ETSI TS 103 172 V2.2.2 (2013-04)

Semnături și infrastructuri electronice (ESI);
Profilul de bază PAdES

Referin ă
RTS/ESI-000104rev1

Cuvinte
cheie semnătură electronică, PAdES, profil, securitate

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANTA

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucrative enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Cuprins

Drepturi pentru proprietate intelectuala

cuvânt înainte

Această specificație tehnică (TS) a fost produsă de Comitetul tehnic ETSI pentru semnături și infrastructuri electronice (ESI).

Introducere

TS 102 778-3 [1] (PAdES-3 de acum înainte) și TS 102 778-4 [9] (PAdES-4 de acum înainte) specifică formatele pentru semnăturile electronice avansate construite pe PDF ISO-32000 [2]. Documentul respectiv definește un număr de proprietăți de semnătură opționale semnate și nesemnate, ceea ce duce la suport pentru o serie de variații ale conținutului semnăturii și cerințe puternice de procesare.

Pentru a maximiza interoperabilitatea în comunitățile care aplică PAdES în anumite medii, este necesar să se identifice un set comun de opțiuni care sunt adecvate pentru acel mediu. O astfel de selecție se numește de obicei profil.

Prezentul document prezintă TS 101 903 [11] contexte de semnături în care sunt utilizate semnăturile AdES și, în special, utilizarea acestuia în contextul „Directivei 2006/123/CE [i.2] a Parlamentului European și a Consiliului din 12 decembrie. 2006 privind serviciile pe piața internă” (Directiva UE privind serviciile de acum înainte).

1 Domeniul de aplicare

Prezentul document definește un profil de bază pentru PAdES care oferă caracteristicile de bază necesare pentru o gamă largă de cazuri de utilizare în afaceri și guvernamentale pentru ca procedurile și comunicațiile electronice să fie aplicabile unei game largi de comunități atunci când există o nevoie clară de interoperabilitate a semnăturilor AdES. utilizate în documente electronice pentru a fi schimbate peste granițe. În special, acesta ia în considerare nevoile de semnătură electronică în contextul Directivei UE privind serviciile [i.1].

Profilul definește patru niveluri de conformitate diferite care abordează cerințele incrementale pentru a menține valabilitatea semnăturilor pe termen lung, astfel încât toate cerințele abordate la un anumit nivel să fie întotdeauna abordate și de nivelurile de mai sus. Fiecare nivel necesită prezența anumitor atribute PAdES, profilate adecvat pentru a reduce opționalitatea cât mai mult posibil și cu referire la formele care sunt specificate în PAdES [1] și [9].

Clauza 4 identifică cele patru niveluri de conformitate și arată cum aceste niveluri ar putea cuprinde ciclul de viață al semnăturilor electronice.

Clauza 5 oferă detalii despre modul în care cerințele vor fi prezentate pe parcursul prezentului document.

Clauza 6 profilează atributele PAdES pe termen scurt.

Clauza 7 profilează o semnătură PAdES pentru care un Furnizor de servicii de încredere a generat un simbol de încredere (indicativ de marcare a timpului sau marcaj de timp) care demonstrează că semnătura în sine a existat de fapt la o anumită dată și oră.

Clauza 8 profilează atributele PAdES pe termen lung care abordează disponibilitatea pe termen lung a materialului de validare a semnăturii.

Clauza 9 profilează atributele PAdES pe termen lung care abordează disponibilitatea și integritatea pe termen lung a materialului de validare a semnăturii.

NOTĂ: Prezentul document folosește anumite forme verbale (de exemplu , poate, trebuie, nu și ar trebui) ca cheie cuvinte pentru a semnifica cerințe, în conformitate cu Regulile de redactare ETSI, clauza 14a [i.7].

2 Referințe

Referințele sunt fie specifice (identificate prin data publicării și/sau numărul ediției sau numărul versiunii), fie nespecifice. Pentru referințe specifice, se aplică doar versiunea citată. Pentru referințele nespecifice, se aplică cea mai recentă versiune a documentului de referință (inclusiv orice modificări).

