

Sändlista

Ert tjänsteställe, handläggare

Ert datum

Er beteckning

Vårt tjänsteställe, handläggare

Vårt föregående datum

Vår föregående beteckning

FST CIO, Daniel Vikström

Instruktion – Totalsträckskrypterade applikationer för samtal och meddelanden

1. Bakgrund

Underrättelsehotet mot Försvarsmakten är högt och avlyssning av telefonsamtal och meddelanden är kända tillvägagångssätt hos hotaktörer.

2. Instruktion

I syfte att:

- Försvåra avlyssning av samtal och meddelanden som sänds via telefonnätet.
- Försvåra spoofing av telefonnummer.

Ska följande åtgärder vidtas:

- Använd en totalsträckskrypterad¹ applikation för alla samtal och meddelanden till motparter i och utanför Försvarsmakten som har möjlighet att använda totalsträckskrypterad applikation.

2.1. Utpekad applikation

Försvarsmakten använder Signal som totalsträckskrypterad applikation.

¹ Teknik som innebär att endast avsändare och mottagare har tillgång till ett meddelande i klartext.

(DVI)



Huvudskälet till valet av Signal är att applikationen har en stor spridning bland myndigheter, industri, partners, allierade och andra samhällsaktörer. Bidragande skäl är att Signal har genomgått flera oberoende externa säkerhetsgranskningar, signifikanta fynd vid dessa har omhändertagits. Säkerheten i Signal antas därför vara tillräcklig för att försvåra avlyssning av samtal och meddelanden.

Signal är fri och öppen programvara och innebär inga investeringar eller licenskostnader för Försvarsmakten.

Signal finns i versioner för iPhone, iPad, Android och de vanligaste operativsystemen för persondatorer. Signal stödjer samtal, meddelanden, gruppmeddelanden, gruppsamtal och videosamtal.

Handledning för konfiguration och användning av Signal publiceras på Försvarsmaktens intranät.

2.1.1. Sekretessbelagd information i Signal

DET INTE ÄR TILLÅTET ATT SÄNDA SÄKERHETSSKYDDSKLASSIFICERADE UPPGIFTER MED SIGNAL

Det är tillåtet att använda signal för samtal och meddelanden som innehåller sekretessbelagda uppgifter som inte är säkerhetsskyddsklassificerad. Åtgärder ska vidtas för att meddelanden som innehåller sekretess inte lagras längre än nödvändigt.

Det är inte tillåtet att hantera filer som innehåller sekretessbelagda uppgifter i Signal.

2.2. Andra applikationer

Verksamheter som har behov av annan totalsträckskrypterad applikation hemställer till FST CIO om godkännande. Hemställan ska redogöra för verksamhetsbehov och en initial lämplighetsbedömning av applikationen.

3. Avgränsning

Denna instruktion gäller inte för samtal och meddelande som behandlar säkerhetsskyddsklassificerad information. Vid överföring av sådan information ska ett godkänt signalskyddssystem användas.

Att använda signalskyddssystem, till exempel ROBOT, uppfyller kravet i punkt 2.



4. Beslut

Denna instruktion har beslutats av brigadgeneral Mattias Hanson. I den slutliga handläggningen har deltagit överste, Jan Engman, överste Daniel Harlin, överstelöjtnant Johan Strömquist, it-säkerhetsstrateg Fredrik Börjesson och som föredragande chefsingenjör Daniel Vikström.

Hanson, Mattias

FM CIO

Handlingen är fastställd i Försvarsmaktens elektroniska dokument- och ärendehanteringssystem.

Sändlista

HKV

AST, LG, I 13, I 19, I 21, K 3, K 4, P 4, P 7, P 18, A 8, A 9, Lv 6, Ing 2, T 2,
SWEDEC, SkyddC, MSS

MS, 1.ubflj, 3.sjöstriflj, 4.sjöstriflj, Amf 1, Amf 4, MarinB, SSS

FS, F 7, F 16, F 17, F 21, Hkpflj, LSS

MR Syd, MR Väst, MR Mitt, MR Norr, HvSS

FMLOG, FMTS, FömedC

MHS K, MHS H, FM HRC

LedR, FMTIS, FMUndSäkC

SOG