Utgåva	Diarienummer	Ärendetyp
2.0	11FMV11104-3:2	3.5
Ansvarig Enhet	Datum	Sida
AK Led	2012-06-19	1(11)

FMV Handläggare, telefon

Thomas Dahlbeck

Arbetsutgåva och datum

Datasluss - Introduktion och användningsfall

FMV
Försvarets materielverk
115 88 Stockholm
Besöksadress: Banérgatan 62

Tel: 08-782 40 00
Fax: 08-667 57 99

registrator@fmv.se
www.fmv.se

Org.nr: 202100-0340
VAT nr: SE202100-0340-01

Innehållsförteckning

1 INTRODUKTION 3

1.1 INLEDNING 3
1.2 REFERENSER 3
1.3 DEFINITIONER 3

2 ÖVERSIKT 4

2.1 ALLMÄNT 4
2.2 SKILLNAD MELLAN GARM TYP 2 OCH GARM TYP 3 4
2.3 AVGRÄNSNINGAR 4

3 KOMMUNIKATIONSTYPER 6

3.1 DUBBELRIKTAD INFORMATIONSÖVERFÖRING MELLAN SAMMA ELLER OLIKA INFORMATIONSSÄKERHETSNIVÅ 6
3.2 ENKELRIKTAD INFORMATIONSÖVERFÖRING FRÅN LÄGRE TILL HÖGRE INFORMATIONSSÄKERHETSNIVÅ 6
3.3 ENKELRIKTAD INFORMATIONSÖVERFÖRING FRÅN HÖGRE TILL LÄGRE INFORMATIONSSÄKERHETSNIVÅ 6

4 ÖVERFÖRINGSTYPER 7

4.1 ÖVERFÖRING AV MEDDELANDEN 7
4.2 ÖVERFÖRING AV FILER 7
4.3 ÖVERFÖRING MED KONTROLL AV CERTIFIKAT 7

5 EXEMPEL PÅ ANVÄNDNINGSFALL 8

5.1 EXEMPEL 1 – ÖVERFÖRING AV E-POST MED SMTP 8
5.2 EXEMPEL 2 – FFT INFORMATIONSUTBYTE MED NFFI 8
5.3 EXEMPEL 3 - UTBYTE AV LUFTLÄGESINFORMATION I CAPDE 10

6 PROCESSER FÖR IMPLEMENTERING OCH ANVÄNDNING AV DATASLUSS GARM TYP 2 OCH 310

6.1 ALLMÄNT 10
6.2 BEHOVSPRÖVNING 10
6.3 DEFINITION 11
6.4 FRAMTAGNING 11
6.5 PAKETERING 11
6.6 INSTALLATION/DRIFTSÄTTNING 11
6.7 ADMINISTRATION 11

1 Introduktion

1.1 Inledning

Detta dokument är en del i kravspecifikationerna för generell datasluss Garm typ 2 och typ 3.

Dokumentet beskriver hur Försvarsmakten avser använda Garm typ 2 och typ 3. Beskrivningen utgörs av en översiktlig beskrivning samt ett antal typiska användningsfall samt en översiktlig beskrivning av de processteg som avses gälla för användning av Garm typ 2 och typ 3.

1.2 Referenser

Ref. nr.	Dokument	Dok. nr.
1	DIT04	HKV

1.3 Definitioner

Förkortning	Definition/förklaring
Garm	Försvarsmakten datasluss

2 Översikt

2.1 Allmänt

Generell datasluss ska utgöra en gemensam plattform som skall stödja förmågan att flytta information mellan två separerade system eller nät. Samtidigt ska den kunna vara en del i ett intrångsskydd och genomföra kontroller på transporterat data. System skall kunna kommunicera med generell datasluss som i sin tur skickar kontrollerat data vidare till ett målsystem. Generell datasluss ska kontrollera semantik och filtrera innehållet, allt enligt fördefinierade regler. Generell datasluss skall säkerställa att endast kontrollerat och filtrerat data förs mellan två nät, utan att något metadata eller annan dold trafik kan passera med skickat data.

