Datum	Diarienummer	Ärendetyp
ange	ange	ange
	Dokumentnummer	Sida
	ange	1(23)

<SYSTEM> <VERSION>

IT-SÄKERHETSSPECIFIKATION
DEFINIERA (ITSS-D)

Innehåll

1 Basfakta 7
1.1 Giltighet och syfte 7
1.2 Revisionshistorik 7
1.3 Terminologi och begrepp 7
1.4 Bilageförteckning 7
1.5 Referenser 7
2 Inledning 8
2.1 Syfte 8
2.2 Kravnivå 8
2.3 Systemöversikt 8
3 Systembeskrivning 9
3.1 Förutsättningar 9
3.1.1 Avsedd användning av systemet 9
3.1.2 Systemets driftmiljö 9
3.1.3 Tänkta användare av systemet 9
3.1.4 Information 9
3.2 Systemets arkitektur 10
3.3 Systemets gränsytor 10
3.4 Säkerhetsförmågor 10
4 Sammanställning av säkerhetskrav 11
4.1 KSF-krav 11
4.2 Fastställd kravnivå 11
4.3 Funktionella säkerhetskrav 11
4.3.1 Gemensamma krav (SFGK) 11
4.3.2 Behörighetskontroll (SFBK) 11
4.3.3 Säkerhetsloggning (SFSL) 11
4.3.4 Intrångsskydd (SFIS) 12
4.3.5 Intrångsdetektering (SFID) 12
4.3.6 Skydd mot skadlig kod (SFSK) 12
4.3.7 Skydd mot röjande signaler (SFRS) 12
4.3.8 Skydd mot obehörig avlyssning (SFOA) 12
4.4 Assuranskrav 12
4.4.1 Systemutvecklingens livscykel (SALC) 13
4.4.2 Arkitektur och design (SADE) 13

4.4.3 Installation och drift (SAOP) 13
4.4.4 Administrativa rutiner (SARU) 13
4.4.5 Systemintegrationstest (SATS) 13
4.4.6 Riskanalys och sårbarhetsanalys (SARA) 13
4.5 Tillkommande säkerhetskrav 14
4.5.1 Verksamhetskrav 14
4.5.2 Riskmitigerande krav 14
4.5.3 Regelverkskrav 14
5 Säkerhetskrav på omgivningen 16
5.1 Funktionella krav 16
5.2 Fysiska krav 16
5.3 Administrativa krav 17
5.4 Organisatoriska krav 17
6 Tolkning av säkerhetskrav 18
6.1 Funktionella säkerhetskrav 19
6.1.1 Gemensamma krav (SFGK) 20
6.1.2 Behörighetskontroll (SFBK) 20
6.1.3 Säkerhetsloggning (SFSL) 20
6.1.4 Intrångsskydd (SFIS) 20
6.1.5 Intrångsdetektering (SFID) 20
6.1.6 Skydd mot skadlig kod (SFSK) 20
6.1.7 Skydd mot röjande signaler (SFRS) 20
6.1.8 Skydd mot obehörig avlyssning (SFOA) 21
6.2 Assuranskrav 21
6.2.1 Systemutvecklingens livscykel (SALC) 21
6.2.2 Arkitektur och design (SADE) 21
6.2.3 Installation och drift (SAOP) 21
6.2.4 Administrativa rutiner (SARU) 21
6.2.5 Systemintegrationstest (SATS) 21
6.2.6 Riskanalys och sårbarhetsanalys (SARA) 22
7 Uppfyllande av säkerhetskrav 23

Mallinformation 18FMV6730-4:1.2

Datum	Utgåva Version	Beskrivning	Ansvarig
2018-11-08	1.0	Mall för ITSS-D	DAOLO

Mallinstruktion

Denna mall ska användas för att ta fram IT-säkerhetsspecifikation *Definiera* ITSS-D.

ITSS-D är en bilaga till ISD-D, och innehåller tolkade och nerbrutna IT-säkerhetskrav baserade på legala krav och verksamhetskrav, vars källor är identifierade ITSS-I.

