Consorci
Administració Oberta
de Catalunya

Guia d'usuari per a la solució al problema que presenten les darreres versions d'Adobe (a partir de la 9) en la signatura amb targeta de 2048 bits i Windows XP.

Març 2013

Generalitat de Catalunya

Data: 14/03/2013

Consorci de governs locals per a la societat de la informació

Consorci
Administració Oberta
de Catalunya

Índex

Consorci
Administració Oberta
de Catalunya

1. Introducció

En aquesta guia s'indica una solució alternativa al problema que presenta la signatura de PDF, amb certificats digitals en targeta de 2048 bits, amb les versions 9 i 10 d'Adobe i Sistema operatiu Windows XP.

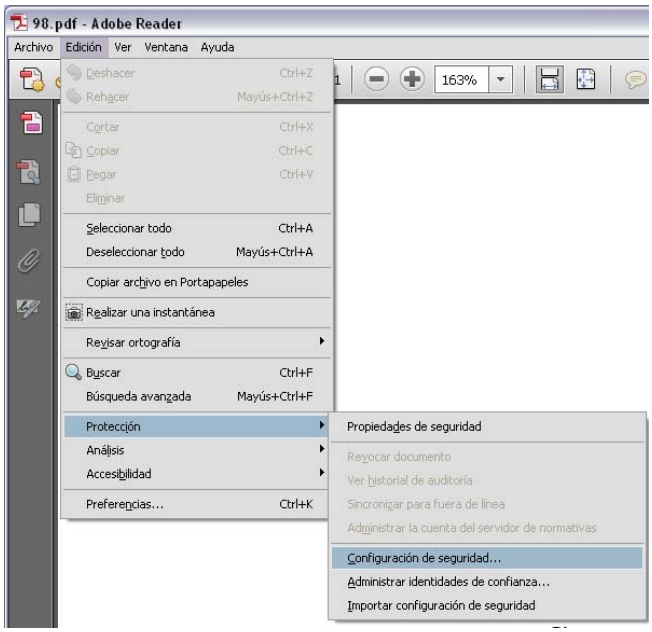
2. Configuració

Amb Windows XP existeix un problema al signar amb sha256 documents PDF amb Adobe 9 i 10 amb targetes de 2048 bits. A sota es detalla la casuística.

Amb Windows XP (Adobe 9 i superiors) signa per defecte amb SHA256 i el certificat de la targeta l'agafa mitjançant el CSP de Windows que és on hi ha el problema. Aleshores, el workaround per fer funcionar la signatura SHA256 amb Windows XP i Adobes 9 i superiors, és habilitar la configuració del dispositiu criptogràfic i així que la selecció del certificat sigui la de la targeta mateix i no del magatzem de certificats de Windows.

A continuació es detallen els passos per configurar el dispositiu criptogràfic en l'Adobe Reader 10:

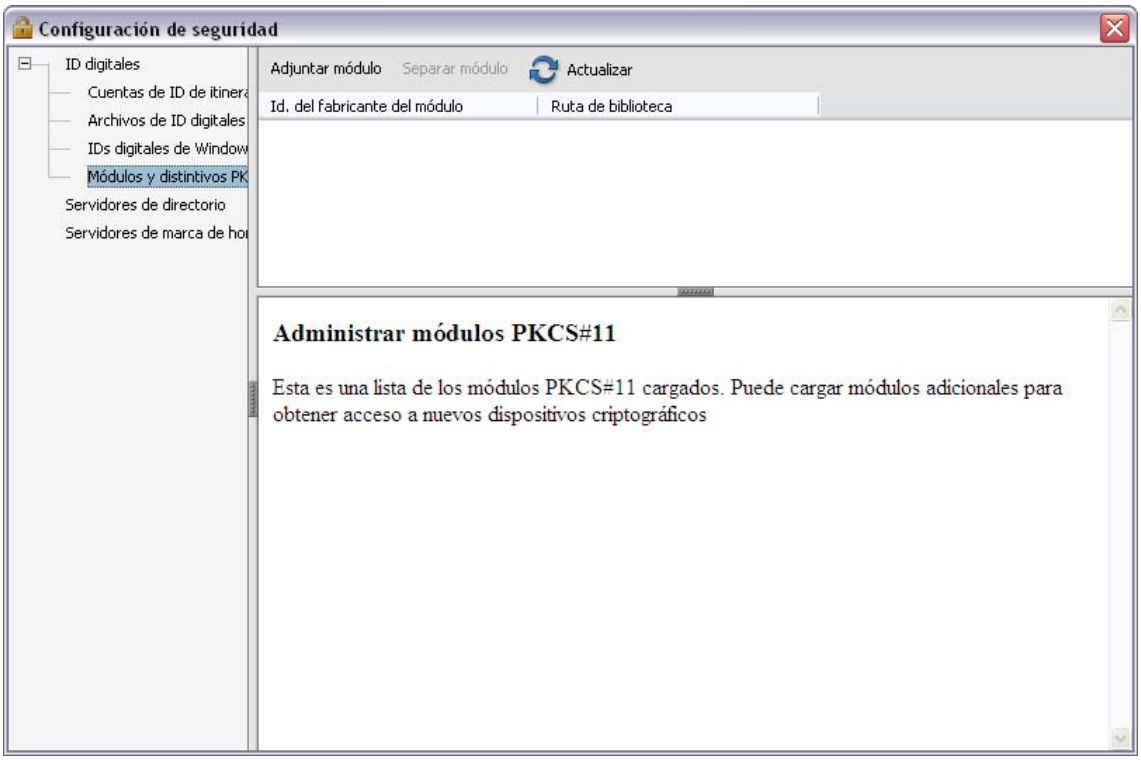
1. Edició --> Protecció --> Configuració de Seguretat