Man skall kunna anpassa generell datasluss efter behov genom att definiera vilken/vilka typer av information som skall kunna passera. Detta görs genom att ett filter för avsedd kommunikation som paketeras och laddas ned till aktuell datasluss.

Ett filter tillför funktionen att kunna ta emot en viss typ av information och innehåller en specifikation som beskriver vilken syntax en specifik typ av information skall ha för att data ur dessa meddelanden skall lyftas in i generell datasluss. Sedan filtreras informationen, enligt filterregeln för detta meddelandefilter, innan informationen lyfts över till det andra systemet.

Filtret styr hur data ska tas emot av generell datasluss, hur det är formaterat, hur information ska processas och innan det skickas vidare till målsystemet.

Generell datasluss skall initialt konfigureras från en administratörsnod där aktuellt filter installeras samt att vissa konfigurationsparametrar som t.ex. IP adresser kan konfigureras.

Alla händelser av betydelse för säkerheten, t.ex. autentiseringar, samt alla konfigurationsförändringar skickas till en externt logg- och larmsystem.

Generell datasluss skall säkerställa att det inte kan skapas en förbindelse mellan olika system/nät.

Generell datasluss är inte en ren mjukvaruprodukt utan en kombination av hård och mjukvara.

2.2 Skillnad mellan Garm typ 2 och Garm typ 3

Skillnaderna mellan generell datasluss Garm typ 2 och Garm typ 3 är att Garm typ 3 är en ”ruggad” och RÖS-godkänd version med fiberanslutningar av Garm typ 2.

Programkod skall vara densamma för bägge versionerna (typ 2 och typ 3) för att filter och programkod för tjänstenoderna som utvecklas skall gå att använda på bägge versionerna.

2.3 Avgränsningar

Garm typ 2 och 3 är inte ett komplett system där man enkelt kan konfigurera vilket eller vilka filter som skall användas samt vilka parametrar som gäller för dessa filter utan för varje tillämpning av Garm typ 2 och 3 tas det fram specifika filter som paketeras tillsammans med programvaran för tjänstenoderna i signerade paket för respektive individnummer av Garm typ 2 och 3.

Eventuella krav på redundans löses ej av Garm typ 2 och 3 utan måste lösas av de system som kräver detta.

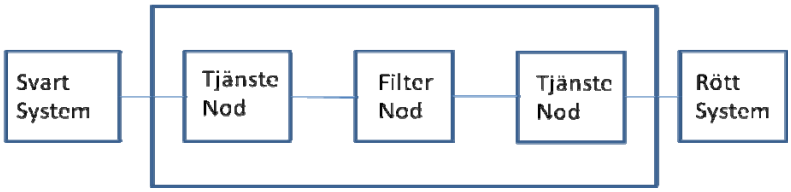
Datasluss är avsett att användas för att möjliggöra informationsöverföring mellan miljöer som inte får ha trafikförbindelse. Av denna anledning får inte nätverkstrafik passera genom dataslussen.

Hantering och analys av säkerhetsloggar ingår inte i datasluss utan hanteras av respektive system som skall använda datasluss enligt direktiv och beslut i samband med godkännande av filter för respektive tillämpning. Detta innebär att eventuella krav på mellanlagring av loggar innan det kan skickas vidare till ett loghanteringssystem ska hanteras utanför GARM typ 2 och 3.

Virusskydd och skydd mot skadlig kod ingår inte i GARM typ 2 och 3 utan löses av anslutna system.

