

Programa de la Història Clínica Compartida a Catalunya

Especificacions per a la connexió dels centres al sistema

Juny de 2009

© Generalitat de Catalunya.

Departament de Salut

Edita: Programa de la Història Clínica Compartida a Catalunya (HCCC)



Sumari

1. Introducció	Pàg. 4
1.1 Objectiu	
1.2 Referències	
2. Requisits del sistema d'informació clínica	Pàg. 4
2.1 Requisits d'accés personal al sistema d'informació	
2.2 Requisits de perfil de relació professional-pacient	
3. Arquitectura del sistema HCCC tipologia dels requisits per a les Comunicacions entre els seus components	Pàg. 6
4. Requisits per a connexions pròpies del sistema HCCC	Pàg. 8
4.1 Requisits generals	
4.2 Requisits per al professional	
4.3 Requisits per a l'accés a consultar informació de l'HCCC (a través de servidors de publicació)	
4.4 Requisits per al professional	
4.4.1 Actualització de dades al sistema índex des del servidor de publicació	
4.4.2 Tallafocs IP	
4.4.3 Servidor web SSL	
4.4.4 Certificat CATCert	
4.4.5 Sincronització de temps	
4.5 Requisits per al subministrament d'informacions al repositori central de l'HCCC amb actualització del sistema índex, mitjançant SFTP	
4.5.1 Tallafocs IP	

4.5.2 Usuari únic per l'SFTP

4.6 Requisits per fer possible l'accés per part del sistema índex de l'HCCC a informacions en repositoris propis dels centres assistencials

4.6.1 Tallafocs IP

4.6.2 Servidor web SSL

4.6.3 No volatilitat de les dades

4.6.4 Sincronització de temps

4.6.5 Requisits d'infraestructura i disponibilitat

5. Formats per a la publicació de dades i missatges en el sistema HCCC

Pàg. 14

1. Introducció

1.1. Objectiu

Aquest document descriu el conjunt de requisits que, de conformitat amb els criteris del conveni tipus per implantar el Programa d'Història Clínica Compartida a Catalunya (HCCC), obligatòriament han de complir les institucions d'assistència sanitària per accedir a la plataforma central de la solució HCCC, tant per accedir a la informació continguda en l'HCCC com per subministrar-n'hi.

Els requeriments per a la connexió dels centres al sistema de l'HCCC es poden diferenciar entre requisits del sistema d'informació de la mateixa entitat titular dels centres assistencials que s'hagin de connectar amb l'HCCC i requisits per a la connexió i comunicació amb els sistemes centrals i específics de l'HCCC.

1.2. Referències

Els tipus de certificats que proveeix el CATCert estan llistats a:

- http://www.catcert.net/web/cas/serveis/cataleg_serveis_certificats.jsp.

2. Requisits del sistema d'informació clínica

D'acord amb els requeriments del sistema d'informació de les entitats, s'entén per “aplicació d'estació clínica” o “aplicació d'història clínica de centre” tot component del sistema o sistemes d'informació que utilitzin els professionals d'un centre sanitari per veure o incorporar dades de salut d'una persona concreta, amb dades que la identifiquin.

2.1. Requisits d'accés personal al sistema d'informació

L'accés d'una persona a un sistema d'informació que compregui aplicació d'estació clínica cal que es realitzi per un sistema d'acreditació personal mitjançant una de les tres modalitats següents:

a) Contrasenya robusta, és a dir, que tingui les següents característiques:

- Longitud mínima: 8 caràcters.
- Estar composta per lletres (minúscules i majúscules), noms i símbols.
- Contenir com a mínim dues majúscules.
- Contenir com a mínim dos símbols.
- Tenir un símbol entre les posicions segona i sisena.
- No contenir el nom o cognom de l'usuari.
- Ser significativament distinta d'altres contrasenyes anteriors.
- No ser un nom o una paraula comuns.
- Historial de contrasenyes recordades: 3 contrasenyes recordades.
- Període màxim de renovació de contrasenyes: 90 dies.
- Període mínim de renovació de contrasenyes: 2 dies.

