Estàndard tècnic de signatura electrònica ordinària d'acte negocial de membre de la comunitat universitària

Text aprovat pel Comitè de Direcció Executiu el 22 de desembre de 2014, actuant per delegació del Consell de Govern

Universitat Oberta de Catalunya

SUMARI

1. Continguts generals de l'estàndard tècnic de signatura electrònica

Identificació textual	Estàndard tècnic de signatura electrònica ordinària d'acte negocial de membre de la comunitat universitària.
Identificació numèrica	1.3.6.1.4.1.43653.1.5.1.1.2
Data d'emissió	[Cal indicar-ne la data d'emissió.]
Identificador de l'emissor	Comitè de Direcció Executiu, actuant per delegació del Consell de Govern d'acord amb allò establert en l'article 13.2 de les NOF (Acord GOV/140/2010, de 3 d'agost), l'article 4 del Reglament del Consell de Govern i l'Acord de Consell de Govern de 15 de juliol de 2013.
Àmbit d'aplicació de l'estàndard	Aquest estàndard resulta aplicable a la generació i validació de les signatures ordinàries dels actes negocials que hagin portat a terme els membres de la comunitat universitària.

2. Període autoritzat de signatura

Inici del període autoritzat de signatura	Des del moment de l'aprovació d'aquest document.
Final del període autoritzat de signatura	Aquest estàndard tècnic té una durada indefinida.

3. Normes generals

3.1 Normes de contingut de la signatura

3.1.1. Creació de la signatura

La creació de la signatura electrònica es fa mitjançant l'ús de la paraula de pas del membre de la comunitat universitària, assignada per la UOC.

3.1.2. Verificació inicial de la signatura

No és aplicable, atès que la verificació de la paraula de pas sempre és definitiva.

3.1.3. Verificació definitiva de la signatura

La verificació definitiva de la paraula de pas es porta a terme emprant el sistema corporatiu d'identificació i autenticació (directori), que manté l'evidència permanent de les operacions d'autenticació.

Un cop s'ha verificat la paraula de pas, es genera l'evidència electrònica de la signatura generada, que es compon d'un registre en suport electrònic, en base de dades, amb les informacions següents:

- Identificació de la signatura electrònica ordinària d'autorització del servei per part del signatari (*autoritzacioServei*)
- Identificador únic de la persona, assignat per la UOC (*IDP*)
- Nom del signatari (*nom*)
- Primer cognom del signatari (*cognom1*)
- Segon cognom del signatari, quan escaigui (*cognom2*)
- Document d'identitat del signatari (*idDocument*)
- Identificació del servei i del tràmit en relació amb el qual es genera la signatura electrònica ordinària (*idTipusServei*, *idOrigenServei*)
- Entitat gestora del servei (*entitatGestora*)
- Data de creació del registre evidencial (*dataCreacio*)
- Identificació de la sessió del Campus Virtual (*sessioCV*)
- IP de connexió del signatari (*ipConnexio*)
- Identificació del procés i del període temporal aplicable a l'autorització conferida pel signatari, d'acord amb el servei o tràmit corresponent (*idProcesOrigen*, *idPeriodeOrigen*)
- Quatre camps per a informacions addicionals, d'ús opcional (*infoExtra1*, *infoExtra2*, *infoExtra3*, *infoExtra4*)
- Contingut del document signat (*contingut*), codificat en base64

Sobre la manifestació d'aquest registre en format XML es genera una signatura separada XAdES-T, que s'incorpora al registre.

3.1.4. Manteniment evidencial de la signatura

El manteniment evidencial del registre descrit en la secció anterior es porta a terme mitjançant la generació d'un codi HMAC sobre la signatura electrònica del registre i l'HMAC del registre immediatament anterior, de manera que es crea una cadena de registres que garanteix que no es pot alterar la seqüència ordenada dels registres, i tampoc no se'n pot impedir l'addició o l'eliminació.

La clau emprada per a generar el codi HMAC se selecciona d'una llista, a partir de l'aplicació d'una funció modular sobre l'identificador únic del signatari.

3.2. Normes de segellament de data i hora de la signatura

3.2.1. Normes sobre estampació de segells de data i hora

3.2.1.1. Verificació definitiva de la signatura electrònica

Període cautelar aplicable abans de verificar la signatura	Les signatures se segellen immediatament.
Termini màxim per a segellar la signatura electrònica	Les signatures se segellen immediatament.

3.2.1.2. Manteniment evidencial de la signatura electrònica

Termini màxim per a tornar a segellar la signatura electrònica	Atès que la modificació dels registres afectaria la integritat d'aquesta cadena, no es tornen a segellar les signatures electròniques.