- Det färdigställda dokumentet börjar med kap 1 Basfakta.
- Sidorna innan dess innehåller beskrivningar kring vad ITSS-D innehåller och att tänka på i arbetet. Dessa sidor tas bort i det färdigställda dokumentet.
- Instruktion om vad som ska stå under varje rubrik i det skarpa dokumentet anges i gul text. Den texten ska raderas innan dokumentet färdigställs.
- Svart text kan användas direkt i det färdigställda dokumentet.
- Ersätt Systemnamn med systemets namn och versionsnummer.
- Ta bort rubriker som inte är relevanta och lägg till egna rubriker där så behövs.

Omfattning av ITSS-D

Informationssäkerhetsdeklaration Definiera (ISD-D) består av ett huvuddokument och tre bilagor;

- Bilaga 1 Analysunderlag Definiera (AU-D)
- Bilaga 2 IT-säkerhetsspecifikation Definiera (ITSS-D)
- Bilaga 3, IT-säkerhetsarkitektur (ITSA)

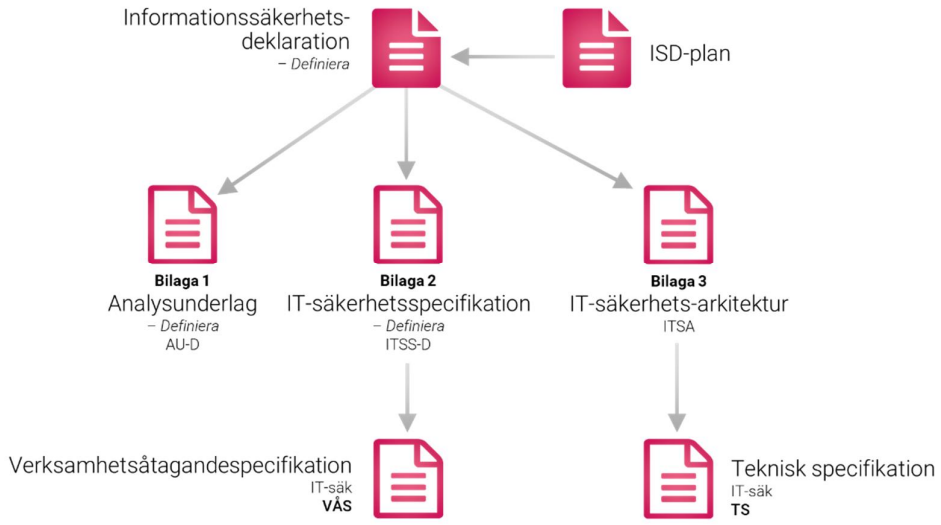
Dessa bilagor innehåller detaljer och analysunderlag för informationssäkerhetsdeklarationen där detta dokument utgör bilaga 2.

Figur nedan visar relationen mellan ISD-D och upphandlingsunderlagen Teknisk Specifikation (TS) och VerksamhetsÅtagandeSpecifikation (VÅS). *Definiera* ska resultera i TS och VÅS.

ITSS-D förser VÅS med krav på IT-säkerhetsarbete och ITSA förser TS med tolkade IT-säkerhetskrav.

ISD-planen, som är en del av genomförandeprojektets projektplan, styr IT-säkerhetsarbetet och är ett viktigt indata till dokumentet ISD-D.

Upphandlingsunderlagen är separata dokument och ingår inte i ISD 3.0.



Dokumentstruktur Informationssäkerhetsunderlag Definiera

ITSS-D omfattar:

- Säkerhetskrav
  - Fastställd av exponeringsnivå
  - Fastställd av konsekvensnivå
  - Fastställd av kravnivå
- Tolkade MUST KSF funktionella- och assuranskrav
- Tillkommande krav, d.v.s verksamhetens krav på
  - Riktighet
  - Tillgänglighet

- Spårbarhet

Att tänka på i arbetet med ITSS-D

Kraven dokumenteras och utvecklas succesivt i IT-säkerhetsspecifikationer i *Identifiera* ITSS-I, *Definiera* ITSS-D, *Realisera* ITSS-R och eventuellt *Vidmakthålla* ITSS-V. Dessa dokument utgör spårbarheten i IT-säkerhetslösningen.

