

ЗАТВЕРДЖЕНО

Наказ Міністерства юстиції України,
Адміністрації Державної служби
спеціального зв'язку та захисту
інформації України

05 грудня 2013 року № 2563/5/645

**Перелік стандартів у сфері електронного цифрового підпису для
гармонізації з європейськими та міжнародними стандартами**

1. ISO/IEC 15946-2 «Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 2: Digital Signatures»
2. ISO/IEC 15946-4 «Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 4. Digital signatures giving message recovery»
3. ISO/IEC 15946-5:2009 «Information technology – Security techniques – Cryptographic techniques based on elliptic curves – Part 5: Elliptic curve generation»
4. ISO/IEC 9797-3:2011 «Information technology – Security techniques – Message Authentication Codes (MACs) – Part 3: Mechanisms using a universal hash-function»
5. ISO/IEC 10118-4:1998 «Information technology – Security techniques – Hash-functions – Part 4: Hash-functions using modular arithmetic»
6. ISO/IEC 9796-2:2010 «Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms»
7. ISO/IEC 9796-3:2006 «Information technology – Security techniques – Digital signature schemes giving message recovery – Part 3: Discrete logarithm based mechanisms»
8. ISO/IEC 29150:2011 «Information technology – Security techniques – Signcryption»
9. ISO/IEC FDIS 29192-4 «Information technology – Security techniques – Lightweight cryptography – Part 4: Mechanisms using asymmetric techniques»
10. ISO/IEC 9798-2 «Information technology – Security techniques – Entity authentication – Part2. Mechanisms using symmetric encipherment algorithms»
11. ISO/IEC 9798-4 «Information technology – Security techniques – Entity authentication – Part4. Mechanisms using cryptographic check function»
12. ISO/IEC 9798-5 «Information technology – Security techniques – Entity

- authentication – Part5. Mechanisms using zero knowledge techniques»
13. ISO/IEC 9798-6 «Information technology – Security techniques – Entity Authentication – Part 6. Mechanisms using manual data transfer»
14. CWA 14167-1:2003 «Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1: System Security Requirements»
15. CWA 14167-2:2004 «Cryptographic module for CSP signing operations with backup – Protection profile – CMCSOB PP»
16. CWA 14167-4:2004 «Cryptographic module for CSP signing operations – Protection profile – CMCSO PP»
17. CWA 14169:2004 «Secure signature-creation devices «EAL 4+»
18. ETSI TS 101 456:2005 «Electronic Signatures and Infrastructures (ESI). Policy Requirements for certification authorities issuing qualified certificates»
19. ETSI TR 102 437:2006 «Electronic Signatures and Infrastructures (ESI); Guidance on TS 101 456 (Policy Requirements for certification authorities issuing qualified certificates)»
20. ETSI TS 102 778:2009 «Electronic Signatures and Infrastructures (ESI). – PDF Advanced Electronic Signature Profiles; CMS Profile based on ISO 32000-1»
21. ETSI TS 102 778-1:2009 «Electronic Signatures and Infrastructures (ESI). – PDF Advanced Electronic Signature Profiles. – Part 1: PAdES Overview – a framework document for PAdES»
22. ETSI TS 102 778-2:2009 «Electronic Signatures and Infrastructures (ESI) – PDF Advanced Electronic Signature Profiles – Part 2: PAdES Basic – Profile based on ISO 32000-1»
23. ETSI TS 102 778-3:2009 «Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced – PadES-BES and PAdES-EPES Profiles»
24. ETSI TS 102 778-4:2009 «Electronic Signatures and Infrastructures (ESI) – PDF Advanced Electronic Signature Profiles – Part 4: PAdES Long Term – PadES LTV Profile»
25. ETSI TS 102 778-5:2009 «Electronic Signatures and Infrastructures (ESI) – PDF Advanced Electronic Signature Profiles – Part 5: PAdES for XML Content – Profiles for XAdES signatures»
26. ETSI TS 102 231:2006 «Electronic Signatures and Infrastructures (ESI) - Provision of harmonized Trust-service status information»
27. ETSI TR 102 272:2003 «Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies»
28. ETSI TR 102 158:2003 «Electronic Signatures and Infrastructures (ESI); Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates»
29. RFC 3739 Internet X.509 «Public Key Infrastructure: Qualified Certificates Profile»
30. RFC 4510 «Lightweight Directory Access Protocol (LDAP): Technical

