

ЗАТВЕРДЖЕНО

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

29 березня
№ 1017/5/2016

2017 року

Зарєє... України
" 29 " Березня 2017 р.
32 38 428/30291
Керівник роз...
органу

ЗМІНИ

до Вимог до структури об'єктних ідентифікаторів
для криптоалгоритмів, що є державними стандартами

Таблиці 2, 3 розділу II викласти в такій редакції:

«Таблиця 2

Об'єктні ідентифікатори криптографічних алгоритмів

Опис	Скорочена назва	Значення
Криптографічні алгоритми	alg	1.2.804.2.1.1.1.1
Симетричні криптографічні алгоритми	sym	1.2.804.2.1.1.1.1.1
Алгоритм ДСТУ ГОСТ 28147:2009	Gost28147	1.2.804.2.1.1.1.1.1.1
Алгоритм ДСТУ ГОСТ 28147:2009 в режимі простої заміни	Gost28147ecb	1.2.804.2.1.1.1.1.1.1.1
Алгоритм ДСТУ ГОСТ 28147:2009 в режимі гамування	Gost28147ctr	1.2.804.2.1.1.1.1.1.1.2
Алгоритм ДСТУ ГОСТ 28147:2009 в режимі гамування зі зворотним зв'язком	Gost28147cfb	1.2.804.2.1.1.1.1.1.1.3
Алгоритм ДСТУ ГОСТ 28147:2009 в режимі вироблення імітовставки	Gost28147cmac	1.2.804.2.1.1.1.1.1.1.4
Алгоритм криптографічного перетворення за ДСТУ	Gost28147wrap	1.2.804.2.1.1.1.1.1.1.5

ГОСТ 28147:2009 в режимі гамування зі зворотним зв'язком для захисту ключа шифрування даних		
Алгоритм НМАС із геш-функцією за ГОСТ 34.311-95	HmacGost34311	1.2.804.2.1.1.1.1.1.2
Алгоритм ДСТУ 7624:2014	Dstu7624	1.2.804.2.1.1.1.1.1.3
Алгоритм ДСТУ 7624:2014 в режимі простої заміни (ECB)	Dstu7624ecb	1.2.804.2.1.1.1.1.1.3.1
Алгоритм ДСТУ 7624:2014 в режимі «Калина-128/128-ECB»	Dstu7624ecb(128)	1.2.804.2.1.1.1.1.1.3.1.1
Алгоритм ДСТУ 7624:2014 в режимі «Калина-256/256-ECB»	Dstu7624ecb(256)	1.2.804.2.1.1.1.1.1.3.1.2
Алгоритм ДСТУ 7624:2014 в режимі «Калина-512/512-ECB»	Dstu7624ecb(512)	1.2.804.2.1.1.1.1.1.3.1.3
Алгоритм ДСТУ 7624:2014 в режимі гамування (CTR)	Dstu7624ctr	1.2.804.2.1.1.1.1.1.3.2
Алгоритм ДСТУ 7624:2014 в режимі «Калина-128/128-CTR»	Dstu7624ctr(128)	1.2.804.2.1.1.1.1.1.3.2.1
Алгоритм ДСТУ 7624:2014 в режимі «Калина-256/256-CTR»	Dstu7624ctr(256)	1.2.804.2.1.1.1.1.1.3.2.2
Алгоритм ДСТУ 7624:2014 в режимі «Калина-512/512-CTR»	Dstu7624ctr(512)	1.2.804.2.1.1.1.1.1.3.2.3
Алгоритм ДСТУ 7624:2014 в режимі гамування зі зворотним зв'язком по шифротексту (CFB)	Dstu7624cfb	1.2.804.2.1.1.1.1.1.3.3
Алгоритм ДСТУ 7624:2014 в режимі «Калина-128/128-CFB-128»	Dstu7624cfb(128)	1.2.804.2.1.1.1.1.1.3.3.1
Алгоритм ДСТУ 7624:2014 в режимі «Калина-256/256-CFB-256»	Dstu7624cfb(256)	1.2.804.2.1.1.1.1.1.3.3.2
Алгоритм ДСТУ 7624:2014 в режимі «Калина-512/512-CFB-512»	Dstu7624cfb(512)	1.2.804.2.1.1.1.1.1.3.3.3
Алгоритм ДСТУ 7624:2014 в режимі	Dstu7624cmac	1.2.804.2.1.1.1.1.1.3.4

