasjon med webtjeneren i domenet skal være med IPSec.

IPSec gir støtte for autentisering, og administratoren kan velge mellom tre forskjellige måter datamaskiner kan autentisere seg ovenfor hverandre. Autentiseringsmetodene er Kerberos (standard autentiseringsprotokoll mellom Windows 2000 datamaskiner) (9), kjennskapet til en tekststreng, og bruken av sertifikater.

Det kan også settes i domenet at datamaskiner som meldes inn i domenet automatisk skal få utstedt et sertifikat for autentisering av eksterne datamaskiner. På denne måten kan nye datamaskiner i domenet helt automatisk klargjøres for IPSec.

Det å kreve at all kommunikasjon i domenet skal kjøre over IPSec virker kanskje fristende, men det er forbundet en del problemer med dette. Nye datamaskiner vil ikke kunne melde seg inn i domenet, da all kommunikasjon med AD krever IPSec. Nye datamaskiner vil heller ikke kunne få utstedt et sertifikat for autentisering av datamaskinen ovenfor eksterne datamaskiner, da kommunikasjonen med CA også krever IPSec. Domenepolitikken gir imidlertid mulighet for å tillate at sertifikater kan utstedes av CA til datamaskiner utenfor domenet uten IPSec. Her må brukeren på datamaskinen utenfor domenet autentisere seg ovenfor CA-en som for eksempel domeneadministratoren, og få utstedt et sertifikat for autentisering av datamaskinen ovenfor andre datamaskiner. Med et gyldig sertifikat vil den nye datamaskinen kunne kommunisere over IPSec med AD, og kunne melde seg inn i domenet.

5.8 Filkryptering

Operativsystemet Windows 2000 gir støtte for kryptering av filer på harddisken, og brukere kan enkelt kryptere filer eller en katalog (med alle filene og katalogene denne måtte inneholde) ved å

åpne en spesiell dialogboks. Dette er en funksjonalitet lagt til filsystemet, og kalles Encrypting File System (EFS).

EFS krever at brukere besitter et basis EFS sertifikat for å kunne kryptere filer. Alle Windows 2000 CA-er kan utstede slike sertifikater, og når en Windows 2000 datamaskin opererer utenfor et domene, kan brukeren selv utstede et basis EFS sertifikat til seg selv (gjøres automatisk første gang brukeren krypterer en fil). Dette betyr at en bærbar datamaskin uten nettverkstilkobling og uten medlemskap i et domene, også støtter kryptering av filer på harddisken.

Windows 2000 PKI opererer også med EFS gjenvinningsagenter, som er en rolle utvalgte brukere i domenet eller brukere lokalt på datamaskinene kan inneha. En gjenvinningsagent vil kunne dekryptere alle filer kryptert på den gitte datamaskinen og/eller i domenet. Dette er selvfølgelig svært fornuftig i ethvert kontormiljø hvor ledelsen kan ha behov for å få tilgang til de jobbrelaterte dokumentene til en ansatt, selv om vedkommende skulle være syk, sluttet, eller lignende. Alle EFS gjenvinningsagenter vil kunne dekryptere alle krypterte filer, så sant filen ble kryptert etter at gjenvinningsagenten var definert i domenet.

Lokal politikk på en datamaskin uten domenemedlemskap, er satt opp slik at det i utgangspunktet bare er lokal administrator som er standard gjenvinningsagent for krypterte filer, lagret på den lokale datamaskinen (8). Hvor godt en bruker sine krypterte filer er beskyttet, er dermed i dette tilfellet avhengig av at den lokale administratoren har et godt passord. Dette er ikke alltid sant, da et standard oppsatt Windows 2000 operativsystem (på for eksempel en bærbar datamaskin), vil være sårbar for at noen overskriver det krypterte passordet til gjenvinningsagenten (lokal administrator) med et nytt passord. Det eksisterer disketter som kan brukes til å starte opp den bærbare datamaskinen, uten å starte Windows 2000 operativsystemet. Programmer på disketten vil så overskrive passordfilen til Windows 2000 (8).

