Verksamheten för samhällets
informations- och cybersäkerhet
cert@cert.se

Kurir för it-incidentrapportering – snabbguide – användare

Innehåll

1. Förord

1.1. Inledning

Detta dokument tar upp programvara Kurir 2.0, vilket används för att rapportera it-incidenter mellan myndighet och MSB.

Detta dokument vänder sig till den som ska använda programvaran för kryptering och dekryptering av incidentrapporter.

1.2. Dokumentets syfte

Detta dokument tar upp hur man använder programmet, t.ex. läser in kryptonycklar för att sedan kryptera och dekryptera filer.

Dokumentets syfte är inte att beskriva alla funktioner som finns i programmet, utan endast de funktioner som används i Kurir 2.0 för it-incident rapportering.

Innan användning bör användaren även har läst dokumentet Kurir för it-incidentrapportering – Hanteringsregler.

1.3. Dokumentets innehåll

Denna snabbguide beskriver övergripande användning, steg för steg. Endast de viktigaste procedurerna för hantering av kryptonycklar och kryptering/dekryptering av information beskrivs.

Eftersom programmet erbjuder flera olika sätt att lösa samma uppgift på har denna snabbguide valt att beskriva ett säkert sätt att utföra aktuell uppgift på. Användare förväntas ha normal datorvana, t.ex. för att hantera filer i utforskaren.

1.4. Referenser

#	Ref	Rubrik	Ver	Datum
1	[Hant]	Kurir för it-incidentrapportering – Hanteringsregler	1.0	2016-03-21
2	[Install]	Kurir för it-incidentrapportering – snabbguide - installation	1.0	2016-03-21
3	[Anv]	Kurir för it-incidentrapportering – snabbguide – användare (Detta dokument)	1.0	2016-03-21
#	**Ref**	**Rubrik**	**Ver**	**Datum**
4	[Man]*	Kurir user manual (på CD) (Tutus)	1.0.0	141007

* = Leverantörens manual, innehåller flera hanteringsregler och funktioner, men dessa gäller inte för Kurir it-incident.

2. Checklista

Här följer en förenklad checklista på vad man ska göra i processen. Checklistan utgår ifrån MSBs rekommendationer att programvara är installerad på en fristående dator. Checklistan är tänkt att användas som repetition för användare som redan har skickat och tagit emot krypterad information flertalet gånger. Detta är ett tänkt scenario som i verkligheten kan se lite annorlunda ut beroende på myndighet.

2.1 Inledningsarbete

1) **Skriv din it-incidentrapport** på en av myndigheten godkänd dator för hantering av it-incidentrapporter.

2) Överför filen med it-incidentrapporten till ett medium som passar dator med Kurir it-incident installerat (t.ex. USB eller CD)

3) Gå till den dator som har programvaran för kryptering
(Här kallad **dator med Kurir it-incident**)

2.2 Förarbete

1) Ta fram en giltig kryptonyckel med lösenord (vid osäkerhet vilken nyckel som är giltig kan detta kontrolleras genom att kontakta MSB/CERT-SE på cert@cert.se).

2) Bryt plomberingen (alla kryptonycklar har levererats plomberade från MSB), vid uppbrytning av plombering,
skriv datum på CD-skivan innehållandes kryptonyckel när plomberingen bröts.

2.3 Kryptonyckelhantering

1) Starta programmet Kurir.

2) Logga in i programmet genom att skriva in lösenordet som angavs vid installation och importera kryptonyckel till programmet från CD (med tillhörande lösenord).

3) CD med kryptonyckel och lapp med lösenord ska även i fortsättningen förvaras så att ingen obehörig kan ta del av dessa. En använd kryptonyckel har ett betydligt större skyddsvärde än en oanvänd kryptonyckel.

2.4 Kryptering

1) Kryptera (med vald kryptonyckel) (drag´n´drop).

2) Flytta över den krypterade filen (drag´n´drop) till ett lagringsmedium som får användas i den dator som har e-post för att skicka den krypterade filen med (t.ex. USB eller CD).

2.5 Sändning/Mottagning

1) Sändning och mottagning av krypterade filer sker på en internetansluten dator med ordinarie e-postfunktion.

