Tabelul de Concordanţă la proiectul legii
cu privire la semnătura electronică şi documentul electronic

<table>
<tr><td colspan="6">1. Titlul actului comunitar, subiectul şi scopul reglementat de către actul dat
Directiva 1999/93/CE a Parlamentului Euroepan şi a Consiliului din 13 decembrie 1999 privind un cadru comunitar pentru semnăturile electronice
Subiectul – semnătura electronică
Scopul – Crearea unui cadru de utilizare a semnăturilor electronice în cadrul pieţei comune
Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community Framework for electronic signatures
The subject – electronic signatures
The goal – Creation of a framework of use of electronic signatures in the common market</td></tr>
<tr><td colspan="6">2. Titlul actului normativ naţional, subiectul şi scopul reglementat de către actul dat
Proiectul Legii privind semnătura electronică şi documentul electronic
Subiectul – semnătura electronică şi documentul electronic
Scopul – stabilirea regimul juridic al semnăturii electronice şi al documentelor electronice, inclusiv cerinţelor principale faţă de valabilitatea acestora şi cerinţelor principale faţă de serviciile de certificare
Draft Law on electronic signature and electronic document
The subject – electronic signature and electronic document
The goal - establishing the legal status of electronic signatures and electronic documents, including the essential requirements to their validity and essential requirements to certification services</td></tr>
<tr><td colspan="6">3. Gradul de compatibilitate
Compatibilă</td></tr>
<tr><td>4. Prevederile şi cerinţele reglementărilor comunitare (articolul, paragraful,
punct)</td><td>5. Prevederile actului normativ
naţional (capitolul, articolul, sub-paragraful, punctul etc.)</td><td>6. Compatibilitatea între proiect si Reglementarea Comunitara
(complet compatibil, parţial compatibil, nu este compatibil, vid legislativ naţional).</td><td>7. Motivele ce explică că proiectul este parţial compatibil sau incompatibil</td><td>8. Instituţia responsabilă</td><td>9. Termenul limită pînă cînd urmează
a se asigura compatibilitatea completă a actului naţional</td></tr>
</table>

Articolul 1 (1) Obiectivul prezentei directive este să faciliteze utilizarea semnăturilor electronice şi să contribuie la recunoaşterea lor legală. Prezenta directivă stabileşte un cadru legal pentru semnăturile electronice şi pentru anumite servicii de certificare pentru a asigura buna funcţionare a pieţei interne.	**Articolul 1** (1) Prezenta lege stabileşte regimul juridic al semnăturii electronice şi al documentului electronic, inclusiv cerinţele principale faţă de valabilitatea acestora şi cerinţele principale faţă de serviciile de certificare.	Compatibil			
Articolul 2 **Definiţii:** 1. „semnătură electronică" înseamnă date în formă electronică, ataşate la sau logic asociate cu alte date în formă electronică şi care sunt utilizate ca metodă de autentificare;	**Articolul 4** (2) Semnătura electronică simplă - date în formă electronică, ataşate la sau logic asociate cu alte date în formă electronică şi care sunt utilizate ca metodă de autentificare	Compatibil			
2. „semnătură electronică avansată" înseamnă o semnătură electronică ce îndeplineşte următoarele cerinţe: (a) face trimitere exclusiv la semnatar; (b) permite identificarea semnatarului; (c) a fost creată prin mijloace pe care semnatarul le poate păstra exclusiv sub controlul său şi (d) este legată de datele la care se raportează astfel încât orice modificare ulterioară a datelor poate fi detectată;	**Articolul 4** (3) Semnătura electronică avansată necalificată este o semnătură electronică ce îndeplineşte următoarele cerinţe: a) face trimitere exclusiv la semnatar b) permite identificarea semnatarului c) a fost creată prin mijloace pe care semnatarul le poate păstra exclusiv sub controlul său şi d) este legată de datele la care se raportează astfel încît orice modificare ulterioară a datelor poate fi detectată	Compatibil			

