| Utfärdad av | Dokument nr. | Klassificering |
|---|---|---|
| Magnus Juntti | KSF-ODIN-001 | Öppen |
| Godkänd av | Utgåva | Datum |
| | 1.0 | 2016-07-02 |

# Analys av Kravuppfyllnad KSF 2.0

## ODIN Security Log Server

| Utfärdad av | Dokument nr. | Klassificering |
|---|---|---|
| Magnus Juntti | KSF-ODIN-001 | Öppen |
| Godkänd av | Utgåva | Datum |
| | 1.0 | 2016-07-02 |

# Innehållsförteckning

| Utfärdad av | Dokument nr. | Klassificering |
|---|---|---|
| Magnus Juntti | KSF-ODIN-001 | Öppen |
| Godkänd av | Utgåva | Datum |
| | 1.0 | 2016-07-02 |

# 1 Revisionshistorik

| Utgåva | Datum | Författare | Ändringar |
|---|---|---|---|
| 1.0 | 2016-07-02 | Magnus Juntti | Första utgåva |

# 2 Definitioner och Akronymer

| Definition | Beskrivning |
|---|---|
| KSF | Krav på SäkerhetsFunktioner |
| NTP | Network Time Protocol |
| IDS | Intrusion Detection System |

# 3 Referenser

| ID | Dokument ID | Titel |
|---|---|---|
| 1 | SYD-ODIN-001 | System Design Description ODIN Security Log Server and ODIN Log Concentrator |
| 2 | REQ-ODIN-002 | System Requirements Specification ODIN |
| 3 | ATD-ODIN-001 | Acceptance Test Description ODIN Security Log Server |
| 4 | ATR-ODIN-001 | Acceptance Test Report ODIN Security Log Server |
| 5 | 2016-INS-002 | Utvecklingsprocess ODIN |
| 6 | SUG-ODIN-001 | Systems User's Guide ODIN Security Log Server |
| 7 | SUG-ODIN-002 | Systems User's Guide ODIN Log Concentrator |
| 8 | SUG-ODIN-003 | Systems Installation Guide ODIN Security Log Server |
| 9 | SUG-ODIN-004 | Systems Installation Guide ODIN Log Concentrator |
| 10 | SUG-ODIN-006 | TAK/TEID for ODIN Security Log Server |
| 11 | SUG-ODIN-009 | Software User's Guide ODIN NIDS Tools |
| 12 | REQ-ODIN-003 | System Requirements Specification ODIN NIDS Option |
| 13 | 2016-INS-003 | Utvecklingsmiljö ODIN. *) |
| 14 | REQ-ODIN-001 | System Hardware Requirements ODIN |
| 15 | REP-ODIN-001 | ODIN Security Log Server System Hardening Report |
| 16 | REP-ODIN-002 | ODIN Log Concentrator System Hardening Report |
| 17 | ATD-ODIN-003 | Acceptance Test Description ODIN Log Concentrator |
| 18 | ATR-ODIN-003 | Acceptance Test Report ODIN Log Concentrator |

| Utfärdad av | Dokument nr. | Klassificering |
|---|---|---|
| Magnus Juntti | KSF-ODIN-001 | Öppen |
| Godkänd av | Utgåva | Datum |
| | 1.0 | 2016-07-02 |

*) Detta dokument är omfattad av strikt företagssekretess. Endast relevanta personer i projekt som använder ODIN kommer få ta del av detta och då endast i syfte att påvisa uppfyllnad av KSF-krav.

| Utfärdad av | Dokument nr. | Klassificering |
|---|---|---|
| Magnus Juntti | KSF-ODIN-001 | Öppen |
| Godkänd av | Utgåva | Datum |
| | 1.0 | 2016-07-02 |

# 4 Syfte

Detta dokument syftar till att påvisa hur ODIN Security Log Server hjälper ett system att uppfylla KSF 2.0. Det syftar även till att påvisa kravuppfyllnad mot för ODIN som singulär enhet relevanta krav ur KSF 2.0.

Kravuppfyllnaden redovisas mot HSIS-kraven.

| Utfärdad av | Dokument nr. | Klassificering |
|---|---|---|
| Magnus Juntti | KSF-ODIN-001 | Öppen |
| Godkänd av | Utgåva | Datum |
| | 1.0 | 2016-07-02 |

# 5 Förutsättningar

Följande förutsättningar för användningen och konfigurationen av ODIN i systemet gäller för att detta dokument ska vara relevant.

1. ODIN skall vara inkopplad med diod enligt ref [1] inklusive NTP-överföring via NTP broadcast.
2. ODIN Log Concentrator eller egen funktion som motsvarar denna skall användas
3. OSSEC agent skall användas för integritetskontroll på alla klienter.
4. OSSEC agent eller odin-logcollector för Windows skall användas för överföring av loggar från Windows-klienter
5. Loggar skall överföras till ODIN på syslog-format utan att ha omformatterats av någon OSSEC manager på vägen. Detta innebär att användning av OSSEC managers syslog output i en koncentrator inte uppfyller detta. ODIN Log Concentrator uppfyller kravet. Se ref [1] för mer information.
6. ODIN skall fysiskt skyddas från åtkomst från icke-behöriga. Detta inkluderar systemadministratörer i systemet som övervakas av ODIN.
7. Operatörer som hanterar ODIN skall samtliga vara behöriga till all information i ODIN
8. Operatörer som hanterar ODIN får inte ha systemadministratörsrättigheter i systemet som ODIN är ansluten till
9. Om NIDS-funktion är aktiverad förutsätts att adekvat nätverks-”sniffing” är implementerad och skickas till dedicerade nätverksinterface i ODIN. Detta kan tex utföras genom användning av nätverks-tap eller switchars ”monitor”-portar.
10. Det förutsätts att alla filer som importeras i ODIN är fria från skadlig kod, dvs Anti-Virus scanning måste ske innan import då ODIN saknar sådana funktioner.