Når datamaskinen blir medlem av et domene, vil gjenvinningspolitikken kontrolleres på domenenivå, og det er i utgangspunktet kun domeneadministratoren som da er gjenvinningsagent. Dette betyr at de lokale administratorene fratas rollen som gjenvinningsagenter på de respektive datamaskinene, for filer som krypteres etter at medlemskapet i domenet er opprettet.

Siden den private nøkkelen korresponderende til gjenvinningssertifikatet til domene-administrator ligger lokalt i domeneadministrators profil på datamaskinen som er domenekontroller/AD, vil ikke filene lokalt på andre datamaskiner kunne gjenvinnes uten at den private nøkkelen eksporteres fra AD, og importers på den lokale datamaskinen.

Tester viser at lokale brukere ikke får lov til å kryptere lokale filer hvis ingen gjenvinnings-politikk er definert for systemet på domenenivå, etter at datamaskinen er innmeldt i domenet. En datamaskin må eksplisitt melde seg ut av domenet, for at lokal administrator igjen skal bli gjenvinningsagent for krypterte filer lokalt på datamaskinen. Det er kun filer som krypteres etter utmeldelse av domenet som får lokal administrator som gjenvinningsagent.

En del programmer slik som Microsoft Word vil lage temporære filer når autoriserte brukere manipulerer (har åpnet) den krypterte filen. De temporære filene vil være kopier av filen ukryptert, og vil kunne leses av andre samtidig som en autorisert bruker jobber med det krypterte dokumentet. Løsningen på dette problemet er å markere hele katalogen som kryptert,

slik at alle filer i katalogen, inkludert de temporære filene, vil være kryptert til enhver tid.

Grunnet tidligere restriksjoner på eksport av kryptografiske algoritmer benytter Windows 2000 utenfor Nord-Amerika den symmetriske krypteringsalgoritmen DESX, med 40-bits effektive nøkler (17). I Nord-Amerika benyttes DESX med 128-bits nøkler, og DESX er en utvidelse av DES, som benytter 56-bits effektive nøkler (13). Et uttømmende søk (prøve alle nøkler) vil være det mest effektive angrepet mot EFS utenfor Nord-Amerika, og med dagens maskinkraft vil alle 40-bits nøkler kunne prøves innen rimelig tid (26). Windows 2000 måtte følge disse restriksjonene i 1999, men det er ukjent om dette er gjeldende for Windows 2000 operativ-systemer man kjøper i dag.

5.9 Signering av kode

Applikasjoner og andre gitte filtyper kan i Windows 2000 digitalt signeres med en privat nøkkel korresponderende til et sertifikat. Filer som kan signeres er noen typer eksekverbare filer slik som exe-filer, kabinettfiler, Certificate Trust Lists (CTL) filer og katalogfiler. Kabinettfiler er komprimerte filer som inneholder andre filer slik som endrede eller nye filer som kommer med en Service Pack. CTL-filer inneholder CTL-er, som er root CA-sertifikater med brukerdefinerte reduserte bruksområder. Katalogfiler inneholder informasjon om pakker, for eksempel hotfixes som installeres på systemet. Windows 2000 gir ikke støtte for signering av andre filer enn de ovennevnte, noe som betyr at for eksempel Word-dokumenter og PowerPoint-presentasjoner ikke kan signeres.

Verktøyet benyttet for digitalt å signere filer og verifisere disse kalles Authenticode. Authenticode kommer ikke med standard Windows 2000 operativsystemet, men må lastes ned fra Microsoft sine websider (4). Når filer signeres med Authenticode, blir sertifikatet hektet på filen sammen med signaturen.