2.6 Dekryptering

1) Flytta över den krypterade filen till ett lagringsmedium som passar datorn med Kurir it-incident (t.ex. USB eller CD).

2) Starta programmet Kurir it-incident och kontrollera att kryptonyckel finns inläst i programvaran.

3) Dekryptera (automatiskt vald kryptonyckel) (drag´n´drop).

4) Flytta över den dekrypterade klartextfilen (drag´n´drop) till ett lagringsmedium som passar det systemet med vilken man ämnar läsa filen på (t.ex. USB eller CD).

2.7 Nödradera

Programvaran innehåller en funktion för nödradering om installationen (med tillhörande importerade kryptonycklar och logg) snabbt behöver tas bort.

2.8 Logg

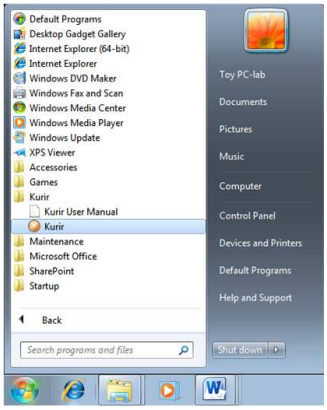
Programvaran innehåller en loggfunktion. Vid behov kan denna logg användas för att spåra gjorda händelser t.ex. krypterat/ dekrypterat/ kryptonyckelhantering.

3. Hantering

Programmet ger en hel del valmöjligheter, dels i hur man arbetar t.ex. vart man lagrar information, men även hur man initierar det arbete man vill utföra. Nedan illusteras ett sätt att använda programmet.

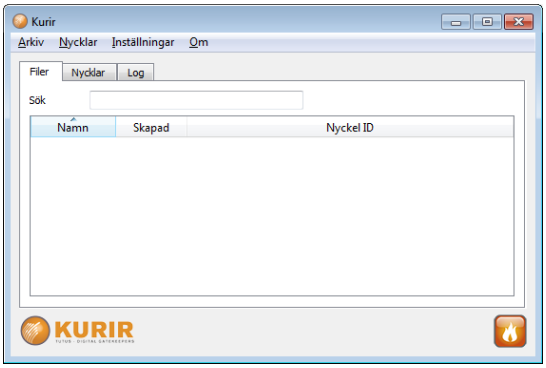
För att starta programmet:

1) **Klicka**: Start/All Programs/Kurir/Kurir



2) Ange **Lösenord**

3) **Klart!**

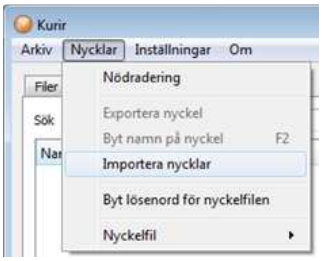


3.1. Nycklar

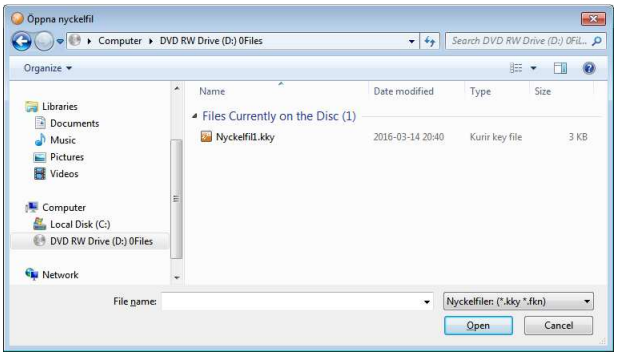
3.1.1. Importera nycklar

För att kunna kryptera/dekryptera filer, måste en kryptonyckel importeras.