Notera att om systemet har lägre klassificering än HEMLIG/SECRET så kan vissa av förutsättningarna vara annorlunda beroende på vilka KSF-krav som ska mötas och med vilken assurans.

| Utfärdad av | Dokument nr. | Klassificering |
|---|---|---|
| Magnus Juntti | KSF-ODIN-001 | Öppen |
| Godkänd av | Utgåva | Datum |
| | 1.0 | 2016-07-02 |

# 6 KSF Kravuppfyllnad

Detta kapitel redovisar, per säkerhetsfunktion, hur ODIN är en del av kravuppfyllnaden av KSF-kraven för systemet. För varje krav redovisas krav-ID, text, samt om användning av ODIN resulterar i hel kravuppfyllnad eller delvis. Det redovisas också huruvida kravet är relevant på ODIN som enhet och om ODIN därmed uppfyller kravet. För varje krav som anses uppfyllt hänvisas till dokumentation som beskriver de delar som kravet avses.

Notera att endast de krav som har en specifik kravtext finns med i beskrivningen. Krav som utgått eller flyttats är inte med vilket medföljer att det kan finnas ”hål” i KSF kravnumrering.

## 6.1 Läsanvisning

Kolumnen ”ODIN” anger uppfyllnad i ODIN som enskild enhet och kolumnen ”System” anger uppfyllnad i Systemet som använder ODIN om ODIN har någon påverkan på uppfyllnaden av kravet. N/A i en kolumn anger att detta inte är relevant med avseende på ODIN eller användning av ODIN utan måste uppfyllas av andra delar av systemet.

## 6.2 Gemensamma Krav

Samtliga dessa krav rör ODIN men inte systemet ODIN övervakar.

### 6.2.1 Skydd av Säkerhetsfunktionen

| Krav id | Kravbeskrivning | Uppfylld av |
|---|---|---|
| HSG-5-1 | Säkerhetsfunktionen skall tillsammans med övriga säkerhetsfunktioner i IT-systemet upprätthålla en säkerhetsdomän som skyddar mot manipulering eller störningar både från sådana subjekt och från sådana användare som tillhör respektive inte tillhör denna domän. | Inkoppling med diod enl. ref [1]<br>Förutsättningar angående fysiskt skydd och separation av behörigheter för olika operatörsroller som hanterar systemet. |
| HSG-5-2 | Säkerhetsfunktionen skall tillsammans med övriga säkerhetsfunktioner i IT-systemet ha möjlighet att tillgodose egen tillförlitlig tid. | Inkoppling med diod enl. ref [1] |
| HSG-5-3 | Säkerhetsfunktionen skall säkerställa att endast behörig administratör kan förvalta säkerhetsfunktionen och sköta dess säkerhetsinställningar. | Förutsättningar angående fysiskt skydd och separation av behörigheter för olika operatörsroller som hanterar systemet. |

| Utfärdad av | Dokument nr. | Klassificering |
|---|---|---|
| Magnus Juntti | KSF-ODIN-001 | Öppen |
| Godkänd av | Utgåva | Datum |
| | 1.0 | 2016-07-02 |

### 6.2.2 Assuranskrav

| Krav id | Kravbeskrivning | Uppfylld av |
|---|---|---|
| HSG-8-1 | Säkerhetsfunktionen skall vara metodiskt framtagen, testad och granskad. | Referenser [2], [3] och [4] visar på kravställning på funktioner samt process för metodiskt test och evaluering.<br><br>Granskning sker som del i systemackreditering |
| HSG-8-2 | All dokumentation rörande säkerhetsfunktionen skall vara märkt med unik referens. | Unikt dokument-ID finns på all dokumentation till ODIN |
| HSG-8-3 | Det skall finnas dokumentation som beskriver resultatet av den granskning som genomförts av en oberoende instans. | Ej uppfyllt |
| HSG-8-4 | Det skall finnas dokumentation som på ett informellt sätt och på en detaljerad nivå beskriver hur säkerhetsfunktionen är uppbyggd. Dokumentationen skall innehålla en beskrivning av all hårdvara och mjukvara som används för att uppnå erforderlig säkerhetsfunktionalitet. | Se ref [1] |
| HSG-8-5 | Det skall finnas dokumentation som på ett informellt och detaljerat sätt beskriver hur de funktionella säkerhetskraven är implementerade i säkerhetsfunktionen. | Se ref [1] och ref [2] |
| HSG-8-6 | Det skall finnas dokumentation som beskriver fastställda metoder för leverans av säkerhetsfunktionen. | Se ref [5] |
| HSG-8-7 | Dokumentationen över fastställda metoder för leverans skall även omfatta hur man med hjälp av metoderna upptäcker modifieringar eller skillnader mellan utgiven respektive erhållen leverans av säkerhetsfunktionen. Vidare skall dokumentationen beskriva hur man upptäcker om någon obehörigen utger sig för att vara ansvarig utgivare av en leverans. | Se ref [5] |
| HSG-8-8 | Det skall finnas dokumentation som beskriver vilka nödvändiga steg som måste vidtas för att erhålla en säker installation och | Se ref [1] och ref [8] samt ref [9] för ODIN Log Concentrator |