3. „semnatar” înseamnă o persoană care deţine un dispozitiv de creare a semnăturii şi care acţionează fie în nume propriu, fie în numele persoanei fizice, al persoanei juridice sau al entităţii pe care le reprezintă;	**Articolul 2** u) semnatar – o persoană care deţine un dispozitiv de creare a semnăturii şi care acţionează fie în nume propriu, fie în numele persoanei fizice, al persoanei juridice sau al entităţii pe care le reprezintă	Compatibil			
4. „date de creare a semnăturii” înseamnă date unice, precum codurile sau cheile criptografice private, care sunt utilizate de semnatar pentru a crea o semnătură electronică;	j) date de creare a semnăturii electronice – date unice, precum codurile sau cheile criptografice private, care sunt utilizate de semnatar pentru a crea o semnătură electronică	Compatibil			
5. „dispozitiv de creare a semnăturii” înseamnă unităţi de software sau hardware configurate, utilizate pentru punerea în aplicare a datelor de creare a semnăturii;	l) dispozitiv de creare a semnăturii electronice – unităţi de software şi (sau) hardware configurate, utilizate pentru punerea în aplicare a datelor de creare a semnăturii	Compatibil			
6. „dispozitiv securizat de creare a semnăturii” înseamnă un dispozitiv de creare a semnăturii care îndeplineşte cerinţele prevăzute la anexa III;	m) dispozitiv securizat de creare a semnăturii electronice – dispozitiv de creare a semnăturii care întruneşte cerinţele prevăzute de aliniate 3) şi 4) din articolul 8 din prezenta lege	Compatibil			
7. „date de verificare a semnăturii” înseamnă date, precum codurile sau cheile criptografice publice, care sunt utilizate în scopul verificării unei semnături electronice;	k) date de verificare a semnăturii electronice – date, precum şi codurile sau cheile criptografice publice, care sunt utilizate în scopul verificării unei semnături electronice	Compatibil			

8. „dispozitive de verificare a semnăturii” înseamnă unităţi de software sau hardware configurate, utilizate la aplicarea datelor de verificare a semnăturilor;	n) dispozitive de verificare a semnăturii electronice – unităţi de software sau hardware configurate, utilizate la aplicarea datelor de verificare a semnăturilor	Compatibil			
9. „certificat” înseamnă o atestare electronică ce raportează datele de verificare a semnăturilor la o persoană şi confirmă identitatea respectivei persoane;	e) certificat al cheii publice - document electronic ce conţine cheia publică, semnat cu semnătura electronică a prestatorului de servicii de certificare, document ce atestă apartenenţa cheii respective titularului certificatului cheii publice şi permite identificarea acestui titular	Parţial compatibil	În sensul proiectului de lege naţional se utilizează noţiunea de „certificat al cheii publice”, deoarece certificării se supune anume cheia publică în conformitate cu art.31 şi 32 şi certificatul este legat de această.		
10. „certificat calificat” înseamnă un certificat care îndeplineşte cerinţele prevăzute la anexa I şi este eliberat de un prestator de servicii de certificare care îndeplineşte cerinţele prevăzute la anexa II;	d) certificat calificat al cheii publice – certificat al cheii publice care întruneşte cerinţele prevăzute de articolul 32 din prezenta lege şi este eliberat de un prestator de servicii de certificare, care întruneşte cerinţele prevăzute de articolul 27 din prezenta lege	Compatibil			
11. „prestator de servicii de certificare” înseamnă orice entitate sau persoană fizică sau juridică ce eliberează certificate sau prestează alte servicii referitoare la semnăturile electronice;	s) prestator de servicii de certificare – întreprinzător individual sau persoana juridică care prestează servicii de certificare	Compatibil			
12. „produs asociat semnăturii electronice” înseamnă unităţi de hardware sau software sau componente	t) produs asociat semnăturii electronice – unităţi de hardware sau software sau componente specifice ale	Compatibil			