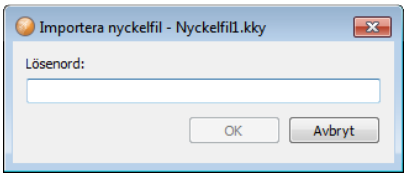
1) **Klicka**: Meny Nycklar/Importera nycklar



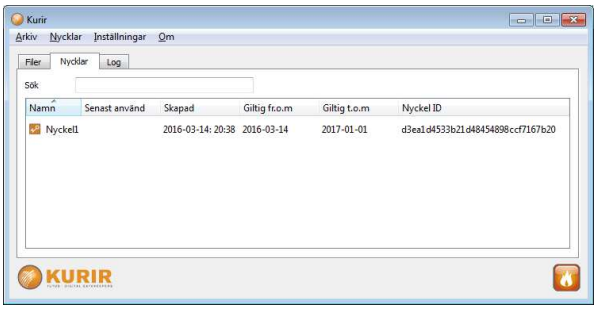
2) Klicka dig fram till aktuell **Nyckelfil**



3) Ange **Lösenord** till Nyckelfil



4) **Klart!** (Nyckel visas i Flik Nycklar)



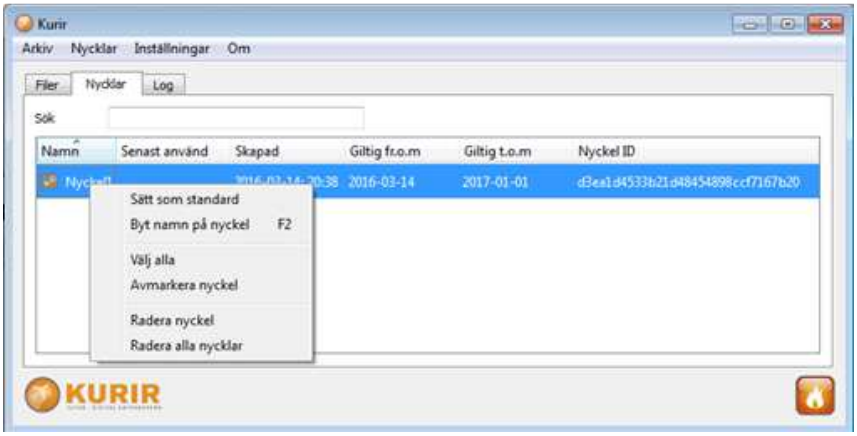
3.1.2. Standardnyckel

Vid behov, kan man med funktionen standardnyckel ange den kryptonyckeln som alltid användas vid kryptering.

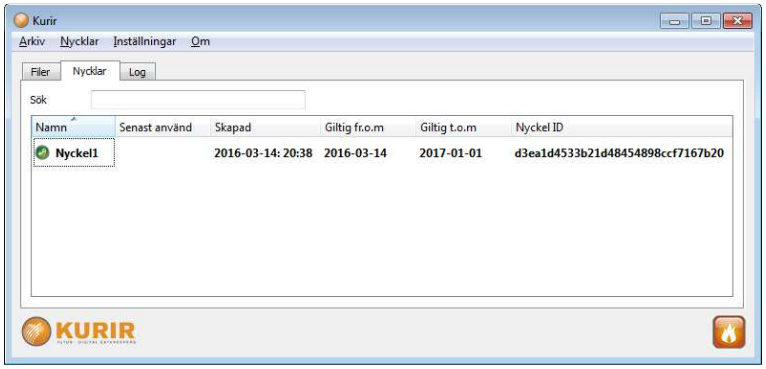
Kryptonyckel för kryptering kan även väljas för hand varje gång man väljer att kryptera en fil. Vid dekryptering sker alltid automatiskt utpekning av kryptonyckel.

För att välja Standard nyckel:

