

Encryptie deel III; Windows 2000 EFS

Auteur

Leon Kuunders is als security consultant en managing partner werkzaam bij NedSecure Consulting.

E-mail leon.kuunders@nedsecure.nl

Inleiding

In het eerste artikel uit deze reeks is ingegaan op de mogelijkheden om met PGP bestanden en volumes te coderen, zodat gegevens vertrouwelijk blijven voor geautoriseerde gebruikers. Na een uitstapje naar e-mailencryptie gaat dit deel van de reeks wederom in op bestandsencryptie. Meer specifiek: de encryptiemogelijkheid die Microsoft heeft ingebouwd in Windows 2000 (en Windows XP) komt aan bod: het Encrypted File System (EFS). Een overzicht van wat EFS is, hoe het werkt, hoe het kan worden gebruikt en waar rekening mee gehouden moet worden als men het op bredere schaal in wil zetten.

Wat is Windows 2000 EFS?

Gebruikers van Windows NT kunnen met behulp van de rechten die aan bestanden worden toegekend andere gebruikers toegang tot hun bestanden geven en ontfangen. Het is echter mogelijk om deze bescherming te omzeilen. Een aanvallende fysieke toegang heeft tot de harde schijf waarop de bestanden staan kan een NT-systeem starten vanaf een floppydisk en een tool als NTFSdos gebruiken om bestanden vanaf de schijf te kopiëren, zonder gehinderd te worden door de op het bestand geplaatste rechten. De bescherming op deze bestanden wordt dus geregeld door, en is afhankelijk van, het besturingssysteem.

Windows 2000 EFS lost dit probleem op door de beveiliging (versleuteling) van bestanden via het bestandssysteem te regelen. Bestanden die naar schijf worden geschreven worden in gecodeerd formaat, middels symmetrische en asymmetrische encryptie, opgeslagen. Rechtstreekse toegang verkrijgen tot deze bestanden maakt ze dus niet leesbaar. Alleen de gecodeerde vorm van het bestand kan worden benaderd. Zonder de juiste privé-sleutel kan een bestand niet gedecodeerd worden. De vertrouwelijkheid van gegevens kan hiermee zelfs in het geval van diefstal van bijvoorbeeld een laptop worden gegarandeerd.

Het cryptografische algoritme dat wordt gebruikt door EFS is DESX, met een maximale (symmetrische) sleutellengte van 128 bits. Bij de introductie van Windows 2000 was deze sleutellengte nog voorbehouden aan gebruikers uit de USA en Canada en moesten internationale gebruikers gebruik maken van de 56 bits variant. Dankzij de versoepelde exportrestricties op zwaardere encryptie is het voor internationale gebruikers inmiddels mogelijk om de encryptie-upgrade voor Windows 2000 (high-encryption-pack) te installeren. Daarbij staat EFS het in principe toe om meerdere cryptografische algoritmes te gebruiken. Er zijn op dit moment echter nog geen extra modules hiervoor beschikbaar en de vraag is of dit op (korte) termijn wel gebeurt.

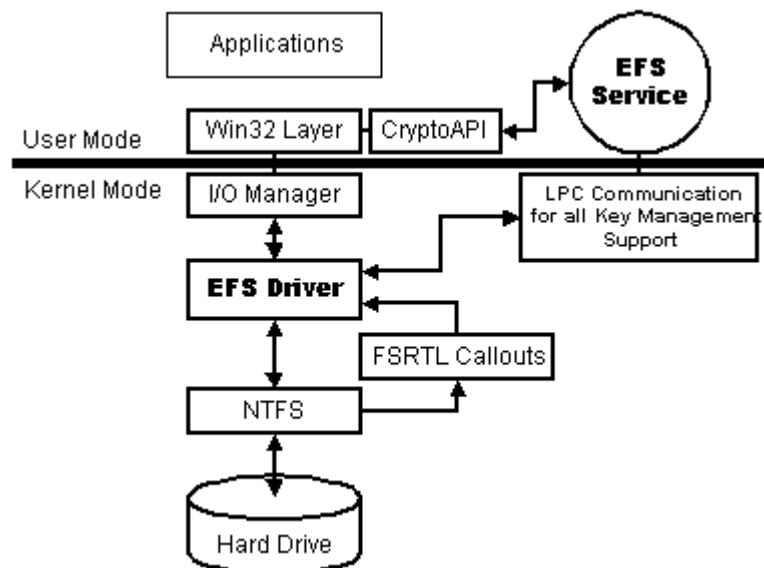
Hoe werkt Windows 2000 EFS?