ITSS-D dokumenterar kravtolkningen av MUST KSF samt verksamhetskraven (tillkommande krav) och utgör den grund som IT-säkerhetsarkitekturen (ITSA) baseras på. ITSS-D är även grunden till kraven i Verksamhetsåtagandespecifikationen, VÅS i upphandling och inför *Realisera*.

1 Basfakta

1.1 Giltighet och syfte

Detta kapitel ska entydigt identifiera systemet.

Detta dokument är ITSS-D för <System> <version> inför FMV VHL S3-beslut.

1.2 Revisionshistorik

Detta kapitel ska entydigt identifiera detta dokument.

Datum	Utgåva Version	Beskrivning	Ansvarig

Tabell 1 - Revisionshistorik

1.3 Terminologi och begrepp

Följande tabell innehåller specifika begrepp som gäller för detta dokument. En generell lista återfinns i ref [1].

Term (förkortning)	Definition	Källa	Kommentarer/ Anmärkningar
<term>	<Definition>	<Källa>	
<term>	<Definition>	<Källa>	
<term>	<Definition>	<Källa>	

Tabell 2 - Terminologi och begrepp i detta dokument

1.4 Bilageförteckning

Detta dokument har inga bilagor.

1.5 Referenser

Dokumenttitel	Dokumentbeteckning, datum	Utgåva nr
[1] ISD Begrepp och förkortningar	18FMV6730-8:1.1	1
[2] ISE Granskningsinstruktion	18FMV6730-8:1.2	1
[3] <Dokumentnamn>	<dokumentid., åååå-mm-dd>	<nr>

Tabell 3 - Referenser

2 Inledning

2.1 Syfte

Detta kapitel innehåller grundläggande information om systemet samt en övergripande systembeskrivning (högnivåbeskrivning). Systemöversikten beskriver systemets tänkta användning samt säkerhetsfunktionalitet.

ITSS-D omfattar funktionella krav (tekniska) och icke-funktionella krav (assurans) från ett IT-systemperspektiv. Ingångsvärden hämtas från AU-D och ITSS-I. Syftet med ITSS-D är att dokumentera tolkade MUST KSF samt motivera vald kravnivå baserat på exponering och konsekvenser men även tolkningar i balans med tillkommande krav.

ITSS-D är den kravmassa som, ur ett informationssäkerhetsperspektiv, utvecklingen/upphandlingen sker utifrån. ITSS-D är ett dokument som utvecklar de dimensionerande faktorerna från ISD-I såsom hur ett system exponeras mot omvärlden. En genomtänkt ITSS-D är en förutsättning för upphandling av ett realiserbart IT-system.

2.2 Kravnivå

Initial kravnivå enligt FM MUST KSF version XX för aktuellt system är: *Grund/Utökad/Hög*, enligt referens XX.

De säkerhetskrav som systemet avser att implementera styrs av systemets ISD-Strategi (referens XX) och ISD-Plan (referens XX). .

2.3 Systemöversikt

Systemöversikten ska kortfattat beskriva systemets användning och säkerhetsmekanismer samt dess övergripande systemarkitektur. Beskrivningen ska ge en översiktlig bild över systemets IT-säkerhetsförmåga och dess tänkta användning.

Den tänkta driftmiljön för systemet ska också beskrivas. Varje teknisk eller miljöfaktor som systemet är beroende av ska tas med i beskrivningen.