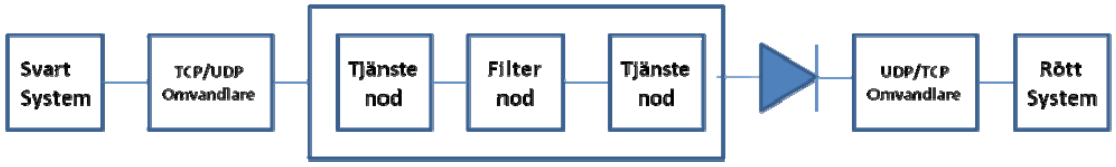
3 Kommunikationstyper

3.1 Dubbelriktad informationsöverföring mellan samma eller olika informationssäkerhetsnivå



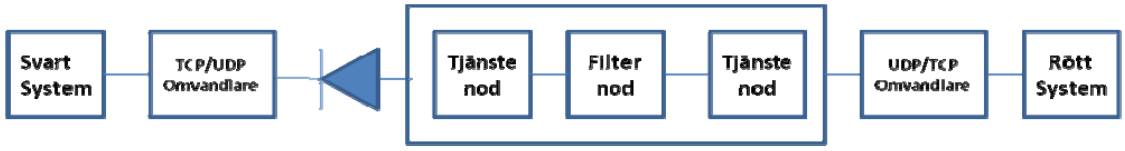
Informationen som flyttas mellan svart och rött system kontrolleras av filternoden som i vissa fall även kan fungera som en mjukvarudiod.

3.2 Enkelriktad informationsöverföring från lägre till högre informationssäkerhetsnivå



Med hjälp av en datadiod kan man med hög assurans säkerställa att ingen information kan läcka ut från det nät eller system med högre informationssäkerhetsnivå till system eller nät med lägre informationssäkerhetsnivå.

3.3 Enkelriktad informationsöverföring från högre till lägre informationssäkerhetsnivå



Med hjälp av en datadiod kan man med hög assurans säkerställa att inga angrepp kan ske från det nät eller system med lägre informationssäkerhetsnivå till system eller nät med högre informationssäkerhetsnivå.

4 Överföringstyper

4.1 Överföring av meddelanden

Med väl definierade syntax och protokoll på meddelanden kan filter tas fram för generell datasluss som medger att meddelanden kan överföras mellan olika system med olika informationssäkerhetsklass.

4.2 Överföring av filer

Filter för denna typ av överföring kontrollerar att filen är av rätt typ och format och kan i vissa konfigurationer även kontrollera att visst innehåll ej finns med.

4.3 Överföring med kontroll av certifikat

Filter för denna typ av överföring bygger på att det finns ett förtroende för certifikatet och den person eller system som sänder informationen. Förutom kontroll av certifikatet sker även kontroll på att meddelandet eller filen har rätt struktur.

5 Exempel på användningsfall

5.1 Exempel 1 – Överföring av E-post med SMTP

Detta exempel beskriver tre olika användningsfall för överföring av e-post med SMTP.

För alla användningsfall i detta exempel skall tjänstenoderna kunna fungera som en MTA enligt RFC 4409 och kunna ta emot SMTP-meddelanden enligt RFC 5322 med MIME format enligt RFC 2045 och SMIME enligt RFC 3851 med text/plain och UTF 8.

Mottagande tjänstenod omvandlar e-post meddelandet till ett intermediärformat och skickar över det till filternoden. I dessa användningsfall tar tjänstenoden även bort eventuella bilder och bifogade filer. Tjänstenoden bygger även om headern till bara en mottagare och tar bort all annan headerinformation

Filternoden verifierar den digitala signaturen samt kontrollerar att bodyns text har svensk teckenuppsättningen och i övrigt inte innehåller någon dold information som t.ex. url, text eller bild.
Filternoden kontrollerar även avsändaren och mottagarens domän och namn mot godkända adresser (vitlista).

Efter dessa kontroller skickar filternoden meddelandet vidare till nästa tjänstenod som bygger ihop meddelandet igen och skickar det till mottagaren.

De tre användningsfallen för överföring av E-post med SMTP utgörs av följande:

a) SMTP-meddelande sänds från den svarta sidan av dataslussen för att sändas vidare till system på den röda sidan.

b) SMTP-meddelande sänds från den röda sidan på dataslussen för att sedan sändas vidare till system på den svarta sida.

c) SMTP-meddelande sänds dubbelriktat mellan system på svart och röd sida via dataslussen.

5.2 Exempel 2 – FFT informationsutbyte med NFFI

Detta exempel på användningsfall beskriver informationsutbyte med Friendly Force Tracking (FFT) via NFFI-gränsytan (NATO Friendly Force Information) .

Informationsutbytet kan ske dels ske mellan blått nät (Mission Restricted) och annan nation/organisations blått nät och dels mellan rött nät (Secret) och annan organisations nät (Secret).