b) Contrasenya explícitament autoritzada per acord favorable de la Comissió de Seguiment de l'HCCC, prevista en el **conveni tipus per implantar l'HCCC**, segons la petició d'ús en la sol·licitud de la institució d'incorporació al sistema d'informació de l'HCCC. La descripció d'aquesta contrasenya autoritzada s'incorporarà al corresponent conveni tipus signat per la institució.

c) Un sistema de certificat digital per a l'accés dels professionals a l'aplicació d'estació clínica.

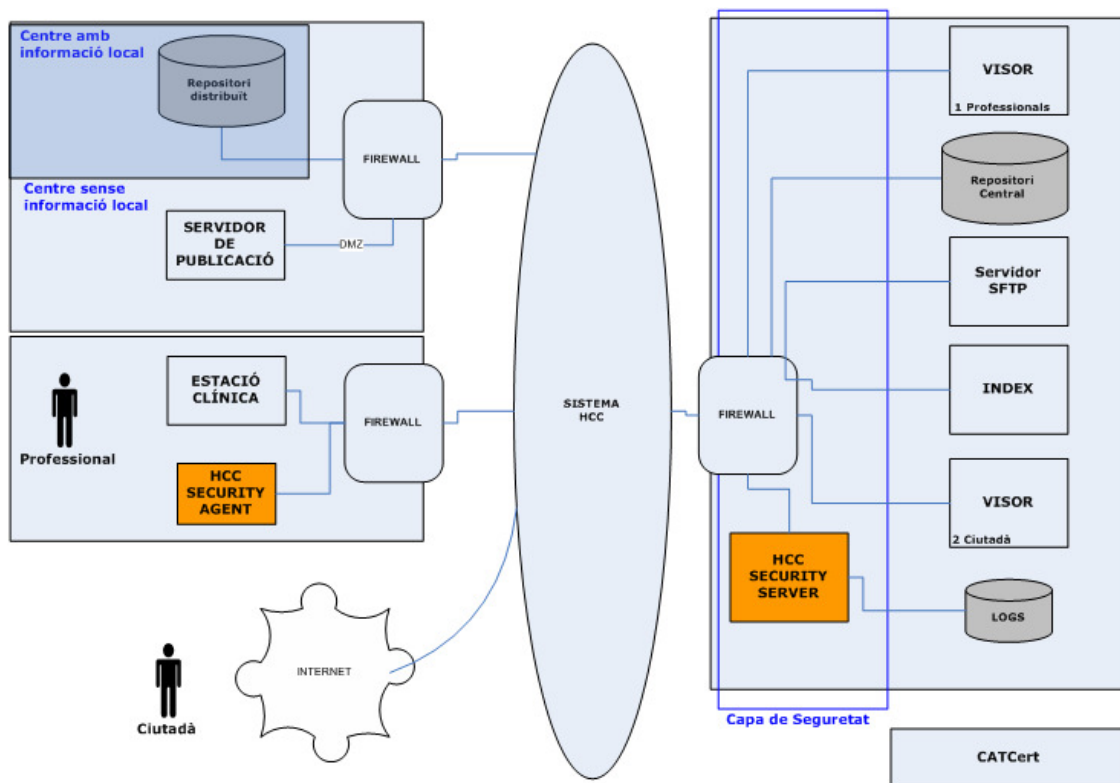
2.2. Requisits de perfil de relació professional-pacient

L'accés d'una persona a un sistema d'informació que compregui aplicació d'estació clínica cal que es realitzi per un sistema d'autorització de perfils professionals que defineixin la tipologia de la relació assistencial entre el professional i el ciutadà o pacient, que justifica l'accés del professional a dades de salut de la persona concreta en qüestió.

