Republica Moldova

SERVICIUL DE INFORMAŢII ŞI SECURITATE

ORDIN Nr. 64
din 07.12.2006

cu privire la aprobarea Normelor tehnice în domeniul semnăturii digitale

Publicat : 03.08.2007 în Monitorul Oficial Nr. 112-116 art Nr : 481 Data intrarii in vigoare : 03.08.2007

MODIFICAT
OSIS32 din 23.06.10, MO110-113/02.07.10 art.390

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 şi semnătura digitală (Monitorul Oficial al Republicii Moldova, 2004, nr. 132-137, art. 710), –

O R D O N:

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 Informaţii şi Securitate al Republicii Moldova.
3. Prezentul ordin intră în vigoare la data publicării în Monitorul Oficial al Republicii Moldova.

DIRECTORUL SERVICIULUI
DE INFORMAŢII ŞI SECURITATE Ion URSU

Nr. 64. Chişinău, 7 decembrie 2006.

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

NORME TEHNICE
în domeniul semnăturii digitale

I. Dispoziţii generale

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

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

3. În sensul prezentului document următoarele noţiuni şi abrevieri semnifică:

statutul certificatului – starea certificatului cheii publice la un timp determinat. Statutul certificatului este determinat de lista certificatelor revocate;

funcţie hash – funcţie criptografică care corespunde următoarelor condiţii: funcţia este unidirecţionată şi posedă complicitate algoritmică înaltă de depistare a coliziunilor;

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

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

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

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

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

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

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

ITU-T (International Telecommunication Union Telecommunication Standardization Sector) – standard al Uniunii Internaţionale de Telecomunicaţii în domeniul telecomunicaţiilor. Textele de referinţă sînt publicate pe site-ul www.itu.int;

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

SM – standard naţional al Republicii Moldova.

validarea datelor şi protocolul serverului de certificare - procedura de confirmare a validităţii şi corectitudinii documentelor electronice semnate cu semnătura digitală, valabilităţii certificatelor cheilor publice şi posedării sau existenţei datelor.

[Pct.3 al.15) introdus prin OSIS32 din 23.06.10, MO110-113/02.07.10 art.390]

II. Crearea şi administrarea cheilor publice şi private

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

[Pct.4 în redacţia OSIS32 din 23.06.10, MO110-113/02.07.10 art.390]

[Pct.5 exclus prin OSIS32 din 23.06.10, MO110-113/02.07.10 art.390]

6. Lungimea minimă a cheilor publice şi private constituie:

1) 2048 biţi pentru algoritmul RSA pentru utilizatorii semnăturii digitale;

2) 4096 biţi pentru algoritmul RSA pentru centrele de certificare;

3) 2048 biţi pentru algoritmul DSA;

4) 160 biţi pentru algoritmul DSA pe baza curbelor eliptice;

5) 512 biţi pentru algoritmul SM GOST 34.10:2006.

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

8. Administrarea cheilor publice şi 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 şi 6 luni – pentru centrul de certificare de nivel superior;

1 an şi 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 şi 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 şi 6 luni – pentru centrele de certificare de nivelul al doilea;

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

10^1. 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 şi protocolul serverului de certificare (DVCS) şi certificatului cheii publice, ce corespunde cheii private a serviciului, constituie 2 ani şi 6 luni.

[Pct.10^1 introdus prin OSIS32 din 23.06.10, MO110-113/02.07.10 art.390]

10^2. Termenul de valabilitate a cheii private a utilizatorului semnăturii digitale şi certificatului cheii publice, ce corespunde cheii private a utilizatorului semnăturii digitale, constituie 1 an.

[Pct.10^2 introdus prin OSIS32 din 23.06.10, MO110-113/02.07.10 art.390]

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

12. Suportul material, ce conţine cheia privată a persoanei împuternicite a centrului de certificare şi a utilizatorului semnăturii digitale, trebuie să corespundă cerinţelor standardului

FIPS 140-2 Security Requirements For Cryptographic Modules, nivelele 3 sau 4, sau SMV CWA 14169:2008 Dispozitive de siguranţă pentru crearea semnăturilor "EAL4+" sau SMV ISO/CEI 19790:2008 Tehnologia informaţiei. Tehnici de securitate. Cerinţe de securitate pentru module criptografice.

[Pct.12 în redacţia OSIS32 din 23.06.10, MO110-113/02.07.10 art.390]

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

[Pct.13 în redacţia OSIS32 din 23.06.10, MO110-113/02.07.10 art.390]

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

15. Schimbarea neplanificată a cheilor publice şi 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 şi private ale persoanei împuternicite a centrului de certificare de nivel superior, această persoană:

creează o pereche nouă de chei (privată şi publică);

creează certificatul cheii publice sub formă de document electronic ce conţine cheia publică veche şi îl semnează cu semnătura digitală folosind cheia privată nouă;

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

creează certificatul cheii publice sub formă de document electronic ce conţine cheia publică nouă şi îl semnează cu semnătura digitală folosind cheia privată nouă.