Documentele la care se face referire care nu sunt găsite a fi disponibile public în locația așteptată pot fi găsite la http://docbox.etsi.org/Reference.

NOTĂ: Deși orice hyperlinkuri incluse în această clauză erau valabile la momentul publicării, ETSI nu poate garanta valabilitatea lor pe termen lung.

2.1 referințe normative

Următoarele documente de referință sunt necesare pentru aplicarea prezentului document.

[1] ETSI TS 102 778-3: „Semnături și infrastructuri electronice (ESI); Profiluri de semnătură electronică avansată PDF; Partea 3: PAdES îmbunătățit - Profiluri PAdES-BES și PAdES-EPES”.

NOTĂ: Disponibil ca standard ISO sau direct din Adobe PDF Reference http://www.adobe.com/devnet/pdf/pdf_reference.html în special partea 1, clauza 12.8 poate fi preluată de la http://www.adobe.com/content/dam/Adobe/en/devnet/acrobat/pdfs/PDF32000_2008.pdf.

[2] ISO 32000:2008 (toate părțile): „Managementul documentelor – Format document portabil”.

NOTĂ: Disponibil la http://www.adobe.com/content/dam/Adobe/en/devnet/acrobat/pdfs/PDF32000_2008.pdf.

[3] ETSI TS 101 733: „Semnături electronice și infrastructuri (ESI); CMS Advanced Electronic Signatures (CAdES)”.

NOTĂ: Disponibil la http://www.etsi.org/deliver/etsi_ts/101700_101799/101733/.

[4] IETF RFC 3852 (2004): „Cryptographic Message Syntax (CMS)”.

NOTĂ: Disponibil la http://tools.ietf.org/rfcmarkup/3852.

[5] IETF RFC 2634 (1999): „Servicii de securitate îmbunătățite pentru S/MIME”.

NOTĂ: Disponibil la http://tools.ietf.org/rfcmarkup/2634.

[6] IETF RFC 5035 (2007): „Actualizare a serviciilor de securitate îmbunătățite (ESS): Adăugarea agilității algoritmului CertID”.

NOTĂ: Disponibil la http://tools.ietf.org/rfcmarkup/5035.

[7] ETSI TS 102 176-1: „Semnături și infrastructuri electronice (ESI); Algoritmi și parametri pentru semnături electronice sigure; Partea 1: Funcții hash și algoritmi asimetrici”.

NOTĂ: Disponibil la http://www.etsi.org/deliver/etsi_ts/102100_102199/10217601/.

[8] ECRYPT II (Rețeaua Europeană de Excelență în Criptologie II): „ECRYPT II Yearly Report on Algorithms and Keysizes”.

[9] ETSI TS 102 778-4: „Semnături și infrastructuri electronice (ESI); Profiluri de semnătură electronică avansată PDF; Partea 4: PAdES pe termen lung - Profil PAdES LTV”.

NOTĂ: Disponibil la http://www.etsi.org/deliver/etsi_ts/102700_102799/10277804/.

[10] ETSI TS 103 173: „Semnături și infrastructuri electronice (ESI); Profil de bază CAdES”.

NOTĂ: Disponibil la http://www.etsi.org/deliver/etsi_ts/103100_103199/103173/.

[11] ETSI TS 101 903: „Semnături electronice și infrastructuri (ESI); XML Advanced Electronic Signatures (XAdES)”.

2.2 Referințe informative

Următoarele documente de referință nu sunt necesare pentru aplicarea prezentului document, dar ajută utilizatorul în ceea ce privește un anumit domeniu.

[i.1] Decizia 2011/130/UE a Comisiei din 25 februarie 2011; de stabilire a cerințelor minime pentru prelucrarea transfrontalieră a documentelor semnate electronic de autoritățile competente în temeiul Directivei 2006/123/CE a Parlamentului European și a Consiliului privind serviciile pe piața internă [notificată sub documentul C(2011) 1081].

