



Generalitat de Catalunya  
Departament de Salut

# **Programa d'Història Clínica Compartida a Catalunya.**

## **Sistema de Seguretat**

**Maig de 2007**

Aquesta és la versió v8 d'aquest document. Podeu consultar si es tracta de la darrera versió al web <http://www.gencat.cat/salut/hccc>

## ÍNDEX

1.	Sistema de Seguretat .....	3
2.	Resum Funcional .....	6
2.1	Conceptes del disseny de seguretat.....	6
2.2	Components de la solució .....	7
2.3	Cas d'ús 1: Accés a HCCC per part del professional assistencial. ....	10
2.4	Cas d'ús 2: Accés a HCCC per part del ciutadà/na. ....	12
2.5	Consultes del SIDX als repositoris de dades clíniques. ....	14
2.6	Cas d'ús 4: Publicació de documents clínics mitjançant Web Services. ....	16
2.7	Cas d'ús 5: Publicació de documents clínics mitjançant SFTP. ....	18
2.8	Glossari de termes. ....	20

## **1. Sistema de Seguretat**

El sistema de seguretat de la HCCC es basa en la implantació d'una infraestructura de seguretat capaç d'actuar en totes les sol·licituds i transferències d'informació entre tots els components per garantir que totes les transferències d'informació que es realitzin entre tots els components responen a peticions vàlides en el model d'autorització definit i queden enregistrades per futures auditories en un repositori centralitzat.

En tots els processos es mantenen els següents principis de seguretat:

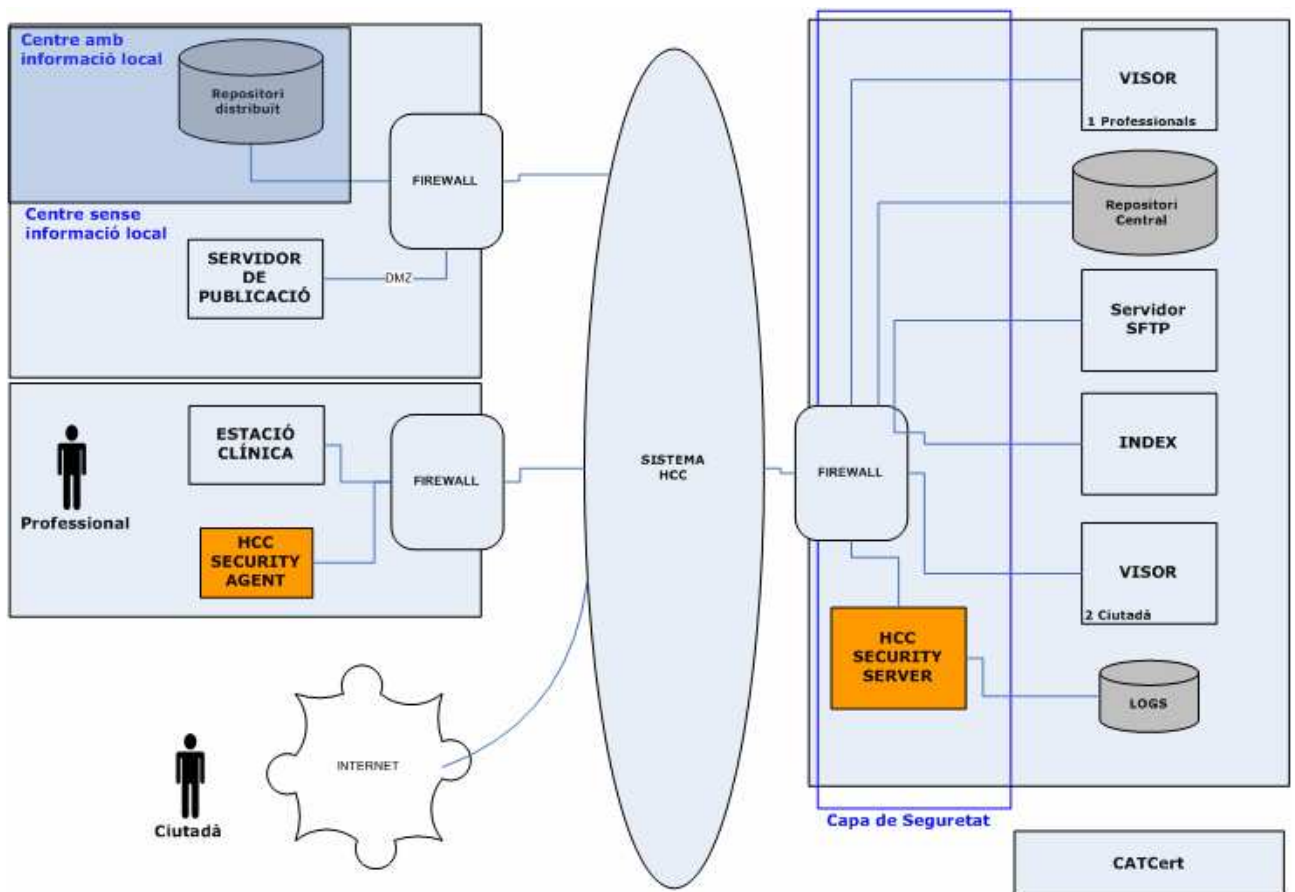
- La seguretat a nivell de xarxa garanteix que no sigui possible la connexió directa entre els diferents actors i/o components (per exemple, no és possible que el professional connecti directament amb el Visor).
- S'enregistren en les traces de la capa de seguretat totes les activitats que es consideren rellevants.
- Totes les comunicacions es realitzen utilitzant protocols segurs que garanteixin la seva confidencialitat i integritat.
- Totes les comunicacions venen garantides en origen per la firma electrònica pròpia de cada institució d'assistència sanitària o servidor d'aplicació.
- Las comunicacions entre actors i/o components que impliquen transferència de informació d'identitat aprofiten el model OASIS i especialment les tasques relacionades amb la federació d'identitats (ús d'assertions SAML, firma XML, etc.).

