Region Halland

Kontinuitetsplan SITHS

Hitta i dokumentet

Syfte
Revokeringslista i normalläge
Utfärda SITHS-kort – ge ut HCC
Använda SITHS-kort - komma åt spärrlistor för HCC
Kontaktuppgifter och leverantörsförteckning
Beställare, förvaltning och driftpart
SITHS-organisation Region Halland
Komprometterad CA
Kontinuitet
Felärenden
Uppdaterat från föregående version

Syfte

I händelse att vi inte kan lita på SITHS CA ska rutiner finnas för avbrottshantering.

Revokeringslista i normalläge

SITHS använder två funktioner på central nivå för revokeringskontroll; CRL och OCSP. Funktionen används för att läsa eller skriva spärrinformation. CRL är tillgänglig över två oberoende url-adresser. OCSP är tillgänglig över en url-adress. För att läsa eller skriva krävs öppningar i brandväggskonfigurationen. Centrala revokeringslistan uppdateras varje gång en ändring genomförs. Om ingen ändring görs i centrala revokeringslistan uppdateras den var 24:e timme.

CRL

http://www.carelink.se/siths-ca/ca003.crl (IP: 217.16.192.80 efter ändring av Företagsuppgifter Carelink -> Inera). Läs mer i dokumentet: CRL-hämtning av revokeringslista SITHS/mall avbrottsplan. Spärrtjänst är nåbar via:

- *SITHS CA v3*
  - Sjunet ldap://sithscrl.carelink.sjunet.org/cn=SITHS%20CA%20ver%203,o=SITHS%20CA,c=SE?certificateRevocationList;binary? (IP: 82.136.149.44) eller
  - Internet http://www.carelink.se/siths-ca/ca003.crl (IP: 80.76.157.219)
- *SITHS CA CrossBorder*
  - Sjunet ldap://sithscrl.carelink.sjunet.org/cn=SITHS%20CA%20CrossBorder%20,o=SITHS%20CA,c=SE?
  - Internet http://www.carelink.se/siths-ca/ca004.crl

OCSP

http://sithsocsp.trust.telia.com (IP: 82.136.160.42 respektive 194.237.208.174). Varje certifikat (på kort eller i funktionscertifikat) innehåller information om var spärrinformation finns tillgänglig. Olika versioner pekar på olika adresser (url). Spärrtjänst är nåbar via:

- *SITHS CA v3*

Region Halland

    - Sjunet
      http://sithsocsp.trust.telia.com (IP: 82.136.160.42 respektive 194.237.208.174)
    - Internet
      Saknas ännu (http://ocsp.preprod.trust.telia.com är tillgänglig över Internet).
- *SITHS CA CrossBorder*
    - Sjunet
      http://sithsocsp.trust.telia.com
    - Internet
      Saknas ännu (http://ocsp.preprod.trust.telia.com är tillgänglig över Internet).

En genomförd spärr från SITHS Admin (eller SITHS Självadministration) skrivs till spärrtjänsterna **CRL** respektive **OCSP** inom 10 minuter (dygnet runt);

- en publicering av ny CRL sker därefter inom 5 minuter (dygnet runt) då ny spärr registrerats
- en publicering av ny CRL sker minst en (1) ggr per dygn även om ingen ny revokeringsbegäran registrerats

Det finns dessutom en OCSP tjänst med samma innehåll.

SITHS v3 (gamla typen av certifikat tom 201301)
För att lösa detta hämtar BizTalk hem en revokeringslista från http://80.76.157.219/siths-ca/ca003.crl vilket motsvarar http://www.carelink.se/siths-ca/ca003.crl, detta sker vid tre olika tider. Varje 20m, var 3:e timme och var 6:e timme, syftet med att hämta vid flera olika tillfällen är att reducera risken att listan av någon anledning blir korrupt och dessa listor läggs på en lokal webbserver.

SITHS v1 (nya typen av certifikat from 201301)
För version 1 hämtas motsvarande från http://crl2.siths.sjunet.org/sithstype1cav1.crl. Varje 20m, var 3:e timme och var 6:e timme, syftet med att hämta vid flera olika tillfällen är att reducera risken att listan av någon anledning blir korrupt och dessa listor läggs på en lokal webbserver.

DNS
Observera att DNS:en är konfigurerad att hämta in anrop till ovanstående adresser.
Läs mer i dokumentet: CRL-hämtning av revokeringslista SITHS/mall avbrottsplan

När centrala revokeringslistan inte är nåbar
Hur en applikation ska agera när revokeringslistan inte är nåbar hanteras inom applikationen med flera valmöjligheter:

- Ignorera spärrkontrollen med effekt att spärrade certifikat accepteras (PIN-kod och behörighet krävs dock fortfarande)
- Applikationen kan själv hämta hem revokeringslistan med regelbunden intervall och välja att lita på senast sparade även om giltighetstiden gått ut.
- Stoppa inloggningar (normalläge om inte annat konfigurerats)

Viktigt att spärrkontrollen återaktiveras om den slås av under allvarligt läge!

Lokal revokeringslista och informationsspridning

- För lokal kontroll behöver revokeringslistan också sparas ner lokalt. Detta ska göras av RGS IT Service 1 gång per dygn, fram till dess att revokeringslistan kan nås från fler ställen.
- RA och Servicedesk (servicedesk@regionhalland.se) får ett SMS och mejl till RA-brevlådan från Inera AB. RA kontrollerar med RGS IT-service.

- Under avbrottet ska KRA manuellt registrera inkommande revokeringar och vid särskilt kritiska fall se till att behörigheter kopplade till dessa HCC tillfälligt dras in.
- När SITHS åter är i drift informeras detta enligt ovan.
  RA ansvarar för att till TIB informeras när ett avbrott i revokeringslistan pågått längre än tolv timmar. TIB hålls kontinuerligt informerad om status.