1) **Klicka-höger** på aktuell kryptonyckel och välj: **Sätt som standard**

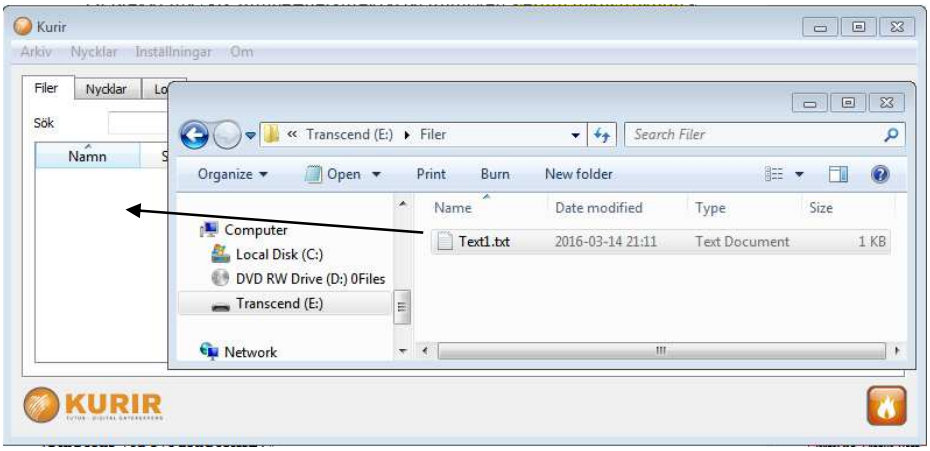


2) **Klart!** (Nyckel-ikonen blir grön)

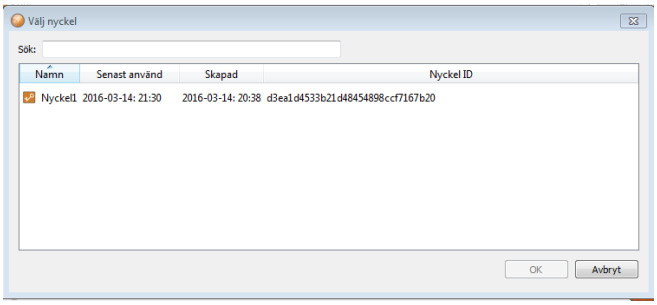


3.2. Kryptera

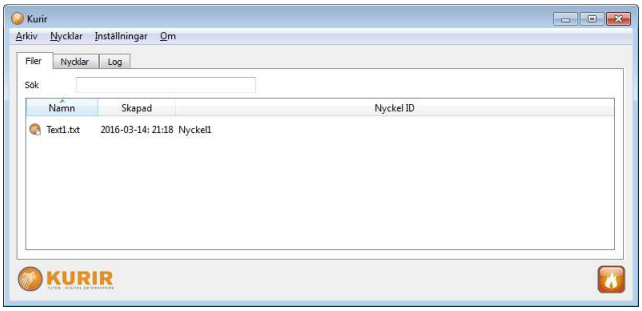
1) **Dra** klartext-fil från Windows utforskare till någon plats i programmet.



2) Om inte standardnyckel är vald, dubbelklicka på **den kryptonyckel som ska användas**



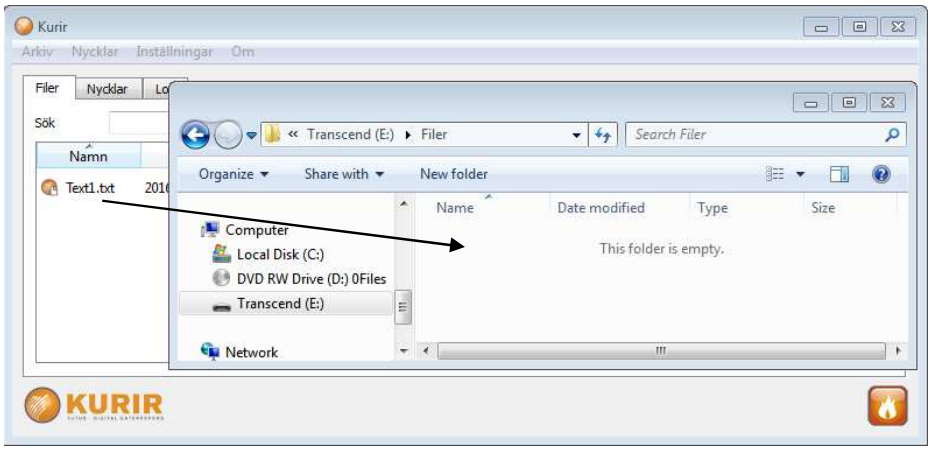
3) **Klart!** (Den krypterade filen syns i fliken filer utan filändelsen .kke)