Via Authenticode kan brukeren velge om filen skal signeres med hashfunksjonen SHA-1 eller MD5, og om det skal refereres til et publiseringssted for informasjon om filen brukeren signerte. Publiseringsstedet må være en adresse til en webside, som den som vil verifisere signaturen til filen kan besøke. Det vil alltid være lurt for eksempel å ha en kopi over alle signaturer på en annen datamaskin enn den som filen er lastet ned fra. Hvis datamaskinen filen er lastet ned fra er kompromittert, vil filen potensielt kunne være endret og signert på nytt. Informasjon om siste signering og resultatet av signeringen vil da ligge på webtjeneren (annen maskin enn signert fil er lastet ned fra). Brukeren kan også velge å benytte en tidsstemplingstjeneste. Når filen senere verifiseres vil denne tjenesten garantere at filen eksisterte på det gitte tidspunktet.

Det er to mulige måter å verifisere signaturen til en signert fil, enten ved å åpne egenskaper/ properties til filen eller benytte Authenticode. En verifikasjon av signaturen til filen krever tilgang til CA sin annulleringsliste, og det er opptil brukeren om hun vil konsultere websiden som beskriver filen som er signert, og sjekke tidsstemplingstjenesten.

Ved verifikasjon av en signatur tilhørende et sertifikat i kjeden, sjekker Windows 2000 gyldighetsperioden for sertifikatets annulleringsliste. Hvis gyldighetsperioden ikke er over, vil ikke systemet forsøke å kontakte oppbevaringsstedet for annulleringslisten. Windows 2000

stoler da på lokalt cachede annulleringslister. Hvis gyldighetsperioden er forbi for en gitt annulleringsliste, kontaktes oppbevaringsstedet for denne annulleringslisten.

Et problem med verifikasjon av signaturer av kode i Windows 2000, er at systemet ikke sjekker lokalt lagrede og installerte annulleringslister. Systemet sjekker kun cachede annulleringslister, lastet ned automatisk fra publiseringsstedene da gyldighetsperioden på forrige annulleringsliste var forbi, og ikke brukerens installerte annulleringslister. Dette var et problem da noen utga seg for å være ansatt i Microsoft, og fikk utstedt to sertifikater for kodesignering fra Verisign. Sertifikatene har en gyldighetsperiode frem til januar 2004, men sertifikater for kodesignering fra Verisign inneholder ikke en referanse til oppbevaringsstedet for annulleringslisten. Microsoft måtte derfor publisere en fiks (crlupd.exe) som inneholdt en annulleringsliste med disse sertifikatene, og en annulleringshåndterer som konsulterer også lokalt installerte annulleringslister. Det anbefales at denne fiksen installeres på alle datamaskiner i domenet.

En bruker kan signere en fil med et annullert sertifikat uansett om ovennevnte fiks er installert eller ikke. Brukeren får ingen beskjed om at sertifikatet er annullert, selv om det er oppført som annullert i lokalt cachet og installert annulleringsliste. Detteburde rettes opp i senere versjoner av Windows 2000 PKI.

6 TOTALVURDERING

Microsoft har med sin integrering av PKI i Windows 2000, gitt brukerne en god plattform for økt datasikkerhet. Microsoft har også holdt seg til de standardene som andre PKI-systemer stort sett benytter, noe som øker samspillevnen med andre PKI-produkter.

Inndelingen av CA-er i typene Enterprise og Standalone er fornuftig, men vi savner muligheten for å skru av den automatiske utstedelsen av sertifikater i Enterprise CA-er, og kreve manuell godkjenning. Vi savner også muligheten for automatisk å utstede et sett av sertifikater til nye brukere i domenet, og muligheten for å opprette egne sertifikatmaler. Flere av sertifikatmalene støtter både signering og kryptering, noe som betyr at samme nøkkelpar benyttes til både signering og kryptering. Dette bør unngås da den private nøkkelen benyttet til kryptering bør tas vare på etter at sertifikatet har utgått, og den private nøkkelen benyttet til signering bør fjernes etter at sertifikatet har utgått.