| Krav id | Kravbeskrivning | Uppfylld av |
|---|---|---|
| | start av säkerhetsfunktionen. | |
| HSG-8-9 | Det skall finnas dokumentation som beskriver hur en systematisk konfigurationsstyrning av säkerhetsfunktionen genomförs samt vilka delar eller komponenter av säkerhetsfunktionen som ingår i denna konfigurationsstyrning samt hur uppföljning av dessa delar eller komponenter möjliggörs. | Se ref [5] |
| HSG-8-10 | Dokumentationen skall också beskriva genomförande av uppföljning/versionhantering avseende:<br>• designdokument,<br>• implementationsdokument,<br>• konfigurationsdokument,<br>• testdokument,<br>• administratörsdokument<br>• användardokument<br>• säkerhetsbrister | Se ref [5] |
| HSG-8-11 | Konfigurationsstyrningen skall för varje ingående och relevant del eller komponent omfatta:<br>• designdokument,<br>• implementationsdokument,<br>• konfigurationsdokument,<br>• testdokument,<br>• administratörsdokument<br>• användardokument, och<br>• dokument över kända säkerhetsbrister för respektive del eller komponent. | Se ref [1], [3], [4], [6] för ODIN<br>Se ref [1], [7], [17], [18] för ODIN Log Concentrator<br>Se ref [5] för utvecklingsprocess |
| HSG-8-12 | Konfigurationsstyrningen skall vara så utformad att endast behöriga kan utföra förändringar i de delar eller komponenter som omfattas av konfigurationsstyrningen. | Se ref [5] samt ref [13]. |
| HSG-8-13 | Det skall finnas dokumentation som detaljerat beskriver vald metod för acceptans av leveranser samt vilka delar eller komponenter av säkerhetsfunktionen som omfattas av denna acceptansmetod. | Se ref [5] |
| HSG-8-14 | Det skall finnas dokumentation som beskriver hur behörig administratör | Se ref [6] samt ref [7] för ODIN Log Concentrator |

| Krav id | Kravbeskrivning | Uppfylld av |
|---|---|---|
| | konfigurerar, administrerar och förvaltar säkerhetsfunktionen på ett korrekt sätt så att erforderlig säkerhetsnivå kan erhållas och bibehållas. | |
| HSG-8-15 | Det skall finnas dokumentation som beskriver hur säkerhetsfunktionen ur säkerhetssynpunkt skyddas i utvecklingsmiljön under framtagandet av säkerhetsfunktionen. Dokumentationen skall också påvisa att de redovisade åtgärderna efterlevs. | Se ref [13] |
| HSG-8-16 | Det skall finnas dokumentation över vilka testfall med tillhörande utfall som genomförts. | Se ref [3] samt ref [4] |
| HSG-8-17 | Det skall finnas dokumentation som påvisar hur testfallen korrelerar mot uppställda funktionella säkerhetskrav. | Se följande kapitel i detta dokument samt deras referenser. |
| HSG-8-18 | Testfallen skall inkludera både sådana tester som kontrollerar säkerhetsfunktionens funktionalitet och sådana tester som kontrollerar frånvaron av oönskade beteende inom säkerhetsfunktionen. Testfallen skall vara utförda av en oberoende instans. | Se ref [3]<br><br>OBS: Ej utförda av oberoende instans |
| HSG-8-19 | Det skall finnas en dokumenterad analys som påvisar att all dokumentation rörande säkerhetsfunktionens användning är:<br>• fullständig,<br>• tydlig,<br>• konsekvent<br>• fri från missledande och orimliga riktlinjer eller åtgärder.<br>Vidare skall analysen påvisa att dokumentationen rörande säkerhetsfunktionens användning beaktar alla driftsituationer för säkerhetsfunktionen. Dokumentationen skall också beskriva alla gjorda antaganden rörande den tilltänkta miljö som säkerhetsfunktionen är avsedd att fungera i. | Ej uppfylld av ODIN leverantör. Får påvisas genom oberoende granskning av projekt som använder ODIN |

## 6.3 BehörighetsKontroll

Dessa krav är till del relevanta för ODIN och i sin helhet relevanta för systemet som ODIN är ansluten till. Notera att ODIN skall vara separerat från systemet och därmed ha behörighetskontroll skilt från systemets behörighetskontroll.

### 6.3.1 Funktionella Säkerhetskrav

| Krav id | Kravbeskrivning | ODIN | System |
|---|---|---|---|
| HSBK-4-1 | Säkerhetsfunktionen för behörighetskontroll skall förhindra åtkomst till IT-systemets subjekt och objekt av användare och subjekt som inte har behörighet och åtkomsträttigheter i IT-systemet. | Se ref [2] för krav och ref [3] och [4] för testfall. | N/A |
| HSBK-4-2 | Säkerhetsfunktionen för behörighetskontroll skall unikt identifiera och autenticera en användare innan åtkomst av någon funktionalitet eller tilldelning av åtkomsträttigheter får ske i det IT-system som skyddas av säkerhetsfunktionen. | Se ref [2] för krav och ref [3] och [4] för testfall. | N/A |
| HSBK-4-3 | Säkerhetsfunktionen för behörighetskontroll skall autenticera en användare vid:<br>• inloggning,<br>• upphävande att tillfälligt åtkomstskydd<br>• vid byte av säkerhetsattribut för autenticering.<br>• när tiden för tidsbegränsad användning av IT-systemets resurser har gått ut. | Se ref [2] för krav och ref [3] och [4] för testfall. | N/A |
| HSBK-4-4 | Säkerhetsfunktionen för behörighetskontroll skall uppfylla kraven för stark autentisering enligt HKV MUST ITSA TSA krav för signalskyddssystem. | Om option TAK/TEID är vald används KrAPI, se ref [10] för användning | N/A |
| HSBK-4-5 | Säkerhetsfunktionen för behörighetskontroll skall kunna vidta automatiska åtgärder vid | Autentisering sker mot TAK/TEID för | N/A |

