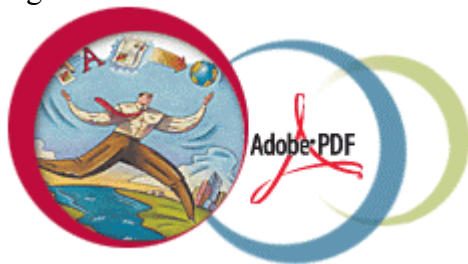


Digitala Signaturer

I det datoriserade samhälle vi har idag flödar det mängder av dokument som måste skrivas ut och få en signatur i form av en oläslig kråka som i princip vem som helst kan ha satt dit. Detta har historiskt sett varit det enda sättet att juridiskt binda en individ till ett beslut, identifiering, godkännande eller liknande.

Digitala Signaturer med Adobe Acrobat

Men om vi ska ha som ett mål att minimera pappersanvändandet och kanske bli det papperslösa samhället så erbjuder Adobe bra lösningar för att hantera elektroniska dokument. Tidigare kanske du fick skickat till dig en fin PDF-fil, var tvungen att skriva ut den, manuellt signera den och sen faxa den tillbaka. Inte en vidare bra lösning, eller hur.



Funktioner som digitala signaturer ger är:

Enkel signering – Här kan en eller flera signera att de t.ex. har läst eller godkänt dokumentet.

Ändringskontroll – Efter att dokumentet är signerat så kan dokumentet inte ändras utan att på nytt signera det. Skulle det inte vara signerat på nytt så framkommer det att det har ändrats sedan signaturen blev ditsatt.

Verifiering – Du kan vara säker på att det dokument som du får upp på din skärm är oförändrat sen den som skickade det till dig signerade det. Dessutom kan du vara säker på att dokumentet härstammar från den som signerade det genom att verifiera signaturen med hjälp av ett användarcertifikat. För att mottagaren ska kunna göra verifieringen så måste du skicka med användarcertifikatet. Det behöver du bara skicka med första gången du ska skicka ett dokument till någon. Om man sitter i ett nätverk så kan alla användare på företaget ha certifikaten i en delad mapp. Ett annat alternativ är att publicera det på Internet.

Det system som levereras med Acrobat kallas självsigneringskydd. Det går att skapa ett personligt certifikat där bara du har lösenordet, eller så kan en grupp dela på ett gemensamt certifikat då det inte är viktigt vem i avdelningen som signerat. Det innebär att du delar certifikatet direkt med den mottagande parten istället för att blanda in en tredje part. Men skulle företaget ha som policy att använda ett annat system, t.ex. VeriSign så stöds det via så kallade insticksprogram. Vill du även använda certifikat samt kryptera när du skickar e-mail så stöder VeriSign Microsoft Outlook, Netscape Navigator, Outlook Express, Eudora m.fl. Det går att pröva i 60 dagar gratis. Är du bara intressera av certifiering och kryptering av e-mail så finns en helt gratis lösning hos www.thawte.com som fungerar lika bra.

Förhindra förnekande – Det här förhindrar att när man väl satt sin signatur så kan man inte förneka sitt ansvar vid ett senare tillfälle om det skulle uppkomma en tvist. Därför är det ju viktigt att det lösenord som du valt inte är för enkelt eller att du skrivit ner det på en lapp som ligger under musmattan.

Jämförelse – Du kan ta två signerade dokument och använda kommandot för jämförelse för att se skillnaderna mellan dokumenten. I det fallet visas sidorna sida vid sida och ändringarna markeras.

