IBM Crypto Competence Center

SFED – Secure File Encryption for Desktops

Forsendelse af filer via e-mail er blevet en meget udbredt metode til at udveksle data af forskellig art. Imidlertid er forsendelsen ikke sikker, da en e-mail, som sendes ukrypteret over det åbne internet, kan læses af alle. Udbredelsen af sikre e-mailsystemer og digital signatur vil afhjælpe dette problem – men det er ikke alle, der endnu har anskaffet sig en digital signatur (et certifikat) og kun et fåtal har sat deres e-mailsystemer op til at kunne modtage og afsende sikre emails. En af årsagerne til dette er at man skal kende modtagerens certifikat for at kunne sende krypteret til vedkommende. Der er derfor behov for på en nem og sikker måde at kunne kryptere filer, som skal forsendes over det åbne internet, inden de vedhæftes en email og sendes.

Mobile lagermedier som USB-stick, memory cards mv. har specielle fordele, fordi de er nemme at transportere og kan opbevare store datamængder. På grund af størrelsen er risikoen for, at de bliver væk eller bliver stjålet dog forøget, og de egner sig derfor ikke til opbevaring af fortrolige data. Kryptering af filerne vil gøre opbevaring af fortrolige data på de mobile lagermedier mere sikker mod afsløring over for uvedkommende.

SFED er et Windows program, der kan kryptere filer, så de ikke kan læses af uvedkommende. Programmet benytter de nyeste standarder for kryptering og kan endvidere kryptere indholdet af mapper og opbygge en selvudpakkende fil, så dekrypteringen kan foretages, uden at SFED behøver at være installeret på modtagerens maskine.

SFED kan således opbygge en fil indeholdende en hel mappestruktur, som gendannes ved dekrypteringen. Denne fil er det nemt at flytte til et mobilt datamedie eller forsende via e-mail.

IBM har stor ekspertise indenfor udvikling af sikkerhedsløsninger og har i mange år været markedsledende indenfor udvikling af hard- og software til kryptografi. Det danske krypto-kompetencecenter blev startet i 1980'erne i forbindelse med etablering af Dankort-systemet. Centret er siden vokset støt og rummer i dag et stort antal specialister indenfor områder som kryptografi, PKI, key management, smart cards mv.

FORDELE

Sikker løsning

SFED er bygget på IBM's velrenommerede krypto-biblioteker. De nyeste krypteringsmetoder benyttes og lange nøgler giver stor sikkerhed mod brute force angreb. Adgangen til at dekryptere en fil sikres af et password. Password kan være mellem 8 og 256 tegn lange og skal inkludere specialtegn eller tal. SFED gennemtvinger et minimumsniveau af passwordkvalitet, og de krypterede filer er sikret mod gentagne forsøg på at gætte password. Metoden følger PKCS#5 standarden.

Hvis det ønskes, kan SFED sikre at originalfiler slettes og overskrives med tilfældige tegn efter krypteringen for at gøre det sværere at gendanne filerne.

Fleksibel løsning

Løsningen giver mulighed for sikker transport af filer via usikre medier som det åbne internet og sikker opbevaring på USB-keys. Filerne er sikret uanset transportmetode, og der er mulighed for at kryptere både enkeltfiler og hele mapper, samt for at danne selvudpakkende filer som kan dekrypteres uden at SFED skal være installeret på den maskine, hvor dekrypteringen foretages.

Brugervenlig løsning

SFED leveres i en installationspakke, som nemt afvikles på de understøttede Windows systemer.

Brugeren behøver ikke kende modtagerens certifikat på forhånd og skal ikke gennem en søgning efter, og installation af dette i sit e-mailprogram.

Efter installationen er SFED tilgængelig i content-menuen, der fås ved at højreklikke på en fil eller en mappe. Encrypt og Decrypt funktioner kan vælges.

Brugerdialogerne er logisk opbygget, og det er sikret, at processen kan afbrydes undervejs.

FAKTA	
Krypteringsalgoritme	AES med 128 bits nøgle
MAC algoritme:	HMAC-SHA-256
Platforme:	Windows 2000/XP Pro/XP Home/Server 2003

SUPPORT

Der kan tilkøbes vedligeholdelse indeholdende adgang til nye releases.

IBM har PKI- og sikkerhedseksperter, som kan yde rådgivning og support på alle niveauer.

Kontaktinformation

For yderligere oplysninger kan IBM's Crypto Competence Center kontaktes på ccc@dk.ibm.com

Endvidere er SFED beskrevet på adressen:
ibm.com/security/products/SFED.html

IBM Danmark A/S
Nymøllevej 91
2800 Kgs. Lyngby
Danmark
+45 45 23 30 00 Telefon
+45 45 93 24 20 Telefax

IBM's hjemmeside findes på Internettet på adressen **ibm.com**

Der er flere oplysninger om IBM Global Services på **ibm.com**/services

Der kan være henvisninger til eller oplysninger om IBM-produkter (maskiner eller programmer), -programmering eller -serviceydelser, som ikke er introduceret i Danmark. Sådanne henvisninger eller oplysninger betyder ikke nødvendigvis, at IBM på et senere tidspunkt vil introducere det pågældende i Danmark.

Henvisning til IBM-produkter, -programmering eller -serviceydelser betyder ikke, at kun IBM-produkter, -programmering eller -serviceydelser kan benyttes.

Materialet er vejledende og kan indeholde billeder af modeller, der er under udvikling.

Trykt i Sverige

XXBEEXXXXX-2 (XX/02) XX