Aspekter att beakta och definiera är

- Systemet
- Systemets kontext (bl a omgivande system och fysisk miljö)
- Systemgränsyta, inkl gränssnitt
- Kontextgränsytan

Figur Systemöversikt

Figur 1 Systemöversikt

3 Systembeskrivning

I detta kapitel ges en utförlig beskrivning av systemet. I beskrivningen definieras systemets förutsättningar, arkitektur, gränsytor samt säkerhetsförmågor.

IT-systemets arkitektur ska lista systemkomponenter och beskriva hur de tillsammans bygger upp systemet.

IT-systemets alla logiska och fysiska gränsytor ska beskrivas för att ge en bild av den attackyta de utgör.

IT-systemets säkerhetsförmågor ska beskrivas på en detaljnivå som är tillräcklig för att ge läsaren en allmän förståelse för dessa. Beskrivningen förväntas vara mer detaljerad än den som ges i kapitlet Inledning.

När systemets arkitektur och säkerhetsförmågor beskrivs skall det framgå vilka delar som tillhör systemet och vilka som är externa beroenden.

3.1 Förutsättningar

Information i detta kapitel kan hämtas från ITSA och AU-D.

Säkerhetsrelevant information kring systemets förutsättningar måste redovisas så att den rätta kravnivån för systemet ska kunna fastställas, därmed måste följande framgå:

- avsedd användning av systemet, d.v.s. det verksamhetsstöd det erbjuder
- hur dess driftmiljö är beskaffad, t.ex. vad gäller fysiskt skydd av systemet
- vilka de tänkta användarna av systemet är
- vilken information som lagras, överförs och bearbetas i systemet

3.1.1 Avsedd användning av systemet

Beskriv den tänkta användningen av systemet ur användarens perspektiv i termer av bearbetning, lagring och överföring av information.

3.1.2 Systemets driftmiljö

Beskriv fysiskt skydd, tillträdesbegränsning och andra förutsättningar som är säkerhetsrelevanta.

3.1.3 Tänkta användare av systemet

Användarroller i systemet ska redovisas och eventuell gruppering av användare efter åtkomst till resurser och information ska identifieras.

3.1.4 Information

Förteckna typ av information, mängd, skyddsvärde, sekretessklassning, eventuella andra hanteringsregler (t.ex. från lagkrav) kring information som lagras, bearbetas, överförs i eller utförs ut ur systemet.

Hänvisa till ITSA och systemets säkerhetsanalys (AU-D) där så är lämpligt.

3.2 Systemets arkitektur

För att kunna identifiera säkerhetskraven för systemet är det nödvändigt att specificera systemets övergripande arkitektur.

Arkitekturbeskrivningen ska identifiera systemets komponenter och beskriva hur de samverkar och vilka informationsflöden som finns.

Hänvisa till systemets ITSA.

3.3 Systemets gränsytor

IT-systemets alla logiska och fysiska gränsytor ska identifieras och beskrivas. Beskrivningen ska, förutom definition av gränssnitt och fysisk placering, identifiera vilken information som är tänkt att utbytas vid gränsytan och hur utbytet är tänkt att ske.

Referens till den, eller de, komponent(er) i arkitekturbeskrivningen som utgör gränsytan, samt eventuella komponenter som är avsedda att skydda gränsytan eller kontrollera informationsutbytet däröver ska också ges.

Hänvisa till systemets ITSA.

3.4 Säkerhetsförmågor

Medan systemarkitekturen beskriver systemets uppbyggnad och vilka komponenter som ingår i systemet, beskrivs här systemets säkerhetsförmågor och de säkerhetsfunktioner som systemet tillhandahåller.

Hänvisa till systemets ITSA.

4 Sammanställning av säkerhetskrav

Syftet med Sammanställning av säkerhetskrav är att identifiera de säkerhetskrav som gäller för systemet. Säkerhetskraven kan delas in i två kategorier; KSF-krav samt Tillkommande Säkerhetskrav.

4.1 KSF-krav

I detta kapitel redovisas resultatet från fastställandet av kravnivå och alla de kravkomponenter som följer av kravnivån.

Assuransklassen SASS anges inte i detta underlag, då denna klass berör granskning av detta dokument.