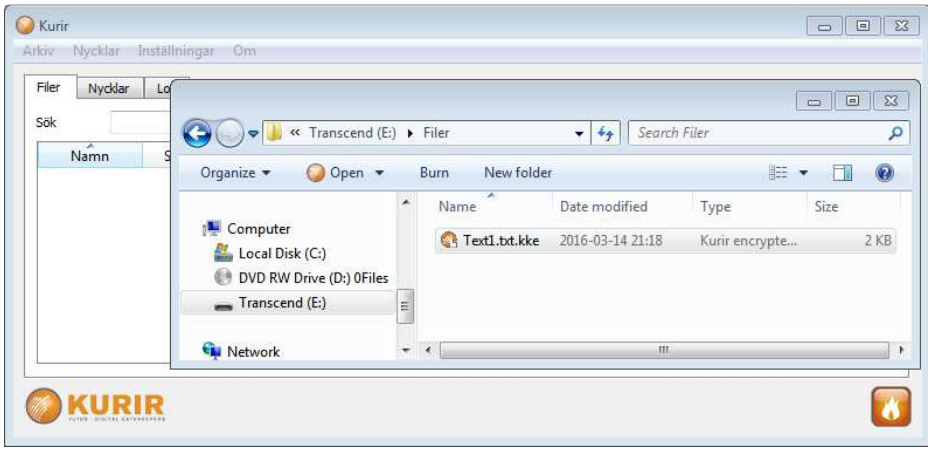
3.2.1. Flytta fil

Vid behov, flytta den krypterade filen till önskat ställe, men för att få radering med överskrivning, måste ”drag´n´drop” användas.

1) **Dra** Krypto-fil från programmet utforskare till någon plats på datorn via windows utforskare.

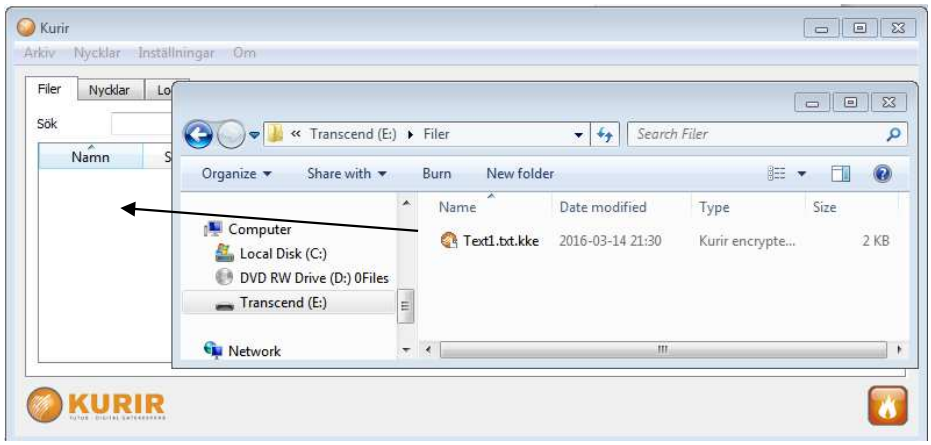


2) **Klart!** (Den krypterade filen syns i utforskaren med filändelsen kke)..

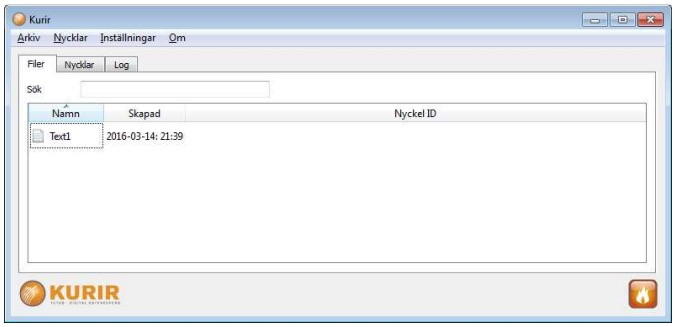


3.3. Dekryptera

1) **Dra** kryptotext-fil från Windows utforskare till någon plats i programmet (kryptonyckel väljs automatiskt bland importerade kryptonycklar).