[i.2] Directiva 2006/123/CE a Parlamentului European și a Consiliului din 12 decembrie 2006 privind serviciile pe piața internă.

[i.3] Decizia 2009/767/CE a Comisiei din 16 octombrie 2009 modificată prin CD 2010/425/UE din 28 iulie 2010 de stabilire a măsurilor care facilitează utilizarea procedurilor prin mijloace electronice prin „ghișeele unice” în temeiul Directivei 2006/123/CE din Parlamentul European și al Consiliului privind serviciile pe piața internă.

[i.4] ETSI TS 102 231: „Semnături și infrastructuri electronice (ESI); Furnizarea de informații armonizate privind starea serviciului de încredere”.

[i.5] ETSI TS 101 533-1: „Semnături și infrastructuri electronice (ESI); Securitatea sistemelor de conservare a datelor; Partea 1: Cerințe pentru implementare și management”.

[i.6] ETSI TS 102 640-1: „Semnături și infrastructuri electronice (ESI); Poștă electronică înregistrată (REM); Partea 1: Arhitectură”.

[i.7] Reguli de redactare ETSI (EDR).

NOTĂ: Conținut în directivele ETSI: http://portal.etsi.org/Directives/home.asp.

3 Definiții și abrevieri

3.1 Definiții

În sensul prezentului document, se aplică următorii termeni și definiții:

generator: orice parte care creează sau adaugă atribute unei semnături

NOTĂ: Acesta poate fi semnatarul sau orice parte care verifică inițial sau menține în continuare semnătura.

element de protocol: element al protocolului care poate include elemente de date și/sau elemente de procedură

element de serviciu: element de serviciu care poate fi furnizat folosind unul sau mai multe elemente de protocol

NOTĂ: Toate elementele de protocol alternativ oferă un serviciu echivalent utilizatorilor protocolului.

furnizor de servicii de încredere: organism care operează unul sau mai multe servicii de încredere (electronice).

NOTĂ: Vezi [i.4].

verificator: entitate care validează sau verifică o semnătură electronică

3.2 Abrevieri

În sensul prezentului document, se aplică abrevierile date în PAdES-3 [1] și următoarele:

TSL Lista de stare de încredere

NOTĂ: Vezi [i.4].

4 Niveluri de conformitate

Prezenta specificație definește patru niveluri de conformitate, așa cum este indicat mai jos.

Aplicațiile care gestionează semnăturile în conformitate cu cerințele specificate în clauza 6 pot revendica conformitatea B-Level (nivel de bază).

Aplicațiile care gestionează semnături conform cu B-Level și, de asemenea, conform cerințelor specificate în clauza 7, pot revendica conformitatea T-Level (Timp de încredere pentru existența semnăturii).

Aplicațiile care gestionează semnături conform cu T-Level și, de asemenea, conform cerințelor specificate în clauza 8 a prezentului document, pot revendica conformitatea LT-Level (nivel pe termen lung).

Aplicațiile care gestionează semnături conform cu LT-Level și, de asemenea, conform cerințelor specificate în clauza 9 a prezentului document, pot revendica conformitatea LTA-Level (Long Term with Archive time-stampile).

Aceste niveluri de conformitate sunt definite pentru a cuprinde ciclul de viață al semnăturii electronice, și anume:

a) Profiluri de nivel B încorporarea unor proprietăți semnate și nesemnate atunci când semnătura este de fapt generate.

NOTA 1: Se consideră că acest nivel este suficient pentru a se conforma Deciziei 2011/130/UE a Comisiei din 25 februarie 2011 [i.1].

b) T-Level profilează generarea, pentru o semnătură existentă, a unui token de încredere care demonstrează că semnătura în sine exista de fapt la o anumită dată și oră.

c) LT-Level profilează încorporarea întregului material necesar pentru validarea semnăturii în semnătură.
Acest nivel este înțeles pentru a aborda disponibilitatea pe termen lung a materialului de validare.

d) Profiluri LTA-Level încorporarea de jetoane de marcare temporală care permit validarea semnăturii pe termen lung
după generarea sa. Acest nivel este înțeles pentru a aborda disponibilitatea și integritatea pe termen lung a materialului de validare.

