

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, що  
підлягають перегляду**

1. ДСТУ ISO/IEC 8825-1:2008 «Інформаційні технології. ASN.1 правила кодування. Частина 1. Специфікація правил базового кодування (BER), правил канонічного кодування (CER) і правил витонченого кодування (DER)»
2. ДСТУ ISO/IEC 8825-2:2008 «Інформаційні технології. ASN.1 правила кодування. Частина 2. Специфікація правил упакованого кодування (PER)»
3. ДСТУ ISO/IEC 8825-4:2008 «Інформаційні технології. ASN.1 правила кодування. Частина 4. Специфікація правил кодування XML (XER)»
4. ДСТУ ISO/IEC 8825-5:2008 «Інформаційні технології. ASN.1 правила кодування. Частина 5. Відображення визначень W3C XML-схем в ASN.1»
5. ДСТУ EN 14890-1:2008 «Прикладний інтерфейс для смарт-карток, використовуваних як безпечні засоби створення підписів. Частина 1. Основні вимоги»
6. ДСТУ EN 14890-2:2008 «Прикладний інтерфейс для смарт-карток, використовуваних як безпечні засоби створення підписів. Частина 2. Додаткові послуги»
7. ДСТУ CWA 14365-2 «Настанова з використання електронних підписів. Частина 2. Профіль захисту для програмних засобів створення підпису»
8. ДСТУ CWA 14170:2008 «Вимоги безпеки для застосувань створення підписів»
9. ДСТУ CWA 14171:2008 «Загальні рекомендації для верифікації електронних підписів»
10. ДСТУ CWA 14365-1:2008 «Настанова з використання електронних підписів. Частина 1. Юридичні та технічні аспекти»
11. ДСТУ ETSI TS 101 733:2009 «Електронні підписи та інфраструктури (ESI). CMS-розширені електронні підписи (CAdES)»
12. ДСТУ ETSI TS 102 734:2009 «Електронні підписи й інфраструктури; Профілі CMS розширених електронних підписів, що ґрунтуються на

- TS 101 733 (CAAdES)»
13. ДСТУ ETSI TS 101 903:2009 «XML-розширені електронні підписи (XAdES)»
  14. ДСТУ ETSI TS 102 904:2009 «Електронні підписи й інфраструктури. Профілі розширених електронних підписів XML, що ґрунтуються на TS 101 903 (XAdES)»
  15. ДСТУ ETSI TS 101 862:2009 «Профіль посилених сертифікатів»
  16. ДСТУ ETSI TS 101 861: 2009 «Профіль штемпелювання часу»
  17. ДСТУ ETSI TS 102 176-1:2009 «Електронні підписи й інфраструктури (ESI). Алгоритми й параметри для безпечних електронних підписів Частина 1. Геш-Функції й асиметричні алгоритми»
  18. ДСТУ ETSI TS 102 176-2:2009 «Електронні підписи й інфраструктури (ESI). Алгоритми й параметри для безпечних електронних підписів. Частина 2. Протоколи безпечного каналу й алгоритми для засобів накладання підпису»
  19. ДСТУ ETSI TS 102 023:2009 «Електронні підписи й інфраструктури (ESI). Вимоги політики для органів штемпелювання часу»
  20. ДСТУ ETSI TS 102 047:2009 «Міжнародна гармонізація форматів електронних підписів»
  21. ДСТУ ETSI TS 102 045:2009 «Електронні підписи й інфраструктури (ESI). Політика підписів для розширеної бізнес-моделі»
  22. ДСТУ ISO/IEC 8824-1:2008 «Інформаційні технології. Нотація абстрактного синтаксису (ASN.1) Частина 1: Специфікація базової нотації»
  23. ДСТУ ISO/IEC 8824-2:2008 «Інформаційні технології. Нотація абстрактного синтаксису 1 (ASN.1). Частина 2. Специфікація інформаційного об'єкту»
  24. ДСТУ ISO/IEC 8824-3:2008 «Інформаційні технології. Нотація абстрактного синтаксису 1 (ASN.1) Частина 3. Специфікація обмежень»
  25. ДСТУ ISO/IEC 8824-4:2008 «Інформаційні технології Нотація абстрактного синтаксису 1 (ASN.1) Частина 4: Параметризація специфікацій ASN.1»
  26. ДСТУ CWA 14167-3:2008 «Криптографічний модуль для послуг генерування ключів провайдером послуг сертифікації. Профіль захисту CMCKG-PP»
  27. ДСТУ ISO/IEC 8825-3:2008 «Інформаційні технології. ASN.1-правила кодування. Частина 3. Специфікація керівної нотації кодування (ECN)»
  28. ДСТУ ISO/IEC 13888–2002 «Інформаційні технології. Методи захисту. Неспростовність: Частина 1. Загальні положення 1»
  29. ДСТУ ISO/IEC 13888–2002 «Інформаційні технології. Методи захисту. Неспростовність: Частина 3. Механізми з використанням асиметричних методів»
  30. ДСТУ ISO/IEC 14888–2002 «Інформаційні технології. Методи захисту.