3.2.2. Normes de processament de la cadena de certificació

Definició del punt fiable	Certificats arrel de les entitats de certificació admeses per la

de certificació	Universitat Oberta de Catalunya.
Limitació de la longitud màxima de la cadena de certificació	No s'estableix cap limitació a la longitud màxima de la cadena de certificació.
Conjunt inicialment acceptable d'estàndards de certificació	Model de certificat de segellament de data i hora (`1.3.6.1.4.1.43653.1.3.1.8.1`).
Definició de condicions respecte als noms emprats als certificats	No s'estableix cap limitació en relació amb l'ús dels noms inclosos en els certificats. En tot cas, la validació s'ha de restringir a la cadena de certificació jeràrquica. No es podran establir relacions de certificació encreuada ni altres models de confiança fora del control de la Universitat Oberta de Catalunya.
Definició de condicions addicionals respecte al tractament de les normatives de certificació en el processament de la cadena de certificació	Es permet de forma expressa l'establiment d'equivalències de normatives de certificació, per a admetre els certificats dels usuaris de les entitats de certificació admeses que hagin estat declarades equivalents amb els anteriors OID.

3.2.3. Normes de comprovació d'informacions de revocació de certificats

Tipus de certificats sobre els quals es portaran a terme les comprovacions	Cal comprovar la vigència del certificat de signatari i de tots els certificats de la cadena de certificació corresponent, a excepció del punt fiable.
Requisit de comprovació dels certificats	La comprovació dels certificats es farà preferentment amb OCSP i, en cas que aquest protocol no estigui disponible, mitjançant consulta de la CRL més recent.

3.3. Normes d'ús d'algorismes

3.3.1. Algorismes emprats pel signatari

Llista d'algorismes admesos	RSA

RSA:

Identificació de l'algorisme	SHA512 amb RSA
Longitud mínima de la clau	2048
Altres paràmetres	No s'estableixen.

3.3.2. Algorismes emprats per als certificats del signatari

Llista d'algorismes admesos	RSA

RSA:

Identificació de l'algorisme	SHA1 amb RSA
	SHA256 amb RSA
	SHA384 amb RSA
	SHA512 amb RSA
Longitud mínima de la clau	1024
Altres paràmetres	No s'estableixen.

3.3.3. Algorismes emprats per als certificats de l'entitat de segellament de data i hora

Llista d'algorismes admesos	RSA

RSA:

Identificació de l'algorisme	SHA512 amb RSA
Longitud mínima de la clau	2048
Altres paràmetres	No s'estableixen.

3.3.4. Algorismes emprats per als certificats de l'entitat de certificació

Llista d'algorismes admesos	RSA
RSA:	
Identificació de l'algorisme	SHA1 amb RSA
	SHA256 amb RSA
	SHA384 amb RSA
	SHA512 amb RSA
Longitud mínima de la clau	2048
Altres paràmetres	No s'estableixen.

4. Normes específiques

4.1. Normes de confiança dels certificats del signatari

Aquestes normes s'apliquen a la signatura del registre evidencial.

4.1.1. Normes de processament de la cadena de certificació

Definició del punt fiable de certificació	Certificats arrel de les entitats de certificació admeses per la Universitat Oberta de Catalunya.
Limitació de la longitud màxima de la cadena de certificació	No s'estableix cap limitació pel que fa a la longitud màxima de la cadena de certificació.
Conjunt inicialment acceptable d'estàndards de certificació	Certificats de nivell 3 i 4 de l'estàndard de certificació de persona jurídica de la Universitat Oberta de Catalunya (`1.3.6.1.4.1.43653.1.3.1.10`).
Definició de condicions respecte als noms emprats als certificats	No s'estableix cap limitació en relació amb l'ús dels noms inclosos en els certificats. En tot cas, la validació s'ha de restringir a la cadena de certificació jeràrquica. No es podran establir relacions de certificació encreuada ni altres models de confiança fora del control de la Universitat Oberta de Catalunya.
Definició de condicions addicionals respecte al tractament de les normatives de certificació en el processament de la cadena de certificació	Es permet de forma expressa l'establiment d'equivalències de normatives de certificació, per a admetre els certificats dels usuaris de les entitats de certificació admeses que hagin estat declarades equivalents amb els anteriors OID.

4.1.2. Normes de comprovació d'informacions de revocació de certificats

Tipus de certificats sobre els quals es portaran a terme les comprovacions	Cal comprovar la vigència del certificat de signatari i de tots els certificats de la cadena de certificació corresponent, a excepció del punt fiable.
Requisit de comprovació dels certificats	La comprovació dels certificats es farà preferentment amb OCSP i, en cas que aquest protocol no estigui disponible, mitjançant consulta de la CRL més recent.