| Krav id | Kravbeskrivning | ODIN | System |
|---|---|---|---|
| | autenticeringsfel. Sådana åtgärder skall omfatta nekande av åtkomst till IT-systemet samt låsning av berörd användares konto under en viss tid. | H/S. Hänvisning till KrAPI och hur låsning av kort sker. | |
| HSBK-4-6 | Säkerhetsfunktionen för behörighetskontroll skall möjliggöra olika definierade roller. | Ej relevant i ODIN. Enda rollen i ODIN är ”secuadm” | ODIN separerat från övrigt system. Tilldelning av behörighet i ODIN är att lika med tilldelning av behörighet till roll ”secuadm” |
| HSBK-4-7 | Säkerhetsfunktionen för behörighetskontroll skall säkerställa att det inte finns någon roll, användare eller subjekt som har behörighet eller åtkomst till samtliga subjekt och objekt som återfinns i det IT-system som säkerhetsfunktionen är avsedd att skydda. | Se kapitel 5 | Se kapitel 5 |
| HSBK-4-8 | Säkerhetsfunktionen för behörighetskontroll skall säkerställa att behörig administratör, som har till uppgift att sköta säkerheten i det IT-system som säkerhetsfunktionen är avsedd att skydda, inte i något avseende har behörighet eller åtkomst till säkerhetsloggarna i samma IT-system. | Se kapitel 5 | Se kapitel 5 |
| HSBK-4-9 | Säkerhetsfunktionen för behörighetskontroll skall säkerställa att behörig administratör, som har till uppgift att hantera och granska säkerhetsloggarna i det IT-system som säkerhetsfunktionen är avsedd att skydda, inte i något avseende har samma behörighet eller åtkomst som den behöriga administratör som har till uppgift att sköta säkerheten i samma IT-system. | Se kapitel 5 | Se kapitel 5 |

| Krav id | Kravbeskrivning | ODIN | System |
|---|---|---|---|
| HSBK-4-10 | Säkerhetsfunktionen för behörighetskontroll skall säkerställa låsning av sådana säkerhetsattribut som kan anses vara röjda till sådana användare eller subjekt som inte har behörighet och åtkomsträttigheter till IT-systemet. Låsningen skall ske direkt eller vid nästa inloggning. | Process för CRL-uppdatering på förband samt instruktion i ref [6] och ref [10] för uppdatering av CRL. | N/A |
| HSBK-4-11 | Säkerhetsfunktionen för behörighetskontroll skall säkerställa att alla användare kan göras individuellt ansvariga (dvs oavvislighet) för sina vidtagna åtgärder i IT-systemet. | Se ref [1] angående förutsättningar för skydd av root-lösen | Uppfylls i och med loggning i ODIN. Förutsätter att systemet logga relevanta händelser. |

### 6.3.2 Skydd av Säkerhetsfunktionen

| Krav id | Kravbeskrivning | ODIN | System |
|---|---|---|---|
| HSBK-5-1 | Säkerhetsfunktionen för behörighetskontroll skall kunna upprätthålla ett definierat säkert tillstånd när hela eller delar av den funktionalitet som innehåller data rörande;<br>• tilldelade rättigheter för roller,<br>• användare som tillhör en roll,<br>• rollernas relationer och restriktioner,<br>är korrupt eller oåtkomlig. | Användning av KrAPI vilket är en ackrediterad produkt.<br><br>Integration med Linux PAM. Se ref [3] och [4] för testfall. | N/A |
| HSBK-5-2 | Säkerhetsfunktionen för behörighetskontroll skall kunna upprätthålla ett definierat säkert tillstånd när de säkerhetsattribut som används för autenticering och styrning av åtkomst är korrupta eller oåtkomliga. | Användning av KrAPI vilket är en ackrediterad produkt.<br><br>Integration med Linux PAM. Se ref [3] och [4] för testfall. | N/A |
| HSBK-5-5 | Säkerhetsfunktionen för | Alla operatörer i | N/A |

| | | | |
|---|---|---|---|
| | behörighetskontroll skall kunna förse definierade och genom beslut bestämda administrativa roller med möjligheten att verifiera riktigheten på den exekverbara kod som rör säkerhetsfunktionen. | ODIN kan utföra dessa operationer då alla operatörer är säkerhets-adminstratörer | |