specifice ale acestora, destinate să fie utilizate de un prestator de servicii de certificare în vederea prestării de servicii de certificare a semnăturilor sau destinate să fie utilizate în scopul creării sau al verificării semnăturilor electronice;	acestora, destinate pentru utilizare de un prestator de servicii de certificare la prestarea serviciilor de certificare sau pentru crearea sau verificarea semnăturilor electronice				
13. „acreditare voluntară” înseamnă orice autorizaţie care prevede drepturi şi obligaţii specifice prestării de servicii de certificare, acordată, la cererea prestatorului de servicii de certificare în cauză, de către organismul public sau privat responsabil cu elaborarea respectivelor drepturi şi obligaţii şi de supravegherea respectării acestora, în cazul în care prestatorul de servicii de certificare nu are dreptul să exercite drepturile care decurg din autorizaţie până nu a primit decizia respectivului organism.	a) acreditare voluntară – autorizaţie care prevede drepturi şi obligaţii specifice prestării de servicii de certificare, acordată, la cererea prestatorului de servicii de certificare în cauză, de către organul competent de stabilirea drepturilor şi obligaţiilor respective şi de supravegherea respectării acestora, în cazul în care prestatorul de servicii de certificare nu are dreptul să exercite drepturile care decurg din autorizaţie pînă nu a primit decizia organului respectiv	Compatibil			
Articolul 3 **Acces la piaţă** (1)Statele membre nu condiţionează prestarea de servicii de certificare de nici o autorizaţie prealabilă. (2)Fără să aducă atingere dispoziţiilor alineatului (1), statele membre pot introduce sau menţine sisteme de acreditare voluntară destinate să amelioreze nivelul serviciilor de certificare prestate.	**Articolul 26 alin. (1)** Prestatorii de servicii de certificare dispun de dreptul de a trece procedura de acreditare.	Compatibil			

Articolul 5 **Efectele juridice ale semnăturilor electronice** (1) Statele membre se asigură că semnăturile electronice avansate care se bazează pe un certificat calificat şi sunt create printr-un dispozitiv securizat de creare de semnături: (a) îndeplinesc cerinţele legale ale unei semnături în ceea ce priveşte datele în format electronic în aceeaşi măsură în care o semnătură de mână îndeplineşte cerinţele în ceea ce priveşte datele scrise sau tipărite pe hârtie şi (b) sunt acceptabile ca probe în justiţie.	**Articolul 4 alin (4)** Semnătura electronică avansată calificată este o semnătură electronică care îndeplineşte toate cerinţele semnăturii electronice avansate necalificate şi, suplimentar: a) se bazează pe un certificat calificat emis de un prestator de servicii de certificare acreditat în domeniul aplicării semnăturii electronice avansate calificate; b) este creată cu utilizarea dispozitivului securizat de creare a semnăturii electronice şi se verifică securizat cu utilizarea dispozitivului de verificare a semnăturii electronice şi/sau produsului asociat semnăturii electronice care dispun de confirmarea corespunderii cerinţelor prevăzute de prezenta lege.. **Articolul 5 alin. (2):** Semnătura electronică avansată calificată dispune de aceeaşi valoare juridică ca şi semnătura olografă. **Articolul 5 alin. (1):** Semnătura electronică, indiferent de gradul de protecţie, are efecte juridice şi este acceptată ca probă, inclusiv în justiţie.	Compatibil			
Articolul 5 **Efectele juridice ale semnăturilor electronice**	**Articolul 5 alin. (1):** Semnătura electronică, indiferent de gradul de protecţie, are efecte	Compatibil			

(2) Statele membre se asigură că unei semnături electronice nu i se refuză eficienţa juridică şi posibilitatea de a fi acceptată ca probă în justiţie din simplul motiv că: — se prezintă în format electronic sau — nu se bazează pe un certificat calificat sau — nu se bazează pe un certificat calificat eliberat de un prestator acreditat de servicii de acreditare sau — nu este creată printr-un dispozitiv securizat de creare de semnături.	juridice şi este acceptată ca probă, inclusiv în justiţie, chiar dacă: a) se prezintă în format electronic, sau b) nu se bazează pe un certificat eliberat de un prestator acreditat de servicii de certificare, sau c) nu se bazează pe un certificat calificat, sau d) nu este creată printr-un dispozitiv securizat de creare a semnăturii.				
Articolul 7 **Aspecte internaționale** Statele membre se asigură că certificatele pe care un prestator de servicii de certificare stabilit într-o ţară terţă le eliberează pentru public ca certificate calificate sunt recunoscute ca fiind echivalente din punct de vedere legal cu certificatele eliberate de prestatorii de servicii de certificare stabiliţi în Comunitate în cazul în care: (a) prestatorul de servicii de certificare îndeplineşte cerinţele prevăzute de prezenta directivă şi a fost acreditat în cadrul unui sistem voluntar de acreditare iniţiat într-un stat membru sau (b) un prestator de servicii de certificare stabilit în Comunitate care îndeplineşte cerinţele prevăzute de prezenta	**Articolul 6. Recunoaşterea semnăturilor electronice străine** (1) Certificat al cheii publice eliberat de către un prestator de servicii de certificare cu domiciliul sau cu sediul într-un alt stat este recunoscut ca fiind echivalent din punct de vedere al efectelor juridice cu certificat al cheii publice eliberat de un prestator de servicii de certificare cu domiciliul sau cu sediul în Republica Moldova, dacă: a) prestatorul de servicii de certificare cu domiciliul sau sediul în alt stat a fost acreditat în cadrul regimului de acreditare, în condițiile prevăzute de prezenta lege; b) un prestator de servicii de certificare acreditat, cu domiciliul sau cu sediul în Republica Moldova, garantează certificatul;	Compatibil			

