

REPUBLICA MOLDOVA
SERVICIUL DE INFORMAȚII
ȘI SECURITATE



РЕСПУБЛИКА МОЛДОВА
СЛУЖБА ИНФОРМАЦИИ И
БЕЗОПАСНОСТИ

ORDIN
cu privire la aprobarea Normelor tehnice în domeniul semnăturii digitale

nr. 64 din 07.12.2006

Monitorul Oficial nr.112-116/481 din 03.08.2007

* * *

Întru executarea Hotărîrii Guvernului nr.945 din 5 septembrie 2005 “Cu privire la centrele de certificare a cheilor publice” (Monitorul Oficial al Republicii Moldova, 2005, nr.123-125, art.1020), în temeiul art.36 alin.(2) al Legii nr.264-XV din 15 iulie 2004 cu privire la documentul electronic și semnătura digitală (Monitorul Oficial al Republicii Moldova, 2004, nr.132-137, art.710)

ORDON:

1. Se aprobă Normele tehnice în domeniul semnăturii digitale (se anexează).
2. Controlul executării prezentului ordin se atribuie domnului Valentin Dediu, director adjunct al Serviciului de Informații și Securitate al Republicii Moldova.
3. Prezentul ordin intră în vigoare la data publicării în Monitorul Oficial al Republicii Moldova.

**DIRECTORUL SERVICIULUI
DE INFORMAȚII ȘI SECURITATE**

Ion URSU

Chișinău, 7 decembrie 2006.
Nr.64.

Aprobate
prin Ordinul directorului Serviciului
de Informații și Securitate
al Republicii Moldova
nr.64 din 7 decembrie 2006

NORME TEHNICE
în domeniul semnăturii digitale

I. DISPOZIȚII GENERALE

1. Prezentele Norme tehnice sînt elaborate în conformitate cu Legea nr.264-XV din 15 iulie 2004 cu privire la documentul electronic și semnătura digitală, Hotărîrea Guvernului nr.945 din 5 septembrie 2005 “Cu privire la centrele de certificare a cheilor publice” și stabilesc normele și cerințele de conformitate cu standardele și recomandările în domeniul semnăturii digitale, principiile de formare a infrastructurii cheilor publice, creare și administrare a cheilor publice, private și a certificatelor cheilor publice, creare și verificare a semnăturii digitale și de fixare a timpului.

2. Prezentele Norme tehnice reprezintă un document de reglementare în domeniul semnăturii digitale și sînt obligatorii pentru persoanele juridice care prestează servicii de certificare a cheilor publice și alte servicii ce țin de semnătura digitală, precum și pentru utilizatorii semnăturii digitale.

3. În sensul prezentului document următoarele noțiuni și abrevieri semnifică:
statutul certificatului – starea certificatului cheii publice la un timp determinat. Statutul certificatului este determinat de lista certificatelor revocate;

funcție hash – funcție criptografică care corespunde următoarelor condiții: funcția este unidirecționată și posedă complicitate algoritmică înaltă de depistare a coliziunilor;

fixarea timpului – procedură de atribuire documentului electronic a unei mărci temporale astfel încât să se excludă posibilitatea modificării documentului cu păstrarea mărcii temporale atribuite anterior;

marcă temporală (time-stamp) – atribut al documentului electronic care, prin semnătura digitală, adevărește că informația a existat la un timp determinat;

CWA (CEN Workshop agreement) – Acordul grupului de lucru al Comitetului European de Standardizare. Textele de referință sînt publicate pe site-ul www.cenorm.be;

DSA (Digital Signature Algorithm) – algoritm criptografic asimetric al semnăturii digitale. Textele de referință sînt publicate pe site-ul www.nist.gov;

FIPS (Federal Information Processing Standard) – standard federal de prelucrare a informației. Textele de referință sînt publicate pe site-ul www.nist.gov;

IETF (Internet Engineering Task Force) – Grup operativ al ingineriei Internetului. Textele de referință sînt publicate pe site-ul www.ietf.org;

ISO/IEC (International Organization for Standardization / International Electrotechnical Commission) – Organizația Internațională de Standardizare / Comisia Internațională pentru Electrotehnică. Site-ul oficial www.iso.org;

ITU-T (International Telecommunication Union Telecommunication Standardization Sector) – standard al Uniunii Internaționale de Telecomunicații în domeniul telecomunicațiilor. Textele de referință sînt publicate pe site-ul www.itu.int;