NOTA 2: Nivelurile b) la d) sunt adecvate atunci când validitatea tehnică a semnăturii trebuie păstrată pentru o perioadă de timp.
perioada de timp de la crearea semnăturii în care expirarea certificatului, revocarea și/sau învechirea
algoritmului reprezintă o problemă. Nivelul specific aplicabil depinde de context și de cazul de utilizare.

Toate nivelurile de conformitate până la LTA folosesc atribute definite în PAdES [1] și [9] și specificațiile subiacente.

Atunci când datele semnate sunt schimbate între părți, expeditorul ar trebui să folosească cel puțin semnături conform unui nivel care să permită părților care se bazează să aibă încredere în semnătură în momentul schimbului.

NOTA 3: Arhivarea sau conservarea semnăturilor electronice pe termen lung necesită, în general, conformitatea cu nivelul LTA.
Utilizarea nivelului LTA este considerată o tehnică adecvată de conservare și transmitere a datelor semnate.
Conformitatea la nivelul inferior este suficientă atunci când este combinată cu tehnici de protecție suplimentare
adecvate, cum ar fi utilizarea sistemelor conforme cu TS 101 533-1 [i.5].

NOTA 4: Evaluarea eficacității altor tehnici de conservare și transmitere a datelor semnate nu intră în domeniul de aplicare al
prezentului document. Cititorul este sfătuit să ia în considerare instrumentele legale în vigoare și standardele aferente,
cum ar fi TS 101 533-1 [i.5] sau TS 102 640-1 [i.6] pentru a evalua caracterul adecvat al acestora.

5 Cerințe generale

5.1 Cerințe de algoritm

Generatorii sunt referiți la legile naționale aplicabile cu privire la algoritmi și lungimile cheilor.

De asemenea, se recomandă generatorilor să ia în considerare cea mai recentă versiune a TS 102 176-1 [7] în scopuri de ghidare și cel mai recent raport anual ECRYPT2 D.SPA.x [8] pentru recomandări suplimentare, atunci când selectează algoritmi și lungimile cheilor.

Algoritmul MD5 nu trebuie utilizat ca algoritm de rezumat.

5.2 Cerințe de conformitate

Profilurile din prezentul document definesc cerințele pentru generatorii de semnături PAdES [1] și [9].

Un verificator trebuie să poată accepta o semnătură care să conțină orice elemente/proprietăți conforme cu PAdES [1] și [9], dar acest profil nu specifică nicio cerință de procesare privind elementele/proprietățile prezente în semnătură, așa cum este destinat să fie utilizat. împreună cu o specificație care descrie procesarea în timpul validării semnăturii.

Cerințele sunt grupate în patru categorii diferite, fiecare având identificatorul corespunzător. Tabelul 1 definește aceste categorii și identificatorii lor.

Tabelul 1: Categorii de cerințe

Identificator	Cerință privind generatorul
M	Generatorul va include elementul în semnătură.
O	Generatorul poate include elementul în semnătură.

Elementele opționale definite în PAdES-3 [1] dar nespecificate în prezentul document sunt tratate ca „O” ca mai sus.

Anumite elemente de serviciu pot fi furnizate de diferite elemente de protocol la alegerea utilizatorului. În aceste cazuri, semantica lui M și O definită în tabelul de mai sus depinde de cerințele pentru elementul de serviciu însuși. Tabelele 2 și 3 (fiecare se aplică unei cerințe diferite privind elementul de serviciu) definesc această semantică.

Tabelul 2: Cerințe pentru serviciul obligatoriu cu opțiuni

Identificatorul de cerințe pentru Element de serviciu / protocol	Cerință privind generatorul
Serviciu = M	Generatorul va furniza serviciul prin includerea unui element de protocol ales din lista de opțiuni.
Alegerea protocolului = O	Generatorul poate utiliza acest element de protocol pentru furnizarea elementelor de serviciu obligatorii.