directivă garantează certificatul sau (c) certificatul sau prestatorul de servicii de certificare este recunoscut în temeiul unui acord bilateral sau multilateral între Comunitate şi ţări terţe sau organizaţii internaţionale.	c) certificatul sau prestatorul de servicii de certificare care l-a eliberat este recunoscut prin aplicarea unui acord bilateral sau multilateral între Republica Moldova și alte state sau organizații internaționale, pe baza de reciprocitate. Semnătura electronică şi documentul electronic semnat prin intermediul acesteia nu pot fi considerate lipsite de putere juridică doar în baza faptului că certificatul cheii publice a fost eliberat în corespundere cu normele unui stat străin.				
Anexa I **Cerinţe privind certificatele calificate** Certificatele calificate trebuie să cuprindă: (a) o menţiune care să indice că certificatul este eliberat ca certificat calificat; (b) identificarea prestatorului de servicii de certificare, precum şi a ţării în care este stabilit; (c) numele semnatarului sau un pseudonim identificat ca atare; (d) posibilitatea includerii, atunci când este cazul, a unei calităţi speciale a semnatarului, în funcţie de utilizarea pe care urmează să o aibă certificatul; (e) datele de verificare a semnăturii care corespund datelor de creare a semnăturii sub controlul semnatarului;	**Articolul 32 alin (2)** Certificatul cheii publice trebuie să conţină următoarele informaţii: a) numărul unic de înregistrare a certificatului cheii publice; b) datele de identificare ale prestatorului de servicii de certificare care a eliberat certificatul cheii publice; c) date de identificare şi alte date ale titularului certificatului cheii publice, în funcţie de scopul pentru care se eliberează certificatul, precum şi informaţiile necesare pentru comunicarea cu acesta; d) cheia publică; e) data şi ora la care începe şi încetează termenul de valabilitate a certificatului cheii publice;	Compatibil			

(f) indicarea începutului şi a sfîrşitului perioadei de valabilitate a certificatului; (g) codul de identitate al certificatului; (h) semnătura electronică avansată a prestatorului de servicii de certificare care eliberează certificatul; (i) limitele sferei de utilizare a certificatului, după caz; (j) limitele valorii tranzacţiilor pentru care poate fi utilizat certificatul, atunci când este cazul.	f) date despre algoritmul criptografic al semnăturii electronice; g) după caz, restricţiile la utilizarea certificatului cheii publice sau limitele valorii operaţiunilor în care acesta poate fi utilizat; h) alte informaţii stabilite de prezenta lege. **Articolul 32 alin (3)** ***Certificatul calificat al cheii publice*** se emite de către prestatorul de servicii de certificare acreditat şi suplimentar trebuie să conţină următoarele informaţii: a) menţiune care să indice că certificatul este eliberat ca certificat calificat; b) posibilitatea includerii, atunci cînd este cazul, a unei calităţi speciale a semnatarului, în funcţie de utilizarea pe care urmează să o aibă certificatul; c) datele de verificare a semnăturii care corespund datelor de creare a semnăturii sub controlul semnatarului.				
Anexa II **Cerinţe privind prestatorii de servicii de certificare care eliberează certificate calificate** Prestatorii de servicii de certificare trebuie: (a) să demonstreze fiabilitatea necesară	**Articolul 29** (1) Prestatorul de servicii de certificare este obligat: a) să verifice autenticitatea datelor indicate în cererea de certificare a cheii publice în baza documentelor ce confirmă datele în cauză;	Compatibil			