Estan detallats en el conveni tipus (annex 5) les tipologies dels perfils de relació assistencial autoritzades per a l'accés al visor de l'HCCC.

3. Arquitectura del sistema HCCC i tipologia dels requisits per a les comunicacions entre els seus components

Es mostra a títol informatiu el diagrama dels components participants en el sistema HCCC. A la dreta hi ha els components de l'arquitectura de la plataforma central, i a l'esquerra, els components dels agents que s'hi comuniquen, tant els ciutadans individuals com les institucions assistencials, i, dins d'aquestes, els professionals i els components del sistema d'informació que intervenen en el sistema HCCC.



participants. Es resumeixen en una taula els requisits que han de complir les institucions d'atenció sanitària amb l'objectiu d'integrar-se en la plataforma de seguretat de l'HCCC segons les opcions de participació per les quals optin.

Tipologia Requisits	Només accés al visor de l'HCCC (lectura)	Accés al visor i sistema índex i custòdia de documents en dipòsit central	Accés al visor i sistema índex i custòdia de documents en sistema propi
Requisits generals (punt 4.1)	Sí	Sí	Sí
Requisits per al professional de salut (punt 4.2)	Sí	Sí	Sí
Requisits per a l'accés a consultar informació de l'HCCC (punt 4.3)	Sí	Sí	Sí
Requisits per al subministrament de dades al sistema índex de l'HCCC (punt 4.4)	No	Sí	Sí
Requisits per al subministrament d'informacions a repositori central del Departament de Salut amb actualització del sistema índex, mitjançant SFTP (punt 4.5)	No	Sí	No
Requisits per fer possible l'accés per part del sistema índex de l'HCCC a informacions en repositoris propis dels centres assistencials (punt 4.6)	No	No	Sí

Els criteris segons els quals es realitza la divisió per **tipologia** entre les institucions assistencials són els següents:

- Es considera l'escenari de **només accés al visor de l'HCCC (només lectura)** per a aquelles institucions que únicament accedeixin al sistema HCCC per efectuar la lectura d'històries clíniques a les quals estiguin autoritzades, amb independència que aquest escenari es consideri excepcional.

- Es considera l'escenari d'accés **al visor i al sistema índex i custòdia de documents en repositori central del Departament de Salut** per a aquelles institucions que accediran al sistema HCCC per fer la lectura d'històries clíniques que els estiguin autoritzades i que, a més, realitzaran la custòdia de documents en el repositori central de l'HCCC. Això implica que disposaran també d'un servidor de publicació.
- Es considera l'escenari d'accés **al visor i al sistema índex i custòdia de documents en sistema propi** per a aquelles institucions que accediran al sistema HCCC per dur a terme la lectura d'històries clíniques que els estiguin autoritzades i que, a més, efectuaran la custòdia de documents en repositori o repositoris propis. Això implica que disposaran també d'un servidor de publicació.

4. Requisits per a connexions pròpies del sistema HCCC

4.1. Requisits generals

Tots els fitxers amb dades personals tractades a l'HCCC se suposen ja conformes a la Llei de protecció de dades.

Es requereix que la institució assistencial disposi d'un equip tallafocs IP en el qual es configuren convenientment les regles expressades en els requisits descrits als apartats que segueixen a continuació.

També es requereix que els equips informàtics estiguin protegits de programes virulents mitjançant un programa antivirus actualitzat.

Igual que es requereix protecció lògica de l'accés a les dades, també es requereix una protecció física de l'accés a aquestes dades, és a dir, només els professionals autoritzats hi haurien de tenir accés.

Per una altra part, és requisit general que totes les proves que efectuïn les institucions assistencials, i concretament en les comunicacions amb la plataforma de reproducció de la plataforma central de l'HCCC, es duguin a terme utilitzant dades despersonalitzades, és a dir, sense que es pugui reconèixer cap persona real.