Granskning av ITSS genomförs, enligt klassen SASS, av SystGL som en del i ISD-processen.

4.2 Fastställd kravnivå

För aktuellt system gäller kravnivå *Grund (G) / Utökad (U) / Hög (H).*

Se konsekvens- och exponeringsanalys i AU-D.

4.3 Funktionella säkerhetskrav

4.3.1 Gemensamma krav (SFGK)

Krav ID	Kravtext

Tabell 4 – Funktionella krav – Gemensamma krav

4.3.2 Behörighetskontroll (SFBK)

Krav ID	Kravtext

Tabell 5 – Funktionella krav - Behörighetskontroll

4.3.3 Säkerhetsloggning (SFSL)

Krav ID	Kravtext

Tabell 6 – Funktionella krav – Säkerhetsloggning

4.3.4 Intrångsskydd (SFIS)

Krav ID	Kravtext

Tabell 7 – Funktionella krav - Intrångsskydd

4.3.5 Intrångsdetektering (SFID)

Krav ID	Kravtext

Tabell 8 – Funktionella krav - Intrångsdetektering

4.3.6 Skydd mot skadlig kod (SFSK)

Krav ID	Kravtext

Tabell 9 – Funktionella krav - Skydd mot skadlig kod

4.3.7 Skydd mot röjande signaler (SFRS)

Krav ID	Kravtext

Tabell 10 – Funktionella krav – Skydd mot röjande signaler

4.3.8 Skydd mot obehörig avlyssning (SFOA)

Krav ID	Kravtext

Tabell 11 – Funktionella krav – Skydd mot obehörig avlyssning

4.4 Assuranskrav

Assuransklassen SASS anges inte i detta underlag, då denna klass berör granskning av detta dokument.

Granskning av ITSS genomförs, enligt klassen SASS, av SystGL som en del i ISD-processen.

Observera att krav som avser evaluerarens (ISE) åtgärder, dvs E-kraven i respektive assuransklass, ska inte förtecknas i denna ITSS-D. Dessa krav omfattas av ISE granskningsinstruktion, ref ([2]).

4.4.1 Systemutvecklingens livscykel (SALC)

Krav ID	Kravtext

Tabell 12 – Icke-funktionella krav – Systemutvecklingens livscykel

4.4.2 Arkitektur och design (SADE)

Krav ID	Kravtext

Tabell 13 – Icke-funktionella krav – Arkitektur och design

4.4.3 Installation och drift (SAOP)

Krav ID	Kravtext

Tabell 14 – Icke-funktionella krav – Systemutvecklingens livscykel

4.4.4 Administrativa rutiner (SARU)

Krav ID	Kravtext

Tabell 15 – Icke-funktionella krav – Installation och drift

4.4.5 Systemintegrationstest (SATS)

Krav ID	Kravtext

Tabell 16 – Icke-funktionella krav – Systemintegrationstest

4.4.6 Riskanalys och sårbarhetsanalys (SARA)

Krav ID	Kravtext

Tabell 17 – Icke-funktionella krav – Riskanalys och sårbarhetsanalys

4.5 Tillkommande säkerhetskrav

Tillkommande säkerhetskrav härrör från analyser utanför KSF säkerhetsmodell, och dokumenteras i AU-D.

Dessa säkerhetskrav kan exempelvis härröra från genomförda Verksamhetsanalyser eller Risk- och sårbarhetsanalyser. Även andra analyser kan resultera i säkerhetskrav på systemet, t.ex. från flygsäkerhetskrav, behandling av personuppgifter eller andra regelverk och författningar.

Dessa analyser ska identifiera mätbara säkerhetsmål för systemet eller för dess miljö som erhålls utifrån identifierade hot, verksamhetskrav och författningskrav.