### 6.3.3 Förvaltning av Säkerhetsfunktionen

| Krav id | Kravbeskrivning | ODIN | System |
|---|---|---|---|
| HSBK-6-1 | Det skall gå att lägga till, ta bort eller på annat sätt förändra vilka kontroller som skall utföras för att säkerställa säkerhetsattributens kvalité. | Användning av KrAPI vilket är en ackrediterad produkt. | N/A |
| HSBK-6-2 | Det skall gå att lägga till, ta bort eller på annat sätt förändra vilka åtkomsträttigheter som behöriga användare har till IT-systemets subjekt och objekt. Sådana åtkomsträttigheter skall omfatta:<br>• skapa,<br>• läsa,<br>• skriva,<br>• exekvera,<br>• ta bort. | Alla operatörer i ODIN är behörig till all information enligt kapitel 5. | N/A |
| HSBK-6-3 | Det skall gå att lägga till, ta bort eller på annat sätt förändra vid vilka tillfällen en användare skall autenticera sin identitet. | Endast autentisering vid inlogg via KrAPI | N/A |
| HSBK-6-4 | Det skall gå att lägga till, ta bort eller på annat sätt förändra vilka säkerhetsattribut som skall användas för användare, subjekt och objekt som kontrollmekanism vid styrning av åtkomst. | Alla operatörer i ODIN är behörig till all information enligt kapitel 5. Således ej relevant i ODIN då sådan funktion skulle inverka negativt på möjligheten att snabbt | N/A |

| | | | |
|---|---|---|---|
| | | analysera loggar | |
| HSBK-6-5 | Det skall gå att lägga till, ta bort eller på annat sätt förändra vilka åtgärder som skall vidtas vid autenticeringsfel. | Autentisering sker mot TAK/TEID för H/S. Autentiseringsfel hanteras av KrAPI eftersom autentisering sker mot kortet primärt. ODIN evaluerar bara certifikat från kort och vidtar inga åtgärder utgående från detta. | N/A |
| HSBK-6-6 | Det skall gå att lägga till, ta bort eller på annat sätt förändra vid vilka tillfällen låsning av sådana säkerhetsattribut som kan anses vara röjda skall ske. | Sker i så fall genom konfigurering av KrAPI. ODIN innehåller default-konfiguration av KrAPI. | N/A |

### 6.3.4 Assuranskrav

Dessa krav har enbart analyserats med avseende på uppfyllnad i ODIN som enskild enhet, inte i systemet som ODIN är anslutet till.

| Krav id | Kravbeskrivning | Anmärkning |
|---|---|---|
| HSBK-8-1 | Det skall finnas dokumentation som beskriver behörighetspolicyn som ligger till grund för utformningen av säkerhetsfunktionen för behörighetskontroll. Dokumentationen skall också beskriva vilka roller, behörigheter och åtkomsträttigheter som behörighetspolicyn omfattar. | Hanteras av förband som hanterar ODIN och systemet. |
| HSBK-8-2 | Det skall finnas dokumentation som på en övergripande nivå beskriver hur säkerhetsfunktionen för behörighetskontroll är uppbyggd samt hur denna lösning stämmer överens med vald behörighetspolicy. | Se ref [1] samt behörighetspolicy på förband som använder ODIN. |

| Krav id | Kravbeskrivning | Anmärkning |
|---|---|---|
| HSBK-8-3 | Det skall finnas dokumentation som på en detaljerad nivå beskriver vilket syfte de olika relevanta användargränssnitten som återfinns i säkerhetsfunktionen har, samt hur användning av dessa gränssnitt sker. | Se ref [6] |
| HSBK-8-23 | Det skall finnas dokumentation som beskriver sådana sårbarheter som genom utförd penetrationstestning och analys av hypotetiska brister förekommer respektive kan förekomma i säkerhetsfunktionen. Penetrationstestningen och analysen skall utföras av en oberoende instans. | Ej uppfylld av ODIN leverantör. Får påvisas genom oberoende granskning av projekt som använder ODIN |

## 6.4 SäkerhetsLoggning

### 6.4.1 Funktionella Säkerhetskrav

| Krav id | Kravbeskrivning | ODIN | System |
|---|---|---|---|
| HSSL-4-1 | Säkerhetsfunktionen för säkerhetsloggning skall i en säkerhetslogg registrera sådana händelser som är av betydelse för säkerheten i IT-systemet och omfatta:<br>• användning av kontrollmekanismer för autenticering,<br>• åtkomst till subjekt och objekt<br>• förändringar av åtkomst- och behörighetslistor. | ODIN lagrar det som sänds till den. Se ref [1]. Kravet faller ut på systemets konfiguration. | Måste konfigureras så att denna typ av loggar sänds till ODIN |
| HSSL-4-2 | Säkerhetsfunktionen för säkerhetsloggning skall tillsammans med varje enskild registrerad händelse, även registrera datum och tid för händelsen samt användarens eller subjektets identitet. | ODIN lagrar det som sänds till den. Se ref [1]. Kravet faller ut på systemets konfiguration. | Måste konfigureras så att dessa attribut ingår i loggar som sänds till ODIN |
| HSSL-4-3 | Säkerhetsfunktionen för säkerhetsloggning skall säkerställa att spårning av missbruk, försök till | ODIN lagrar det som sänds till den. Se ref [1]. | Måste konfigureras så att denna typ av |

| Krav id | Kravbeskrivning | ODIN | System |
|---|---|---|---|
| | missbruk samt sådana potentiella felkonfigurationer av IT-systemet som skulle kunna äventyra säkerheten, kan genomföras. | Kravet faller ut på systemets konfiguration. | händelser ingår i loggar som sänds till ODIN |
| HSSL-4-4 | Säkerhetsfunktionen för säkerhetsloggning skall säkerställa att alla registrerade händelser i säkerhetsloggen kan presenteras i läsbar form och att granskning av de registrerade händelserna kan genomföras. | Se ref [1], [2], [6] | Uppfyllt i och med ODIN |
| HSSL-4-5 | Säkerhetsfunktionen för säkerhetsloggning skall möjliggöra verktygsbaserad granskning av registrerade händelser i säkerhetsloggen. Granskningen skall baseras på möjligheten att sortera samt utsöka registrerade händelser. | Se ref [1], [2], [6] | Uppfyllt i och med ODIN |
| HSSL-4-6 | Säkerhetsfunktionen för säkerhetsloggning skall möjliggöra säkerhetskopiering av säkerhetsloggen. Sådan säkerhetskopiering skall ske genom utskrift eller kopiering till andra lagringsmedia. | Se ref [1], [2], [6] | Uppfyllt i och med ODIN |
| HSSL-4-7 | Säkerhetsfunktionen för säkerhetsloggning skall säkerställa att registrerade händelser inte raderas, skrivs över eller på annat sätt förstörs som en följd av fel på säkerhetsfunktionen eller att säkerhetsloggen är full. | Se ref [1], [2], [6] | Uppfyllt i och med ODIN |