En stor fordel med Windows 2000 PKI er muligheten for finkornet kontroll med bruken av sertifikater i domenet. Hvilke brukere og datamaskiner som skal kunne få utstedt hvilke typer sertifikater fra hvilke CA-er, er oversiktlig realisert. Domeneadministratoren kan også enkelt definere forskjellige politikker på domenenivå, som overstyrer de enkelte politikkene på de enkelte datamaskiner i domenet. For eksempel defineres gjenvinningsagenter for krypterte filer på domenenivå, en politikk for beskyttelse av nettverkspakker (IPSec) defineres på domenenivå, og mapping av sertifikater til brukerkontoer på webtjenere kan defineres i AD.

CA-ene kan automatisk publisere sertifikater til AD, noe som gjør det enklere å finne sertifikater i domenet. Gyldighetsperioden til de utstedte sertifikatene settes til å utløpe før gyldighetsperioden til sertifikatet til CA-en. Dette er fornuftig, da det aldri vil forekomme situasjoner hvor et sertifikat utstedt til en bruker ikke kan verifiseres, da CA-en sitt sertifikat har

utgått.

Windows 2000 PKI opererer ikke med kryssertifikater, men har et alternativ for å realisere tilsvarende funksjonalitet. Domeneadministratoren kan legge inn på domenenivå at alle brukere i domenet skal stole på en gitt root CA, noe som er ekvivalent med at hele domenet kryssertifiserer den gitte root CA-en.

Alle CA-er kan enkelt sikkerhetskopieres, og det gis støtte for inkrementell sikkerhetskopiering. Sensitive data, slik som CA-en sine private nøkler, krypteres basert på et inntastet passord, og det blir opptil administratoren å huske på disse passordene.

Nøkkelpar opprettes på PKI-klientene, med unntak av ved bruk av Key Management Service (KMS), for utveksling av sikker e-post. Uten bruk av KMS, vil de private nøklene ligge kryptert på datamaskinen nøkkelparet ble opprettet på. Konsekvensen av dette er at en administrator ikke vil automatisk kunne sikkerhetskopiere brukernes private nøkler i klartekst. Alle nøkkelpar tilhørende en bruker og datamaskin tas vare på, uansett bruksområde. Dette betyr at de private nøklene for konfidensialitet og integritet lagres kryptert på systemet.

Støtten for sikker e-post, sikker webtrafikk, og beskyttelse av nettverkspakker fungerer bra. Filkryptering fungerer også bra, men her må den private nøkkelen til gjenvinningsagentene passes godt på. Mest sannsynlig krypteres filene med en 40-bits nøkkel, som er alt for lite med dagens teknologi.

Signering av kode fungerer bra, men det er ønskelig med funksjonalitet for å signere egne dokumenter, slik som PowerPoint-presentasjoner, brev, bilder, og filmsnutter. Det anbefales å installere fiksen som også sjekker lokalt installerte annulleringslister.

Håndtering av annulleringslister er applikasjonsavhengig, og dette er kanskje den største kritikken mot Windows 2000 PKI. Våre tester viser at applikasjonene stort sett bare sjekker cachede annulleringslister, og ikke annulleringslistene brukeren eksplisitt har installert.

7 VIDERE ARBEID

Microsoft hevder at mange av de problemene vi har skissert med Windows 2000 PKI, er rettet på i Windows XP. Det ville vært interessant å se på de nye løsningene, og særlig muligheten for å signere for eksempel Word-dokumenter og PowerPoint-presentasjoner.

Vårt arbeid har ikke sett på bruken av smartkort i Windows 2000 domener, og det vil derfor vært interessant å studert integrasjonen av smartkort i Windows XP PKI. Windows XP integrerer støtten for smartkort inn i operativsystemet.