Tabelul 3: Cerințe pentru serviciul opțional cu opțiuni

Identificatorul de cerințe pentru Element de serviciu / protocol	Cerință privind generatorul
Serviciu = O	Generatorul poate furniza serviciul prin includerea unui element de protocol ales din lista de opțiuni.
Alegerea protocolului = O	Dacă generatorul decide să furnizeze serviciul, atunci ea poate utiliza acest element de protocol.

Prezentul document prezintă cerințe noi pentru fiecare element de serviciu și protocol în formă tabelară. Mai jos urmează structura tabelului.

Tabelul 4: Cerințe pentru serviciul opțional cu opțiuni

Element de serviciu / protocol	Referin ă	Cerință privind generatorul	Cerințe/note suplimentare
Serviciu:			
Alegerea 1			
Alegerea 2			

Coloana Serviciul / Elementul de protocol va identifica elementul de serviciu sau elementul de protocol căruia i se aplică cerința. Elementele de serviciu care pot fi implementate de diferite elemente de protocol (adică utilizatorii pot alege mai multe elemente de protocol) construiesc tabele cu mai mult de un rând.

Column Reference va face referire la clauza relevantă a standardului în care elementul este definit pentru prima dată. Referința este la PAdES-3 [1], cu excepția cazului în care se indică în mod explicit altfel.

Coloana Cerință pe generator va conține un identificator al cerinței, așa cum este definit în tabelul 1, legat de elementul de protocol corespunzător pentru generator.

Coloana Note / Cerințe suplimentare vor conține numere care fac referire la note și/sau litere care fac referire la cerințe suplimentare. Atât notele, cât și cerințele suplimentare sunt enumerate sub tabel.

Profilurile pot fi afectate de reglementările aplicabile; prin urmare, implementatorii ar trebui să verifice orice reglementare națională care ar putea afectează aceste profiluri.

6 Cerințe pentru conformitatea B-Level

Această clauză definește cerințele pe care trebuie să le îndeplinească semnăturile PAdES care pretind conformitatea cu nivelul B.

Clauza actuală specifică cerințele de conformitate pentru semnăturile electronice pe termen scurt. Această clauză profilează de fapt semnăturile PAdES-BES (semnături care nu încorporează semnătură-politică-identificator) și PAdES-EPES (semnături care încorporează semnătură-politică-identificator).

Toate atributele profilate de PAdES Partea 3 [1] și specificate în ISO 32000-1 [2] se aplică așa cum este menționat în acele specificații, dacă nu este menționat altfel aici. De asemenea, PAdES Partea 3 prevede că „Cerințele pentru manipularea semnăturilor PDF specificate în ISO 32000-1, clauza 12.8 se aplică, cu excepția cazului în care sunt înlocuite [...]”. Următoarele clauze vor aplica aceeași strategie.

NOTA 1: Având în vedere că semnăturile PAdES sunt plicate în interiorul unui document PDF și sunt detașate în sensul unui Semnătură CMS, plasarea semnăturii este implicită de PAdES-3 [1] și ISO 32000 [2]. În ISO 32000 [2], secțiunea 12.8.3.3.1 citește „Nici o date nu vor fi încapsulate în câmpul PKCS#7 SignedData”, nu va fi dată aici nicio reformulare, totuși cititorii ar trebui să fie conștienți de faptul că dependențele subtile exista.

În consecință, următoarele proprietăți PAdES sunt abordate direct în această clauză:
SignedData.certificates, intrarea M din dicționarul de semnături (oferă un timp de semnare revendicat, cum ar fi CAdES [3], clauzele 5.1 și 5.9.1), certificat de semnare. Alte tipuri de conținut, rezumat de mesaje, identificator de politică de semnătură, atribute de semnatar, tip de conținut, ștampilă de timp de conținut și intrările Locație și Motiv din dicționarul de semnături sunt abordate în mod inerent.