### 6.4.2 Skydd av Säkerhetsfunktionen

| Krav id | Kravbeskrivning | ODIN | System |
|---|---|---|---|
| HSSL-5-1 | Säkerhetsfunktionen för säkerhetsloggning skall kunna upprätthålla ett definierat säkert | Se ref [6] för hantering av full disk. Se kapitel 5 | Systemet måste hantera detta då det är ett krav på |

| | | | |
|---|---|---|---|
| | tillstånd när händelser inte kan loggas. | för inkoppling. Enkelriktad inkoppling omöjliggör kontroll från ODIN:s sida. | logproducenter. |
| HSSL-5-2 | Säkerhetsfunktionen för säkerhetsloggning skall säkerställa att ingen användaraktivitet i IT-systemet får ske om säkerhetsloggen är avstängd. | N/A | Systemet måste hantera detta |

### 6.4.3 Förvaltning av Säkerhetsfunktionen

| Krav id | Kravbeskrivning | ODIN | System |
|---|---|---|---|
| HSSL-6-1 | Det skall gå att lägga till, ta bort eller på annat sätt förändra vilka säkerhetsrelevanta händelser som skall registreras i säkerhetsloggen. | Registrerar allt som sänds till den. Se ref [1]. | Systemet måste hantera detta då det är ett krav på logproducenter. |
| HSSL-6-2 | Det skall gå att lägga till, ta bort eller på annat sätt förändra vilka övriga uppgifter som skall registreras tillsammans med varje enskild säkerhetsrelevant händelse. | Registrerar allt som sänds till den. Se ref [1]. | Systemet måste hantera detta då det är ett krav på logproducenter. |

### 6.4.4 Assuranskrav

Se gemensamma krav

## 6.5 IntrångsSkydd

Denna säkerhetsfunktion är ej relevant för ODIN då ODIN är en del av det system som ska skyddas. ODIN har inga externa gränsytor, endast gränsytor mot det övervakade systemet. Gränsytor mot externt media såsom filimport hanteras av andra säkerhetsfunktioner.

## 6.6 IntrångsDetektion

### 6.6.1 Funktionella Säkerhetskrav

| Krav id | Kravbeskrivning | ODIN | System |
|---|---|---|---|
| HSID-4-1 | Säkerhetsfunktionen för intrångsdetektering skall säkerställa | ODIN registrerar alla händelser och | Se kapitel 5 |

| Krav id | Kravbeskrivning | ODIN | System |
|---|---|---|---|
| | detektering av redan genomförda samt pågående intrång. | en larmfunktion. Se ref [1] | |
| HSID-4-2 | Säkerhetsfunktionen för intrångsdetektering skall tillsammans med varje enskild registrerad händelse, även registrera datum och tid för händelsen samt användarens eller subjektets identitet. | ODIN lagrar det som sänds till den. Se ref [1]. Kravet faller ut på systemets konfiguration. Används NIDS-option till ODIN är kravet uppfyllt enligt ref [1]. | Se kapitel 5 om OSSEC-agenter. Systemets NIDS-funktion måste säkerställa detta om inte ODIN:s NIDS används då inkoppling av denna måste ske ändamålsenligt. |
| HSID-4-3 | Säkerhetsfunktionen för intrångsdetektering skall säkerställa att alla registrerade händelser kan presenteras i en form som går att tolka för den som är behörig och att granskning av de registrerade händelserna kan genomföras. | Se ref [1], [2], [6]. Om NIDS-option är vald, se ref [11], [12]. | Se kapitel 5 om OSSEC-agenter. Systemets NIDS-funktion måste säkerställa detta om inte ODIN:s NIDS används då inkoppling av denna måste ske ändamålsenligt. |
| HSID-4-4 | Säkerhetsfunktionen för intrångsdetektering skall möjliggöra verktygsbaserad granskning av registrerade händelser. Granskningen skall baseras på möjligheten att sortera samt utsöka registrerade händelser. | Se ref [1], [2], [6] | Uppfyllt i och med ODIN |
| .HSID-4-5 | Säkerhetsfunktionen för intrångsdetektering skall genom automatisk analys kunna avgöra om definierade regler har överskridits. Dessa definierade regler skall omfatta sådana händelser som är kända att representera missbruk av eller intrång i IT-system. | Se ref [1], [2], [6]. Om NIDS-option är vald, se ref [11], [12]. | Systemet måste konfigureras så att sådana händelser skickas till ODIN så att ODIN kan klassificera dem. |
| HSID-4-6 | Säkerhetsfunktionen för intrångsdetektering skall säkerställa att spårning av missbruk samt försök till missbruk som skulle kunna äventyra säkerheten i IT- | Se ref [1], [2], [6] Om NIDS-option är vald, se ref [11], [12]. | Systemet måste konfigureras så att sådana händelser skickas till ODIN så att |