31. Цифрові підписи з доповненням» Частина 1. Загальні положення»  
ДСТУ ISO/IEC 14888–2002 «Інформаційні технології. Методи захисту. Цифрові підписи з доповненням Частина 2. Механізми на основі ідентифікаторів»
32. ДСТУ ISO/IEC 14888–2002 «Інформаційні технології. Методи захисту. Цифрові підписи з доповненням Частина 3. Механізми на основі сертифікатів»
33. ДСТУ ISO/IEC 10118-1:2000 «Інформаційні технології. Методи захисту. Геш функції. Частина 1. Загальні положення»
34. ДСТУ ISO/IEC 10118-2:2000 «Інформаційні технології. Методи захисту. Геш функції. Частина 2. Геш функції, що використовують п-бітний блоковий шифр»
35. ДСТУ ISO/IEC 10118-3:2004 «Інформаційні технології. Методи захисту. Геш функції. Частина 3. Спеціалізовані геш функції»
36. ДСТУ ISO/IEC 13335-1:2004 «Інформаційні технології. Методи захисту. Керування інформацією й безпекою технології комунікацій. Частина 1. Поняття й моделі для інформації й керування безпекою технології комунікацій»
37. ДСТУ ISO/IEC 15946-1:2008 «Інформаційні технології. Методи захисту. Криптографічні методи, засновані на еліптичних кривих. Частина 1. Загальні положення»
38. ДСТУ ISO/IEC 15946-3:2008 «Інформаційні технології. Методи захисту. Криптографічні перетворення, що ґрунтуються на еліптичних кривих. Частина 3. Установлення ключів»
39. ДСТУ ISO/IEC 9594-8 «Інформаційні технології. Взаємозв'язок відкритих систем. Каталог: Основні положення щодо сертифікації відкритих ключів та сертифікації атрибутів»
40. ДСТУ ISO/IEC 9797-1 «Інформаційні технології. Методи захисту. Коди автентифікації повідомлень (MACs). Частина 1. Механізми, що використовують блокові шифри»
41. ДСТУ ISO/IEC 9797-2 «Інформаційні технології. Методи захисту. Коди автентифікації повідомлень (MACs). Частина 2. Механізми, що використовують спеціалізовані геш-функції»
42. ДСТУ ISO/IEC 18014-1:2006 «Інформаційні технології. Методи захисту. Послуги штемпелювання часу – Частина 1: Структура»
43. ДСТУ ISO/IEC 18014-2:2006 Інформаційні технології. Методи захисту. Послуги штемпелювання часу. Частина 2. Механізми, що генерують незалежні токени
44. ДСТУ ISO/IEC 18014-3:2006 «Інформаційні технології. Методи захисту. Послуги штемпелювання часу. Частина 3. Механізми, що виробляють зв'язані токени»
45. ДСТУ ISO/IEC 9798-1:1997 «Інформаційні технології. Методи. Автентифікації сутності. Частина 1. Загальні положення»
46. ДСТУ ISO/IEC 9798-3:1998 «Інформаційні технології. Методи захисту. Автентифікація сутності. Частина 3. Механізми , що використовують

- методи цифрового підпису»
47. ДСТУ ISO/IEC TR 13335-1:2001 «Інформаційні технології. Настанова для керування ІТ безпекою. Частина 5. Настанова керування безпекою мережі»
  48. ДСТУ-П CWA 14172-1 «Настанова EESSI з оцінювання відповідності. Частина 1: Загальні положення»
  49. ДСТУ-П CWA 14172-2 «Настанова EESSI з оцінювання відповідності. Частина 2. Послуги та процеси органу сертифікації»
  50. ДСТУ-П CWA 14172-3 «Настанова EESSI з оцінювання відповідності. Частина 3. Надійні системи, що управляють сертифікатами для електронних підписів»
  51. ДСТУ-П CWA 14172-4 «Настанова EESSI з оцінювання відповідності. Частина 4. Застосовування для накладання підпису та загальні настанови з перевірки електронного підпису»
  52. ДСТУ-П CWA 14172-5 «Настанова EESSI з оцінювання відповідності. Частина 5. Безпечні засоби створення підпису»
  53. ДСТУ-П CWA 14172-6 «Настанова EESSI з оцінювання відповідності. Частина 6. Засіб створення підписів, що підтримує підписи, крім кваліфікованих»
  54. ДСТУ-П CWA 14172-7 «Настанова EESSI з оцінювання відповідності. Частина 7. Криптографічні модулі, використовувані провайдерами послуг сертифікації для операцій підписування та послуг генерування ключів»
  55. ДСТУ-П CWA 14172-8 «Настанова EESSI з оцінювання відповідності. Частина 8. Послуги та процеси органу штемпелювання часу»
  56. ДСТУ ISO/IEC 18014-1:2006 «Інформаційні технології. Методи захисту. Послуги штемпелювання часу. Частина 1. Основні положення»
  57. ДСТУ ISO/IEC 18014-2:2006 «Інформаційні технології. Методи захисту. Послуги штемпелювання часу. Частина 2. Механізми, що виробляють незалежні токени»
  58. ДСТУ ISO/IEC 18014-3:2006 «Інформаційні технології. Методи захисту. Послуги штемпелювання часу. Частина 3. Механізми, що виробляють зв'язані токени»
  59. «Інформаційні технології. Криптографічний захист інформації. Функція гешування»
  60. ДСТУ ISO/IEC 27000 «Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Overview and vocabulary»
  61. ДСТУ ISO/IEC 27001 «Інформаційні технології. Методи захисту. Система управління інформаційною безпекою. Вимоги»
  62. ДСТУ ISO/IEC TR 13335-1:2004 «Інформаційні технології. Посібник з управління безпекою інформаційних технологій. Частина 1. Управління та планування безпекою ІТ»
  63. ДСТУ ISO/IEC TR 13335-2:2004 «Інформаційні технології. Посібник з