NOTA 2: PAdES Partea 3 [1] interzice utilizarea atributelor timp de semnare, contrasemnătură, referință de conținut, identificator de conținut, indicii de conținut și locație semnatar. PAdES Partea 3 [1] interzice utilizarea atributului angajament-tip-indicație pentru PAdES-BES și permite utilizarea acestuia pentru PAdES-EPES.

6.1 Atribute definite în CMS Signature

6.1.1 Plasarea certificatului de semnare

Tabelul 5

Element de serviciu / protocol	Referin ă	Cerința generatorului	Cerințe suplimentare/note a, b
SignedData.certificates CMS [4], clauza 5.1		M	

Cerințe suplimentare:

a) Generatorul va include certificatul de semnare în câmpul SignedData.certificates.

b) Pentru a facilita construirea căii, generatorii ar trebui să includă în câmpul SignedData.certificates toate certificatele care nu sunt disponibile verificatorilor care pot fi utilizate în timpul construirii căii. În cazul semnăturii bazate pe certificate calificate și a căror verificare este de așteptat să se bazeze pe TSL-uri (în special pe listele de încredere, astfel cum sunt definite în CD 2009/767/CE modificat prin CD 2010/425/UE [i.3])", generatorul ar trebui să includă toate certificatele intermediare care formează un lanț între certificatul de semnatar și o CA prezentă în TSL și care nu sunt disponibile verificatorilor.

NOTA 1: Un certificat este considerat disponibil pentru verificator dacă sunt cunoscute informații fiabile despre locația sa și permite extragerea automată a certificatului (de exemplu, printr-o extensie de acces la informații despre autoritate sau informații echivalente prezente într-un TSL).

NOTA 2: În cazul general, diferiți verificatori pot avea diferiți parametri de încredere și pot valida certificatul de semnatar prin diferite lanțuri. Prin urmare, este posibil ca generatorii să nu știe ce certificate vor fi relevante pentru construirea căii. Cu toate acestea, în practică, astfel de certificate pot fi adesea identificate în mod clar. În acest caz, se recomandă ca generatoarele să le includă, cu excepția cazului în care pot fi recuperate automat de către verificatori. În cazul specific al unei semnături menite să fie validată prin TSL, se recomandă includerea cel puțin a certificatelor intermediare indisponibile până la, dar fără a include CA-urile prezente în TSL-uri, deoarece TSL-ul este informații care sunt partajate la nivel global de către toți verificatorii.

6.2 Atribute suprascrise în PAdES-3

6.2.1 Ora semnării

Tabelul 6

Element de serviciu / protocol	Referin ă	Cerința generatorului	Cerințe/note suplimentare
Serviciu: furnizați o oră revendicată de semnare	[1], clauza 4.5.3	M	A
Intrarea M în dicționarul de semnături	ISO 32000-1 [2], clauza 12.8.1	M	

Cerință suplimentară:

a) Generatorul trebuie să includă ora UTC revendicată a semnăturii, așa cum este exprimată în [2], clauza 7.9.4 ca conținut a acestui element.

6.3 Atribute definite în ESS

6.3.1 Certificat de semnare

Tabelul 7

Element de serviciu / protocol	Referin ă	Generator Cerin ă	Cerințe/note suplimentare
Serviciu: protecția certificatului de semnare		M	
certificat de semnare ESS	ESS [5], clauza 5.4	O	a,
Certificat de semnare ESS v2	ESS [6], clauza 4	O	ba, b

Cerințe suplimentare:

a) Generatorii vor utiliza fie certificatul de semnare, fie atributul signing-certificate v2, în funcție de funcția hash, folosind, în conformitate cu ESS [6], clauza 2.

b) Generatorii ar trebui să migreze la utilizarea certificatului de semnare ESS v2, de preferință față de certificatul de semnare ESS, în conformitate cu îndrumările privind durata de viață limitată pentru utilizarea SHA-1, prezentate în clauza 9.2 din TS 102 176-1 [7].