Per implementar la capa de seguretat de tota l'arquitectura de HCCC, s'han definit els models d'acreditació, autorització i auditoria. La comunicació viatja sempre xifrada.

S'han desenvolupat els components que a continuació es detalla:

- HCC Security Agent (API HCCSa): és el component que facilita a les institucions assistencials participants en el model d'HCCC la integració de la seguretat del servei HCC amb els seus sistemes. La funcionalitat bàsica d'aquest component és la construcció d'assertions SAML, necessàries per traslladar la informació requerida per l'autorització de les peticions del professional sanitari al servei HCCC. L'assertió SAML generada va signada amb el certificat digital (emès per CatCert) corresponent a la institució sanitària des de la que es realitza la petició.
- HCC Security Server: HCCCs és el component de seguretat en la plataforma central de la HCCC. Aquest component s'encarrega de les tasques següents:
  - Protecció davant atacs i validació d'esquemes dels missatges SOAP y XML en circulació.
  - Validació d'algunes dades.
  - Verificació de assertions SAML.
  - Verificació de certificats.

- Establir connexions amb els diferents servidors, ja que totes les peticions als servidors passen obligatòriament per ell.
- Fer d'intermediari (Proxy) entre el navegador del ciutadà i el Visor.
- Registrar tots els accessos en un repositori centralitzat per futures auditories.



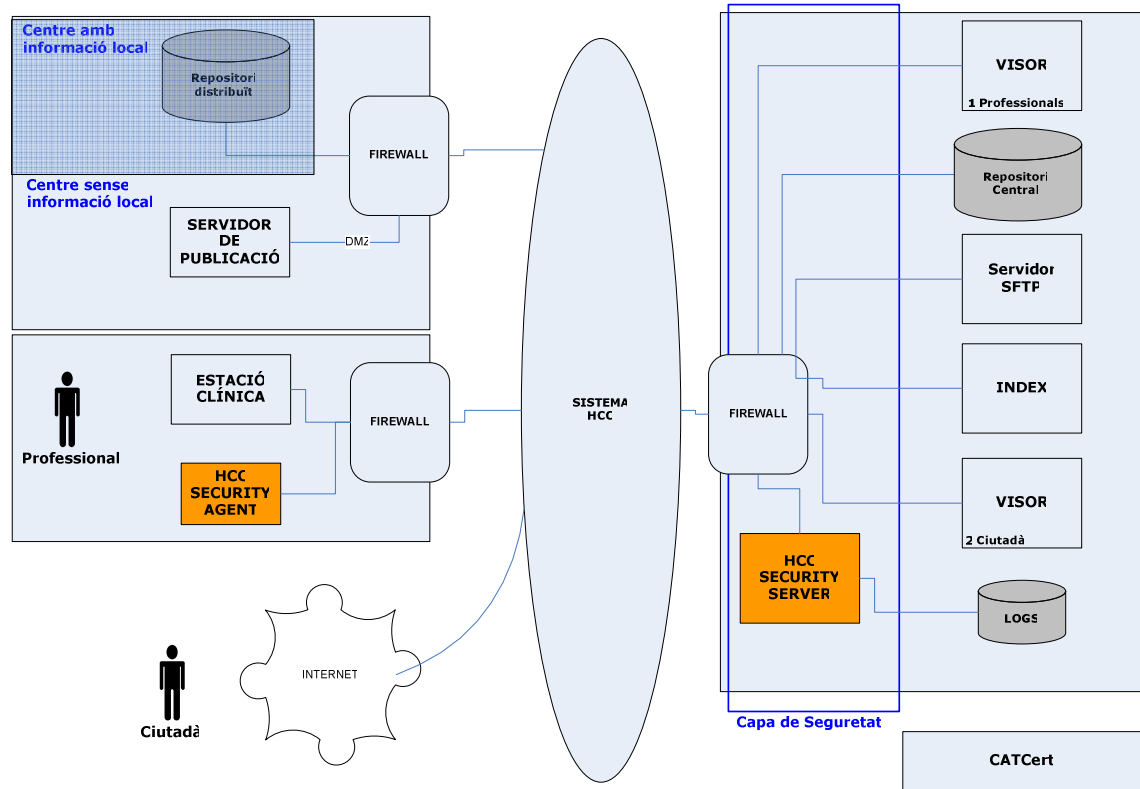
## **2. Resum Funcional**

### **2.1 Conceptes del disseny de seguretat**

La solució de seguretat es basa en els següents conceptes i principis:

- Tots els elements s'identifiquen de forma inequívoca mitjançant certificats de CATCert ([www.catcert.cat](http://www.catcert.cat)).
- Totes les comunicacions fora de la zona protegida es realitzen mitjançant xifrat de comunicacions (SSL).
- Addicionalment, aquestes comunicacions es protegeixen amb un maquinari especialitzat en seguretat i tractament d'XML. Es tracta del HCCSs.
- La informació d'autenticació es rep per part les institucions assistencials autoritzades, delegant-ne el procés. A aquest esquema d'autenticació se l'anomena federació d'identitats.
- La informació d'autenticació s'envia cap a HCC utilitzant una peça de programari anomenada HCCSa. Aquest desenvolupament cal incloure'l en l'aplicació d'estació clínica.
- La informació d'autenticació es transmet dins d'un fitxer SAML.
- Tots els accessos al sistema estan auditats.

## 2.2 Components de la solució



Els components de la plataforma HCCC són els següents:

**HCCSs.** Es tracta del maquinari del nucli de la seguretat i principalment assegura poder garantir la seguretat d'accés i la traçabilitat.

**HCCSa.** És un desenvolupament a mida que caldrà integrar en les aplicacions d'estació clínica per tal de què els professionals puguin accedir al Visor de forma segura.

**Visor.** És l'aplicació a la qual s'hi podran connectar professionals i ciutadans per tal de fer consultes de documents clínics.

**SIDX.** És el servidor d'índexs d'HCC i té la capacitat de saber a on estan localitzats el document clínics, a banda de també ser dipòsit de dades.

**Repositori central.** És el dipòsit centralitzat de les dades clíniques.

**Servidor de publicació.** És l'element mitjançant el qual les institucions assistencials podran indicar que han publicat un document en el seu repositori propi o bé en el repositori central.

**Repositori distribuït.** És un dipòsit de dades localitzat dins d'una institució assistencial.

**Repositori de LOGS.** És el dipòsit a on s'allotjaran les traces de seguretat.

Els components que formen la capa de seguretat són els següents:

**HCCSs.** Es tracta del maquinari del nucli de la seguretat i principalment assegura poder garantir la seguretat d'accés i la traçabilitat.

**HCCSa.** És un desenvolupament a mida que caldrà integrar en les aplicacions d'estació clínica per tal de què els professionals puguin accedir al Visor de forma segura. El facilita el Departament de Salut.

**Fitxer SAML.** Dins d'aquest fitxer s'inclou el CIP o NIA del pacient consultat i les dades del professional que fa la consulta. Es crea a través del HCCSa.