PKCS (Public Key Cryptography Standards) – standarde criptografice cu cheia publică. Textele de referință sînt publicate pe site-ul www.rsalaboratory.com;

RFC (Request for comments) – recomandări ce aprobă documente supuse analizei publice în cadrul procesului coordonat cu Grupul operativ al ingineriei Internetului. Textele de referință sînt publicate pe site-ul www.ietf.org/rfc;

RSA (Rivest, Shamir, Adleman) – algoritm criptografic asimetric al semnăturii digitale, elaborat de către cercetătorii Rivest, Shamir și Adleman. Textele de referință sînt publicate pe site-ul www.rsalaboratory.com;

SM – standard național al Republicii Moldova;

validarea datelor și protocolul serverului de certificare – procedura de confirmare a validității și corectitudinii documentelor electronice semnate cu semnătura digitală, valabilității certificatelor cheilor publice și posedării sau existenței datelor.

[Pct.3 completat prin Ordinul SIS nr.32 din 23.06.2010, în vigoare 02.07.2010]

II. CREAREA ȘI ADMINISTRAREA CHEILOR PUBLICE ȘI PRIVATE

4. Cheile publice și private ale persoanelor împuternicite ale centrelor de certificare a cheilor publice (în continuare – centre de certificare) și ale utilizatorilor semnăturii digitale se creează cu mijloacele semnăturii digitale în conformitate cu cerințele standardului FIPS 140-2 Security Requirements For Cryptographic Modules, nivelele 3 sau 4, sau SMV CWA 14169:2008 Dispozitive de siguranță pentru crearea semnăturilor “EAL4+” sau SMV ISO/CEI 19790:2008 Tehnologia informației. Tehnici de securitate. Cerințe de securitate pentru module criptografice.

[Pct.4 în redacția Ordinului SIS nr.32 din 23.06.2010, în vigoare 02.07.2010]

[Pct.5 exclus prin Ordinul SIS nr.32 din 23.06.2010, în vigoare 02.07.2010]

6. Lungimea minimă a cheilor publice și private constituie:

- 1) 2048 biți pentru algoritmul RSA pentru utilizatorii semnăturii digitale;
- 2) 4096 biți pentru algoritmul RSA pentru centrele de certificare;
- 3) 2048 biți pentru algoritmul DSA;
- 4) 160 biți pentru algoritmul DSA pe baza curbelor eliptice;
- 5) 512 biți pentru algoritmul SM GOST 34.10:2006.

7. Lungimile cheilor publice și private ale persoanelor împuternicite ale centrelor de certificare trebuie să fie mai mari decât lungimile cheilor publice și private ale persoanelor împuternicite ale centrelor de certificare de nivel ierarhic inferior și ale utilizatorilor semnăturii digitale care certifică cheile publice în aceste centre.

8. Administrarea cheilor publice și private se efectuează în conformitate cu recomandările IETF RFC 4210 Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP), IETF RFC 4211 Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF).

9. Termenul de valabilitate a cheii private a persoanei împuternicite a centrului de certificare constituie:

2 ani și 6 luni – pentru centrul de certificare de nivel superior;

1 an și 3 luni – pentru centrele de certificare de nivelul al doilea;

7 luni – pentru centrele de certificare de nivelul al treilea.

Începutul termenului de valabilitate a cheii private se consideră data și ora la care începe termenul de valabilitate a certificatului cheii publice ce-i corespunde.

10. Termenul de valabilitate a certificatului cheii publice, ce corespunde cheii private a persoanei împuternicite a centrului de certificare, constituie:

5 ani – pentru centrul de certificare de nivel superior;

2 ani și 6 luni – pentru centrele de certificare de nivelul al doilea;

1 an și 3 luni – pentru centrele de certificare de nivelul al treilea.

10¹. Termenul de valabilitate a cheii private a serviciului de marcă temporară (TSP), serviciului de verificare on-line a statutului certificatului (OCSP), serviciului de validare a datelor și protocolul serverului de certificare (DVCS) și certificatului cheii publice, ce corespunde cheii private a serviciului, constituie 2 ani și 6 luni.

[Pct.10¹ introdus prin Ordinul SIS nr.32 din 23.06.2010, în vigoare 02.07.2010]

10². Termenul de valabilitate a cheii private a utilizatorului semnăturii digitale și certificatului cheii publice, ce corespunde cheii private a utilizatorului semnăturii digitale, constituie 1 an.