pentru a presta servicii de certificare; (b) să asigure funcţionarea unui serviciu prompt de repertorizare şi a unui serviciu imediat de revocare; (c) să se asigure că data şi ora eliberării sau a revocării unui certificat pot fi determinate cu exactitate; (d) să verifice, prin mijloace corespunzătoare şi în conformitate cu dreptul intern, identitatea şi, atunci când este cazul, calităţile speciale ale persoanei pentru care se eliberează un certificat calificat; (e) să angajeze un personal care să deţină cunoştinţele specifice, precum şi experienţa şi calificările necesare pentru prestarea serviciilor, în special competenţe la nivel de gestionare, expertiză în domeniul tehnologiei semnăturilor electronice şi o bună practică a procedurilor de siguranţă adecvate; de asemenea, trebuie să ştie să aplice proceduri administrative şi de gestionare care să fie adecvate şi în conformitate cu standardele recunoscute; (f) să utilizeze sisteme şi produse fiabile care sunt protejate împotriva modificărilor şi să garanteze siguranţa tehnică şi criptografică a funcţiilor pe care şi le asumă; (g) să ia măsuri împotriva falsificării certificatelor şi, în cazul în care	b) să asigure corespunderea informaţiilor din certificatul cheii publice cu informaţiile prezentate de către titularul certificatului cheii publice; c) să introducă certificatul cheii publice în registrul certificatelor cheilor publice nu mai tîrziu de data şi ora cînd începe să curgă termenul de valabilitate a certificatului; d) să asigure accesul liber la registrul certificatelor cheilor publice; e) să suspende valabilitatea sau să revoce certificatul cheii publice în cazurile prevăzute de lege şi să facă menţiunea respectivă în registrul certificatelor cheilor publice, în termenele stabilite; f) să acopere prejudiciile aduse oricărei entităţi sau persoane fizice, care are încredere în mod rezonabil în datele conţinute în certificatul cheii publice eliberat de către prestatorul de servicii de certificare, prin faptul că a omis să înregistreze revocarea certificatului; g) să înştiinţeze titularul certificatului cheii publice despre faptele care au devenit cunoscute prestatorului de servicii de certificare şi care fac imposibilă utilizarea în continuare a cheii private, precum şi despre revocarea certificatului cheii publice;				

prestatorul de servicii de certificare generează date de creare de semnături, să garanteze confidenţialitatea în decursul procesului de creare a respectivelor date; (h) să deţină resurse financiare suficiente pentru a funcţiona în conformitate cu cerinţele prevăzute de prezenta directivă, în special pentru a suporta responsabilitatea pentru eventualele daune, încheind, de exemplu, o asigurare corespunzătoare; (i) să înregistreze, pe o perioadă corespunzătoare de timp, toate informaţiile pertinente referitoare la un certificat de calitate, în special pentru a putea furniza dovezi de certificare în justiţie. Înregistrările pot fi efectuate prin mijloace electronice; (j) să nu stocheze sau să copieze datele de creare a semnăturii ale persoanelor pentru care prestatorul de servicii de certificare a prestat servicii de gestionare a cheilor; (k) înainte să stabilească o relaţie contractuală cu o persoană care solicită un certificat în sprijinul semnăturii sale electronice, să informeze respectiva persoană, prin mijloace de comunicare durabile, cu privire la termenii şi condiţiile exacte ale utilizării certificatului, inclusiv cu privire la limitele impuse utilizării sale, la	h) să prezinte informaţiile necesare pentru autentificarea semnăturii electronice; i) să solicite eliberarea duplicatului certificatului de acreditare, în cazul pierderii sau deteriorării acestuia; k) să îndeplinească alte obligaţii stabilite de prezenta lege. (2) **Prestatorul de servicii de certificare acreditat în domeniul aplicării semnăturii electronice avansate calificate suplimentar este obligat:** a) să certifice, în modul stabilit de legislaţie, cheia publică a prestatorului de servicii de certificare acreditat în domeniul aplicării semnăturii electronice avansate calificate, destinată certificării cheilor publice; b) să înregistreze, pe o perioadă corespunzătoare de timp, în conformitate cu articolul 33 din prezenta lege, toate informaţiile pertinente referitoare la un certificat calificat, în special pentru a putea furniza dovezi de certificare în justiţie. Înregistrările pot fi efectuate prin mijloace electronice; c) înainte să stabilească o relaţie contractuală cu o persoană care solicită un certificat în sprijinul semnăturii sale electronice, să				