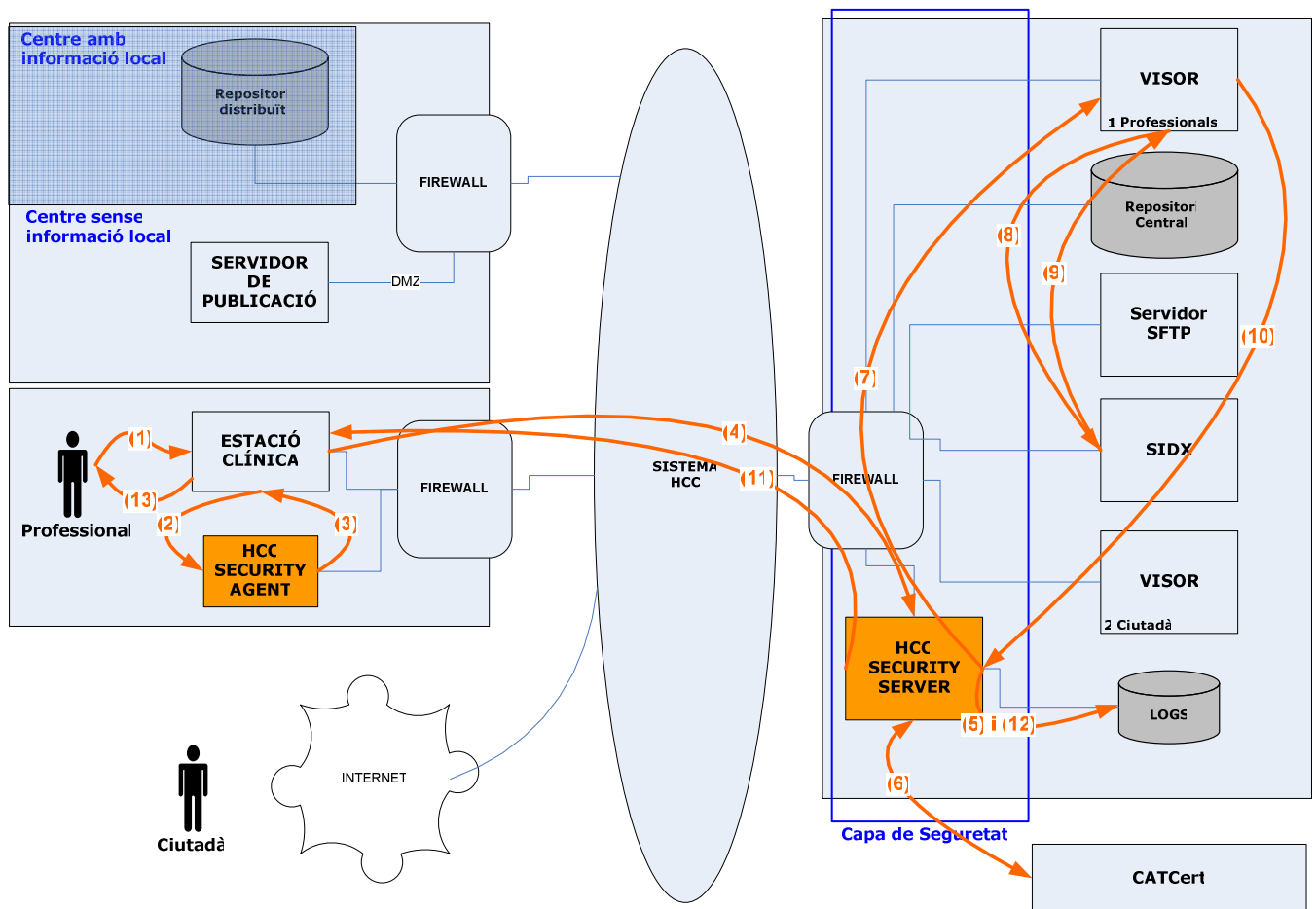
**Certificats digitals.** Es tracta d'elements (físics o en format fitxer) que

permeten que els diferents sistemes acreditin la seva identitat. Els ha emès CATcert.

**Tallafocs (“firewalls”).** Són maquinaris amb la capacitat de permetre o denegar accesos dins de xarxes securitzades.

**Xifrat de comunicacions.** Les comunicacions fora de les xarxes securitzades estaran xifrades per tal que només puguin ser llegides pel destinatari de la informació. HTTPS és el protocol de comunicació web amb SSL.

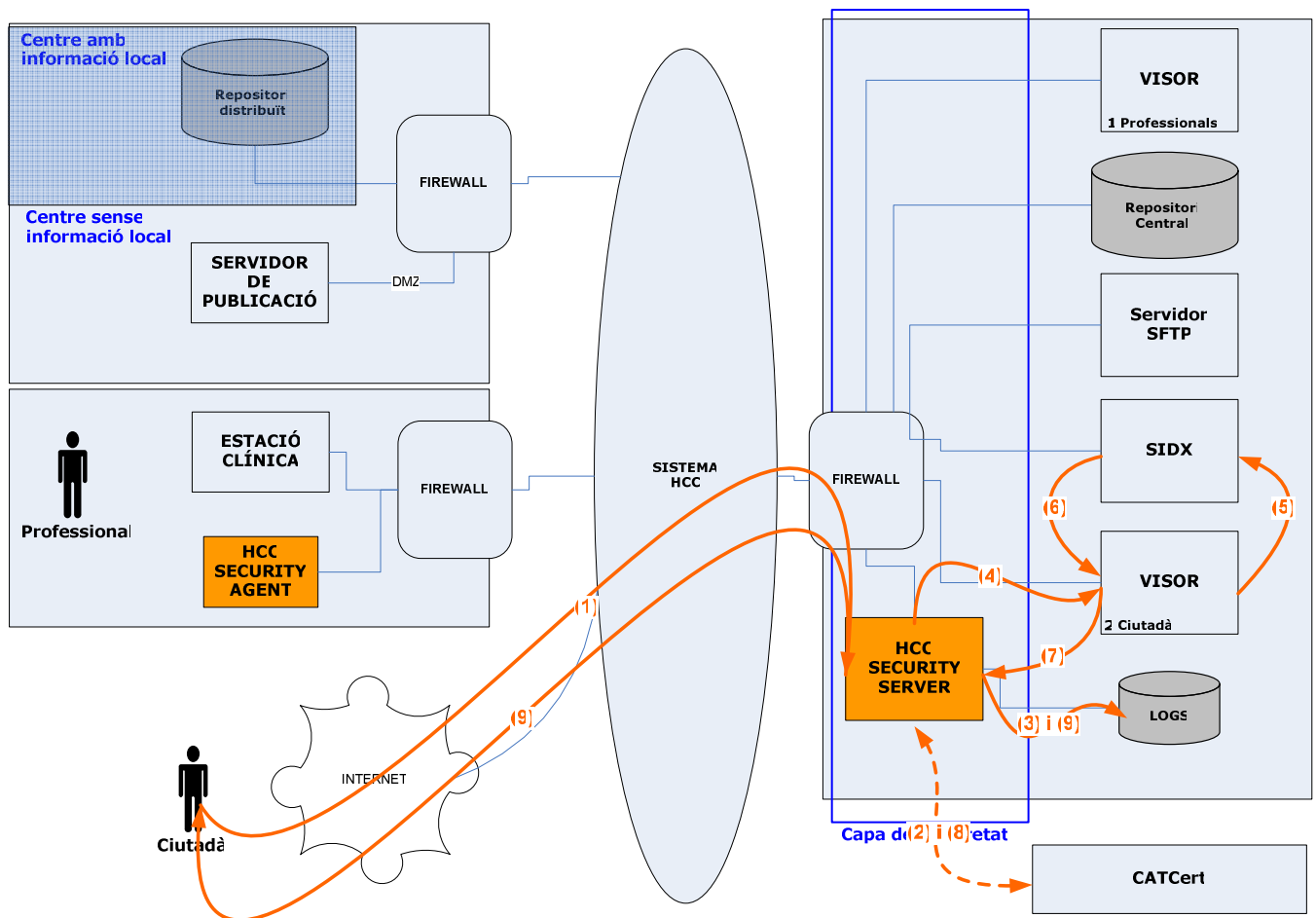
### 2.3 Cas d'ús 1: Accés a HCCC per part del professional assistencial.