[Pct.10² introdus prin Ordinul SIS nr.32 din 23.06.2010, în vigoare 02.07.2010]

11. Cheile private ale persoanelor împuternicite ale centrelor de certificare și ale utilizatorilor semnăturii digitale se păstrează pe suporturi materiale ce realizează funcții criptografice. Operațiunile criptografice de semnare cu utilizarea cheii private trebuie să fie efectuate în microcipul suportului material.

12. Suportul material, ce conține cheia privată a persoanei împuternicite a centrului de certificare și a utilizatorului semnăturii digitale, trebuie să corespundă cerințelor standardului FIPS 140-2 Security Requirements For Cryptographic Modules, nivelele 3 sau 4, sau SMV CWA 14169:2008 Dispozitive de siguranță pentru crearea semnăturilor “EAL4+” sau SMV ISO/CEI 19790:2008 Tehnologia informației. Tehnici de securitate. Cerințe de securitate pentru module criptografice.

[Pct.12 în redacția Ordinului SIS nr.32 din 23.06.2010, în vigoare 02.07.2010]

13. Suportul material ce conține cheia privată a utilizatorului semnăturii digitale suplimentar la standardele enumerate în punctul 12 trebuie să corespundă și cerințelor standardului PKCS#15 Cryptographic Token Information Syntax Standard.

[Pct.13 în redacția Ordinului SIS nr.32 din 23.06.2010, în vigoare 02.07.2010]

14. Schimbarea planificată a cheilor publice și private ale persoanelor împuternicite ale centrelor de certificare se efectuează nu mai devreme de o lună înainte și nu mai târziu de expirarea termenului de valabilitate a cheii private.

15. Schimbarea neplanificată a cheilor publice și private ale persoanelor împuternicite ale centrelor de certificare se efectuează în cazul compromiterii sau al pericolului de compromitere a cheii private.

16. În cadrul procedurii de schimbare a cheilor publice și private ale persoanei împuternicite a centrului de certificare de nivel superior, această persoană:

crează o pereche nouă de chei (privată și publică);

crează certificatul cheii publice sub formă de document electronic ce conține cheia publică veche și îl semnează cu semnătura digitală folosind cheia privată nouă;

crează certificatul cheii publice sub formă de document electronic ce conține cheia publică nouă și îl semnează cu semnătura digitală folosind cheia privată, a cărei termen de valabilitate expiră;

crează certificatul cheii publice sub formă de document electronic ce conține cheia publică nouă și îl semnează cu semnătura digitală folosind cheia privată nouă.

17. În cadrul procedurii de schimbare a cheilor publice și private ale persoanei împuternicite a centrului de certificare de nivelul al doilea sau al treilea, această persoană:

crează o pereche nouă de chei (privată și publică);

certifică cheia publică nouă în centrul de certificare de nivel ierarhic superior.

18. Cheia privată veche a persoanei împuternicite a centrului de certificare își pierde valabilitatea la data creării certificatului cheii publice noi. Certificatul cheii publice vechi a persoanei împuternicite a centrului de certificare își păstrează valabilitatea pînă la expirarea termenului.

19. La expirarea termenului de valabilitate a cheii private, ea se folosește pînă la expirarea termenului de valabilitate a certificatului cheii publice ce corespunde acestei chei private numai pentru semnarea listei certificatelor revocate.

[Pct.19 în redacția Ordinului SIS nr.32 din 23.06.2010, în vigoare 02.07.2010]

19¹. După expirarea termenului de valabilitate a certificatului cheii publice ce corespunde chei private menționate la pct.19, cheia privată se distruge.

[Pct.19¹ introdus prin Ordinul SIS nr.32 din 23.06.2010, în vigoare 02.07.2010]

20. Certificatul cheii publice a persoanei împuternicite a centrului de certificare de nivel superior, ce conține cheia publică nouă și este semnat cu semnătura digitală folosind cheia privată a cărei termen de valabilitate expiră, precum și certificatul cheii publice a persoanei împuternicite a centrului de certificare de nivel superior, ce conține cheia publică veche și este semnat cu semnătura digitală folosind cheia privată nouă, își păstrează valabilitatea pînă la expirarea termenului de valabilitate a certificatului cheii publice vechi.