| Krav id | Kravbeskrivning | ODIN | System |
|---|---|---|---|
| | systemet, kan genomföras. | | ODIN kan klassificera dem. |
| HSID-4-7 | Säkerhetsfunktionen för intrångsdetektering skall säkerställa att registrerade händelser kan analyseras tillsammans med sådana säkerhetsrelevanta händelser som registreras i säkerhetsfunktionen för säkerhetsloggning. | Se ref [1], [2], [6], Om NIDS-option är vald, se ref [11], [12]. | Systemet måste konfigureras så att sådana händelser skickas till ODIN så att ODIN kan klassificera dem. |
| HSID-4-8 | Säkerhetsfunktionen för intrångsdetektering skall säkerställa att registrerade händelser inte raderas, skrivs över eller på annat sätt förstörs som en följd av fel på säkerhetsfunktionen eller till följd av att händelseloggen är full. | Se ref [1], [2], [6], Om NIDS-option är vald, se ref [11], [12]. | Systemets NIDS-funktion måste säkerställa detta om inte ODIN:s NIDS används. HIDS-delen uppfylls av ODIN |

### 6.6.2 Skydd av Säkerhetsfunktionen

| Krav id | Kravbeskrivning | ODIN | System |
|---|---|---|---|
| HSID-5-1 | Efter ett felaktigt beteende från säkerhetsfunktionen eller efter ett serviceuppehåll skall säkerhetsfunktionen för intrångsdetektering återgå till ett definierat säkert tillstånd. | Så länge hårdvaran säkerställer funktion fungerar mjukvaran. Se ref [14]. | Måste säkerställas av korrekt uppstart av OSSEC-agenter u systemet. |

### 6.6.3 Förvaltning av Säkerhetsfunktionen

| Krav id | Kravbeskrivning | ODIN | System |
|---|---|---|---|
| HSID-6-1 | Det skall gå att lägga till, ta bort eller på annat sätt förändra vilka händelser som skall registreras och som möjliggör indikering av sårbarheter i eller missbruk av IT-systemets resurser samt är av betydelse för säkerheten i IT-systemet. | Se ref [6], [11] | Förutsätter att NIDS-inkoppling är gjord på relevanta gränsytor. Uppfylls till del av OSSEC-agenter i systemet men kräver konfiguration i systemet. |

| | | | |
|---|---|---|---|
| HSID-6-2 | Det skall gå att lägga till, ta bort eller på annat sätt förändra vilka händelser skall registreras och som är av betydelse för själva händelseloggen. | Se ref [6], [11] | Förutsätter att NIDS-inkoppling är gjord på relevanta gränsytor. Uppfylls till del av OSSEC-agenter i systemet men kräver konfiguration i systemet. |
| HSID-6-3 | Det skall gå att lägg till, ta bort eller på annat sätt förändra vilka övriga uppgifter som skall registreras tillsammans med varje enskild händelse. | ODIN lagrar det som sänds till den. Se ref [1]. Kravet faller ut på systemets konfiguration. | Måste stödja detta krav. |
| HSID-6-4 | Det skall gå att lägga till, ta bort eller på annat sätt förändra vilka definierade regler som skall användas för genomförande av automatisk analys. | Se ref [6] och [11]. | Uppfyllt i och med ODIN |
| HSID-6-5 | Det skall gå att lägga till, ta bort eller på annat sätt förändra vilka åtgärder som kan vidtas i samband med att den automatiska analysen genomförs. | Se ref [6] och [11]. | Uppfyllt i och med ODIN |

### 6.6.4 Assuranskrav

Se gemensamma krav.

## 6.7 Skadlig Kod

Merparten av dessa krav kan i detta dokument inte mappas mot systemet, endast ODIN själv. Dock är användning av OSSEC och dess integritetskontroll en form av skydd eller snarar detektion av skadlig kod.

### 6.7.1 Funktionella Säkerhetskrav

| Krav id | Kravbeskrivning | ODIN | System |
|---|---|---|---|
| HSSK-4-1 | Säkerhetsfunktionen för skydd mot skadlig kod skall förhindra all åtkomst till IT-systemets resurser | Förutsättningar i kapitel 5. Härdning av | N/A |

| Krav id | Kravbeskrivning | ODIN | System |
|---|---|---|---|
| | av sådana objekt som kan innehålla skadlig kod. | ODIN, se ref [15]. Se ref [16] för ODIN Log Concentrator | |
| HSSK-4-2 | Säkerhetsfunktionen för skydd mot skadlig kod skall säkerställa att ingen skadlig kod kan:<br>• ändra,<br>• förstöra<br>• på annat sätt manipulera objekten,<br>i det IT-system som skyddas av säkerhetsfunktionen. | Förutsättningar i kapitel 5. Härdning av ODIN, se ref [15]. Se ref [16] för ODIN Log Concentrator | N/A |
| HSSK-4-3 | Säkerhetsfunktionen för skydd mot skadlig kod skall använda två av varandra oberoende kontrollmekanismer för skydd mot skadlig kod för de objekt i IT-systemet som skyddas av säkerhetsfunktionen. Den ena kontrollmekanismen skall vara kontroll mot definitionsfil och den andra skall vara konfigurationsstyrning. | Förutsättningar i kapitel 5. Härdning av ODIN, se ref [5], ref [15]. Se ref [16] för ODIN Log Concentrator | N/A |
| HSSK-4-4 | Säkerhetsfunktionen för skydd mot skadlig kod skall säkerställa detektering av skadlig kod genom kontroll av inkommande och utgående informationsflöde. | Förutsättningar i kapitel 5. Anti-Viruskontroll innan filimport. | N/A |
| HSSK-4-5 | Säkerhetsfunktionen för skydd mot skadlig kod skall säkerställa att information inte överförs till eller från IT-systemet utan att kontrollmekanismen definitionsfil används. | Förutsättningar i kapitel 5. Anti-Viruskontroll innan filimport. | N/A |
| HSSK-4-6 | Säkerhetsfunktionen för skydd mot skadlig kod skall genom automatisk analys kunna detektera potentiell skadlig kod. Sådan analys skall omfatta jämförelse mot definitionsfil för de objekt som skyddas av säkerhetsfunktionen. | Förutsättningar i kapitel 5. OSSEC i ODIN | Förutsättningar i kapitel 5, dvs användning av OSSEC-agenter |