El flux d'informació es desenvolupa en els següents passos:

- 1 - El professional intenta accedir a HCCC a través de la seva aplicació d'estació clínica.
- 2 i 3 - L'aplicació d'estació clínica genera un fitxer **SAML** signat amb el seu certificat digital.
- 4 - **L'aplicació d'estació clínica** envia el fitxer SAML al HCCSs utilitzant **SSL**.
- 5 - **L'HCCSs** valida la petició (mitjançant el **certificat del servidor** de l'aplicació d'estació clínica) i la **registra en un log**. Un cop s'ha enviat el fitxer SAML en el primer accés, ja no cal enviar-lo de nou excepte si es finalitza la sessió.
- 6 - L'HCCSs valida el certificat contra **CATCert** (només s'accedeix a CATCert quan s'emeten actualitzacions sobre la validesa dels certificats).
- 7 - L'HCCSs permet el pas cap el **Visor**. El Visor i l'HCCSs utilitzen **certificats i SSL**.
- 8 i 9 - El Visor consulta al SIDX i aquest li serveix els documents clínics demanats. El flux d'informació en les consultes del SIDX es mostra en el cas d'ús 3.
- 10 - El Visor passa la resposta cap l'HCCSs.
- 11 - L'HCCSs li passa la mateixa resposta cap l'estació d'aplicació clínica utilitzant SSL.
- 12 -L'HCCSs registra l'operació de resposta.
- 13 - Es serveix la resposta al professional en format pàgina web.