Dins de les bones pràctiques de la seguretat, és altament aconsellable, una vegada instal·lats i configurats els diferents productes, i abans de passar a producció, dur a terme una auditoria externa de vulnerabilitats remotes d'aquests productes, si no està ja previst dins del pla d'exploració del projecte.

4.2. Requisits per al professional

El professional sanitari s'ha d'identificar en el sistema d'informació de la institució d'assistència sanitària (aplicació d'estació clínica) seguint el conveni tipus. El professional de salut ha de conèixer que en els seus accessos de visualització de l'HCCC es crearà un registre que indicarà quin professional ha consultat informació sobre un pacient concret, quin tipus d'informació ha consultat, segons quin perfil de relació assistencial professional-pacient i en quin moment.

4.3. Requisits per a l'accés a consultar informació de l'HCCC

Els requisits són els següents:

- L'aplicació d'estació clínica ha d'estar protegida per tallafocs IP, el qual ha de tenir implementada una regla per només enviar peticions al Security Service de l'HCCC (HCCSs) i mai a cap altre component de l'HCCC.
- Complir el mètode definit d'accés al visor des de l'aplicació d'estació clínica:
 - Crear una pàgina HTML amb una asserció SAML mitjançant l'HCCSa, sempre que es consultin les dades d'un CIP, per invocar el navegador amb la pàgina que iniciarà la navegació per l'aplicació visor.

- L'assertió SAML comprendrà els següents camps: el CIP i el NIA d'identificació del pacient sobre el qual es realitza la consulta, el nom i els cognoms del professional que la duu a terme, el tipus i el número de document que identifica el professional, el codi del perfil de relació assistencial professional-pacient, la seva categoria professional, el número de col·legiat del professional, el codi de l'organització en la qual desenvolupa les tasques el professional que fa la consulta, i la data i l'hora de creació de l'assertió SAML. El sistema HCCC tindrà establerts els camps de l'assertió SAML que són obligatoris i els que són opcionals.
- La petició ha d'enviar-se mitjançant HTTPS amb TLS 1.0 o SSL 3.0.
- Acreditar i autoritzar de manera precisa el professional segons el que s'ha presentat a l'apartat 2.
- Guardar traces de totes les autoritzacions i acreditacions a l'aplicació d'estació clínica, tant correctes com incorrectes. Addicionalment, cal guardar tota autorització correcta o incorrecta de consulta al visor HCCC, de manera que les traces es puguin consultar transcorreguts almenys dos anys des que es van escriure (això es pot assolir guardant les traces proporcionades per l'HCCSa).
- La data i l'hora de les màquines de l'aplicació d'estació clínica haurien d'estar sincronitzades amb la data i l'hora de la resta de les màquines de l'HCCC.
- L'aplicació d'estació clínica ha d'estar configurada per esborrar automàticament els fitxers temporals que s'hagin generat, en el moment de tancar una sessió i en el moment d'iniciar-la. En especial, cal esborrar els documents de l'HCCC que s'hagin pogut descarregar.

4.4. Requisits per al subministrament de dades al sistema índex de l'HCCC (a través de servidors de publicació)

4.4.1. Actualització de dades al sistema índex des del servidor de publicació

Els missatges emesos en l'actualització de dades utilitzant *web services* des d'un servidor de publicació cap al sistema índex han d'incloure una asserció SAML (sense atributs de contingut, utilitzant el component HCC Security Agent (HCCSa)).

4.4.2. Tallafocs IP

El servidor de publicació del centre assistencial ha d'estar protegit per tallafocs IP, el qual ha de tenir implementades regles perquè només es pugui permetre l'accés de les comunicacions amb origen el servidor de publicació i destinació l'HCCSs de la plataforma central.

4.4.3. Servidor web SSL

El servidor web de publicació s'ha de configurar per comunicar-se mitjançant SSL, amb l'objectiu de xifrar la comunicació amb el servidor HCCSs de la plataforma central.