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

creează o pereche nouă de chei (privată şi publică);

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

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

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

[Pct.19 în redacţia OSIS32 din 23.06.10, MO110-113/02.07.10 art.390]

19[1]. După expirarea termenului de valabilitate a certificatului cheii publice ce corespunde chei private menţionate la pct. 19, cheia privată se distruge.

[Pct.19[1] introdus prin OSIS32 din 23.06.10, MO110-113/02.07.10 art.390]

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

21. Procedura de schimbare a cheilor publice şi 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 şi administrarea certificatelor cheilor publice

22. Procedurile de certificare a cheilor publice (identificarea, autentificarea şi înregistrarea

utilizatorilor semnăturii digitale, recepţionarea cererilor de certificare a cheilor publice, crearea certificatelor cheilor publice, suspendarea, restabilirea valabilităţii şi 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 cerinţele 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 cerinţelor standardului ITU-T X.509, versiunea 3, standardului SMV ISO CEI 9594-8:2007 Tehnologia informaţiei. Interconexiunea sistemelor deschise. Linii directoare: Structura certificatului cheii publice şi a atributului sau recomandării ETF RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile şi IETF RFC 3739 Qualified Certificates Profile. Structurile certificatelor cheilor publice ale persoanelor împuternicite ale centrelor de certificare şi ale utilizatorilor semnăturii digitale sînt prezentate în anexele 1 şi 2 la prezentele Norme tehnice.

[Pct.25 modificat prin OSIS32 din 23.06.10, MO110-113/02.07.10 art.390]

26. Listele certificatelor revocate trebuie să corespundă cerinţelor standardului ITU-T X.509, versiunea 2, standardului SMV ISO CEI 9594-8:2007 Tehnologia informaţiei. Interconexiunea sistemelor deschise. Linii directoare: Structura certificatului cheii publice şi 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 OSIS32 din 23.06.10, MO110-113/02.07.10 art.390]

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

28. Statutul certificatului cheii publice se stabileşte 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;

[Pct.28 subpct.3) în redacţia OSIS32 din 23.06.10, MO110-113/02.07.10 art.390]

4) IETF RFC 4523 Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates.

[Pct.28 subpct.4) în redacţia OSIS32 din 23.06.10, MO110-113/02.07.10 art.390]

28^1. Structura certificatului serviciului verificării on-line a statutului certificatului (OCSP) este prezentată în anexa nr. 3 la prezentele Norme tehnice.

[Pct.28^1 introdus prin OSIS32 din 23.06.10, MO110-113/02.07.10 art.390]

IV. Crearea şi verificarea semnăturii digitale

29. Semnătura digitală se creează cu mijloacele semnăturii digitale în conformitate cu cerinţele standardului SMV CWA 14170:2007 Cerinţele de securitate pentru aplicaţiile de creare a semnăturii.

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

31. Formatul semnăturii digitale trebuie să corespundă cerinţelor standardului PKCS=7 Cryptographic Message Syntax Standard sau IETF RFC 5126 CMS Advanced Electronic

Signatures (CAdES) şi XML Advanced Electronic Signatures (XAdES)..

[Pct.31 modificat prin OSIS32 din 23.06.10, MO110-113/02.07.10 art.390]

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

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

3) SM GOST R 34.10:2006 Tehnologia informaţională. Securitatea criptografică a informaţiei. Procesele de formare şi 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 informaţiei. Tehnici de securitate. Semnături digitale cu anexă. Partea 2: Mecanisme bazate pe o descompunere în factori a unui întreg.

[Pct.32 subpct.5) în redacţia OSIS32 din 23.06.10, MO110-113/02.07.10 art.390]

33. Algoritmii funcţiei hash trebuie sa corespundă cerinţelor prevăzute de unul din următoarele standarde:

1) SM ISO/CEI 10118-1:2006 Tehnologia informaţiei. Tehnici de securitate. Funcţii hash. Partea 1: Generalităţi; SM ISO/CEI 10118-2:2006 Tehnologia informaţiei. Tehnici de securitate. Funcţii hash. Partea 2: Funcţii hash utilizînd un algoritm de cifrare pe blocuri de n biţi; SM ISO/CEI 10118-3:2006 Tehnologia informaţiei. Tehnici de securitate. Funcţii hash. Partea 3: Funcţii hash dedicate; SM ISO/CEI 10118-4:2006 Tehnologia informaţiei. Tehnici de securitate. Funcţii hash. Partea 4: Funcţii hash utilizînd aritmetica modulară;

2) SM GOST R 34.11:2006 Tehnologia informaţională. Securitatea criptografică a informaţiei. Funcţia hash;

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

[Pct.33 subpct.3) în redacţia OSIS32 din 23.06.10, MO110-113/02.07.10 art.390]

V. Fixarea timpului

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

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

[Pct.35 modificat prin OSIS32 din 23.06.10, MO110-113/02.07.10 art.390]

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

[Pct.36 introdus prin OSIS32 din 23.06.10, MO110-113/02.07.10 art.390]

VI. Validarea datelor şi protocolul serverului de certificare

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

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

[Capitolul VI introdus prin OSIS32 din 23.06.10, MO110-113/02.07.10 art.390]