7 Cerințe pentru conformitatea T-Level

Această clauză definește acele cerințe pe care trebuie să le îndeplinească semnăturile PAdES conforme cu B-Level pentru a fi și conforme cu T-Level. În consecință, semnăturile PAdES care susțin conformitatea cu Nivelul T al prezentului profil vor fi construite pe semnături conforme cu Nivelul B.

O semnătură PAdES conformă cu T-Level va fi o semnătură conformă cu B-Level pentru care un Furnizor de servicii de încredere [i.4] a generat un token de încredere (indicativ de marcare a timpului sau marcaj de timp) care dovedește că semnătura în sine a existat cu adevărat la o anumită dată și oră.

NOTĂ: Semnăturile PAdES conforme cu T-Level din prezenta specificație sunt, în consecință, semnăturile PAdES-BES sau EPES profilate corespunzător conform cerințelor definite în această clauză.

7.1 Serviciul așa cum este definit în CAdES

7.1.1 Timp de încredere pentru existența semnăturii

Tabelul 8 prezintă în continuare furnizarea simbolului de încredere care dovedește existența semnăturii la o anumită dată și oră. Furnizarea Serviciului: timpul de semnare de încredere este profilat ca în Profilul de referință CAdES [10] clauza 7 extinsă prin opțiunea de a furniza o ștampilă de timp a documentului în locul unui atribut de ștampilă de timp a semnăturii PAdES Partea 3 [1], clauza 4.5.2 sau marca de timp.

Tabelul 8

Element de serviciu / protocol	Referin ă	Generator Cerin ă	Cerințe/note suplimentare
Serviciu: timp de încredere pentru existența semnăturii	[1], clauza 4.5.2 [3], clauza 4.4.1	M	
atribut semnătură-timp-stampilă	[1], clauza 4.5.2 [3], clauza 6.1 [3], clauza 4.4.1	O	a, b, c, d
marca temporală	[3], clauza 4.4.1	O	e
document -time-stamp	[9], clauza A.2	O	d

Cerințe suplimentare:

a) Prezentul profil recomandă utilizarea mărcilor de timp ca atestare a timpului de existență a semnăturii în locul marcajelor de timp.

b) O semnătură PAdES care susține conformitatea cu nivelul T poate conține mai multe ștampile de timp și semnătură atribute.

c) Generatorul va folosi codificarea DER pentru orice semnătură-timp-stampilă.

d) Semnăturile de nivel B, așa cum sunt prezentate în clauza 6, vor rezerva spațiu pentru ștampila semnăturii. atributul [1], clauza 4.5.2, dacă se anticipează propagarea acestora la un nivel de conformitate mai ridicat. În mod alternativ, un document-ștampilă de timp poate servi acestui scop, care acoperă întregul document, inclusiv valoarea semnăturii și poate fi aplicat înainte de DSS și DSS/VRI.

e) Dacă se utilizează un marcaj de timp, atunci nu este încorporat niciun atribut suplimentar în semnătură. Este responsabilitatea TSP generează marcajul de timp pentru a oferi încrederea necesară în timpul semnăturii.

8 Cerințe pentru conformitatea la nivel LT

Această clauză definește acele cerințe pe care trebuie să le îndeplinească semnăturile PAdES conforme cu T-Level pentru a fi, de asemenea, conforme cu LT-Level. În consecință, semnăturile PAdES care susțin conformitatea cu Nivelul LT al prezentului profil vor fi construite pe semnături conforme cu Nivelul T.

Prin urmare, implementările care pretind conformitatea cu nivelul de conformitate LT construiesc formularul PAdES-LTV (PAdES Partea 4 [9], clauza 4) pe semnături care trebuie să fie conforme cu cerințele T-Level și cu prezenta clauză.