Litteratur

(1) Christman S. (2001): Guide to the Secure Configuration and Administration of Microsoft Windows 2000 Certificate Services, Network Applications Team of the Systems and Network Attack Center (SNAC), National Security Agency (NSA)

(2) Coleridge Robert, The Cryptography API, or How to Keep a Secret, Microsoft Developer Network Technology Group, August 1996

(3) Housley R., Ford W., Polk W., Solo D. (1999): RFC2459, Internet X.509 Public Key Infrastructure Certificate and CRL Profile.

(4) http://msdn.microsoft.com/downloads

(5) Internet Security Systems, INC (2000): Windows 2000 Security Technical Reference, ISBN: 0-7356-0858-X, Microsoft Press

(6) ISO 7498-2 Basic Reference Modell for Open Systems Interconnection (OSI) Part 2: Security Architecture, Geneva, Switzerland, 1988

(7) ITU Rec: The Directory: Authentication Framework, Information Technology – Open System Interconnect, 1993.

(8) Jaatun M. G., Dolva T., Mathiassen J., Olsen T., Wicklund P., Windvik R., Testing av kryptert filsystem i Windows 2000, FFI/NOTAT-2001/01810, Forsvarets forskningsinstitutt, 2001

(9) Jaatun M.G., Hornfelt L., KERBEROS ON LINUX - Installation and testing of Heimdal and MIT Kerberos Version 5, FFI/NOTAT-2001/03062, Forsvarets forskningsinstitutt, 2001

(10) Kent S., Atkinson R. (1998) RFC2406 IP Encapsulating Security Payload (ESP)

(11) Kent S., Atkinson R. (1998): RFC2402 IP Authentication Header

(12) Kent S., Atkinson R., RFC2401 Security Architecture for the Internet Protocol, 1998

(13) Kilian J., Rogaway P., How to protect DES against exhaustive key search. In Neal Koblitz, Advances in Cryptology, CRYPTO '96, volume 1109 of Lecture Notes in Computer Science, pages 252-267, 18-22 August 1996. Springer-Verlag

(14) Levi A., Caglayan U. (2000): An Efficient, Dynamic and Trust Preserving Public Key Infrastructure, *IEEE Symposium on Security and Privacy, Proceedings*, 203-214

(15) Madson C., Doraswamy N., RFC2405 The ESP DES-CBC Cipher Algorithm with Explicit IV, 1998

(16) Microsoft MSDN Library: Microsoft Windows 2000 Public Key Infrastructure, April 1999

(17) Microsoft: Enterprise Class Storage in Windows 2000, Operating System, White Paper,

1999

(18) Microsoft: Microsoft Base Cryptographic Provider (http://msdn.microsoft.com/library), 2001

(19) Microsoft: MS Windows 2000 Public Key Infrastructure, Introduction, White Paper, 2001

(20) Microsoft: Public Key Interoperability, Operating System, White Paper

(21) Microsoft: TechNet (http://www.microsoft.com/technet)

(22) NAI Labs, Network Associates, Inc: Windows Data Protection, Oktober 2001

(23) PERLMAN Radia (1999): An Overview of PKI Trust Models, *IEEE Network, Nov-Dec* 13, 6, 38-43.

(24) Ramsdell R., RFC2633 S/MIME Version 3 Message Specification, 1999

(25) Rescorla E., RFC2818 HTTP over TLS, 2000

(26) Schneier B. (1999): Applied Cryptography, John Wiley.

(27) Stallings W. (1999): Cryptography and Network Security, Second Edition, Prentice Hall, Upper Saddle River, New Jersey 07458.

(28) Windvik R., Hallingstad G., Vetland S. E.: ”Konfigurasjon og bruk av Windows 2000 PKI,” FFI/NOTAT 2002/01016, Forsvarets forskningsinstitutt, 2001

(29) Windvik R., Jaatun M. G., Hallingstad G., Security Mechanisms in Windows NT, FFI/NOTAT-2001/01395, Forsvarets forskningsinstitutt, 2001

(30) Wing P., O'Higgins B. (1999): Using Public-Key Infrastructure for Security and Risk Management , *IEEE Communications Magazine, September* 37, 9, 71-73

APPENDIKS

A Terminologi

Algoritme
Regneregel, nøyaktig sett av regler for framgangsmåten ved problemløsning.

