1.0

WinTid

Kryptering av sykemeldingsnotater og ansattlogg

Innholdsfortegnelse

Dokumenthistorikk

Dato	Versjon	Laget av	Godkjent av	Beskrivelse av endring
2018.04		KSH		

1. Om dokumentet

1.1 Dokumentets målsetning

Dette dokumentet inneholder en beskrivelse av hvordan man krypterer eksisterende sykeoppfølgingsnotater og ansattloggelementer samt skrur på kryptering for fremtidige notater.

1.2 Hvem er dokumentet skrevet for?

Dokumentet er beregnet for IT-personell. Dokumentet er også et støtteverktøy for teknikere i CGI Norge AS.

1.3 Oppbygning og oppbevaring

Dokumentet oppbevares hos CGI Norge AS.

1.4 Ansvarlig for vedlikehold av dokumentet

CGI Norge AS er ansvarlig for at dokumentet blir vedlikeholdt.

2. Forutsetninger og forbehold

2.1 Forbehold

Krypteringen forutsetter at WinTid g2 er oppgradert til versjon 13.0.0 eller nyere. Krypteringen benytter en krypteringsnøkkel lagret i klartekst i konfigurasjonsfilene til WinTid g2, WinTidServer og minWinTid, og kunden selv er ansvarlig for å sikre at disse konfigurasjonsfilene ikke er tilgjengelige for uvedkommende.

Dersom WinTid g2 er installert lokalt på brukernes klientmaskiner må man ikke benytte kryptering, da alle som har installert WinTid g2 på sin maskin vil kunne hente ut krypteringsnøkkelen og potensielt benytte denne til å dekryptere data.

Dersom brukere åpner WinTid g2 via filshare må det sørges for at de ikke har tilgang til å åpne filen dashboard.exe.config.

3. Programvare

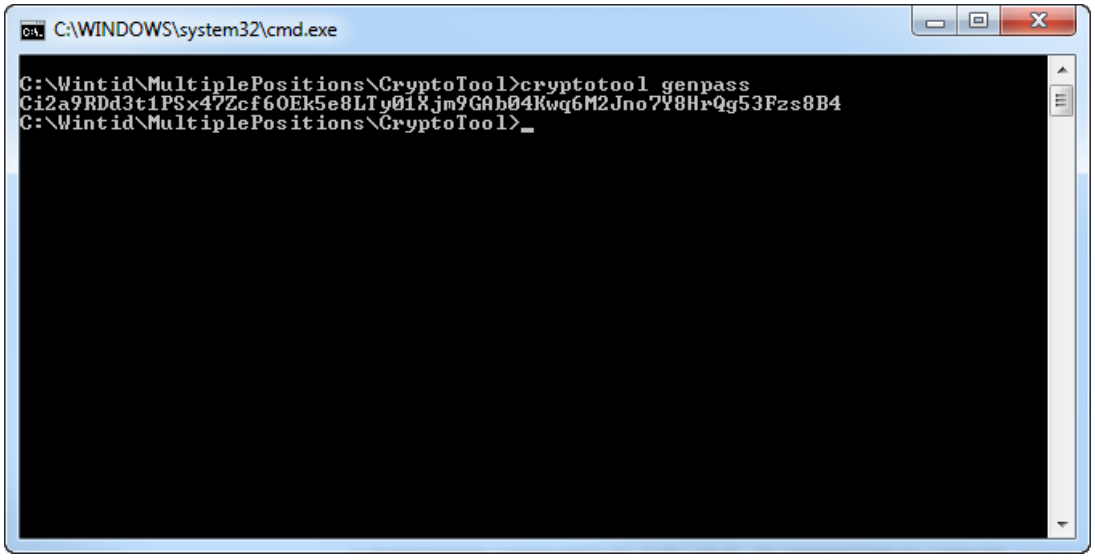
To programmer brukes ved krypteringen. CryptoTool brukes for å generere en krypteringsnøkkel, mens SickLeaveEncryptionTool utfører selve krypteringen av eksisterende data.

3.1 CryptoTool

For å kunne kryptere dataene trenger WinTid en krypteringsnøkkel. En krypteringsnøkkel er en streng bestående av tall og bokstaver. Strengen kan opprettes av kunden selv, men CGI anbefaler at man benytter CryptoTool til å generere en sikker nøkkel. CryptoTool kjøres i et kommandolinjevindu ved å navigere til riktig mappe og skrive

```
cryptotool genpass
```

Når man trykker enter vil det genereres en krypteringsnøkkel på 64 tegn. Denne må kopieres og oppbevares på et trygt sted – det er svært viktig at det finnes en backup av denne strengen.



3.2 SickLeaveEncryptionTool

SickLeaveEncryptionTool må også kjøres fra et kommandolinjevindu. Denne applikasjonen trenger en kunde.config-fil for å vite hvilken databaseserver den skal koble til. Denne config-filen kan for eksempel kopieres fra Dashboard-mappen. I tillegg må det ligge en fil der ved navn SickLeaveEncryptionTool.exe.config, som følger med installasjonen. I denne filen må

krypteringsnøkkelen som er generert legges inn under <appSettings> som verdi til encryptionKey. Som standard ligger dette inne:

```
<add key="encryptionKey" value="key123456"/>
```

key123456 **må** erstattes med krypteringsnøkkelen som er generert med CryptoTool eller andre metoder.