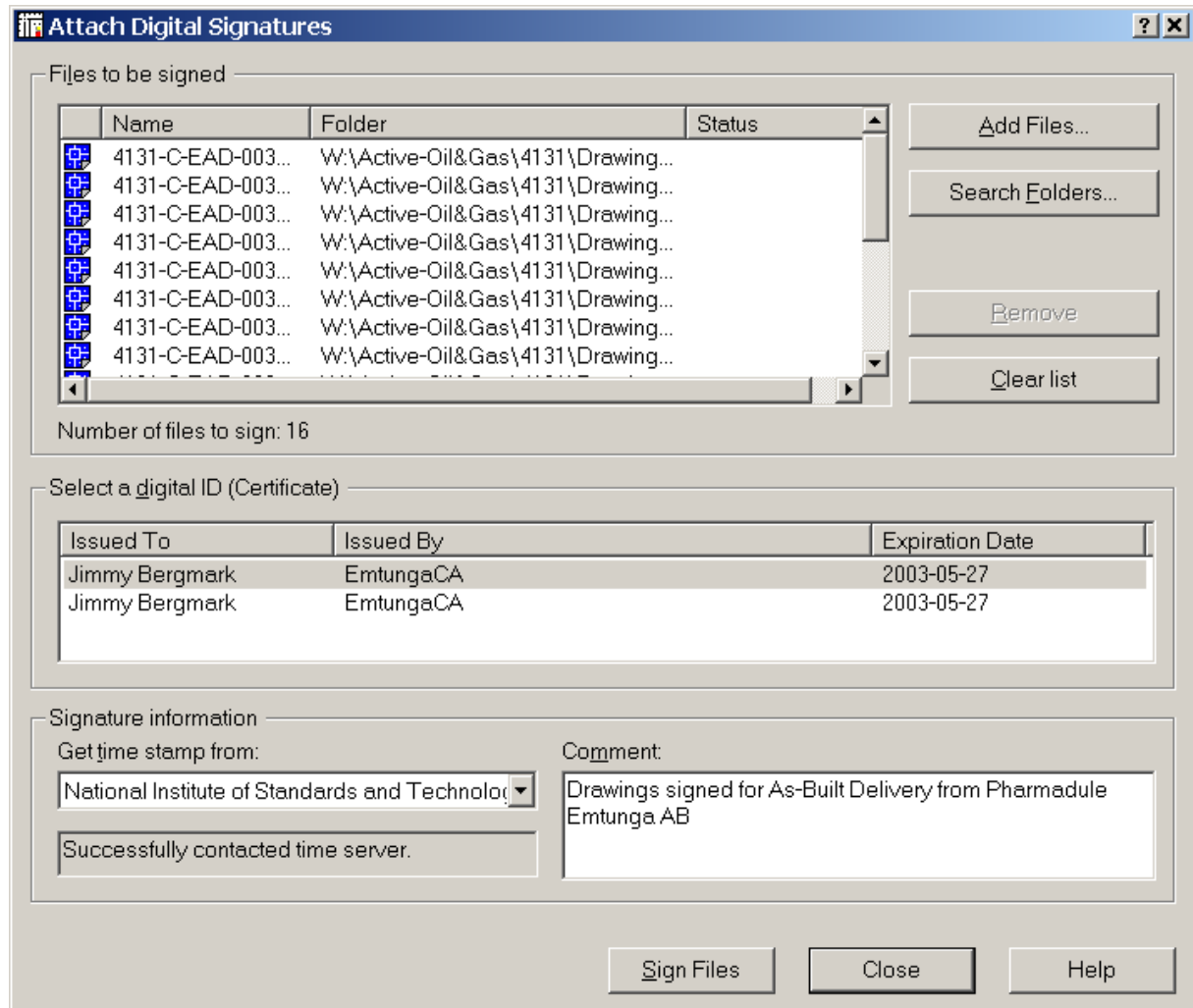
Grafisk koppling – Det går att koppla den digitala signaturen till en inskannad handsignatur eller annan symbol.

Kryptering – Med hjälp av kryptering så kan du välja vilka som ska ha tillgång till att läsa dokumentet genom att ge de ett lösenord.

Den enklaste programvaran är Adobe Acrobat Approval. Som namnet anger är syftet att förutom att fungera som en Acrobat Reader så hanterar det att skapa och verifiera digitala signaturer. Behöver du ytterligare funktioner som att t.ex. skapa PDF-filer så behövs Adobe Acrobat som kostar lite mer än Approval.

Digital Signature Extension för AutoCAD

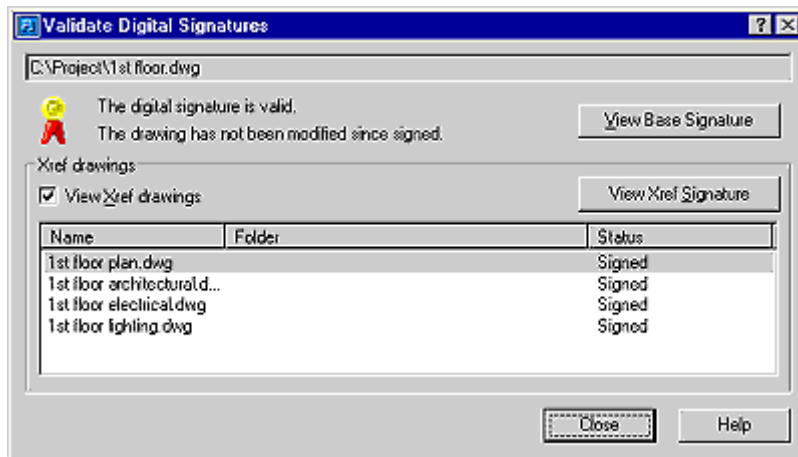
För de som har Autodesk Subscription Program finns möjligheten att ladda ner tilläggfunktionen Digital Signature Extension från deras portal Point A. Med Digital Signature Extension går det att digitalt signera och verifiera DWG-filer.



Funktionalitet är att det på ett säkert sätt går att verifiera identiteten på den som signerat ritningarna. Statusen går att se så att man kan få en verifikation på att ritningen inte har ändrats. Slutligen kan inte den som signerat hävda att han aldrig gjort det.

Med hjälp av Digital Signature Verifier så kan de mottagare som inte har tillägget verifiera den digitala signaturen. Dessutom varnar den att ej auktoriserade ändringar i filen gör att den digitala signaturen inte längre är giltig. Antingen kan den som skickar filerna skicka med Digital Signature Verifier eller så kan de gratis ladda ner den från Internet.

I AutoCAD 2002 så får man upp en dialogbox när man öppnar en signerad ritning som anger statusen. Funktionen går att stänga av med systemvariabeln SIGWARN och anropas manuellt med kommandot SIGVALIDATE. Det går även att se om Xreffarnas status.



Givetvis finns det inte när det gäller säkerhet ett system som inte går att bryta sig in i. Men med digitala signaturer kan man vara relativt säker på att när vi digitalt signerar ett dokument så kan mottagaren verifiera att både ursprung och innehåll är som du vill att det ska vara.

Av Jimmy Bergmark, www.jtbworld.com