Asymmetrisk krypteringsalgoritme
Benytter nøkkelpar, hvor informasjon kryptert med den ene nøkkelen kun kan dekrypteres med den andre nøkkelen, og omvendt.

Autentisering
Prosessen for å bevise at en enhet (bruker, applikasjon eller datamaskin), er det som den utgir seg for å være.

Hashfunksjon
En matematisk funksjon som basert på variabel verdi lengde inn (input-verdi), genererer en fast verdi lengde ut (hashverdi). Hashfunksjonene antas å være enveis. Dette betyr at det er lett å regne ut en hashverdi av en input verdi, men vanskelig å lage en input-verdi som produserer en gitt hashverdi.

Integritet
Forhindring av uautorisert modifikasjon av informasjon.

Konfidensialitet
Forhindring av uautorisert avsløring av informasjon.

Nøkkel
En krypteringsnøkkel brukt i symmetriske eller asymmetriske krypteringsalgoritmer.

Nøkkelpar
Består av en offentlig og privat nøkkel. Det skal ikke være mulig å utlede den private nøkkelen fra den offentlige.

Offentlig nøkkel
Din offentlige nøkkel benyttes av andre til å kryptere data, kun du skal kunne dekryptere med din private nøkkel. Den offentlige nøkkelen publiseres.

PKI
Public Key Infrastructure, også kalt offentlig-nøkkel-infrastruktur.

Privat nøkkel
Din private nøkkel benyttes til å dekryptere data, som er kryptert med din offentlige nøkkel. Den private nøkkelen kan også benyttes til signering. Den private nøkkelen holdes hemmelig.

Sertifikat
Informasjon om en enhets identitet og enhetens offentlige nøkkel, signert med utsteder av sertifikatet sin private nøkkel.

Signatur
Informasjon generert ved hjelp av en hashfunksjon, en asymmetrisk krypteringsalgoritme, og en privat nøkkel.

Symmetrisk krypteringsalgoritme
Samme nøkkel benyttes til kryptering og dekryptering.

Tilgjenglighet
Utstyr og data kan brukes av autoriserte enheter når disse har behov for det.

B Forkortelser

AD	Active Directory
AIA	Authority Information Access
API	Application Program Interface
CA	Certificate Authorities
CBC	Cipher Block Chaining
CDP	CRL Distribution Point
CRL	Certificate Revocation List
CSP	Cryptographic Service Providers
DES	Data Encryption Standard
EFS	Encrypting File System
FTP	File Transfer Protocol
HTTP	Hyper Text Transfer Protocol
IIS	Internet Information Services
IP	Internet Protocol
IPSec	IP Security
ISO	International Organization for Standardization
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
KMS	Key Management Service
LDAP	Lightweight Directory Access Protocol
MIME	Multi-purpose Internet Mail Extension
MD5	Message Digest, Version 5
NTM	Network Trust Model
PKCS	Public Key Cryptography Standards
PKI	Public Key Infrastructure
RA	Registration Authorities
RFC	Request For Comments

RSA	Rivest-Shamir-Adelman
SET	Secure Electronic Transaction
SHA	Secure Hash Algorithm
SP	Service Pack
SR	Service Release
SSL	Secure Sockets Layer
S/MIME	Secure MIME
TCP	Transmission Control Protocol
TLS	Transport Layer Security
VPN	Virtual Private Network

C PKCS

Det amerikanskbaserte firmaet RSA Data Security Inc har utviklet et sett av industristandard grensesnitt for håndtering av asymmetrisk nøkkelkryptografi, kalt Public Key Cryptography Standards (PKCS). PKCS er ingen formell standard, men gir utviklere av asymmetrisk kryptografiprodukter et forslag til syntaks og metode. Windows 2000 tar i bruk en del av PKCS for å blant annet implementere PKI. Tabell C.1 viser de forsjellige PKCS standardene.