EFS gebruikt de attributen die aan een bestand kunnen worden gegeven om te bepalen of het bestand gecodeerd moet worden of niet. Het toekennen van dit attribuut kan per bestand worden gedaan of per folder en gebeurt via het

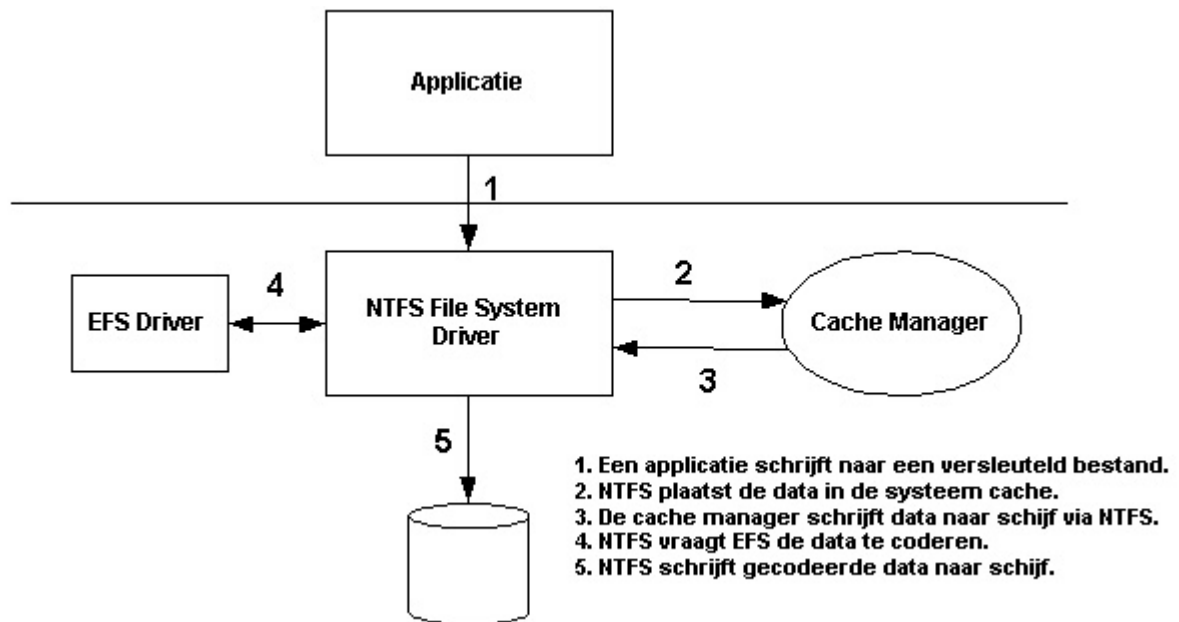
'eigenschappen'-scherm van een bestand of folder. Doordat EFS volledig gebaseerd is op bestandsattributen, is het alleen te gebruiken op NTFS (NT File System) 5 volumes. Oudere NTFS systemen en andere bestandssystemen zoals FAT ondersteunen EFS niet. Dit wil zeggen dat een gecodeerd bestand dat wordt gekopieerd naar zo'n systeem ongecodeerd zal worden opgeslagen.

De encryptie is gebaseerd op de veronderstelling dat een versleuteld bestand alleen te decoderen is door de (originele) eigenaar van het bestand. Het delen van versleutelde bestanden tussen meerdere personen kan wel, maar vraagt om een volledig Windows 2000 gebaseerde IT infrastructuur, waarbij middels de beveiligingspolicy groepen van gebruikers kunnen worden aangemaakt die dergelijke bestanden kunnen coderen en decoderen.

De allereerste keer dat een gebruiker een bestand versleutelt, wordt er door Windows 2000 een sleutelpaar gegenereerd (self-signed bij een stand-alone machine in plaats van een sleutelpaar uitgegeven door een Certificate Authority) of voor de gebruiker aangevraagd bij de domein controller (in het geval van een volledig Windows 2000 gebaseerde infrastructuur). Vervolgens wordt een willekeurige encryptiesleutel gegenereerd, de File Encryption Key (FEK). De FEK wordt gebruikt om het bestand te coderen met een symmetrisch algoritme (voor meer informatie over symmetrische en asymmetrische encryptie zie deel I van deze serie), waarna de FEK wordt versleuteld met de publieke sleutel van het aangevraagde of gegenereerde sleutelpaar (asymmetrische encryptie, gebaseerd op RSA) en met het bestand wordt opgeslagen. EFS is volledig geïntegreerd in de NTFS 5 architectuur zoals deze in Windows 2000 wordt gebruikt (zie figuur 1 en figuur 2).