Utfärda SITHS-kort – ge ut HCC

Förutsättningar
För att utfärda tjänstecertifikat krävs:

- Beställning antingen via KoBe eller på papper
- Åtkomst till HSA
- Åtkomst till webbapplikation SITHS Admin
- Åtkomst till webbapplikation SIS Capture Station
- Åtkomst till Net iD
- Behörig personal

Avbrott i administration av HCC - åtgärder för återstart
Om beställning, spärrning eller andra funktioner för administration av HCC (Health Care Certificate) inte kan genomföras ska Inera AB informeras omgående i syfte att aktivera återstart:

1. Fyll i felanmälningsblankett på Ineras hemsida och skriv händelselogg och bifoga kopia på felanmälningsblankett
2. Ring 0771- 25 10 10 när ett telefonsamtal är att föredra och skriv händelselogg.

Vid behov

1. Kontakta HAK-förvaltning och IT-service
2. Informera RA
3. Informera på intranätet och via mejl till mejlgrupp *RH anställda* (dold grupp)

Avbrottsläge
Normalläge
När funktionen åter är i normalläge återgår man till normalt arbetssätt och manuellt registrerade revokeringar registreras i systemet.
Återkoppling
Avbrott redovisas kontinuerligt i händelseloggen inom RA-organisationen. Verksamheten informeras vid behov via intranätet och via mejl till mejlgrupp *RH anställda* (dold grupp).

Region Halland

Använda SITHS-kort - komma åt spärrlistor för HCC

För att använda tjänstecertifikat krävs åtkomst till:

- Revokeringslistan (spärrlista, CRL).
- Net iD installerad med tillhörande drivrutiner för kortläsare.
- Root-certifikat från SITHS CA installerat korrekt version installerat i datorns certifikatslager.

Avbrottsläge – SITHS kan inte användas
Under avbrott, då det inte finns åtkomst till någon av de senaste revokeringslistorna och/eller online-tjänsten för certifikatverifiering (OCSP-tjänsten), kan den gamla versionen av revokeringslistan användas. Denna uppdateras var 20:e minut av RGS IT Service. Revokeringslistan betraktas som ogiltig efter 24 timmar. I de kontinuitetsplaner som måste finnas för varje system, som använder SITHS, ska information finnas om vad som gäller när revokeringslistan inte längre gäller. I planen ska finnas uppgifter om hur länge revokeringslistan ändå får användas och vad som gäller vid olika långa avbrott.
Om revokeringslistan betraktas som ogiltig ska alternativa inloggnings- och signeringsmetoder i drabbade system användas i enlighet med respektive systems kontinuitetsplan.

Beslut om förlängning av revokeringslistan giltighet beslutas av RA.
Aspekter vid dessa beslut är systemets verksamhetsnytta kopplat till säkerhetsnivån efter informationsklassning.

Informationsspridning
Information om avbrottet förmedlas av RA till ORA som i sin tur informerar verksamhetschefer med flera (se rubrik *Återkoppling*).

Avvikelse
Avvikelserapport ska skrivas och bearbetas och vid behov ska nya och förbättrade rutiner införas.

Normalläge
När funktionen åter är i normalläge gäller ordinarie rutiner för inloggning och arbetssätt det vill säga SITHS ska användas.

Återkoppling
Verksamheten informeras via Intranät och mejl till verksamhetschefer.

Kontaktuppgifter och leverantörsförteckning

Företag	Funktion/e-post	Telefon
Inera AB	Servicedesk (servicedesk@inera.se)	0771- 25 10 10
Inera AB	Förvaltare	08-452 71 60
Inera AB	Säkerhetsansvarig	08-452 71 60
Cygate AB	SITHS@cygate.se	010-878 70 00
TeliaSonera AB	Customer Services	0771-100 400
RGS IT-service	IT-Service	010 4761900
TIB	Tjänsteman i beredskap	112

Beställare, förvaltning och driftpart

- Beställare: SKL och CeHis
- Förvaltare: Inera AB
- Upphandlad driftpart: TeliaSonera och Cygate

SITHS-organisation Region Halland

- AU (huvudansvarig): Henrik Pedersen, Regionkontoret
- ORA / Objektledare: Magnus Öberg
- Säkerhetsansvarig: Anders Nilsson, Regionkontoret

Komprometterad CA

Om komprometterad CA inträffar ska Inera AB omedelbart informera RA om detta.
I händelse av att man inte längre kan lita på HCC ska RA-organisationen informeras.
System som använder HCC för inloggning och/eller signering ska ha funktioner som möjliggör förenklad inloggning och signering som kan tillämpas tills nya HCC skapats.
Respektive systems kontinuitetsplan aktiveras.

Kontinuitet

För att uppnå kontinuitet gäller att:

1. Förebygga och förbereda genom riskanalyser, riskvärdera och riskminska (RA ger uppdrag)
2. Revision (säkerhetsansvarig enligt RAPS)
3. Rapportera punkt 1 och 2 till SITHS förvaltningsgrupp.
4. rapportera avvikelser/händelser (kontinuerligt informera RA)
5. Lära genom orsaksanalys och utvärdering
6. Förbättra
7. Återkoppla
8. Öva

Felärenden

Felärenden hanteras enligt rutin för felanmälan. Avvikelse hanteras enligt regiongemensam rutin *Avvikelser* och regiongemensamt kapitel *405 Avvikelser* i ledningssystemet. Det vill säga fel åtgärdas och händelser/incidenter rapporteras som avvikelse.

Uppdaterat från föregående version

Ändringar i RA organisation och uppdaterade telefonnummer