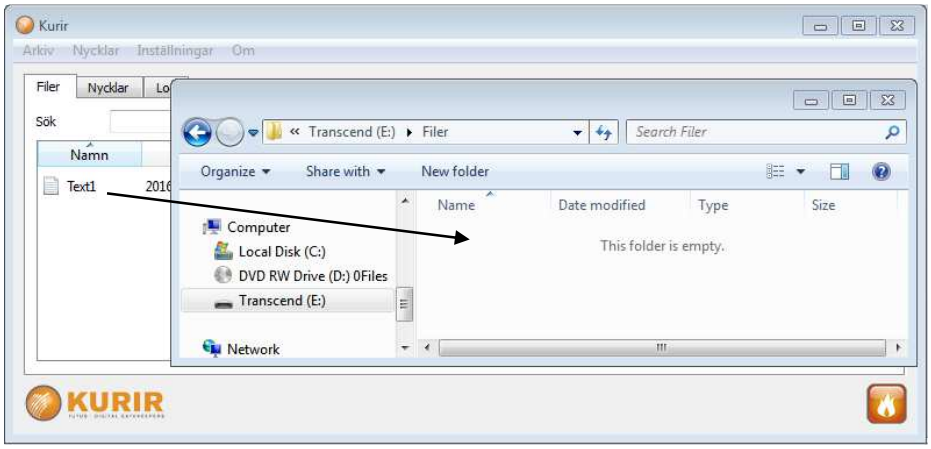
2) **Klart!** (Den dekrypterade filen syns i fliken filer utan sin ursprungliga filändelse).



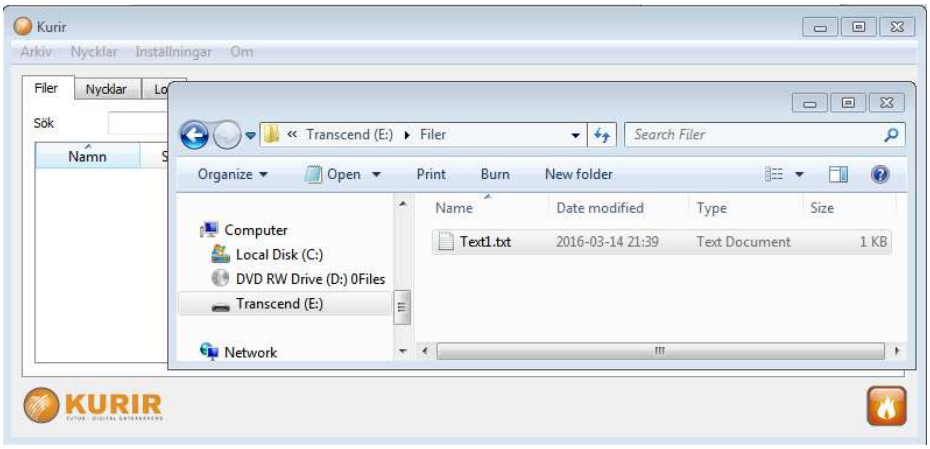
3.3.1. Flytta fil

Vid behov, flytta den krypterade filen till önskat ställe.

1) **Dra** Klartext-fil från programmet till någon plats på datorn genom windows utforskare.



2) **Klart!** (Den dekrypterade filen syns i utforskaren med sin ursprungliga ändelse).

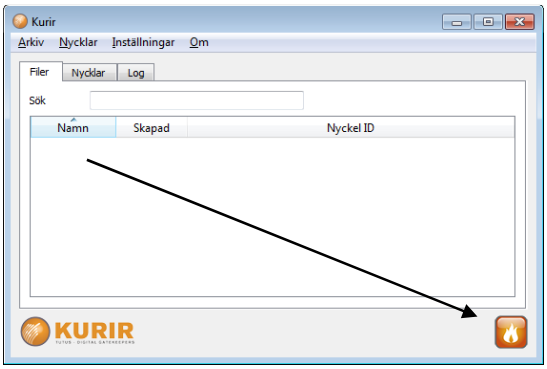


3.4. Filförstörare

Programvaran innehåller ett överskrivningsverktyg som kan användas för att radera filer. Vid behov så kan således kryptonycklar och filer som finns i programmet raderas med stöd av detta verktyg.

För att radera en fil med hjälp av överskrivningsverktyget:

1) **drag´n´drop** objekt (fil/kryptonyckel) från fliken till ikonen.



2) **Varningstext**