вироблення імітовставки (СМАС)		
Алгоритм ДСТУ 7624:2014 в режимі «Калина-128/128-СМАС-128»	Dstu7624cmac(128)	1.2.804.2.1.1.1.1.3.4.1
Алгоритм ДСТУ 7624:2014 в режимі «Калина-256/256-СМАС-256»	Dstu7624cmac(256)	1.2.804.2.1.1.1.1.3.4.2
Алгоритм ДСТУ 7624:2014 в режимі «Калина-512/512-СМАС-512»	Dstu7624cmac(512)	1.2.804.2.1.1.1.1.3.4.3
Алгоритм ДСТУ 7624:2014 в режимі зчеплення шифроблоків (СВС)	Dstu7624cbc	1.2.804.2.1.1.1.1.3.5
Алгоритм ДСТУ 7624:2014 в режимі «Калина-128/128-СВС»	Dstu7624cbc(128)	1.2.804.2.1.1.1.1.3.5.1
Алгоритм ДСТУ 7624:2014 в режимі «Калина-256/256-СВС»	Dstu7624cbc(256)	1.2.804.2.1.1.1.1.3.5.2
Алгоритм ДСТУ 7624:2014 в режимі «Калина-512/512-СВС»	Dstu7624cbc(512)	1.2.804.2.1.1.1.1.3.5.3
Алгоритм ДСТУ 7624:2014 в режимі гамування зі зворотним зв'язком по шифрограмі (OFB)	Dstu7624ofb	1.2.804.2.1.1.1.1.3.6
Алгоритм ДСТУ 7624:2014 в режимі «Калина-128/128-OFB»	Dstu7624ofb(128)	1.2.804.2.1.1.1.1.3.6.1
Алгоритм ДСТУ 7624:2014 в режимі «Калина-256/256-OFB»	Dstu7624ofb(256)	1.2.804.2.1.1.1.1.3.6.2
Алгоритм ДСТУ 7624:2014 в режимі «Калина-512/512-OFB»	Dstu7624ofb(512)	1.2.804.2.1.1.1.1.3.6.3
Алгоритм ДСТУ 7624:2014 в режимі вибіркового гамування із прискореним виробленням імітовставки (ГМАС)	Dstu7624gmac	1.2.804.2.1.1.1.1.3.7
Алгоритм ДСТУ 7624:2014 в режимі «Калина-128/128-ГМАС-128»	Dstu7624gmac(128)	1.2.804.2.1.1.1.1.3.7.1
Алгоритм ДСТУ 7624:2014 в режимі	Dstu7624gmac(256)	1.2.804.2.1.1.1.1.3.7.2

«Калина-256/256-GMAC-256»		
Алгоритм ДСТУ 7624:2014 в режимі «Калина-512/512-GMAC-512»	Dstu7624gmac(512)	1.2.804.2.1.1.1.1.3.7.3
Алгоритм ДСТУ 7624:2014 в режимі вироблення імітовставки і гамування (CCM)	Dstu7624ccm	1.2.804.2.1.1.1.1.3.8
Алгоритм ДСТУ 7624:2014 в режимі «Калина-128/128-CCM-32, 128»	Dstu7624ccm(128)	1.2.804.2.1.1.1.1.3.8.1
Алгоритм ДСТУ 7624:2014 в режимі «Калина-256/256-CCM-32, 256»	Dstu7624ccm(256)	1.2.804.2.1.1.1.1.3.8.2
Алгоритм ДСТУ 7624:2014 в режимі «Калина-512/512-CCM-32, 512»	Dstu7624ccm(512)	1.2.804.2.1.1.1.1.3.8.3
Алгоритм ДСТУ 7624:2014 в режимі індексованої заміни (XTS)	Dstu7624xts	1.2.804.2.1.1.1.1.3.9
Алгоритм ДСТУ 7624:2014 в режимі «Калина-128/128-XTS»	Dstu7624xts(128)	1.2.804.2.1.1.1.1.3.9.1
Алгоритм ДСТУ 7624:2014 в режимі «Калина-256/256-XTS»	Dstu7624xts(256)	1.2.804.2.1.1.1.1.3.9.2
Алгоритм ДСТУ 7624:2014 в режимі «Калина-512/512-XTS»	Dstu7624xts(512)	1.2.804.2.1.1.1.1.3.9.3
Алгоритм ДСТУ 7624:2014 в режимі захисту ключових даних (KW)	Dstu7624kw	1.2.804.2.1.1.1.1.3.10
Алгоритм ДСТУ 7624:2014 в режимі «Калина-128/128-KW»	Dstu7624kw(128)	1.2.804.2.1.1.1.1.3.10.1
Алгоритм ДСТУ 7624:2014 в режимі «Калина-256/256-KW»	Dstu7624kw(256)	1.2.804.2.1.1.1.1.3.10.2
Алгоритм ДСТУ 7624:2014 в режимі «Калина-512/512-KW»	Dstu7624kw(512)	1.2.804.2.1.1.1.1.3.10.3
Геш-функції	hash	1.2.804.2.1.1.1.1.2
Алгоритм ГОСТ 34.311-95	Gost34311	1.2.804.2.1.1.1.1.2.1
Алгоритм ДСТУ 7564-2014	Dstu7564	1.2.804.2.1.1.1.1.2.2