existenţa unui sistem voluntar de acreditare şi la procedurile de contestare şi soluţionare a litigiilor. Aceste informaţii, care pot fi transmise pe cale electronică, trebuie comunicate în scris şi într-un limbaj uşor de înţeles. Elementele pertinente ale informaţiilor trebuie puse, de asemenea, la cerere, la dispoziţia părţilor terţe care beneficiază de certificat; (l) să utilizeze sisteme fiabile pentru a stoca certificatele într-o formă care poate fi verificată, astfel încât: — numai persoanele autorizate să poată introduce şi modifica date; — autenticitatea informaţiei să poată fi controlată; — certificatele să fie disponibile publicului pentru cercetări numai în cazul în care titularul certificatului şi-a dat consimţământul în acest sens şi — toate modificările tehnice care periclitează cerinţele de siguranţă să fie vizibile pentru operator.	informeze respectiva persoană, prin mijloace de comunicare fiabile, cu privire la termenele şi condiţiile exacte de utilizare a certificatului, inclusiv cu privire la limitele impuse utilizării sale, la existenţa unui sistem de acreditare şi la procedurile de contestare şi soluţionare a litigiilor. Aceste informaţii, care pot fi transmise pe cale electronică, trebuie comunicate în scris şi într-un limbaj accesibil. Elementele pertinente ale informaţiilor trebuie puse, de asemenea, la cerere, la dispoziţia părţilor terţe care beneficiază de certificat; d) să păstreze toată informaţia cu privire la certificatul cheii publice ataşat semnăturilor electronice avansate calificate cel puţin 15 ani din momentul revocării sau expirării certificatului, în eventualitatea apariţiei unor litigii.				
Anexa III **Cerinţe privind dispozitivele securizate de creare a semnăturilor** 1. Dispozitivele securizate de creare a semnăturii trebuie cel puţin să asigure, prin mijloace tehnice şi proceduri corespunzătoare, că: (a) datele de creare a semnăturii utilizate pentru crearea semnăturii nu	**Articolul 8 alin (4) şi (5)** (4) Dispozitivele securizate de creare a semnăturii electronice trebuie cel puţin să asigure, prin mijloace tehnice şi proceduri corespunzătoare, că: a) datele de creare a semnăturii utilizate pentru crearea semnăturii nu sînt aplicate decît o singură dată,	Compatibil			

sunt aplicate decât o singură dată, iar confidenţialitatea lor este asigurată în mod rezonabil; (b) datele de creare a semnăturii utilizate pentru crearea semnăturii nu pot fi deduse şi că semnătura este protejată împotriva oricărei falsificări prin mijloace tehnice disponibile la acea dată; (c) datele de creare a semnăturii utilizate la crearea semnăturii pot fi protejate în mod fiabil de semnatarul legitim împotriva utilizării de către alte persoane. 2. Dispozitivele securizate de creare a semnăturii nu trebuie să modifice datele care urmează să fie semnate sau să împiedice prezentarea lor semnatarului înainte de procesul de semnare.	iar confidenţialitatea acestora este asigurată în conformitate cu prezenta lege; b) datele de creare a semnăturii utilizate pentru crearea semnăturii electronice nu pot fi deduse şi că semnătura este protejată împotriva oricărei posibile falsificări prin mijloace tehnice disponibile la acea dată; c) datele de creare a semnăturii utilizate la crearea semnăturii electronice trebuie să fie protejate în mod fiabil de semnatarul legitim împotriva utilizării de către alte persoane. (5) Dispozitivele securizate de creare a semnăturii electronice nu trebuie să modifice datele care urmează să fie semnate sau să împiedice prezentarea lor semnatarului înainte de procesul de semnare.				