21. Procedura de schimbare a cheilor publice și private ale utilizatorilor semnăturii digitale se determină de către utilizatorii semnăturii digitale în conformitate cu recomandările IETF RFC 4210 Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP), IETF RFC 4211 Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF).

III. CREAREA ȘI ADMINISTRAREA CERTIFICATELOR CHEILOR PUBLICE

22. Procedurile de certificare a cheilor publice (identificarea, autentificarea și înregistrarea utilizatorilor semnăturii digitale, recepționarea cererilor de certificare a cheilor publice, crearea certificatelor cheilor publice, suspendarea, restabilirea valabilității și revocarea certificatelor) se efectuează în conformitate cu recomandarea IETF RFC 3647 Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

23. Administrarea certificatelor cheilor publice se efectuează în conformitate cu recomandările IETF RFC 4210 Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP), IETF RFC 4211 Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF).

24. Cererile de certificare a cheilor publice sub formă de document electronic se întocmesc în conformitate cu cerințele standardului PKCS=10: Certification Request Syntax Specification, versiunea 1.7, sau cu recomandarea IETF RFC 2986 Certification Request Syntax Specification.

25. Certificatele cheilor publice sub formă de document electronic trebuie să corespundă cerințelor standardului ITU-T X.509, versiunea 3, standardului SMV ISO CEI 9594-8:2007 Tehnologia informației. Interconexiunea sistemelor deschise. Linii directe: Structura certificatului cheii publice și a atributului sau recomandării IETF RFC 5280 Internet X.509 Public Key

Infrastructure Certificate and Certificate Revocation List (CRL) Profile și IETF RFC 3739 Qualified Certificates Profile. Structurile certificatelor cheilor publice ale persoanelor împuternicite ale centrelor de certificare și ale utilizatorilor semnăturii digitale sînt prezentate în anexele 1 și 2 la prezentele Norme tehnice.

[Pct.25 modificat prin Ordinul SIS nr.32 din 23.06.2010, în vigoare 02.07.2010]

26. Listele certificatelor revocate trebuie să corespundă cerințelor standardului ITU-T X.509, versiunea 2, standardului SMV ISO CEI 9594-8:2007 Tehnologia informației. Interconexiunea sistemelor deschise. Linii directoare: Structura certificatului cheii publice și a atributului sau recomandării IETF RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Structura listei certificatelor revocate este prezentată în anexa nr.4 la prezentele Norme tehnice.

[Pct.26 modificat prin Ordinul SIS nr.32 din 23.06.2010, în vigoare 02.07.2010]

27. Ora suspendării sau restabilirii valabilității certificatului cheii publice se consideră ora publicării (emiterii) listei actualizate a certificatelor revocate (ora indicată în câmpul thisUpdate).

28. Statutul certificatului cheii publice se stabilește în conformitate cu una din următoarele recomandări:

- 1) IETF RFC 2560 Internet X.509 Public Key Infrastructure Online Certificate Status Protocol;
- 2) IETF RFC 2585 Internet X.509 Public Key Infrastructure Operational Protocols: FTP, HTTP;
- 3) IETF RFC 3494 Lightweight Directory Access Protocol version 2 (LDAPv2) to Historic Status;
- 4) IETF RFC 4523 Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates.

[Pct.28 modificat prin Ordinul SIS nr.32 din 23.06.2010, în vigoare 02.07.2010]

28¹. Structura certificatului serviciului verificării on-line a statutului certificatului (OCSP) este prezentată în anexa nr.3 la prezentele Norme tehnice.

[Pct.28¹ introdus completat prin Ordinul SIS nr.32 din 23.06.2010, în vigoare 02.07.2010]

IV. CREAREA ȘI VERIFICAREA SEMNĂTURII DIGITALE

29. Semnătura digitală se creează cu mijloacele semnăturii digitale în conformitate cu cerințele standardului SMV CWA 14170:2007 Cerințele de securitate pentru aplicațiile de creare a semnăturii.

30. Verificarea semnăturii digitale se efectuează cu mijloacele semnăturii digitale în conformitate cu cerințele standardului SMV CWA 14171:2007 Ghid general pentru verificarea semnăturii electronice.

31. Formatul semnăturii digitale trebuie să corespundă cerințelor standardului PKCS#7 Cryptographic Message Syntax Standard sau IETF RFC 5126 CMS Advanced Electronic Signatures (CAAdES) și XML Advanced Electronic Signatures (XAdES).