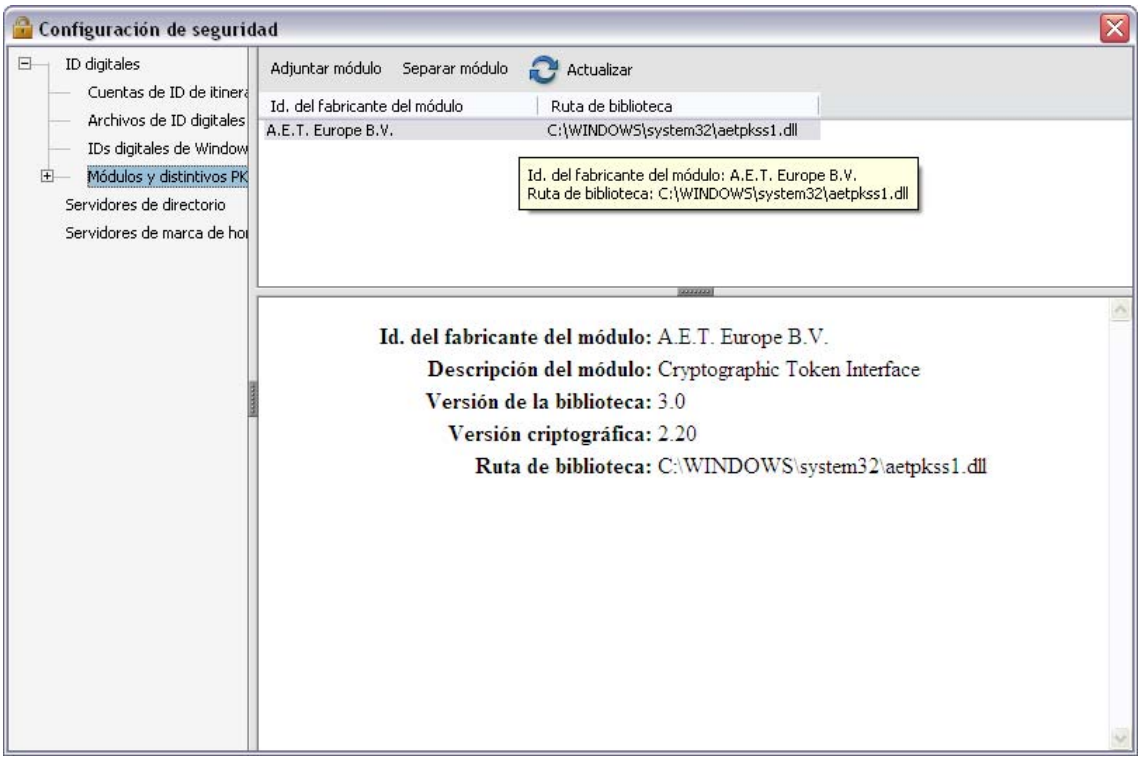


2. IDs Digitals --> Móduls i distintius PKCS#11, no existeix cap opció per realitzar (estan deshabilitades les opcions), per tant cal posar-se momentàniament en una altre opció (per exemple, IDs digitals de Windows) i tornar a Móduls i distintius PKCS#11
3. Ara es mostra un avís en el qual s'ha de marcar la següent opció:
 - Obrir sempre amb el mode protegit desactivat --> Acceptar
4. Reiniciar l'Adobe Reader 10

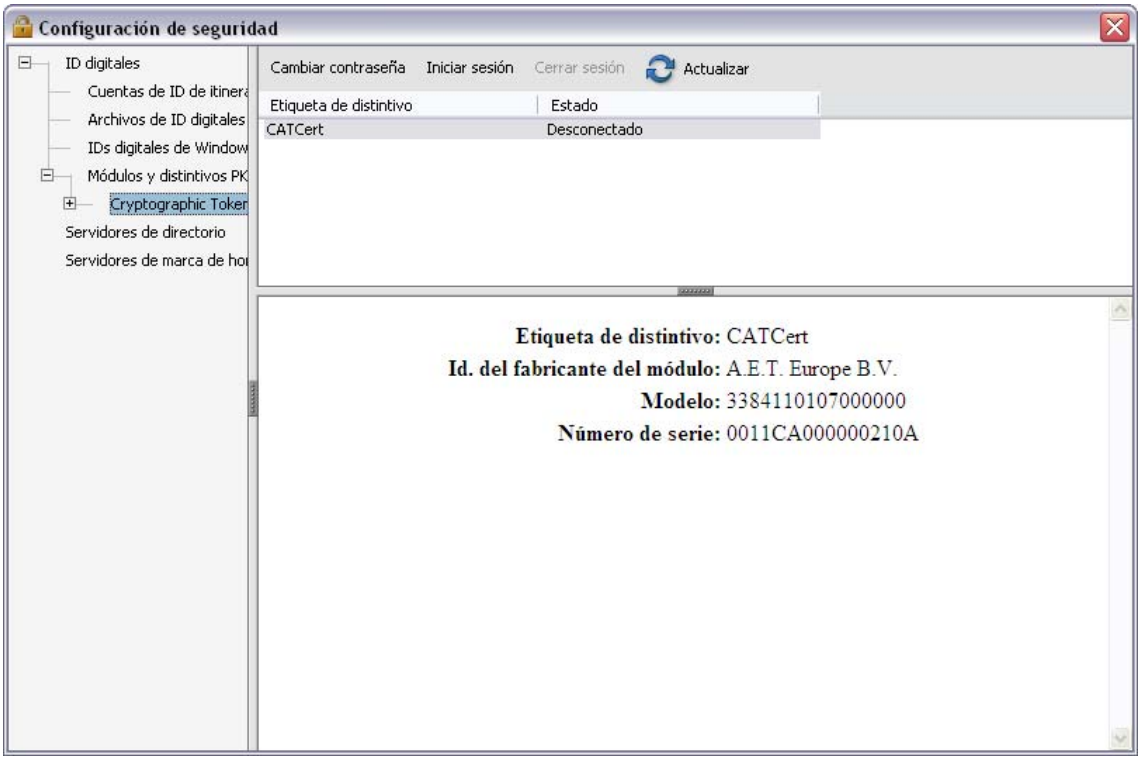
5. Edició --> Protecció --> Configuració de Seguretat

