



**Agència Catalana  
de Certificació**

## Nivells de seguretat del sistema de classificació

Servei de Classificació  
Àrea d'Assessorament i Recerca



Consorci  
Administració Oberta  
de Catalunya



LOCALRET

## Orientació de la classificació

La classificació esta basada en nivells. A cada servei prestat per un proveïdor de serveis d'identificació i autenticació digital que desitgi ser classificat se li atorgarà un nivell en funció de puntuacions que vagi obtenint segons els diferents criteris de classificació (elements d'avaluació).

Aquest sistema de puntuacions està adequadament justificat i permet emetre judicis objectius i raonats sobre el nivell atorgat a un determinat sistema.

Cada nivell representa evidències més idònies que les del nivell anterior per a ser prova en si mateixes.

## Descripció dels nivells

Els nivells es defineixen partint fonamentalment dels següents principis:

- **Garanties creixents o completa creixent:** partint d'un nivell de garantia com evidència molt baix o nul, els següents nivells descriuen escenaris amb garanties creixents, tant si aquestes s'aconsegueixen mitjançant solucions tècniques, de procediment o mitjançant contractes i assumpció de responsabilitats. Es consideren garanties creixents en el sentit d'evidències de major qualitat o més completes en si mateixes. Un determinat nivell compleix els requisits de l'anterior i afegeix els seus propis per a augmentar la completa de l'evidència.
- **Independència tecnològica:** els nivells es definiran de forma conceptual, amb independència de les solucions tècniques que es requereixin per a complir les garanties establertes a cada nivell.
- **Adequació a la legislació:** els nivells s'equipararan amb els termes legals equivalents. L'equivalència ve donada per la definició del terme legal i els requisits o garanties que aquesta definició requereix.



Agència Catalana  
de Certificació

Els nivells definits són:

### **Nivell 0. Sense evidència (identificació al-legada)**

Aquest nivell aglutina tots els serveis d'identificació senzilla, oferint una definició comuna sota la qual agrupar tots els serveis que no compleixen els requisits dels nivells superiors.

En aquest nivell estan inclosos tots els serveis d'identificació i autenticació que:

- No permeten comprovar la identitat de l'usuari que vol accedir al sistema. Els motius poden ser tècnics o de procediment. Alguns d'ells són:
  - Procés de registre inadequat, que no permet assegurar la identitat.
  - No existeixen o no s'ofereixen mecanismes per a comprovar tècnicament la validesa de la credencial presentada.
- No compleixen els requisits necessaris per a aconseguir un nivell superior.



Agència Catalana  
de Certificació

## **Nivell 1. Evidència d'entitat**

L'objectiu d'aquest nivell és agrupar tots aquells serveis que garanteixin la identificació i autenticació dels usuaris d'un sistema.

Aquest nivell es caracteritza perquè afegeix l'existència de mecanismes (tant tècnics, com de procediment) per a identificar l'usuari que accedeix al sistema i comprovar la seva identitat.

Els serveis que aspirin a aconseguir aquest nivell ha de garantir l'autenticació de les entitats. Això implica la utilització de, com a mínim, mecanismes d'autenticació estàtica.

## **Nivell 2. Evidència d'origen de dades**

L'objectiu d'aquest nivell és aglutinar els serveis d'identificació i autenticació que vinculin les dades electròniques amb la identitat (comprovable) de l'entitat d'origen - entenent com entitat origen la que es posa a disposició d'una altra o altres entitats o aplicacions dintre d'un sistema informàtic, ja sigui com autor de les dades, testimoni o com declarant de voluntat.

Aquest nivell es caracteritza per garantir tant la identificació i autenticació de les entitats participants en una comunicació o transacció com l'autenticació de l'origen de les dades intercanviades en aquesta comunicació o transacció.

Afegeix, doncs, respecte a l'anterior nivell la necessitat d'utilitzar mecanismes per a garantir l'origen de les dades electròniques. Per aconseguir això és necessari almenys utilitzar mecanismes amb codis d'autenticació de missatges.



Agència Catalana  
de Certificació

### **Nivell 3. Evidència d'autenticitat documental**

L'objectiu d'aquest nivell és concentrar tots els serveis d'identificació i autenticació amb equivalència legal amb la signatura electrònica avançada.

Els serveis classificats en aquest nivell garanteixen l'autenticitat documental electrònica.

Per a complir els requisits d'autenticitat documental electrònica es necessiten mecanismes per garantir la integritat de les dades electròniques així com per vincular unes dades a una determinada entitat origen dels mateixos.

A la definició actual de signatura electrònica avançada de la Ley 59/2003 de firma electrònica, apareix l'equivalència entre aquesta definició - de tipus legal - i la definició del present nivell. És a dir, els serveis de signatura electrònica avançada compleixen els requisits d'aquest nivell i són susceptibles d'estar classificats en ell.

## **Nivell 4. Evidència de signatura electrònica**

L'objectiu d'aquest nivell és agrupar els serveis de signatura amb equivalència a la signatura manual, és a dir, que l'evidència que generen aquests serveis sigui equivalent a una signatura manual.

Aquest nivell requereix que el mecanisme d'autenticació s'adhereixi a la definició de signatura electrònica reconeguda de la Ley 59/2003 de firma electrònica; o bé un conjunt de mecanismes tècnics i de procediment que ofereixin les mateixes garanties que exigeix la legislació pertinent per a aconseguir l'equivalència directa amb la signatura manual.



Agència Catalana  
de Certificació

## **Nivell 5. Evidència completa de signatura electrònica**

Aquest nivell tracta d'agrupar els serveis que generen evidències pràcticament autocontingudes, que amb molt poques o cap consulta addicional a proveïdors de serveis de certificació serveixin com prova, és a dir, que demostrin que el signant va actuar de pròpia voluntat.

Aquest nivell es caracteritza perquè l'evidència, a més d'ésser de signatura, aporta tots els elements necessaris per a la verificació de la mateixa o referències als mateixos o un informe d'una Autoritat de Validació, degudament autènticat i associat a la resta de l'evidència. Es fa necessari en aquest cas que hi hagi algun tipus de referència temporal en l'evidència generada, doncs d'altra manera, les dades per a la verificació de la signatura no serien útils si no se sap quan es va generar la signatura o quan la va donar per bona el verificador.

Es tracta, doncs, d'un nivell l'evidència autocontinguda - en el millor dels casos.

## **Nivell 6. Evidència de llarga durada de signatura electrònica**

L'objectiu d'aquest nivell és agrupar als proveïdors de serveis d'identificació i autenticació digital que donen les garanties suficients per a generar evidències de signatura arxivada.

Els serveis de nivell 6 són aquells que poden generar evidències que, a més de ser autocontingudes (com ES-X Long de ETSI 101-733) són perdurables en el temps; és a dir, no poden ser falsificades (raonablement) a causa de millores en algorismes o tècniques de criptoanàlisi o a l'augment de la capacitat de càlcul dels ordinadors. Pel fet que passi el temps no té perquè perdre validesa una signatura electrònica que en el passat era vàlida.

Per evitar aquest problema es creen les denominades dades de validació d'arxiu (*Archive Validation Data*.) És una tècnica basada a aplicar un segellat de temps a les dades de validació, les dades de certificats i revocació i la signatura electrònica