[Pct.31 completat prin Ordinul SIS nr.32 din 23.06.2010, în vigoare 02.07.2010]

32. Algoritmii de creare și verificare a semnăturii digitale trebuie să corespundă cerințelor prevăzute de unul din următoarele standarde și recomandări:

- 1) SM ISO/CEI 9796-2:2006 Tehnologia informației. Tehnici de securitate. Scheme de semnături digitale care restabilesc mesaje. Partea 2: Mecanisme bazate pe factorizarea întregului; SM ISO/CEI 9796-3:2006 Tehnologia informației. Tehnici de securitate. Scheme de semnături digitale care restabilesc mesaje. Partea 3: Mecanisme bazate pe logaritm discret;
- 2) SM ISO/CEI 14888-1:2006 Tehnologia informației. Tehnici de securitate. Semnături digitale cu supliment. Partea 1: Generalități; SM ISO/CEI 14888-2:2006 Tehnologia informației. Tehnici de securitate. Semnături digitale cu supliment. Partea 2: Mecanisme bazate pe identitate; SM ISO/CEI 14888-3:2006 Tehnologia informației. Tehnici de securitate. Semnături digitale cu supliment. Partea 3: Mecanisme bazate pe certificat;

3) SM GOST R 34.10:2006 Tehnologia informațională. Securitatea criptografică a informației. Procesele de formare și verificare a semnăturii digitale;

4) IETF RFC 3447 Public Key Cryptography Standards PKCS=1: RSA Cryptography Specifications, versiunea 2.1;

5) FIPS Publication 186-3 Digital Signature Standard (DSS) sau SMV ISO/CEI 14888-2-2009 Tehnologia informației. Tehnici de securitate. Semnături digitale cu anexă. Partea 2: Mecanisme bazate pe o descompunere în factori a unui întreg.

[Pct.32 modificat prin Ordinul SIS nr.32 din 23.06.2010, în vigoare 02.07.2010]

33. Algoritmii funcției hash trebuie să corespundă cerințelor prevăzute de unul din următoarele standarde:

1) SM ISO/CEI 10118-1:2006 Tehnologia informației. Tehnici de securitate. Funcții hash. Partea 1: Generalități; SM ISO/CEI 10118-2:2006 Tehnologia informației. Tehnici de securitate. Funcții hash. Partea 2: Funcții hash utilizând un algoritm de cifrare pe blocuri de n biți; SM ISO/CEI 10118-3:2006 Tehnologia informației. Tehnici de securitate. Funcții hash. Partea 3: Funcții hash dedicate; SM ISO/CEI 10118-4:2006 Tehnologia informației. Tehnici de securitate. Funcții hash. Partea 4: Funcții hash utilizând aritmetica modulară;

2) SM GOST R 34.11:2006 Tehnologia informațională. Securitatea criptografică a informației. Funcția hash;

3) FIPS Publication 180-3 Secure Hash Standard (SHS) sau SM ISO/CEI 10118-3:2006 Tehnologia informației. Tehnici de securitate. Funcții hash. Partea 3: Funcții hash dedicate.

[Pct.33 completat prin Ordinul SIS nr.32 din 23.06.2010, în vigoare 02.07.2010]

V. FIXAREA TIMPULUI

34. Atribuirea mărcii temporale se efectuează în conformitate cu cerințele recomandării IETF RFC 3161 Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).

35. Sincronizarea timpului serviciilor de certificare, inclusiv al mijloacelor tehnice și de program conform destinației, se efectuează în conformitate cu recomandarea IETF RFC 4330: Simple Network Time Protocol (SNTP) sau IETF RFC 1305 :Network Time Protokol (NTP).

[Pct.35 completat prin Ordinul SIS nr.32 din 23.06.2010, în vigoare 02.07.2010]

36. Structura certificatului serviciului de marcă temporală (TSP) este prezentată în anexa nr.3 la prezentele Norme tehnice.

[Pct.36 introdus prin Ordinul SIS nr.32 din 23.06.2010, în vigoare 02.07.2010]

VI. VALIDAREA DATELOR ȘI PROTOCOLUL SERVERULUI DE CERTIFICARE

37. Validarea datelor și protocolul serverului de certificare se efectuează în conformitate cu cerințele recomandării IETF RFC 3029 Data Validation and Certification Server Protocols (DVCS).