Dessa säkerhetsmål för systemet ska jämföras med säkerhetskrav som härrör från KSF och dokumenteras som tillkommande säkerhetskrav. Om säkerhetsmålen redan täcks av säkerhetskrav i KSF, ska referens till detta säkerhetskrav dokumenteras. Säkerhetsmål som identifierats för systemets miljö ska även listas som krav i kapitlet Säkerhetskrav på omgivningen.

4.5.1 Verksamhetskrav

Verksamhetskraven härleds ur analyser i AU-D (redan genomförda och identifierade eller kompletterande analyser).

Krav ID	Kravtext

Tabell 18 – Icke-funktionella krav – Tillkommande verksamhetskrav

4.5.2 Riskmitigerande krav

Riskmitigerande krav härleds ur risk- och sårbarhetsanalyser i AU-D (redan genomförda och identifierade eller kompletterande analyser).

Krav ID	Kravtext

Tabell 19 – Icke-funktionella krav – Riskmitigerande krav

4.5.3 Regelverkskrav

Regelverkskrav härleds ur analyser i AU-D (redan genomförda och identifierade eller kompletterande analyser).

Krav ID	Kravtext

Tabell 20 – Icke-funktionella krav – Legala krav

5 Säkerhetskrav på omgivningen

Syftet med Säkerhetskrav på omgivningen är att identifiera de säkerhetskrav som ställs på systemets driftmiljö. Dessa krav kan uppstå då KSF-krav och övriga krav uppfylls med säkerhetsmekanismer i systemets omgivning.

Vissa krav, eller kravkomponenter, kan hävdas vara helt eller delvis uppfyllda genom att förlita sig på egenskaper hos systemets driftmiljö. Dessa kan vara såväl fysiska, administrativa samt organisatoriska åtgärder. De åberopade åtgärderna kommer därefter att utgöra säkerhetskrav på systemets driftmiljö.

Säkerhetskrav på omgivningen kan också härstamma från ITSA, beroende på hur systemets säkerhetsarkitektur formuleras.

Detta är ett iterativt arbete som genomförs dels tillsammans med SE och dels genom arbete med IT-säkerhetsarkitekturen. Arkitekturarbetet dokumenteras i ITSA.

Följande figur illustrerar kravflödet.

Figur 2 Krav på omgivningen

5.1 Funktionella krav

Krav ID	Kravtext

Tabell 21 – Krav på omgivande miljö – Funktionella krav

5.2 Fysiska krav

Krav ID	Kravtext

Krav ID	Kravtext

Tabell 22 – Krav på omgivande miljö – Fysiska krav

5.3 Administrativa krav

Krav ID	Kravtext

Tabell 23 – Krav på omgivande miljö – Administrativa krav

5.4 Organisatoriska krav

Krav ID	Kravtext

Tabell 24 – Krav på omgivande miljö – Organisatoriska krav

6 Tolkning av säkerhetskrav

Tolkning av säkerhetskraven för systemet innebär att kraven måste definieras på ett systemspecifikt sätt så att de konkret kan omsatts av systemet.

Då de funktionella säkerhetskraven i KSF är formulerade på en allmän nivå som gör dem generellt användbara, måste ISA precisera dessa säkerhetskrav för varje system för att kunna beskriva en sammanställd kravbild för systemet.

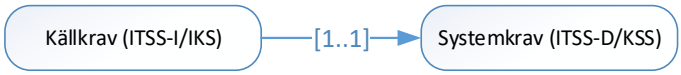
Tolkningen av säkerhetskraven ska vara så entydig att den kan användas som grund för en systemdesign. Tolkningen av säkerhetskrav innebär att visa att KSF-kraven preciseras. Detta innebär att ISE måste verifiera om det preciserade KSF-kravet är mer strikt än det ursprungliga KSF-kravet.

Det kan vara så att vissa funktionella krav uppfylls till viss del av systemet och till viss del av dess omgivning, eventuell i samverkan mellan systemet och dess omgivning (systemkontext). De tolkade kraven måste vara så att de entydigt identifierar vilka krav som gäller för systemet och vilka krav som gäller dess omgivning.