figuur 1. Integratie EFS driver met NTFS

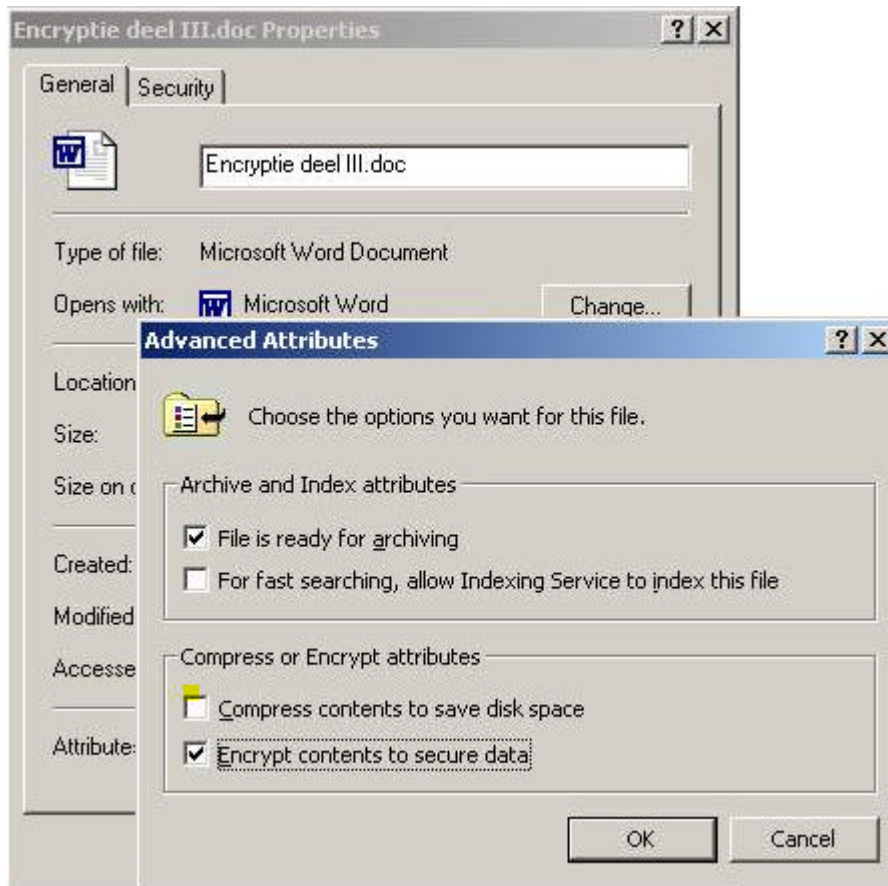


figuur 2. Systeemacties bij schrijven naar schijf

Het sleutelpaar dat is verkregen wordt opgeslagen in de My Certificate Store van de gebruiker (%USERPROFILE%\Application Data\Microsoft\SystemCertificates\My\Certificates), of kan worden opgeslagen op een smartcard, c.q. token. Afhankelijk van de netwerkconfiguratie (volledig Windows 2000 Active Directory of niet) wordt de data recovery agent (DRA) toegekend. Deze DRA wordt gebruikt als extra sleutel om de FEK te coderen. Hiermee wordt de beschikbaarheid van gegevens gegarandeerd. Mocht de gebruiker zijn eigen privé-sleutel verliezen, dan kan met behulp van de DRA de gecodeerde FEK wederom gedecodeerd worden en het bestand weer leesbaar worden gemaakt. Mocht er gebruik worden gemaakt van een stand-alone Windows 2000 werkplek, dan is het sleutelpaar dat als DRA wordt gebruikt het sleutelpaar dat is toegekend aan het lokale Administrator account.

De Praktijk

Starten met EFS voor bescherming van gegevens tegen ongeautoriseerd toegang is kinderlijk eenvoudig. De functionaliteit is te benaderen door de eigenschappen van een bestand op te roepen en de attributen ervan te bekijken (zie figuur 3).



figuur 3. Toekennen encryptie-attribuut

Of een bestand al dan niet versleuteld is en voor wie valt te zien met behulp van de tool EFSdump, geschreven door Mark Russinovich [1] (figuur 4). Hiermee valt het Data Decryption Field (DDF) en het Data Recovery Field (DRF) van een versleuteld bestand uit te lezen.