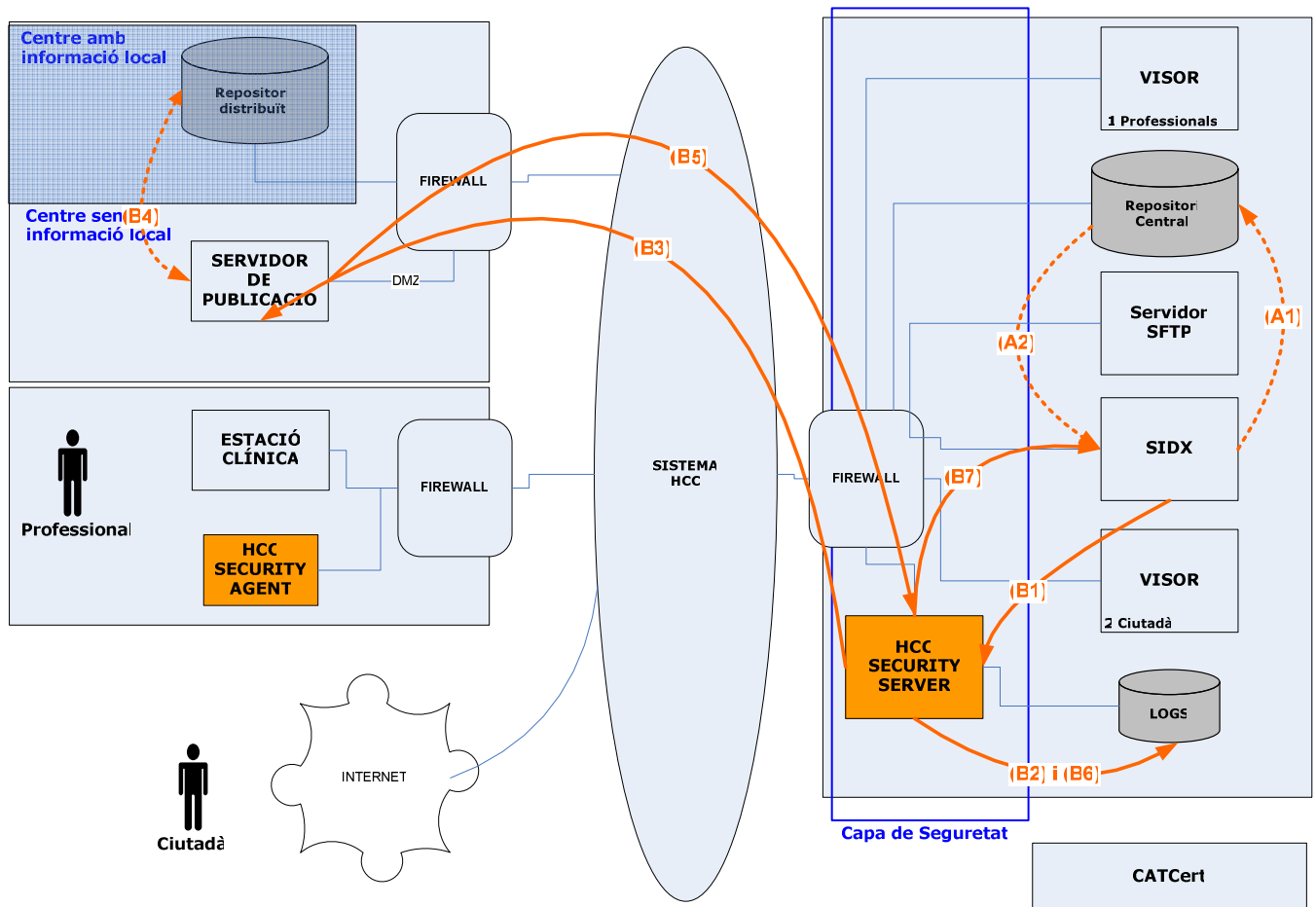
## 2.4 Cas d'ús 2: Accés a HCCC per part del ciutadà/na.



El flux d'informació es desenvolupa en els següents passos:

- 1 - El ciutadà/na intenta accedir a HCCC a través del seu navegador via **HTTPS**. El ciutadà/na tindrà carregat el seu **certificat de CATCert** en el seu PC.
- 2 - L'HCCSs valida el certificat contra **CATCert** (només s'accedeix a CATCert quan s'emeten actualitzacions sobre la **validesa dels certificats**).
- 3 - L'HCCSs valida la petició (mitjançant el **certificat del ciutadà**) i la **registra en un log**.
- 4 - L'HCCSs permet el pas cap el Visor. El Visor i l'HCCSs utilitzen **certificats per acreditar-se i SSL**.
- 5 i 6 - El Visor consulta al SIDX i aquest li serveix els documents clínics demanats. El flux d'informació en les consultes del SIDX es mostra en el cas d'ús 3.
- 7 - El Visor passa la resposta cap l'HCCSs.
- 8 - L'HCCSs **registra la resposta en un log**.
- 9 - L'HCCSs passa la mateixa resposta cap el navegador web del ciutadà utilitzant SSL.

## 2.5 Consultes del SIDX als repositoris de dades clíniques.



El flux d'informació es desenvolupa d'aquesta forma.

Els passos A corresponen a un accés local al repositori central i els B a l'accés a un repositori distribuït.

A1 - El **SIDX** li demana al repositori central la dada clínica que cal consultar. Com que ambdós estan dins de la xarxa interna securitzada, no els cal un filtre addicional de seguretat.

A2 - El **repositori central** li retorna al SIDX la dada clínica.

B1 - El SIDX li demana al HCCSs que vagi a consultar un document clínic a un servidor de publicació en concret. SIDX i HCCSs s'acrediten mitjançant **certificats digitals**.

B2 - L'HCCSs **registra** la petició en un **log**.

B3 - L'HCCSs li demana un document en concret al servidor de publicació de l'institució assistencial (hi ha tres mètodes: **SOAP, XML, URL**).