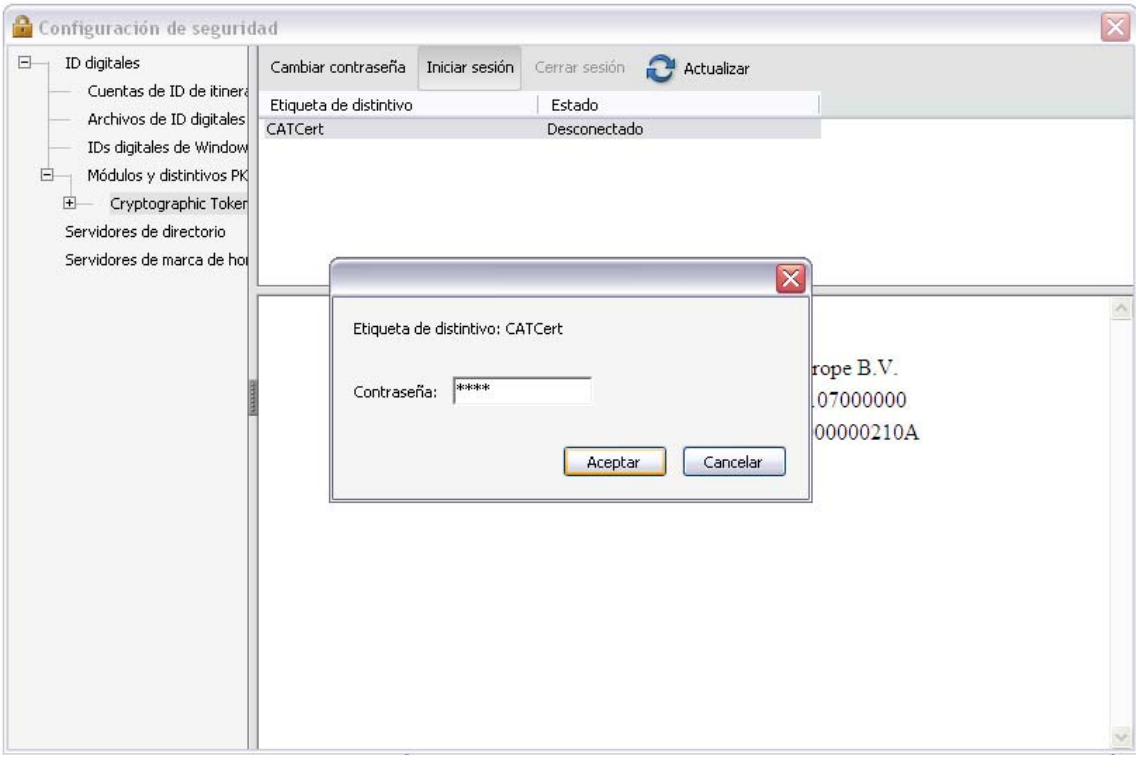
6. IDs Digitals --> Móduls i distintius PKCS#11. Ara ja sí que existeixen varies possibilitats de configuració.
7. Adjuntar Mòdul --> Seleccionar el fitxer de la ruta C:/Windows/System32/aetpkss1.dll