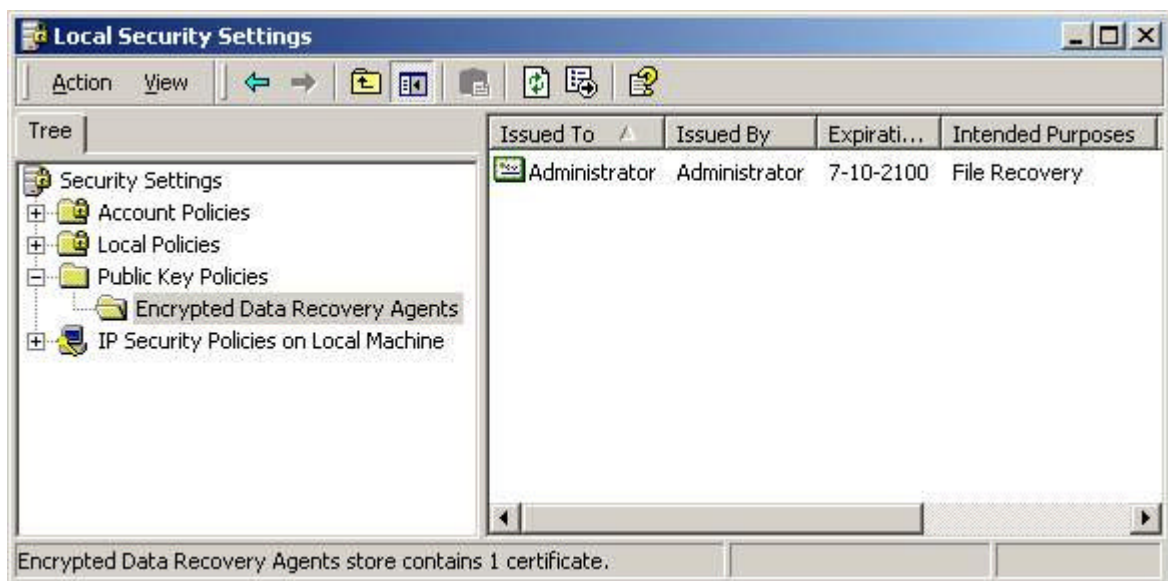
figuur 4. Informatie over versleuteld bestand

Het versleutelen van een volledige folderstructuur (wat wordt aangeraden door Microsoft [2]) vraagt om niet meer dan het aanzetten van het encryptie-attribuut op een folder, op dezelfde manier als te zien in figuur 3 voor een enkel bestand. Op deze manier kan men de folders die door Windows 2000 worden gebruikt om

tijdelijke bestanden in op te slaan versleutelen. In dit geval moet er wel rekening mee worden gehouden dat een bestand dat door een applicatie vanuit de 'TEMP'-folder naar de opslagfolder wordt gekopieerd, versleuteld blijft. Het is in ieder geval aan te raden om alle tijdelijke opslagfolders in Windows 2000 en de gebruikte applicaties zoals Microsoft Word naar dezelfde folder te laten verwijzen.

Waarmee bij EFS rekening gehouden moet worden, is dat de DRA de lokale 'administrator' is indien gebruik gemaakt wordt van stand-alone Windows 2000 configuraties (dit komt veelvuldig voor bij bedrijven met een Windows NT netwerk en Windows 2000 op de laptop clients). Programma's die gebruikt kunnen worden om het wachtwoord van dit lokale account te kraken zijn in ruime mate voorhanden en geven dan ook toegang tot het DRA certificaat en de versleutelde bestanden.

Het aanpassen van de DRA kan door de lokale beveiligingspolicy aan te passen [3] (figuur 5). Het is mogelijk om nieuwe DRA's toe te voegen aan deze policy door de certificaten die daarvoor gebruikt worden vanaf floppydisk of schijf te importeren. Ook het verwijderen van DRA's is mogelijk. Het is echter van belang niet alle DRA's te verwijderen. Doordat het EFS stuurprogramma verwacht dat er een DRA aanwezig is, zal het weigeren een bestand te coderen, dan wel te decoderen, indien geen DRA wordt gevonden. Windows 2000 waarschuwt hier echter niet voor als de DRA wordt verwijderd.



figuur 5. Scherm lokale beveiligingspolicy

Beperkingen van Windows 2000 EFS

Windows 2000 EFS kent een aantal beperkingen. Zo worden bestanden die worden gekopieerd van schijf naar schijf eerst gedecodeerd en daarna opnieuw gecodeerd met een andere FEK. In het scenario waarbij gegevens op een centrale server staan, zal het openen van gecodeerde bestanden op de server ertoe leiden dat de gegevens onversleuteld over het netwerk worden verstuurd naar de werkplek. Het decoderen vindt plaats op de centrale server. Bij grote aantallen versleutelde bestanden kan dit problemen opleveren voor de belasting van de centrale server.