PKCS#	Bruksområde
PKCS #1	Metode for kryptering og dekryptering med den asymmetriske krypteringsalgoritmen RSA
PKCS #3	Protokoll for Diffie-Hellmann nøkkelforhandling
PKCS #5	Metode for å kryptere en melding basert på et valgt passord
PKCS #6	En syntaks for sertifikater knyttet til offentlige nøkler (fases ut til fordel for X.509 versjon 3)
PKCS #7	Generell syntaks for meldinger som inneholder kryptografisk data, slik som digitale signaturer og kryptert data
PKCS #8	Et format for private nøkler og informasjon om disse
PKCS #10	En syntaks for forespørsel om utstedelse av sertifikater
PKCS #11	Et teknologiuavhengig programmeringsgrensesnitt (Cryptoki) for kryptografiske enheter slik som for eksempel smartkort
PKCS #12	En syntaks for å lagre offentlige nøkler, beskyttede private nøkler, sertifikater, og annen kryptografisk relatert informasjon i software

PKCS#	Bruksområde
PKCS #13	Mekanismer for å kryptere og signere data ved hjelp av elliptisk kurvekryptografi
PKCS #14	Generering av tilfeldige tall (pseudo–random)
PKCS #15	Kompletterer PKCS #11

Tabell C.1: PKCS

FORDELINGSLISTE

FFIE **Dato:** 13 March 2002

RAPPORTTYPE (KRYSS AV)	RAPPORT NR.	REFERANSE	RAPPORTENS DATO
X RAPP ☐ NOTAT ☐ RR	2002/01014	FFIE/780/113	13 March 2002
RAPPORTENS BESKYTTELSESGRAD		ANTALL EKS UTSTEDT	ANTALL SIDER
UGRADERT		52	39
RAPPORTENS TITTEL		FORFATTER(E)	
INFRASTRUKTUR FOR TILLITSHÅNDTERING I WINDOWS		WINDVIK Ronny, HALLINGSTAD Geir, VETLAND Stein Erik	
FORDELING GODKJENT AV FORSKNINGSSJEF		FORDELING GODKJENT AV AVDELINGSSJEF:	
Torleiv Maseng		Johnny Bardal	

EKSTERN FORDELING

ANTALL	EKS NR	TIL
		FD
1		v/Gunn Engvig
1		FLO/IKT
1		v/Knut Aksel Sæthre
1		v/Arild Skillinghaug
1		FLO/LAND
1		v/Vigdis Senderud
1		FLO/LUFT
1		FLO/SJØ
1		FO/E
1		v/Christophe R. Birkeland
1		FO/FST
1		FO/I
1		FO/S
1		v/Helge Lægreid
1		v/Lars Venger Gunnarsson
		Politiets Sikkerhetstjeneste
2		v/Suhail Muhstaq
		VSHB
1		v/Ola Holm
1		v/Roger Johnsen

INTERN FORDELING

ANTALL	EKS NR	TIL
14		FFI-Bibl
1		Adm direktør/stabssjef
1		FFIE
1		FFISYS
1		FFIBM
1		FFIN
1		Ronny Windvik, FFIE
1		Martin Gilje Jaatun, FFIE
1		Geir Hallingstad, FFIE
1		Torleiv Maseng, FFIE
1		Stein Erik Vetland, FFIE
1		Lars Hornfelt, FFIE
1		Kjell Olav Nystuen, FFIE
1		Frode Johan Lillevold, FFIE
1		Tor Gjertsen, FFIE
1		Knut Mo, FFIS
1		Arne Sjøvik, FFIS
3		Arkiv, FFIE
		FFI-veven

FFI-K1 Retningslinjer for fordeling og forsendelse er gitt i Oraklet, Bind I, Bestemmelser om publikasjoner for Forsvarets forskningsinstitutt, pkt 2 og 5. Benytt ny side om nødvendig.