4.4.4. Certificat CATCert

El servidor web ha de comptar amb un certificat emès per CATCert. L'utilitzarà per demostrar la seva identitat en la comunicació SSL amb l'HCCSs de la plataforma central.

4.4.5. Sincronització de temps

Perquè les traces es puguin correlacionar satisfactòriament amb unes altres traces del sistema, la data i l'hora de les màquines de l'aplicació haurien d'estar sincronitzades amb la data i l'hora de la resta de les màquines de l'HCCC.

4.5. Requisits per al subministrament d'informacions al repositori central de l'HCCC amb actualització del sistema índex, mitjançant SFTP

4.5.1. Tallafocs IP

El tallafocs IP que protegeixi aquesta operació ha de tenir regles implementades que permetin l'accés al servei SFTP central (plataforma central de l'HCCC).

4.5.2. Usuari únic per l'SFTP

Per facilitar la identificació sobre quin sistema d'informació d'institució assistencial ha realitzat l'actualització d'un fitxer determinat, cada servidor que accedeixi al servei d'SFTP central ha de disposar d'unes credencials pròpies d'accés (usuari i contrasenya). Aquestes credencials haurien d'estar custodiades i ser diferents per a cadascun dels servidors que accedeixin al servei d'SFTP central. Si s'utilitzen certificats com a mitjà d'acreditació, aquests certificats han de seguir la mateixa política.

No és necessària la creació d'una asserció SAML.

4.6. Requisits per fer possible l'accés per part del sistema índex de l'HCCC a informacions en repositoris propis dels centres assistencials

4.6.1. Tallafocs IP

Ha d'existir un tallafocs IP que permeti l'accés de les comunicacions SSL establertes amb origen a l'HCCSs de la plataforma central i destinació el servidor de publicació de l'entitat assistencial.

4.6.2. Servidor web SSL

Ha d'utilitzar-se un servidor web segur que empri SSL 3.0 o TLS 1.0, mitjançant el qual un certificat de servidor (tipus el certificat CDS de CATCert) es connectarà amb el component HCCSs de la plataforma central.

4.6.3. No-volatilitat de les dades

Per poder reconstruir situacions passades, i de conformitat amb la legislació, les dades i els informes que estiguin a la disposició de l'HCCC s'han de guardar vint anys i han de ser localitzables amb el mateix nom de l'arxiu, el seu identificador intern i el seu contingut, amb registre del període de temps accessible des del sistema de l'HCCC.

4.6.4. Sincronització de temps

Perquè les traces es puguin correlacionar satisfactòriament amb unes altres traces del sistema, la data i l'hora de les màquines de l'aplicació haurien d'estar sincronitzades amb la data i l'hora de la resta de les màquines de l'HCCC.

4.6.5. Requisits d'infraestructura i disponibilitat

Per a una disponibilitat permanent dels servidors de publicació per l'HCCC de la informació en repositoris propis d'entitat, que haurà d'estar assegurada, la infraestructura haurà d'estar dotada de:

- Contractació o disposició de línies de corrent redundants.
- Sistemes d'alimentació ininterrompuda (SAI).
- Implantació d'eines que permetin el control de consum de:
 - Espai en el disc.
 - Rendiment CPU.
 - Disponibilitat dels serveis.

- Servei permanent (presencial o localitzable) de manteniment de la infraestructura i del correcte funcionament dels equips necessaris per a la publicació de dades sol·licitables pel sistema índex central de l'HCCC.

5. Formats per a la publicació de dades i missatges en el sistema HCCC

La publicació de missatges i dades entre el sistema central de l'HCCC i els sistemes d'informació de les entitats i els centres adherits a l'HCCC està normalitzada i es descriu en el document "Requisits per a la integració i publicació de dades en la plataforma HCCC per a les institucions assistencials: document tècnic", que es facilita a les institucions que sol·liciten la participació de centres assistencials que en depenen en l'HCCC.