CATCert

Agència Catalana de Certificació

La identificació d'usuaris

3a Jornada sobre TV de Servei: La televisió personal

Jordi Masias Muntada

AOC Administració Oberta de Catalunya

Generalitat de Catalunya

Consorci de governs locals per a la societat de la informació

CATCert
Agència Catalana de Certificació

Contingut

- Introducció: La Tramitació Telemàtica
- Necessitats de Seguretat en Tramitació Telemàtica
- Mecanismes d'identificació i signatura electrònica
- Internet i la signatura electrònica
- La identitat digital i la signatura electrònica a la TDT.

CATCert
Agència Catalana de Certificació

Introducció: La Tramitació Telemàtica: Identitat

Metodes d'identificació:

_ Visual.

_ Per mitjà d'informació coneguda per les parts: "Santo y seña", usuaris i contrasenyes, etc.

_ Per mitjà d'un certificat: Carnet, DNI, Document, Certificat digital, etc.

CATCert
Agència Catalana de Certificació

Introducció: La Tramitació Telemàtica: Signatura

La signatura manuscrita ha estat històricament i és el mètode més emprat per deixar evidència de l'esdeveniment dels actes que composen els procediments administratius.

Gràcies als avanços en tecnologies de la informació, els tràmits administratius poden ser agilitzats i els documents en suport paper poden ser substituïts per documents electrònics més fàcilment accessibles, gestionables i, fins hi tot, automàticament interpretables.

CATCert
Agència Catalana de Certificació

Necessitats de Seguretat en Tramitació Telemàtica

El nou medi necessitarà de noves mesures que assegurin la identitat, autenticitat, integritat, no repudi i confidencialitat de les transaccions.

Identitat: Seran necessaris mecanismes per assegurar la identitat del l'origen o autoria dels documents electrònics.

Integritat: Es voldrà assegurar que els documents no son modificats després de la seva emissió.

Autenticitat: Un cop emès un document, i havent-se assegurat la seva autoria i integritat, es voldrà que el seu emissor no s'en pugui deslligar dels compromisos.

Confidencialitat: En alguns casos, també serà necessari que els documents només puguin ser accedits pels seus destinataris.

CATCert
Agència Catalana de Certificació

Mecanismes d'identificació

La Llei 59/2003 de Signatura Electrònica, que regula la signatura electrònica, la seva eficiència jurídica i la prestació de serveis de certificació, agrupa els mecanismes existents d'identificació en:

Signatura ordinària: és el conjunt de dades en format electrònic, consignats amb d'altres o associats amb ells, que poden ser utilitzats com a mitjà d'identificació del signatari.

Signatura avançada: és la que permet identificar al signatari i detectar qualsevol canvi ulterior de les dades signades, que està vinculada al signatari de manera única i a les dades a que es refereix i que ha estat creada por mitjans que el signatari pot mantenir sota el seu control exclusiu.

Signatura reconeguda: és la signatura electrònica avançada basada en un certificat reconegut i generada mitjançant un dispositiu segur de creació de signatura.

CATCert
Agència Catalana de Certificació

Mecanismes d'identificació i signatura electrònica

Alguns exemples de mecanismes d'identificació són:

Signatura ordinària: **Usuari / Paraula de pas**

Signatura avançada: **Certificat digital en programari**

Signatura reconeguda: **Certificat digital en targeta intel·ligent**

La **signatura reconeguda** és la única que garanteix autenticitat, integr
i no repudi. **És l'únic tipus de signatura electrònica equiparada legalment a la signatura manuscrita**.

CATCert
Agència Catalana de Certificació

Internet i la signatura electrònica

Aplicació de Signatura

Validador

Identificació

Xifrat de les comunicacions

SSL

SSL

Client

Internet

Servidor

CATCert
Agència Catalana de Certificació

La identitat digital i la signatura electrònica a la TDT

Receptor TDT

ADSL

Aplicació d'interacció amb l'administració

CATCert
Agència Catalana de Certificació

La identitat digital i la signatura electrònica a la TDT

Multimedia Home Platform (MHP) és un *middleware* que defineix una plataforma comú pel desenvolupament d'aplicacions interactives per televisió digital, de forma independent tant del proveidor de serveis interactius com del receptor de televisió utilitzat.

A partir de la seva versió 1.1.3, MHP garanteix la seguretat en totes les àrees de desenvolupament mitjançant l'ús de tècniques com la signatura digital, els certificats digitals, algorismes resum i de clau pública.