- Specification Road Map»
31. RFC 4511 «Lightweight Directory Access Protocol (LDAP): The Protocol»
 32. RFC 4512 «Lightweight Directory Access Protocol (LDAP): Directory Information Models»
 33. RFC 4513 «Lightweight Directory Access Protocol (LDAP): Authentication Methods and Security Mechanisms»
 34. RFC 4514 «Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names»
 35. RFC 4515 «Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters»
 36. RFC 4516 «Lightweight Directory Access Protocol (LDAP): Uniform Resource Locator»
 37. RFC 4517 «Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules»
 38. RFC 4518 «Lightweight Directory Access Protocol (LDAP): Internationalized String Preparation»
 39. RFC 4519 «Lightweight Directory Access Protocol (LDAP): Schema for User Applications»
 40. RFC 4523 «Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates»
 41. RFC 4211 Internet X.509 «Public Key Infrastructure Certificate Request Message Format (CRMF)»
 42. PKCS #15 «Cryptographic Token Information Format Standard»
 43. PKCS #12 «Personal Information Exchange Syntax Standard «
 44. PKCS #11 «Cryptographic Token Interface (Cryptoki)»
 45. PKCS #8 «Private-Key Information Syntax Standard»
 46. RFC 5652 «Cryptographic Message Syntax (CMS)»
 47. W3C Recommendation 10 June 2008 XML «Signature Syntax and Processing (Second Edition)»
 48. PKCS #5 «Password-Based Cryptography Standard»
 49. PKCS #10 «Certification Request Syntax Specification»
 50. RFC 2560 «Internet X.509 Public Key Infrastructure Online Certificate Status Protocol – OCSP»
 51. RFC 2631 «Diffie-Hellman Key Agreement Method», June 1999;
 52. RFC 3161 «Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)»
 53. RFC 3370 «Cryptographic Message Syntax (CMS) Algorithms», August 2002
 54. RFC 3852 «Cryptographic Message Syntax (CMS)», July 2004
 55. ISO/IEC 11770-4:2006 «Information technology - Security techniques – Key management – Part 4: Mechanisms based on weak secrets»
 56. ISO/IEC 11770-5:2011 «Information technology – Security techniques – Key management – Part 5: Group key management»
 57. ISO/IEC 15408-1:2009 «Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model»

58. ISO/IEC 15408-2:2008 «Information technology - Security techniques – Evaluation criteria for IT security – Part 2: Security functional components»
59. ISO/IEC 15408-3:2008 «Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance components»
60. ISO/IEC 17799:2005 «Information technology – Security techniques – Code of practice for information security management»
61. ISO/IEC 18028-2:2006 «Information technology - Security techniques – IT network security – Part 2: Network security architecture»
62. ISO/IEC 18028-3:2005 «Information technology - Security techniques – IT network security – Part 3: Securing communications between networks using security gateways»
63. ISO/IEC 18028-4:2005 «Information technology – Security techniques – IT network security – Part 4: Securing remote access»
64. ISO/IEC 18028-5:2006 «Information technology – Security techniques – IT network security – Part 5: Securing communications across networks using virtual private networks»
65. ISO/IEC 18031:2011 «Information technology – Security techniques – Random bit generation»
66. ISO/IEC 18032:2005 «Information technology – Security techniques – Prime number generation»
67. ISO/IEC 18033-1:2005 «Information technology – Security techniques – Encryption algorithms – Part 1: General»
68. ISO/IEC 18033-2:2006 «Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers»
69. ISO/IEC 18033-3:2005 «Information technology – Security techniques – Encryption algorithms – Part 3: Block ciphers»
70. ISO/IEC 18033-4:2005 «Information technology – Security techniques – Encryption algorithms – Part 4: Stream ciphers»
71. ISO/IEC 27002:2005 «Information technology – Security techniques – Code of practice for information security management»
72. ISO/IEC 27004:2009 «Information technology – Security techniques – Information security management – Measurement»
73. ISO/IEC 27005:2008 «Information technology – Security techniques – Information security risk management»
74. ISO/IEC 27006:2007 «Information technology – Security techniques – Requirements for bodies providing audit and certification of information security management systems»
75. ISO/IEC 27011:2008 «Information technology – Security techniques – Information security management guidelines for telecommunications organizations based on ISO/IEC 27002»
76. ISO/IEC 29500-1:2008 «Інформаційні технології – Мови опису документів й оброблення - Формати відкритих офісних XML-файлів – Частина 1: Основи й еталон мови розмітки (Information technology – Document description and processing languages – Office Open XML File