8.1 Profilul extensiilor ISO 32000-1 LTV

8.1.1 Magazin de securitate a documentelor

Tabelul 9

Element de serviciu / protocol	Referin ă	Cerința generatorului	Cerințe/note suplimentare
Serviciu: certificat și valori de revocare		M	
DSS	[9], clauza A.1 [9], clauza A.1	M	a, b, c, d, ef
DSS/VRI		O	

Cerințe suplimentare:

a) Generatorul trebuie să includă setul complet de certificate, inclusiv ancora de încredere atunci când este disponibil în forma unui certificat, care au fost folosite pentru validarea semnăturii și care nu sunt deja prezente. Acest set include certificate necesare pentru validarea certificatului de semnare, pentru validarea oricărui certificat de atribut prezent în semnătură și pentru validarea oricărui certificat de semnare al tokenului de marcare temporală (adică un certificat TSA) deja încorporat în semnătură.

b) În situații diferite de cele identificate în clauza 6.1.1 din prezentul document cerințele a) și b): aplicațiile ar trebui să includă valorile certificatelor în DSS.

c) Prezentul document recomandă evitarea dublării valorilor certificatelor în cadrul semnăturii.

d) Generatorul va include setul complet de date de revocare (răspunsuri CRL sau OCSP) care au fost utilizate în validarea semnatarului și certificatele CA utilizate în semnătură. Acest set include toate informațiile despre starea certificatului necesare pentru validarea certificatului de semnare, pentru validarea oricărui certificat de atribut prezent în semnătură și pentru validarea oricărui certificat de semnare al jetonului de marcare temporală (adică un certificat TSA) deja încorporat în semnătură.

e) Generatorul va folosi codificarea DER pentru valorile-certificat și pentru valorile de revocare.

f) Deși VRI este acceptabilă la acest nivel LT, utilizarea sa ar trebui evitată pentru a maximiza interoperabilitatea.

9 Cerințe pentru conformitatea la nivel LTA

Această clauză definește acele cerințe pe care semnăturile PAdES conforme cu LT-Level trebuie să le îndeplinească pentru a fi, de asemenea, conforme cu LTA-Level. În consecință, semnăturile PAdES care susțin conformitatea cu Nivelul LTA al prezentului profil vor fi construite pe semnături conforme cu Nivelul LT.

O semnătură PAdES conformă cu LTA-Level trebuie să fie o semnătură conformă cu LT-Level la care au fost încorporate unul sau mai multe ștampile de timp ale documentului .

NOTĂ: După cum se precizează în PAdES Partea 4 [9], un formular LTA poate ajuta la validarea semnăturii dincolo de orice eveniment care ar putea limitează valabilitatea acestuia.

Tabelul 10

Element de serviciu / protocol	Referin ă	Cerința generatorului	Cerințe/note suplimentare
Serviciu: timp de încredere pentru existența datelor de validare	[10], clauza 9 [3], clauza 6.5 [9],	M	
document-timp-stamp	clauza 4 [9], clauza A.2	M	a, b, c, 1, 2

Cerințe suplimentare:

a) Semnăturile conforme cu nivelul LTA pot avea mai mult de o ștampilă de timp pentru document aplicată după DSS și DSS/VRI.

b) Înainte de generarea și încorporarea unui atribut document-ștampilă temporală , aplicațiile care susțin conformitatea cu acest profil, vor include tot materialul de validare, care nu se află deja în semnătură, necesar pentru verificarea semnăturii. Acest material de validare include toate certificatele și toate informațiile despre starea certificatului (cum ar fi CRL-urile sau răspunsurile OCSP) necesare pentru:

- validarea certificatului de semnare;
- validarea oricărui certificat de atribut prezent în semnătură; și
- validarea oricărui certificat de semnare a oricărui simbol de marcare temporală (adică un certificat TSA) deja încorporat în semnătură (inclusiv, desigur, orice ștampilă de timp anterioară).

Acest material de validare ar trebui să fie încorporat în DSS.

Istorie

Istoricul documentelor		
V1.1.1	Publicație septembrie 2011	
V2.1.1	martie 2012	Publicare
V2.2.1	octombrie 2012	Publicare
V2.2.2	aprilie 2013	Publicare