38. Structura certificatului serviciului validării datelor și protocolul serverului de certificare (DVCS) este prezentată în anexa nr.3 la prezentele Norme tehnice.

[Cap.VI introdus prin Ordinul SIS nr.32 din 23.06.2010, în vigoare 02.07.2010]

**Structura certificatului cheii publice a persoanei împuternicite
a centrului de certificare**

Certificatul cheii publice a persoanei împuternicite a centrului de certificare conține următoarele câmpuri:

Denumirea (în engleză)	Descrierea	Conținutul	Notă
Câmpurile de bază			
Version	Versiunea	V3	
Serial Number	Numărul de înregistrare a certificatului	Numărul	
Issuer	Datele de identificare ale centrului de certificare, emitent al certificatului	CN = Denumirea certificatului centrului de certificare L = Localitatea S = Statul OU = Subdiviziunea persoanei juridice numele, prenumele persoanei împuternicite a centrului de certificare, IDNP O = Denumirea persoanei juridice, IDNO C = Codul statului	
Validity	Termenul de valabilitate a certificatului	Valabil de la: “_” ____ 20__ oo:mm:ss GMT Valabil pînă la: “_” ____ 20__ oo:mm:ss GMT	
Subject	Datele de identificare ale centrului de certificare, titular al certificatului	CN = Denumirea certificatului centrului de certificare L = Localitatea S = Statul OU = Subdiviziunea persoanei juridice numele, prenumele persoanei împuternicite a centrului de certificare, IDNP O = Denumirea persoanei juridice, IDNO C = Codul statului	
Subject Public Key Info	Cheia publică	Cheia publică a persoanei împuternicite a centrului de certificare	
Signature Algorithm	Algoritmul semnăturii emitentului certificatului	Denumirea algoritmului semnăturii digitale a emitentului certificatului	
Signature Value	Semnătura digitală a emitentului certificatului	Semnătura emitentului în conformitate cu algoritmul utilizat	
Câmpurile auxiliare			
Authority Key Identifier	Identificatorul cheii emitentului certificatului	Identificatorul cheii private a persoanei împuternicite a centrului de certificare, emitentului certificatului	Numai în certifica tele centro r de certifica re subordo nate
Subject Key Identifier	Identificatorul cheii titularului certificatului	Identificatorul cheii private a persoanei împuternicite a centrului de certificare, corespunzătoare prezentului certificat	
Key Usage	Utilizarea cheii	Semnătura digitală în certificate, semnătura digitală în lista certificatelor revocate	CRITIC
Private Key Usage Period	Termenul de valabilitate a cheii private	Nu mai târziu de: “_” ____ 20__ oo:mm:ss GMT	
Certificate Policies	Politica de certificare a	Identificatorul politicii = toate politicile de emitere.	Poate fi

	centrului de certificare	Informațiile calificatorului politicii	CRITIC
Basic Constraints	Restricții de bază	Tipul subiectului = CA Limitarea lungimii lanțului de certificate = lipsește (în certificatul centrului de certificare de nivel superior), sau = 1 (în caz de emitere a certificatelor pentru centrele de certificare subordonate și utilizatorii semnăturii digitale) și = 0 (în caz de emitere a certificatelor numai pentru utilizatorii semnăturii digitale)	CRITIC
CRL Distribution Point	Punctul de distribuție a listei certificatelor revocate	Sursa publicării listei certificatelor revocate	
Authority Information Access	Accesul la informațiile despre centrul de certificare	Modalitatea de acces la informațiile despre centrul de certificare	Numai în certificatele centrelor de certificare subordonate

[Anexa nr.1 în redacția Ordinului SIS nr.32 din 23.06.2010, în vigoare 02.07.2010]

Anexa nr.2
la Normele tehnice în
domeniul semnăturii digitale

Structura certificatului cheii publice a utilizatorului semnăturii digitale

Certificatul cheii publice a utilizatorului semnăturii digitale conține următoarele câmpuri:

Denumirea (în engleză)	Descrierea	Conținutul	Notă
Câmpurile de bază			
Version	Versiunea	V3	
Serial Number	Numărul de înregistrare a certificatului	Numărul	
Issuer	Datele de identificare ale centrului de certificare, emitent al certificatului	CN = Denumirea certificatului centrului de certificare L = Localitatea S = Statul OU = Subdiviziunea persoanei juridice numele, prenumele persoanei împuternicite a centrului de certificare, IDNP O = Denumirea persoanei juridice, IDNO C = Codul statului	
Validity	Termenul de valabilitate a certificatului	Valabil de la: “_” ____ 20__ oo:mm:ss GMT Valabil până la: “_” ____ 20__ oo:mm:ss GMT	
Subject	Datele de identificare ale utilizatorului semnăturii digitale, titular al certificatului	Serialnumber = IDNP a utilizatorului semnăturii digitale CN = Numele, prenumele utilizatorului semnăturii digitale L = Localitatea de domiciliu a utilizatorului semnăturii digitale S = Statul OU = Subdiviziunea persoanei juridice, în care activează utilizatorul semnăturii digitale, după caz O = Denumirea persoanei juridice, IDNO, în care activează utilizatorul semnăturii digitale, după caz P = Telefonul utilizatorului semnăturii digitale, după caz	

		T = Funcția deținută de către utilizatorul semnăturii digitale, după caz C = Codul statului	
Subject Public Key Info	Cheia publică	Cheia publică a utilizatorului semnăturii digitale	
Signature Algorithm	Algoritmul semnăturii emitentului certificatului	Denumirea algoritmului semnăturii digitale a emitentului certificatului	
Signature Value	Semnătura digitală a emitentului certificatului	Semnătura emitentului în conformitate cu algoritmul utilizat	
Cîmpurile auxiliare			
Authority Key Identifier	Identificatorul cheii emitentului certificatului	Identificatorul cheii private a persoanei împuternicite a centrului de certificare, emitentului certificatului	
Subject Key Identifier	Identificatorul cheii titularului certificatului	Identificatorul cheii private a utilizatorului semnăturii digitale, corespunzătoare prezentului certificat	
Key Usage	Utilizarea cheii	Irevocabilitatea	CRITIC
Certificate Policies	Politica de certificare a centrului de certificare	Identificatorul politicii Informațiile calificatorului politicii	Poate fi CRITIC
Subject Alternative Name	Numele alternativ al titularului certificatului	RFC822 Name = Poșta electronică a utilizatorului semnăturii digitale	
Basic Constraints	Restricții de bază	Tipul subiectului = utilizatorul final Limitarea lungimii lanțului de certificate = lipsește	Poate fi și poate fi CRITIC
CRL Distribution Point	Punctul de distribuție a listei certificatelor revocate	Sursa publicării listei certificatelor revocate	
Authority Information Access	Accesul la informațiile despre centrul de certificare	Modalitatea de acces la informațiile despre centrul de certificare	
Qualified certificate Statements	Criteriu ce determină că certificatul este destinat pentru formarea semnăturii cu putere juridică	Identificatorul certificatului, ce determină că certificatul este destinat pentru formarea semnăturii cu putere juridică în conformitate cu actele normative în domeniul semnăturii digitale, poate conține restricții cu privire la aplicarea acestui certificat.	

[Anexa nr.2 în redacția Ordinului SIS nr.32 din 23.06.2010, în vigoare 02.07.2010]

Anexa nr.3
la Normele tehnice în
domeniul semnăturii digitale

**Structura certificatului cheii publice a serviciului de marcă temporală (TSP),
serviciului verificării on-line a statutului certificatului (OCSP) și a
serviciului validării datelor și protocolul serverului
de certificare (DVCS)**

Certificatul cheii publice a serviciilor TSP, OCSP sau DVCS conține următoarele cîmpuri:

Denumirea (în engleză)	Descrierea	Conținutul	Notă
Cîmpurile de bază			
Version	Versiunea	V3	
Serial Number	Numărul de înregistrare a certificatului	Numărul	
Issuer	Datele de identificare ale centrului de certificare, emitent al certificatului	CN = Denumirea certificatului centrului de certificare L = Localitatea S = Statul	