8. IDs Digitals --> Móduls i distintius PKCS#11 --> Cryptographic Token Interface
9. Iniciar sessió --> Inserir PIN

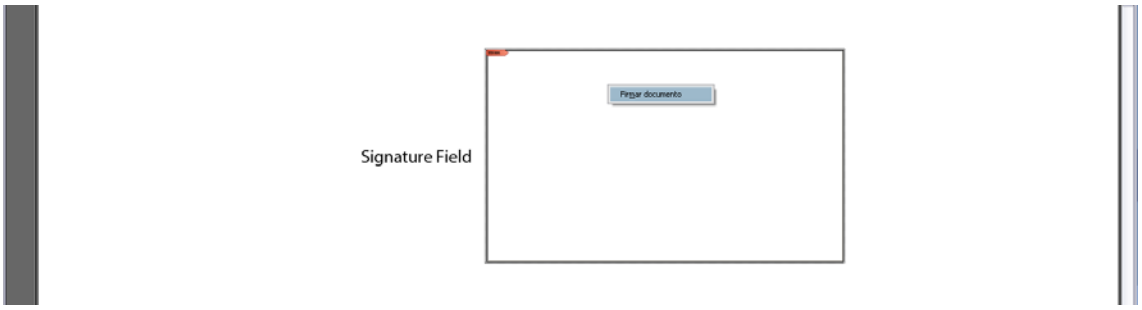


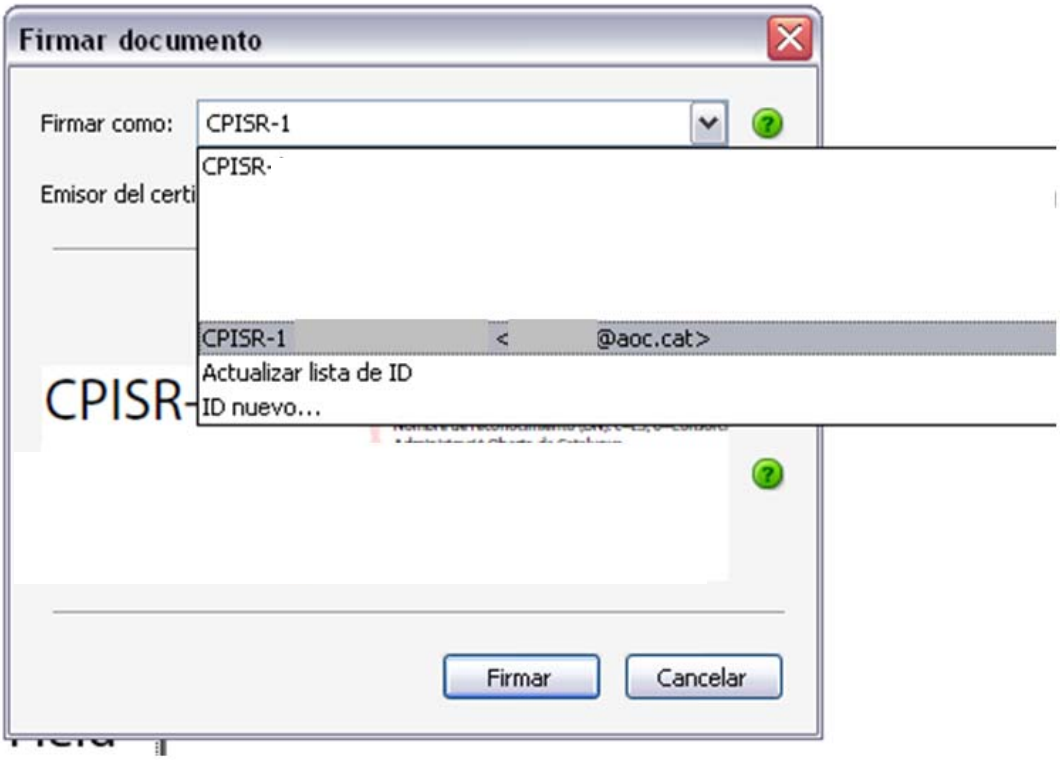


Ara ja es pot realitzar la signatura correctament sempre i quan es selccioni el certificat directament de la targeta: En el desplegable de selecció de certificat per signar, seleccionar el CPISR-1 amb el correu electrònic al final, ja que el CPISR-1 sense correu electrònic és el certificat del magatzem de Windows i aleshores es reproduiria el problema inicial.
Resumint, per exemple si en el desplegable apareix:

- CPISR-1 Toni Prova Prova
- CPISR-1 Toni Prova Prova toni@prova.cat

Seleccionar la segona opció.




Firmar documento
Firmar como:
CPISR-1
CPISR-
Emisor del certi
CPISR-1 < @aoc.cat>
Actualizar lista de ID
ID nuevo...
CPISR-
Firmar
Cancelar