- управління безпекою інформаційних технологій. Частина 2. Управління та планування безпекою ІТ»
64. ДСТУ ISO/IEC TR 13335-3:2004 «Інформаційні технології. Посібник з управління безпекою інформаційних технологій. Частина 3. Методи керування захистом інформаційних технологій»
  65. ДСТУ ISO/IEC 11770-1:2006 «Інформаційні технології. Методи захисту. Керування ключами. Частина 1. Середовище»
  66. ДСТУ ISO/IEC 11770-2:2006 «Інформаційні технології. Методи захисту. Керування ключами. Частина 2. Механізми, базовані на використанні симетричних методів»
  67. ДСТУ ISO/IEC 11770-3:2006 «Інформаційні технології. Методи захисту. Керування ключами. Частина 3. Механізми, базовані на використанні асиметричних методів»
  68. ДСТУ ISO 9735-1:2006 «Електронний обмін даними для адміністрування, у торгівлі і на транспорті (EDIFACT). Правила синтаксису прикладного рівня (номер версії синтаксису: 4, номер редакції синтаксису: 1). Частина 1: Загальні для всіх частин правила синтаксису»
  69. ДСТУ ISO 9735-2:2006 «Електронний обмін даними для адміністрування, у торгівлі і на транспорті (EDIFACT). Правила синтаксису прикладного рівня (номер версії синтаксису: 4, номер редакції синтаксису: 1). Частина 2: Особливості правил синтаксису для пакетного електронного обміну даними»
  70. ДСТУ ISO 9735-3:2006 «Електронний обмін даними для адміністрування, у торгівлі і на транспорті (EDIFACT). Правила синтаксису прикладного рівня (номер версії синтаксису 4, номер редакції синтаксису 1). Частина 3: Особливості правил синтаксису для інтерактивного електронного обміну даними»
  71. ДСТУ ISO 9735-4:2006 «Електронний обмін даними для адміністрування, у торгівлі і на транспорті (EDIFACT). Правила синтаксису прикладного рівня (номер версії синтаксису 4, номер редакції синтаксису 1). Частина 4: Синтаксис і службові повідомлення для пакетного EDI (тип повідомлення CONTRL)»
  72. ДСТУ ISO 9735-5:2006 «Електронний обмін даними для адміністрування, у торгівлі і на транспорті (EDIFACT). Правила синтаксису прикладного рівня (номер версії синтаксису: 4, номер редакції синтаксису: 1). Частина»
  73. ДСТУ ISO 9735-6:2006 «Електронний обмін даними для адміністрування, у торгівлі і на транспорті (EDIFACT). Правила синтаксису прикладного рівня (номер версії синтаксису: 4, номер редакції синтаксису: 1). Частина 6. Повідомлення безпечної автентифікації та підтвердження отримання»
  74. ДСТУ ISO 9735-7:2006 «Електронний обмін даними для адміністрування, у торгівлі і на транспорті (EDIFACT). Правила синтаксису прикладного рівня (номер версії синтаксису: 4, номер

- редакції синтаксису: 1). Частина 7. Правила забезпечення для пакетного обміну електронними даними (конфіденційність)»
75. ДСТУ ISO 9735-8:2006 «Електронний обмін даними для адміністрування, у торгівлі і на транспорті (EDIFACT). Правила синтаксису прикладного рівня (номер версії синтаксису: 4, номер редакції синтаксису: 1). Частина 8: Зв'язані дані в електронному обміні даними»
76. ДСТУ ISO 9735-9:2006 «Електронний обмін даними для адміністрування, у торгівлі і на транспорті (EDIFACT). Правила синтаксису прикладного рівня (номер версії синтаксису: 4, номер редакції синтаксису: 1). Частина 9. Повідомлення управління ключами забезпечення та сертифікатами (тип повідомлення – KEYMAN)»
77. ДСТУ ISO 9735-10:2006 «Електронний обмін даними для адміністрування, у торгівлі і на транспорті (EDIFACT). Правила синтаксису прикладного рівня (версія синтаксису номер 4, номер редакції синтаксису: 1). Частина 10: Службові каталоги синтаксису»
78. ДСТУ ISO/TS 20625:2006 «Обмін електронними даними для управління, торгівлі і транспорту (EDIFACT). Правила генерації файлів XML-схем (XSD) на основі настанови з реалізації EDI(FACT)»

**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**