För detta informationsutbyte ställs det följande krav:

1. Garm typ 2 och 3 med NFFI-filter skall kunna förmedla NFFI meddelanden enligt NFFI version 1.3.
2. Nätverkstrafik skall inspekteras på applikationsnivå.
3. Meddelanden skall kunna tillåtas eller avvisas baserat på källans och/eller mottagarens protokoll, IP-adress och/eller portnummer.
4. *Garm typ 2* och *3* med NFFI-filter skall stödja NFFI IP1 (*NFFI Interface Profile 1, Two way unicast reliable push*. Protokoll för NFFI baserat på TCP.)

5. Garm typ 2 och 3 med NFFI-filter skall kunna kontrollera om Wrapper (*NFFI Wrapper, ett m*eddelandehuvud som används i både IP1 och IP2.) överensstämmer med specifikationen och godkänna eller avvisa meddelande bland annat baserat på detta.
6. Meddelanden skall kunna godkännas eller avvisas baserat på följande fält i Wrapper:
   a. *Message Type* (korrekt värde enligt spec. (= 0))
   b. *Packet Segement Number* (korrekt värde enligt spec.)
   c. *Encoding* (= 0)
   d. *Spare* (korrekt värde enligt spec. (= 0))
   e. *Payload Length* (överensstämmelse med verklig längd på Payload) (*NFFI Payload,* Själva innehållet i ett NFFI-meddelande i form av ett XML-dokument.)
7. Meddelanden bör kunna godkännas eller avvisas baserat på följande fält i Wrapper:
   a. *Destination country/system/subsystem* (jämföra med konfigurerbara värden, eller lista av värden)
   b. *Timestamp* (rimlighetskontroll)
   c. *Encoding* (Enligt filtrets funktionalitet om Payload skall inspekteras)
   d. *Source country/system/subsystem* (jämföra med konfigurerbara värden, eller lista av värden)
   e. *Payload Length* (konfigurerbart maximalt värde)
8. Implementationen bör vara förberedd för att införa andra kodningar/komprimeringar av Payload.
9. Meddelanden skall kunna godkännas eller avvisas baserat på om Payload överensstämmer med NFFI 1.3 XML-schemat i specifikationen.
10. Garm typ 2 och 3 med NFFI-filter bör kunna filtrera meddelande och avvisa hela eller utesluta delar av ett meddelande baserat på följande information i Payload:
    a. Avsändarsystem (*sourceSystem*)
    i. Enligt konfigurerbar lista
    ii. Överenstämmelse med information i Wrapper
    b. Säkerhetsmärkning (attributen *secPolicyName, secClassification* och *secCategoryType*; värdena bör kunna kontrolleras mot en regel definierad som t.ex. ett reguljärt uttryck).
    c. Identitet på enheten som positionsdata gäller (*transponderId* och/eller *unitSymbol, unitShortName*) enligt konfigurerbar lista.
    d. Rimlighet eller geografisk avgränsning i positionsdata, enligt konfigurerbart område.
    e. Märkning av positionsdata med *credibility*
    f. Godtyckliga element eller attribut i Payload (*Ej prioriterat*)
11. Garm typ2 och 3 med NFFI-filter skall kunna hantera NAT.
12. Garm typ 2 och 3 med NFFI-filter skall konstrueras på sådant sätt att NFFI IP2 (*NFFI Interface Profile 2. One-way unreliable push*. Protokoll för NFFI baserat på UDP.)och SIP3 kan implementeras i ett senare skede.
13. Garm typ 2 och 3 med NFFI-filter bör kunna förändra NFFI Payload:
    a. Filtret bör i den första versionen kunna filtrera ur ”Mandatory” fälten i ”positionalData”-sektionen, bygga om strukturen och skicka paketet vidare.
    b. Det bör vara konfigurerbart om filtrering på ”Mandatory” fält ska vara aktivt.

c. Filtret bör i den första versionen kunna filtrera ur ”Mandatory” fälten i ”positionalData”-sektionen, samt valbara sektioner i ”identificationData”, bygga om strukturen och skicka paketet vidare.

14. Accepterade och nekad nätverkstrafik skall loggas.
15. De generella funktionerna för logghantering, administration, tidssynkronisering, ARP mm. som finns i Garm typ 2 och 3 skall kunna användas.
16. NFFI-filtret skall konstrueras på sådant sätt att ytterligare filter lätt kan implementeras.