Notera att även assuranskraven måste tolkas, men denna tolkning påverkar inte systemets design och implementation utan tolkningen sker fortlöpande under utvecklingsarbetet.

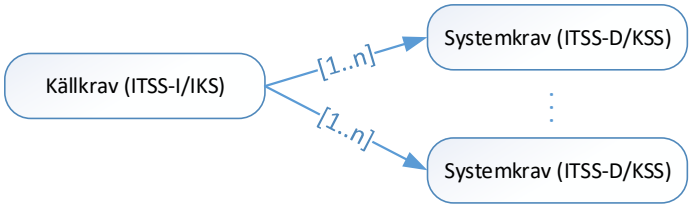
Utifrån ovan angivna krav, samt den säkerhetsarkitektur som beskrivs i ITSA, sammanställer detta kapitel den samlade kravbilden på systemet.

Följande figurer illustrerar möjliga scenarier avseende kravflödet. Ett källkrav, dvs KSF-krav eller tillkommande säkerhetskrav kan direkt formuleras som ett systemkrav. Källkrav kan i detta sammanhang betecknas som IKS-krav (dvs krav som härstammar från SE IntressentKravSammanställning). På motsvarande sätt kan systemkrav betecknas som KSS-krav (KravSammanStällning). Figur 3 nedan visar en direkt mappning mellan källkrav (IKS) och systemkrav (KSS).



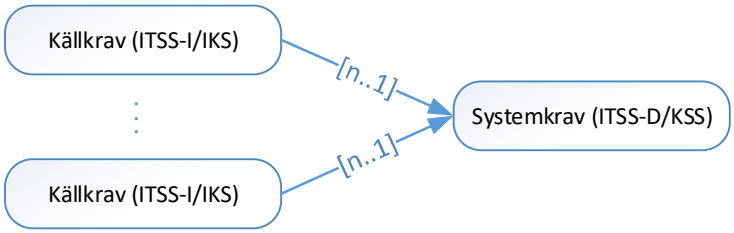
Figur 3 Kravtolkning [1..1]

Figur 4 visar hur ett källkrav delas upp i mindre delar.



Figur 4 Kravtolkning [1..n]

Det är också möjligt att flera kravkällor (identifierade i ITSS-I) renderar samma systemkrav, vilket illustreras i följande figur.

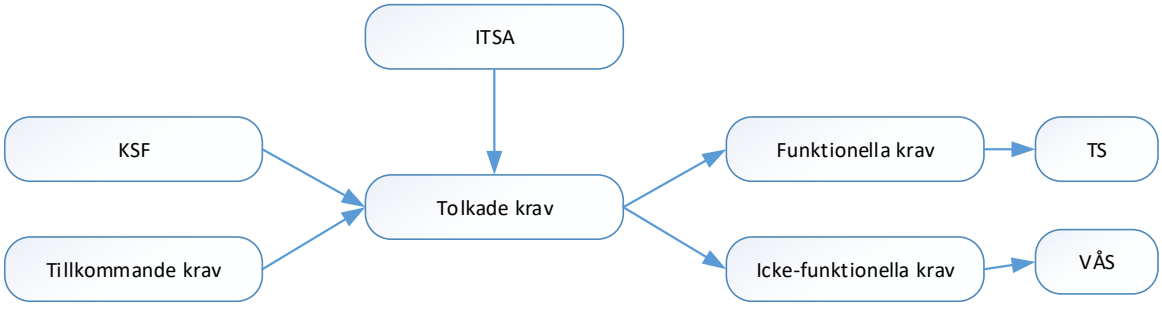


Figur 5 Kravtolkning [n..1]

Det finns också möjligheten att det är källkrav (identifierade i ITSS-I) som av någon anledning inte ska eller bör realiseras i systemet. I dessa fall ska en rationale skrivas för att förklara varför källkravet inte ska eller bör definieras som ett systemkrav. Följande figur illustrerar detta.