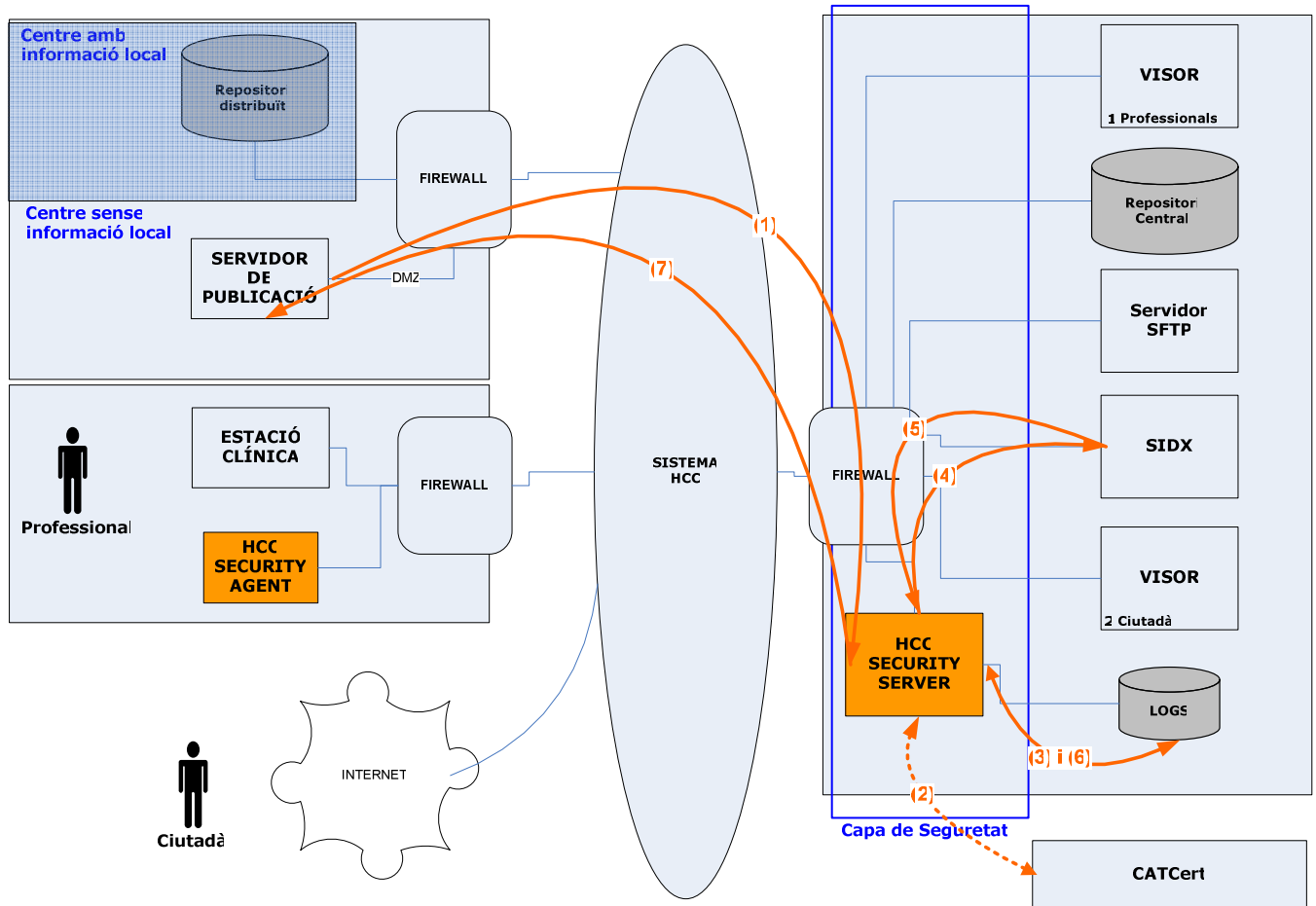
B4 - El servidor de publicació recupera el document consultant el seu repositori distribuït.

B5 - El servidor de publicació retorna al HCCSs el document demanat, emprant el mètode utilitzat en la petició.

B6 - L'HCCSs **registra** la resposta en un **log**.

B7 - L'HCCSs tramet el document demanat cap el SIDX.

## 2.6 Cas d'ús 4: Publicació de documents clínics mitjançant Web Services.



El flux d'informació es desenvolupa en els següents passos:

1 - El **servidor de publicació** envia una petició d'actualització de dades de l'índex cap l'**HCCSs**. La comunicació es realitza amb **web services i SSL**. L'actualització de dades pot ser:

- Indicar una referència ("punter") d'un document publicat en el seu repositori distribuït propi.
- Enviament d'un document cap el repositori central i la seva referència.

2 - L'HCCSs valida l'identitat del servidor de publicació a través del seu **certificat digital**.