Voorts heeft virusprotectiesoftware die op de centrale server draait geen toegang tot de versleutelde bestanden. Alleen door gebruik te maken van bedrijfsleutels voor de DRA en deze toe te kennen aan het account dat gebruikt wordt door de

virusprotectiesoftware kan dit worden bereikt. Het gebruiken van een bedrijfspolicy inclusief bedrijfsleutels is alleen mogelijk indien een volledig op Windows 2000 Active Directory gebaseerd netwerk is geïmplementeerd.

Het opzetten van een goede recovery policy is onontbeerlijk. Het toekennen van de DRA functionaliteit aan het lokale of domein-administratoraccount geeft de beheerders de mogelijkheid om gecodeerde gegevens leesbaar te maken. Alhoewel dit voor veel bedrijven niet direct een probleem is (het merendeel van de beheerders is nu ook al in staat om alle gegevens op het netwerk te lezen), is dit vanuit beveiligingsoogpunt niet wenselijk. Toewijzen van een aparte recovery agent is alleen mogelijk indien dit middels de beveiligingspolicy van het Windows 2000 domein wordt geregeld.

De bescherming van het privé-certificaat van de gebruiker is afhankelijk van de sterkte van het user-id en wachtwoord. Gebruikers die op een onzorgvuldige wijze omgaan met hun wachtwoord geven niet alleen toegang tot hun account, maar tevens tot hun privé-certificaat waarmee bestanden kunnen worden gedecodeerd.

EFS is gebaseerd op transparantie voor de eindgebruiker. Hierdoor is niet direct zichtbaar of een bestand al dan niet is versleuteld. In Windows XP is dit probleem opgelost door naast voor gecomprimeerde bestanden ook gecodeerde bestanden in een alternatieve kleur te laten zien in het Verkenner scherm, in Windows 2000 bestaat deze mogelijkheid echter niet. Door het ontbreken hiervan kan het gebeuren dat bestanden die versleuteld zouden moeten worden niet versleuteld zijn, zonder dat dit wordt opgemerkt.

Conclusie

De eenvoud waarmee EFS kan worden geactiveerd en gebruikt maakt dat het zelfs door de meest onervaren gebruikers kan worden ingezet. Wil men echter bedrijfsbreed gebruikmaken van EFS, dan is het uitrollen van een Windows 2000 Active Directory infrastructuur niet te vermijden. In een omgeving waarbij slechts een beperkt aantal medewerkers van deze EFS-functionaliteit gebruik zal maken geeft het uitrollen van Active Directory een zware belasting op de beheerorganisatie. De mogelijkheid om met de lokale beveiligingspolicy op een Windows 2000 werkplek de randvoorwaarden voor het gebruik van EFS te regelen (bijvoorbeeld het toekennen van een andere DRA dan het lokale administrator-account) heeft dan de voorkeur. Hiermee wordt voorkomen dat het privé-certificaat van de DRA op de lokale schijf te benaderen is.

Voor kleine tot middelgrote firma's is Windows 2000 EFS een toepassing die op een eenvoudige wijze een verhoogd beveiligingsniveau geeft. Door de voorwaarden duidelijk vast te leggen kan het snel in gebruik worden genomen, zonder noemenswaardige problemen. Houd echter in het achterhoofd dat EFS gericht is op de eindgebruiker en dat de met EFS gecodeerde bestanden niet gedeeld kunnen worden. Om bestanden met meerdere personen te delen kan men naast EFS andere producten (zoals het in deel 1 van deze serie behandelde PGP) gebruiken.

Referenties

[1] EFSdump van Mark Russinovich (Sysinternals)
<http://www.sysinternals.com>

Inside Windows 2000 EFS Part 1 & 2 door Mark Russinovich
<http://www.win2000mag.com/Articles/Print.cfm?ArticleID=5387>

<http://www.winntmag.com/Articles/Print.cfm?ArticleID=5592>

[2] Step-by-step Guide to EFS (Microsoft)

<http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/deploy/confeat/efsguide.asp>

<http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/prodtechnol/windows2000serv/deploy/confeat/nt5efs.asp>

[3] Disable/Enable EFS on a Stand-Alone Windows 2000-Based Computer (Microsoft)

<http://support.microsoft.com/support/kb/articles/q243/0/35.asp>

Algemeen

Informatie over Windows 2000 Encrypting File System (EFS) Resources

<http://www.labmice.net/EFS.htm>