Figur 6 Kravtolkning [1..0]

Det övergripande kravflödet i detta skede visas i följande figur.



Figur 7 Övergripande kravflöde

Syftet med kravarbetet är att, tillsamman med SE, producera krav rörande informationssäkerhet som ska tillföras den TS och VÅS som ska användas som underlag för upphandling.

6.1 Funktionella säkerhetskrav

Kraven i detta kapitel ska vara entydiga och unika, för att ligga till grund för kravställning i Teknisk Specifikation (TS).

Kravkälla ska referera till Funktionellt säkerhetskrav alternativt Tillkommande säkerhetskrav enligt ovanstående.

Observera att kraven som ska överföras till TS förtecknas i ITSA. Detta kapitel beskriver den samlade och tolkade kravmängden på en övergripande systemnivå.

6.1.1 Gemensamma krav (SFGK)

Systemkrav	Kravtext (tolkat krav)	Kravkälla

Tabell 25 – Funktionella krav – Gemensamma krav

6.1.2 Behörighetskontroll (SFBK)

Systemkrav	Kravtext (tolkat krav)	Kravkälla

Tabell 26 – Funktionella krav - Behörighetskontroll

6.1.3 Säkerhetsloggning (SFSL)

Systemkrav	Kravtext (tolkat krav)	Kravkälla

Tabell 27 – Funktionella krav - Säkerhetsloggning

6.1.4 Intrångsskydd (SFIS)

Systemkrav	Kravtext (tolkat krav)	Kravkälla

Tabell 28 – Funktionella krav - Intrångsskydd

6.1.5 Intrångsdetektering (SFID)

Systemkrav	Kravtext (tolkat krav)	Kravkälla

Tabell 29 – Funktionella krav - Intrångsdetektering

6.1.6 Skydd mot skadlig kod (SFSK)

Systemkrav	Kravtext (tolkat krav)	Kravkälla

Tabell 30 – Funktionella krav - Skydd mot skadlig kod

6.1.7 Skydd mot röjande signaler (SFRS)

Systemkrav	Kravtext (tolkat krav)	Kravkälla

Tabell 31 – Funktionella krav – Skydd mot röjande signaler

6.1.8 Skydd mot obehörig avlyssning (SFOA)

Systemkrav	Kravtext (tolkat krav)	Kravkälla

Tabell 32 – Krav till TS – Skydd mot obehörig avlyssning

6.2 Assuranskrav

Kraven i detta kapitel ska vara entydiga och unika, för att ligga till grund för kravställning i VÅS.

Kravkälla ska referera till Assuranskrav alternativt Tillkommande säkerhetskrav enligt ovanstående.

6.2.1 Systemutvecklingens livscykel (SALC)

VÅS-krav	Kravtext (tolkat krav)	Kravkälla

Tabell 33 – Krav till VÅS – Systemutvecklingens livscykel

6.2.2 Arkitektur och design (SADE)

VÅS-krav	Kravtext (tolkat krav)	Kravkälla

Tabell 34 – Krav till VÅS – Arkitektur och design

6.2.3 Installation och drift (SAOP)

VÅS-krav	Kravtext (tolkat krav)	Kravkälla

Tabell 35 – Krav till VÅS – Installation och drift

6.2.4 Administrativa rutiner (SARU)

VÅS-krav	Kravtext (tolkat krav)	Kravkälla

Tabell 36 – Krav till VÅS – Administrativa rutiner

6.2.5 Systemintegrationstest (SATS)

VÅS-krav	Kravtext (tolkat krav)	Kravkälla

Tabell 37 – Krav till VÅS – Systemintegrationstest

6.2.6 Riskanalys och sårbarhetsanalys (SARA)

VÅS-krav	Kravtext (tolkat krav)	Kravkälla

Tabell 38 – Krav till VÅS – Riskanalys och sårbarhetsanalys

7 Uppfyllande av säkerhetskrav

Detta kapitel är tomt i ITSS-D, och kommer att kompletteras i ITSS-R.