CATCert
Agència Catalana de Certificació

La identitat digital i la signatura electrònica a la TDT

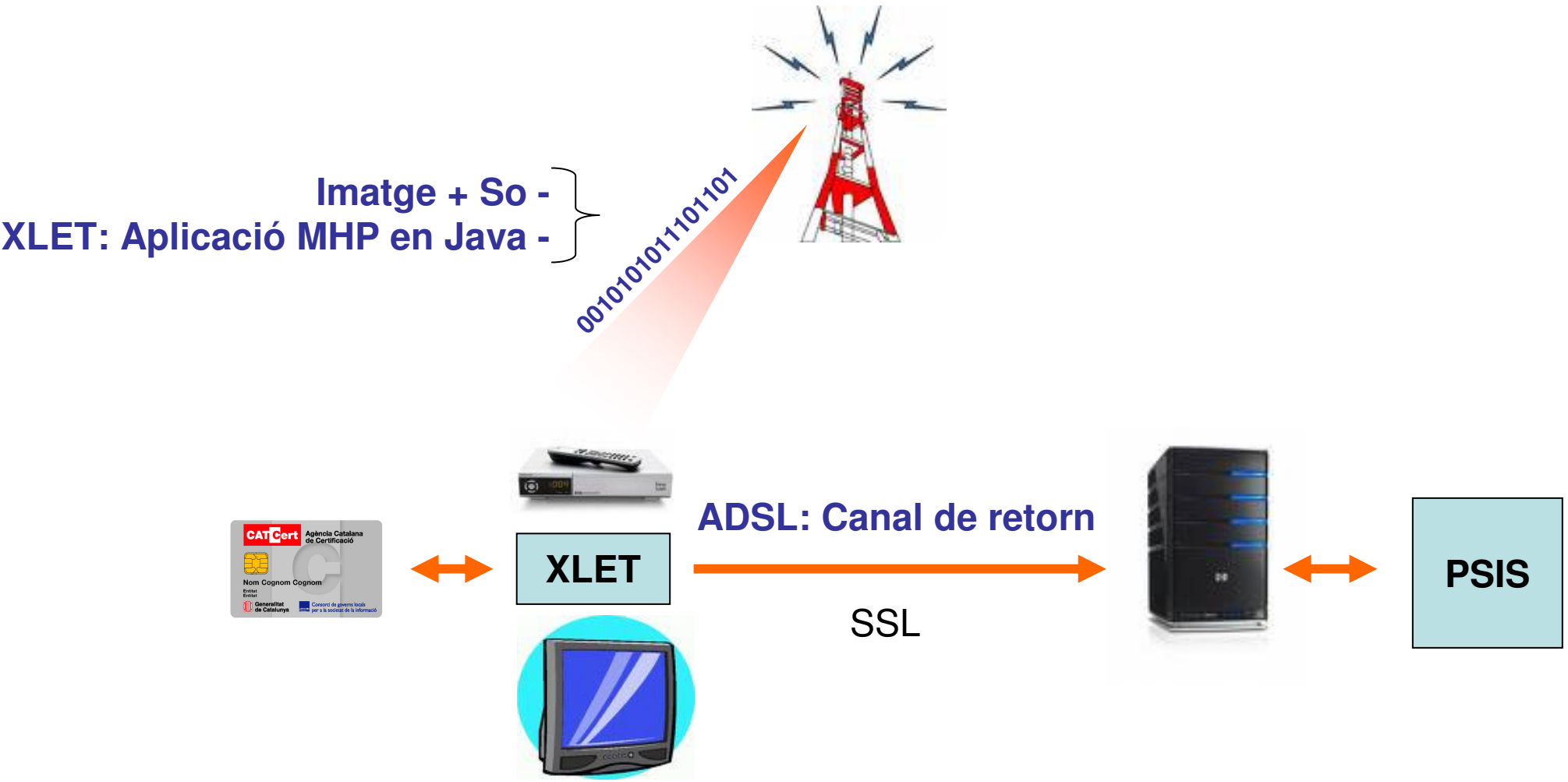
CATCert està participant, amb les empreses Activa Multimedia i C3PO, en el desenvolupament d'un prototipus d'autenticació i SE d'usuaris mitjançant TDT i on un dels primers usos sigui l'accés a tràmits administratius.

El prototipus consisteix en el desenvolupament d'un XLET capaç de:

- Llegir targetes intel·ligents STARCOS 2.3 (Accés certificat digital) i en una segona fase el DNIe
- Realitzar l'autenticació de la citada targeta (Demanar PIN)
- Cridar la funció de signatura de la targeta
- Implementar la part client d'una autenticació SSL amb certificat digital en el canal de retorn