5.3 Exempel 3 - Utbyte av luftlägesinformation i CAPDE

I detta användningsfall skall dataslussen ingå som en komponent i system CAPDE och syfta till att filtrera luftlägesinformation som utbyts mellan C2STRIC/LS10 och andra staters C2−system. C2STRIC/LS10 är anslutna mot en komnod över en krypterad förbindelse som utbyter meddelanden av typ 400:8. Dataslussen sitter bakom komnoden och skall filtrera innehållet i dekrypterade 400:8−meddelandena.

Dataslussen kommer att filtrera UDP−paket innehållande ett eller flera meddelanden enligt en separat beskriven layout. Meddelandena innehåller motsvarande information som sänds för tracks över link 1 enligt STANAG 5501 (Digital Data Link – Link 1), . På röd sida används meddelande 400:8 (GYS 400:8) för att transportera informationen till C2STRIC och LS10. En formatkonverterare ansluts på röd sida av filtret som konverterar 400:8 till det meddelandeformat som sänds genom filtret för utgående trafik och tvärtom för inkommande trafik. På svart sida ansluts en formatkonverterare som konverterar från externt format (ej nödvändigtvis 400:8) till filterformat för inkommande trafik och tvärtom för utgående trafik. Filtret släpper endast igenom fält som finns reprenterade i link 1 enligt STANAG 5501. Värdemängderna kan skilja mellan fält i GYS 400:8 och STANAG 5501. Filtret släpper igenom den värdemängd som motsvarar 400:8.

Formatkonverteraren på röd sida måste lägga till information om vilka avtalsparter som skall få det aktuella meddelandet, fältet "Mottagarpart".

Filterreglerna specificeras per protokollnivå i det totala paketet som utgörs av en Ethernetram.

6 Processer för implementering och användning av Datasluss Garm typ 2 och 3

6.1 Allmänt

Detta är en översiktlig beskrivning av processtegen som måste genomgås för respektive system för implementering och användning av datasluss.

Ansvarig för att denna process följs är Systemägaren för respektive berört system.

6.2 Behovsprövning

För att få påbörja specificering och framtagning av tillämpningsmjukvara för tjänstenod och filter till datasluss krävs det Auktorisationsbeslut B1 enligt FM DIT 04 för användning av datasluss.

I detta steg skall en översiktlig beskrivning av behov och användning av datasluss tas fram och godkännas för vidare framtagning av filterspecifikation.

I samband med detta processteg kontrolleras även om det redan finns ett filter framtaget för denna typ av tillämpning som kan återanvändas i befintligt skick eller med små modifieringar.

6.3 Definition

I detta processteg skall en detaljerad beskrivning av funktion för tjänstenod samt detaljerad beskrivning av filter tas fram och godkännas inför utveckling (Auktorisationsbeslut B2-B3 enligt DIT 04)

6.4 Framtagning

I detta processteg ingår att utveckla tillämpningsmjukvara för tjänstenod och filter inkl. 3:e parts granskning samt godkännande av MUST SÄKK SÄKT.

Filtret inkl användning av datasluss typ 2 och 3 skall även godkännas genom ett auktorisationsbeslut B4 enligt Dit 04.

I filterframtagning ingår även definition av vilka dynamiska parametrar som skall finnas.

6.5 Paketering

Paketering och signering av tillämpningsmjukvaran samt filtret skall ske av Försvarsmakten utpekad organisation.

I detta ingår att lägga in de statiska parametrar som gäller för respektive filter inkl vilken eller vilka serienummer på hårdvaran som det skall fungera på samt revisionsnummer på filtret för denna hårdvara.

6.6 Installation/driftsättning

I det detta processteg ingår distribution av hårdvara och paketerat och signerat filter.

Dessutom ingår slutlig anpassning/konfiguration av dataslussen där platsspecifika parametrar kan läggas in som T.ex. IP-adresser.

6.7 Administration

I detta processteg ingår drift, övervakning, service/utbyte samt insändning av datasluss till centralt förråd/verkstad.