| Krav id | Kravbeskrivning | ODIN | System |
|---|---|---|---|
| HSSK-4-7 | Säkerhetsfunktionen för skydd mot skadlig kod skall, om detektering av skadlig kod sker, automatiskt kunna vidta åtgärder. Sådana åtgärder skall vad gäller kontrollmekanismen definitionsfil, omfatta placering av subjekt eller objekt i karantän samt notifiera behörig administratör och behörig användare. | Förutsättningar i kapitel 5. Anti-Viruskontroll innan filimport. | N/A |
| HSSK-4-8 | Säkerhetsfunktionen för skydd mot skadlig kod skall genomföra kontroller av subjekt och objekt:<br>• under drift,<br>• vid uppstart<br>• när behörig administratör så påkallar. | OSSEC i ODIN | Förutsättningar i kapitel 5, dvs användning av OSSEC-agenter |
| HSSK-4-9 | Säkerhetsfunktionen för skydd mot skadlig kod skall kunna uppdatera skyddet mot skadlig kod automatiskt under betryggande förhållanden. | Stöds ej då nätverksanslutning mot externa system saknas. | N/A |

### 6.7.2 Skydd av Säkerhetsfunktionen

| Krav id | Kravbeskrivning | ODIN | System |
|---|---|---|---|
| HSSK-5-1 | Säkerhetsfunktionen för skydd mot skadlig kod skall genom självtester genomföra riktighetskontroller vid uppstart samt när behörig administratör så påkallar i syfte att demonstrera en korrekt funktionalitet av den underliggande lösningen. | Förutsättningar i kapitel 5. OSSEC saknar riktighetstest och uppfyller därmed inte detta | N/A |
| HSSK-5-2 | Säkerhetsfunktionen för skydd mot skadlig kod skall endast acceptera verifierade och validerade objekt för användning som kontrollmekanism. | Förutsättningar i kapitel 5. OSSEC saknar sådan kontroll och uppfyller därmed inte detta | N/A |
| HSSK-5-3 | Säkerhetsfunktionen för skydd mot | Förutsättningar i | N/A |

| | | | |
|---|---|---|---|
| | skadlig kod skall kunna upprätthålla ett definierat säkert tillstånd när hela eller delar av den funktionalitet som detekterar om skadlig kod förekommer, är korrupt, oåtkomlig eller inaktuell. | kapitel 5. OSSEC saknar sådan funktion och uppfyller därmed inte detta. | |

### 6.7.3 Förvaltning av Säkerhetsfunktionen

| Krav id | Kravbeskrivning | ODIN | System |
|---|---|---|---|
| HSSK-6-1 | Det skall gå att lägga till, ta bort eller på annat sätt förändra vilka typer av skadlig kod som säkerhetsfunktionen skall skydda mot. | Förutsättningar i kapitel 5. | N/A |
| HSSK-6-2 | Det skall gå att lägga till, ta bort eller på annat sätt förändra vilka objekt som skall omfattas av respektive kontrollmekanism i säkerhetsfunktionen. | Förutsättningar i kapitel 5. OSSEC:s konfigurationsfil med avseende på vilka filer som omfattas. | N/A |
| HSSK-6-3 | Det skall gå att uppdatera de kontrollmekanismer som används som skydd mot skadlig kod. | Förutsättningar i kapitel 5. | N/A |
| HSSK-6-4 | Det skall gå att lägga till, ta bort eller på annat sätt förändra de åtgärder som kan vidtas när skadlig kod detekteras. | Förutsättningar i kapitel 5. OSSEC saknar sådan funktion och uppfyller därmed inte detta | N/A |
| HSSK-6-5 | Det skall gå att lägga till, ta bort eller på annat sätt förändra på vilket eller vilka sätt kontroller av IT-systemet sker;<br>• under drift<br>• vid uppstart,<br>• när behörig administratör så påkallar. | OSSEC saknar sådan funktion och uppfyller därmed inte detta. Krav ej uppfyllt. | N/A |

### 6.7.4 Assuranskrav

Se gemensamma krav.

## 6.8 Signalskydd

Dessa krav kan inte uppfyllas av ODIN då ODIN endast är mjukvara och inte uppfyller några krav på assurans i kryptologiska funktioner.

## 6.9 Obehörig Avlyssning

ODIN använder odin-tunnel för kryptering mellan koncentrator och ODIN. Detta är EJ en ackrediterad signalskyddsmekanism varför det endast är att betrakta som en säkerhetshöjande åtgärd som inte uppfyller något krav på signalskydd. ODIN är vidare enbart mjukvara så krav i detta kapitel är inte uppfyllda på något sätt genom användning av ODIN.

## 6.10 Röjande Signaler

Dessa krav kan inte uppfyllas av ODIN då ODIN endast är mjukvara.