Agència Catalana de Certificació

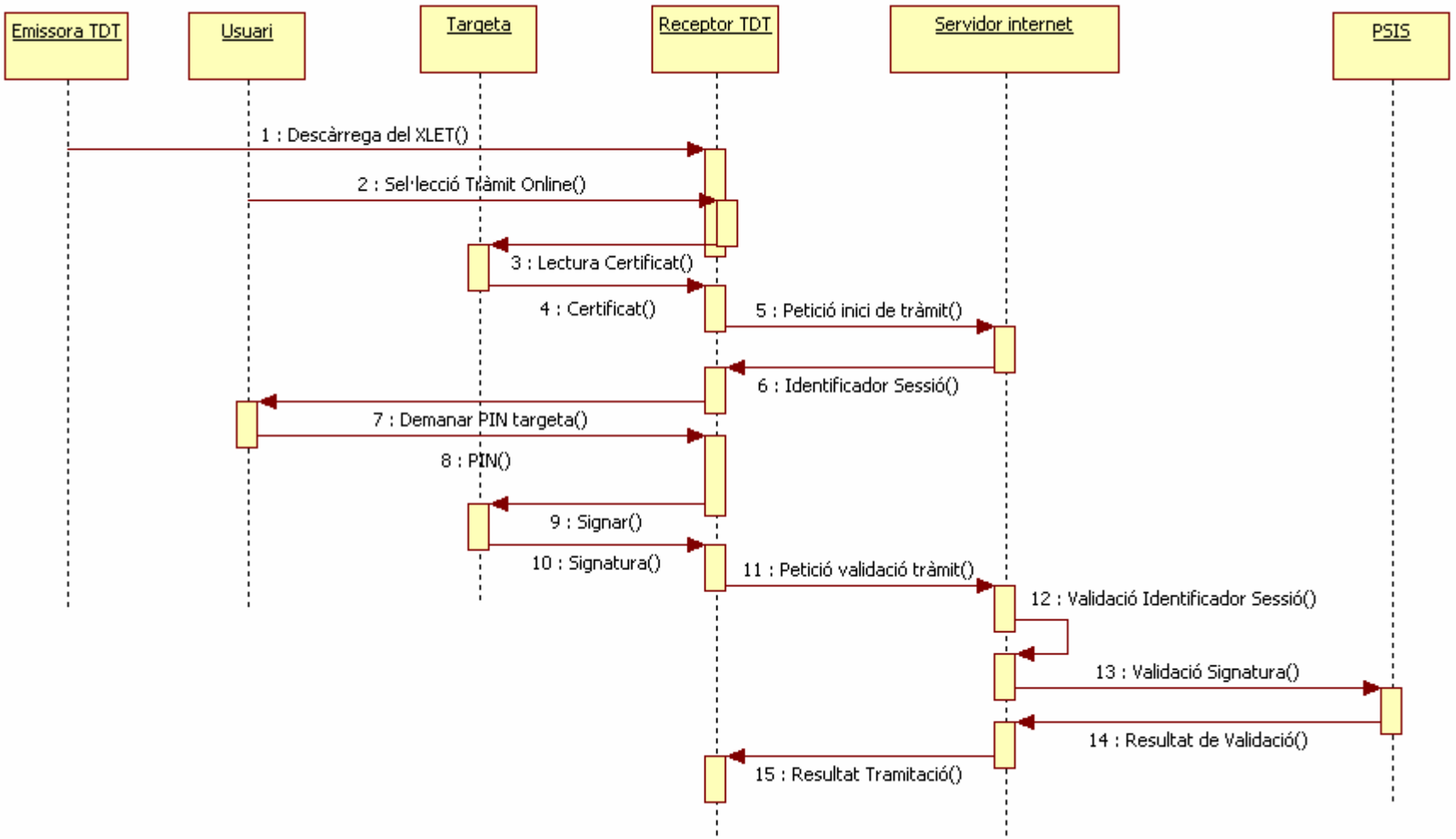
La identitat digital i la signatura electrònica a la TDT



CATCert
Agència Catalana de Certificació

La identitat digital i la signatura electrònica a la TDT

Diagrama de seqüència



CATCert
Agència Catalana de Certificació

La identitat digital i la signatura electrònica a la TDT

En un futur, si el prototipus té èxit, *Atenció Ciutadana* està estudiant oferir alguna aplicació real de cara al 2008. La via estudiada més probable consistiria en la connexió amb les bases de dades de CATSalut utilitzant un Xlet. D'aquesta manera, prèvia autenticació, es permetria consultar els horaris dels metges de capçalera per després demanar hora de consulta.

CATCert
Agència Catalana de Certificació

La identitat digital i la signatura electrònica a la TDT

El projecte està en estat inicial, tot i que tenint en compte que el futur de la identificació digital i de la signatura electrònica passa per la utilització de certificats digitals, pensem que el projecte d''autenticació d'usuaris a la TDT, utilitzant certificats digitals des de l'estàndard MHP és el futur.

Cal continuar treballant en el desenvolupament d'aquesta tecnologia per tal que l'accés a les administracions mitjançant la Televisió Digital Terrestre sigui la gran alternativa per a tots aquells ciutadans que no disposen d'ordinador o que els hi és complexa l'accés a internet.

CATCert
Agència Catalana de Certificació

Moltes gràcies

Més informació:

Jordi Masias Muntada

jmasias@catcert.net