- Formats – Part 1: Fundamentals and Markup Language Reference)»
77. ISO/IEC 29500-2:2008 «Інформаційні технології – Мови опису документів й оброблення – Формати відкритих офісних XML-файлів – Частина 2: Домовленості відкритого пакування (Information technology – Document description and processing languages – Office Open XML File Formats – Part 2: Open Packaging Conventions)»
 78. ISO/IEC 29500-3:2008 «Інформаційні технології. Мови опису документів й оброблення – Формати відкритих офісних XML-файлів. Частина 3. Сумісність і розширюваність розмітки (Information technology – Document description and processing languages – Office Open XML File Formats – Part 3: Markup Compatibility and Extensibility)»
 79. ISO/IEC 29500-4:2008 «Інформаційні технології - Мови опису документів й оброблення – Формати відкритих офісних XML-файлів – Частина 4: Властивості проміжної міграції (Information technology – Document description and processing languages – Office Open XML File Formats - Part 4: Transitional Migration Features)»
 80. ISO/IEC 26300:2006 «Інформаційні технології – Формат відкритого документа для офісних застосувань (OpenDocument) v1.0 (Information technology – Open Document Format for Office Applications (OpenDocument) v1.0)»
 81. ISO 32000-1:2008 «Керування документами. Формат мобільного документа. Частина 1. Формат PDF 1.7 (Document management – Portable document format – Part 1: PDF 1.7)»
 82. ISO 19005-1:2005 «Керування документами. Формат файлів електронних документів для довготривалого зберігання. Частина 1. Використання PDF 1.4 (PDF/A-1) (Document management – Electronic document file format for long-term preservation – Part 1: Use of PDF 1.4 (PDF/A-1)»
 83. ISO/TS 15000-1:2004 «Розширювана мова розмітки для електронного бізнесу (ebXML). Частина 1. Профіль протоколу взаємодії та специфікації угод (ebCPP) (Electronic business eXtensible Markup Language (ebXML) – Part 1: Collaboration-protocol profile and agreement specification)»
 84. ISO/TS 15000-2:2004 «Розширювана мова розмітки для електронного бізнесу (ebXML). Частина 2. Специфікація служби повідомлень (ebMS) (Electronic business eXtensible Markup Language (ebXML) – Part 2: Message service specification)»
 85. ISO/TS 15000-3:2004 «Розширювана мова розмітки для електронного бізнесу (ebXML). Частина 3. Специфікація моделі інформаційного реєстру (ebRIM) (Electronic business eXtensible Markup Language (ebXML) – Part 3: Registry information model specification)»
 86. ISO/TS 15000-4:2004 «Розширювана мова розмітки для електронного бізнесу (ebXML). Частина 4. Специфікація послуг реєстру (ebRS) (Electronic business eXtensible Markup Language (ebXML) – Part 4:

- Registry services specification)»
87. ISO/TS 15000-5:2005 «Розширювана мова розмітки для електронного бізнесу (ebXML). Частина 5. Технічна специфікація базових компонент версії 2.01(ebCCTS) (Electronic Business Extensible Markup Language (ebXML) – Part 5: ebXML Core Components Technical Specification, Version 2.01)»
 88. CWA 16093:2010 «Техніко-економічне обґрунтування для тестового стенду інтероперабельності глобального електронного бізнесу (Feasibility Study for a Global eBusiness Interoperability Test Bed (GTIB))»
 89. CWA 16022:2009 «Графік проекту та управління витратами (Project Schedule and Cost Performance Management (PSCPM))»
 90. CWA 15994:2009 «Процес електронних торгів (eTendering Process)»
 91. CWA 15666:2007 «Специфікація бізнес-вимог, міжгалузевий процес електронних торгів (Business Requirements Specification, Cross industry e-Tendering process)»
 92. CWA 15667:2007 «Специфікація бізнес-вимог, міжгалузевий процес каталогізації (Business Requirements Specification, Cross industry Catalogue Process)»
 93. CWA 15668:2007 «Специфікація бізнес-вимог, міжгалузевий процес створення рахунку (Business Requirements Specification, Cross industry Invoicing Process)»
 94. CWA 15669-1:2007 «Специфікація бізнес-вимог. Процес міжгалузевого замовлення. Частина 2. Специфікація моделі глобального процесу замовлення (Business requirements specification – Cross industry ordering process – Part 1: Global ordering process model definition)»
 95. CWA 15669-2:2007 2007 «Специфікація бізнес-вимог. Процес міжгалузевого замовлення. Частина 2. Транзакція замовлення (Business requirements specification – Cross industry ordering process – Part 2: Order transaction)»
 96. CWA 15669-3:2007 «Специфікація бізнес-вимог. Процес міжгалузевого замовлення. Частина 3. Транзакція зміни замовлення (Business requirements specification – Cross industry ordering process - Part 3: Order change transaction)»
 97. CWA 15669-4:2007 «Специфікація бізнес-вимог. Процес міжгалузевого замовлення. Частина 4. Транзакція відповіді на замовлення (Business requirements specification – Cross industry ordering process – Part 4: Order response transaction)»
 98. CWA 15670:2007 «Специфікація бізнес-вимог, міжгалузевий процес сповіщення про перерахування (Business Requirements Specification, Cross industry Remittance Advice Process)»
 99. CWA 15671:2007 «Специфікація бізнес-вимог, міжгалузевий процес планування (Business Requirements Specification, Cross industry Scheduling Process)»

100. CWA 15672:2007 «Специфікація бізнес вимог, міжгалузевий процес доставки і отримання (Business Requirements Specification, Cross industry Despatch and Receive Process)»
101. CWA 15066:2004 «Транзитна декларація SAD. Модель імплементації (SAD Transit Declaration – Implementation Model)»
102. CWA 15065:2004 «Експортна декларація SAD. Модель імплементації (SAD Exports Declaration – Implementation Model)»
103. CWA 15064:2004 «Імпортна декларація SAD. Модель імплементації (SAD Imports Declaration – Implementation Model)»
104. CWA 14729-1:2003 «Інтраст-система. Частина 1. Модель імплементації (The Intrastat System – Part 1: The Implementation Model)»
105. CWA 14729-2:2003 «Інтраст-система. Частина 2. Настанова по імплементації INSTAT/XML повідомлення. (The Intrastat System – Part 2: Message Implementation Guideline of INSTAT/XML)»
106. CWA 14729-3:2003 «Інтраст-система. Частина 3. Настанова з імплементації INSRES/XML повідомлення (The Intrastat System – Part 3: Message Implementation Guideline of INSRES/XML)»

**Начальник Управління
функціонування центрального
засвідчувального органу
Міністерства юстиції України**

Д.В. Журавльов

**Директор Департаменту криптографічного
захисту інформації Адміністрації
Державної служби спеціального зв'язку
та захисту інформації України**

А.І. Пушкарьов