		OU = Subdiviziunea persoanei juridice numele, prenumele persoanei împuternicite a centrului de certificare, IDNP O = Denumirea persoanei juridice, IDNO C = Codul statului	
Validity	Termenul de valabilitate a certificatului	Valabil de la: “_”_ 20__ oo:mm:ss GMT Valabil pînă la: “_”_ 20__ oo:mm:ss GMT	
Subject	Datele de identificare al centrului de certificare	CN = Denumirea certificatului centrului de certificare L = Localitatea S = Statul OU = Subdiviziunea persoanei juridice O = Denumirea persoanei juridice, IDNO C = Codul statului	
Subject Public Key Info	Cheia publică	Cheia publică a persoanei împuternicite a centrului de certificare	
Signature Algorithm	Algoritmul semnăturii emitentului certificatului	Denumirea algoritmului semnăturii digitale a emitentului certificatului	
Signature Value	Semnătura digitală a emitentului certificatului	Semnătura emitentului în conformitate cu algoritmul utilizat	
Cîmpurile auxiliare			
Authority Key Identifier	Identificatorul cheii emitentului certificatului	Identificatorul cheii private a persoanei împuternicite a centrului de certificare, emitentului certificatului	
Subject Key Identifier	Identificatorul cheii titularului certificatului	Identificatorul cheii private a persoanei împuternicite a centrului de certificare, corespunzătoare prezentului certificat	
Key Usage	Utilizarea cheii	Irevocabilitatea, semnătura digitală	NE-CRITIC
Certificate Policies	Politica de certificare a centrului de certificare	Identificatorul politicii = toate politicile de emitere. Informațiile calificatorului politicii	Poate fi CRITIC
Basic Constraints	Restricții de bază	Tipul subiectului = utilizatorul final Limitarea lungimii lanțului de certificate = lipsește	Poate fi și poate fi CRITIC
CRL Distribution Point	Punctul de distribuție a listei certificatelor revocate	Sursa publicării listei certificatelor revocate	
Extended Key Usage	Domeniul extins de utilizare a cheii	Identificatorul ce determină că certificatul este destinat pentru serviciul de marcă temporară (TSP), pentru serviciului verificării on-line a statutului certificatului (OCSP) sau pentru serviciul validării datelor și protocolul serverului de certificare (DVCS)	CRITIC
Authority Information Access	Accesul la informațiile despre centrul de certificare	Modalitatea de acces la informațiile despre centrul de certificare	

[Anexa nr.3 în redacția Ordinului SIS nr.32 din 23.06.2010, în vigoare 02.07.2010]

Anexa nr.4
la Normele tehnice în
domeniul semnăturii digitale

Structura listei certificatelor revocate (CRL)

Lista certificatelor revocate a centrului de certificare conține următoarele cîmpuri:

Denumirea	Descrierea	Conținutul	Notă
-----------	------------	------------	------

(în engleză)		
Cîmpurile de bază		
Version	Versiunea	V2
Signature	Algoritmul semnăturii emitentului CRL	Denumirea algoritmului semnăturii digitale a emitentului CRL
Issuer	Emitentul CRL	CN = Denumirea centrului de certificare L = Localitatea S = Statul OU = Subdiviziunea persoanei juridice numele, prenumele persoanei împuternicite a centrului de certificare, IDNP O = Denumirea persoanei juridice, IDNO C = Codul statului
This Update	Data emiterii CRL	"__" ____ 20__ oo:mm:ss GMT
Next Update	Data următoarei actualizări a CRL	"__" ____ 20__ oo:mm:ss GMT
Revoked Certificates	Lista certificatelor revocate	userCertificate Numărul de serie a certificatului (CertificateSerialNumber) revocationDate Data revocării sau suspendării valabilității certificatului (Time)
Signature Algorithm	Algoritmul semnăturii emitentului certificatului	Denumirea algoritmului semnăturii digitale a emitentului certificatului
Signature Value	Semnătura digitală a emitentului certificatului	Semnătura emitentului în conformitate cu algoritmul utilizat
Cîmpurile auxiliare		
Authority Key Identifier	Identificatorul cheii emitentului certificatului	Identificatorul cheii private a persoanei împuternicite a centrului de certificare, care a fost utilizat pentru semnarea CRL
CRL Number	Numărul de ordine	Numărul de ordine a CRL
Reason Code	Codul cauzei revocării certificatului	"0" Nu este indicată "1" Compromiterea cheii private "2" Compromiterea centrului de certificare "3" Schimbarea apartenenței "4" Certificatul a fost schimbat "5" Încetarea activității "6" Suspendarea valabilității

[Anexa nr.4 în redacția Ordinului SIS nr.32 din 23.06.2010, în vigoare 02.07.2010]

&

Serviciul de Informații și Securitate

Ordin nr.64 din 07.12.2006 cu privire la aprobarea Normelor tehnice în domeniul semnăturii digitale

//Monitorul Oficial 112-116/481, 03.08.2007