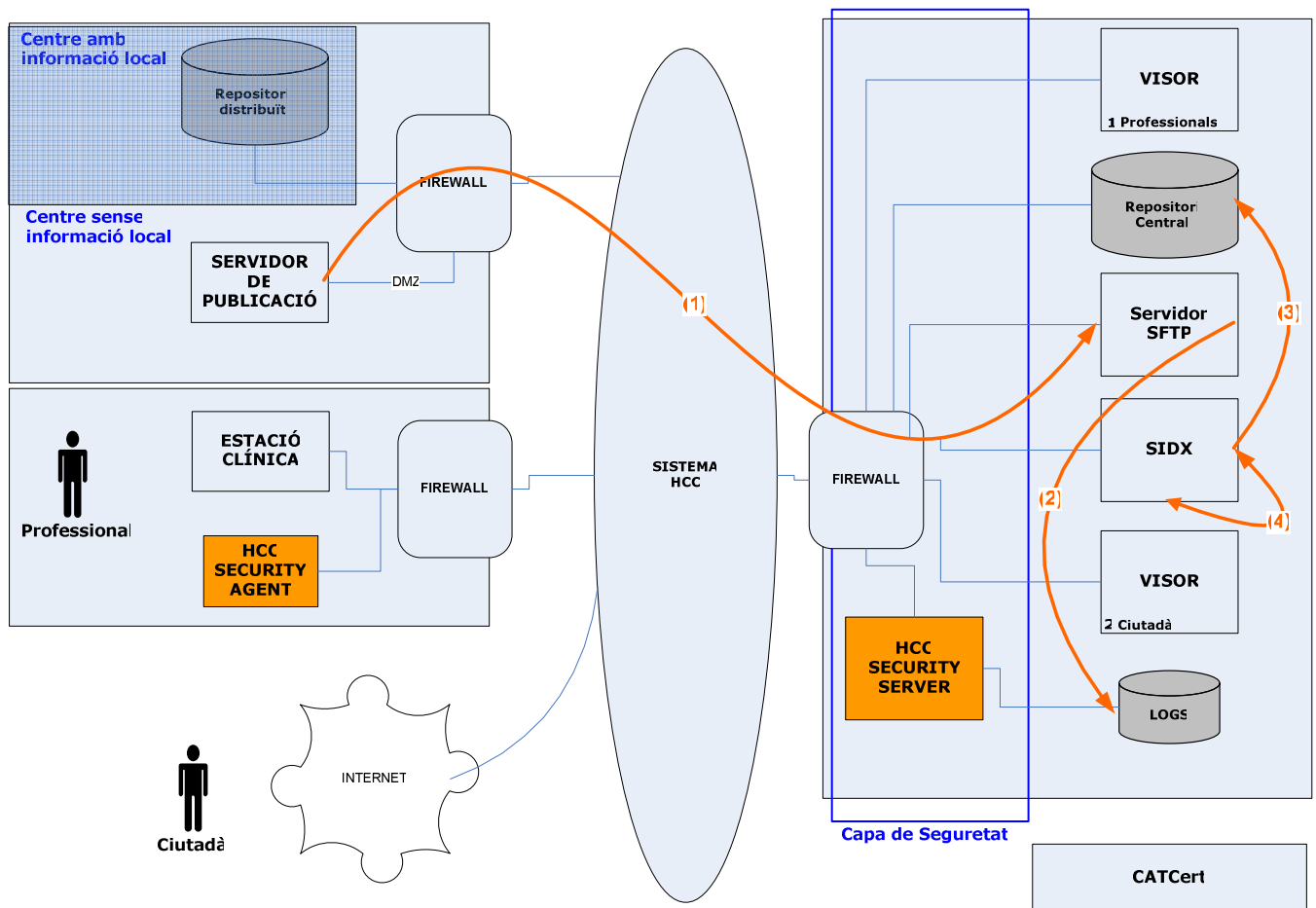
3 - L'HCCSs registra l'accés amb una **traça de log**.

4 i 5 - A través del HCCSs, el servidor de publicació actualitza el **SIDX** sigui només amb la referència del document o bé amb la referència i el propi document.

6 - L'HCCSs registra la resposta amb una **traça de log**.

7 - A través del HCCSs se li retorna resposta al servidor de publicació sobre l'operació completada.

## 2.7 Cas d'ús 5: Publicació de documents clínics mitjançant SFTP.



Aquest flux correspon únicament als casos en que l'entitat assistencial no custodia documents en repositori propi.

El flux d'informació es desenvolupa en els següents passos:

- 1 - El servidor de publicació fa l'enviament del document clínic al servidor de **SFTP**, utilitzant **SSH**. El servidor SFTP deixa el document en un directori.
- 2 - El servidor SFTP deixa una **traça completa** de l'accés realitzat.
- 3 - El component SIDX disposa d'un procés periòdic que diposita aquest document en el **repositori central**.
- 4 - Aquest procés també actualitza els índexs del component SIDX.

## **2.8 Glossari de termes.**

**SSL:** Secure Sockets Layer es un protocol criptogràfic que proporciona comunicacions segures en Internet.

**SFTP:** Es un programa que utilitza Secure Shell per transferir fitxers.

**Certificats Digitals:** Es un document digital mitjançant el qual un tercer fiable (una autoritat de certificació) garanteix la identitat d'un subjecte o entitat.

**XML:** Extended Markup Language.

**HTTPS:** Versió segura del protocol HTTP.

**Tallafocs:** Element de maquinari que controla les comunicacions d'una xarxa.