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>

  <configSections>
    <section name="log4net" type="log4net.Config.Log4NetConfigurationSectionHandler, log4net" />
  </configSections>
  <appSettings>
    <add key="encryptionKey" value="key123456"/>
  </appSettings>

  <log4net>
    <appender name="SickLeaveEncryptionTool" type="log4net.Appender.FileAppender,log4net">
      <param name="File" value="..\\Logg\\sickleavenotes_encryptiontool_log" />
      <param name="AppendToFile" value="true" />
      <layout type="log4net.Layout.PatternLayout,log4net">
        <param name="ConversionPattern" value="%d [%t] %-5p %c - %m%n" />
      </layout>
    </appender>

    <root>
      <level value="INFO" />
      <appender-ref ref="SickLeaveEncryptionTool" />
    </root>

    <renderer renderingClass="Ementor.Medina.Logging.MethodRenderer, Ementor.Medina, Culture=neutral" renderedClass=
    "System.Reflection.MethodBase, mscorlib, Culture=neutral, PublicKeyToken=b77a5c561934e089" />
  </log4net>

</configuration>
```

4. Rutine for kryptering

Dette kapittelet beskriver hvordan krypteringen gjennomføres.

4.1 Forberedelser

Stopp alle WinTid-tjenester, ta minWinTid offline og sørg for at ingen benytter WinTid g2 mens krypteringen gjøres. Dette kan gjerne gjøres i forbindelse med en oppgradering.

4.2 Generer krypteringsnøkkel

Benytt CryptoTool beskrevet i kapittel 3.1 eller egne metoder for å generere en krypteringsnøkkel. Denne strengen bør være på 64 tegn, må tas godt vare på og ikke gjøres tilgjengelig for uvedkommende.

4.3 Legg krypteringsnøkkelen inn i alle relevante konfigurasjonsfiler

Krypteringsnøkkelen må legges inn i flere konfigurasjonsfiler, avhengig av hvordan WinTid kjøres. Hvert program har sin egen applikasjonsspesifikke konfigurasjonsfil, og i alle tilfeller må det legges inn en linje under <appSettings>:

<add key="encryptionKey" value="*Nøkkel*"/>

Nøkkel erstattes med krypteringsnøkkelen som ble generert i 4.2. Denne må omsluttes av hermetegn. Dersom krypteringsnøkkelen for eksempel er *Qm76Hcs9PCn48Gew3Y5RkSj02XxKo12Zgz4DEi9b3M6Bfa0L8Ayq5O7FrWl13Npd* vil linjen se slik ut:

<add key="encryptionKey" value="
Qm76Hcs9PCn48Gew3Y5RkSj02XxKo12Zgz4DEi9b3M6Bfa0L8Ayq5O7FrWl13Npd"/>

4.3.1 WinTid g2

Konfigurasjonsfilen til WinTid g2 ligger under WinTid\Dashboard og heter dashboard.exe.config. Dersom alle brukerne åpner WinTid g2 via WinTidServer er det ikke nødvendig – eller anbefalt – å legge inn krypteringsnøkkelen i dashboard.exe.config.

4.3.2 WinTid Server

Dersom man benytter WinTid Server for å starte WinTid g2 må krypteringsnøkkelen legges inn i filen wintidserver.exe.config under WinTid\WinTidServer. Denne nøkkelen vil overstyre det som eventuelt måtte ligge i dashboard.exe.config-filen til WinTid g2.

4.3.3 minWinTid

Krypteringsnøkkelen må legges inn i filen WinTid\minWinTid\web.config. Dersom man har flere webservere må nøkkelen legges inn på alle serverne.

4.3.4 SickLeaveEncryptionTool

Krypteringsnøkkelen må legges inn i SickLeaveEncryptionTool.exe.config slik at riktig krypteringsnøkkel blir brukt ved kryptering av databasen.

4.4 Kjør SickLeaveEncryptionTool

SickLeaveEncryptionTool kjøres fra et kommandolinjevindu. Naviger til riktig mappe, og skriv

```
SickLeaveEncryptionTool.exe
```

Applikasjonen vil gå gjennom alle sykeoppfølgingsnotater og ansattlogging i databasen og kryptere dem. Dersom det er ansatte som er slettet fra WinTid kan det ligge notater eller loggelementer igjen etter dem som ikke har blitt slettet, grunnet en feil i WinTid som senere har blitt rettet. Programmet vil slette alle slike elementer.

Programmet vil også sette *allow_unencrypted_data* i tabellen wt_system til 0. Dette betyr at dersom det ikke ligger en krypteringsnøkkel i konfigurasjonsfilen til applikasjonen du benytter (WinTid g2/WinTid g2 med WinTid Server/minWinTid) vil man ikke kunne se sykeoppfølgingsnotater eller ansattlogger.