Алгоритм ДСТУ 7564-2014 в режимі «Купина-256»	Dstu7564(256)	1.2.804.2.1.1.1.1.2.2.1
Алгоритм ДСТУ 7564-2014 в режимі «Купина-384»	Dstu7564(384)	1.2.804.2.1.1.1.1.2.2.2
Алгоритм ДСТУ 7564-2014 в режимі «Купина-512»	Dstu7564(512)	1.2.804.2.1.1.1.1.2.2.3
Алгоритм ДСТУ 7564:2014 в режимі «Купина-256 (КАП)»	Dstu7564mac(256)	1.2.804.2.1.1.1.1.2.2.4
Алгоритм ДСТУ 7564:2014 в режимі «Купина-384 (КАП)»	Dstu7564mac(384)	1.2.804.2.1.1.1.1.2.2.5
Алгоритм ДСТУ 7564:2014 в режимі «Купина-512 (КАП)»	Dstu7564mac(512)	1.2.804.2.1.1.1.1.2.2.6
Асиметричні алгоритми	asym	1.2.804.2.1.1.1.1.3
Алгоритм підпису за ДСТУ 4145-2002 з ґеш-функцією за ГОСТ 34.311-95	Dstu4145WithGost34311	1.2.804.2.1.1.1.1.3.1
Поліноміальний базис Формат кодування полів Little-Endian	Dstu4145WithGost34311 (pb)	1.2.804.2.1.1.1.1.3.1.1
Спеціальні еліптичні криві	Dstu4145WithGost34311SpecialCurves(PB)	1.2.804.2.1.1.1.1.3.1.1.1
Формат кодування полів Big-Endian	Dstu4145WithGost34311key Format(PB)	1.2.804.2.1.1.1.1.3.1.1.1.1
Стандартні еліптичні криві	Dstu4145WithGost34311NamedCurves(PB)	1.2.804.2.1.1.1.1.3.1.1.2
Ступінь розширення основного поля стандартної еліптичної кривої $m=163$	Dstu4145WithGost34311m 163(PB)	1.2.804.2.1.1.1.1.3.1.1.2.0
Ступінь розширення основного поля стандартної еліптичної кривої $m=167$	Dstu4145WithGost34311m 167(PB)	1.2.804.2.1.1.1.1.3.1.1.2.1
Ступінь розширення основного поля стандартної еліптичної кривої $m=173$	Dstu4145WithGost34311m 173(PB)	1.2.804.2.1.1.1.1.3.1.1.2.2
Ступінь розширення основного поля стандартної еліптичної кривої $m=179$	Dstu4145WithGost34311m 179(PB)	1.2.804.2.1.1.1.1.3.1.1.2.3
Ступінь розширення основного поля	Dstu4145WithGost34311m 191(PB)	1.2.804.2.1.1.1.1.3.1.1.2.4

стандартної еліптичної кривої $m=191$		
Ступінь розширення основного поля стандартної еліптичної кривої $m=233$	Dstu4145WithGost34311m233(PB)	1.2.804.2.1.1.1.3.1.1.2.5
Ступінь розширення основного поля стандартної еліптичної кривої $m=257$	Dstu4145WithGost34311m257(PB)	1.2.804.2.1.1.1.3.1.1.2.6
Ступінь розширення основного поля стандартної еліптичної кривої $m=307$	Dstu4145WithGost34311m307(PB)	1.2.804.2.1.1.1.3.1.1.2.7
Ступінь розширення основного поля стандартної еліптичної кривої $m=367$	Dstu4145WithGost34311m367(PB)	1.2.804.2.1.1.1.3.1.1.2.8
Ступінь розширення основного поля стандартної еліптичної кривої $m=431$	Dstu4145WithGost34311m431(PB)	1.2.804.2.1.1.1.3.1.1.2.9
Оптимальний нормальний базис Формат кодування полів Little-Endian	Dstu4145WithGost34311onb	1.2.804.2.1.1.1.3.1.2
Спеціальні еліптичні криві	Dstu4145WithGost34311SpecialCurves(ONB)	1.2.804.2.1.1.1.3.1.2.1
Формат кодування полів Big-Endian	Dstu4145WithGost34311keyFormat(ONB)	1.2.804.2.1.1.1.3.1.2.1.1
Стандартні еліптичні криві	Dstu4145WithGost34311NamedCurves(ONB)	1.2.804.2.1.1.1.3.1.2.2
Ступінь розширення основного поля стандартної еліптичної кривої $m=173$	Dstu4145WithGost34311m173(ONB)	1.2.804.2.1.1.1.3.1.2.2.0
Ступінь розширення основного поля стандартної еліптичної кривої $m=179$	Dstu4145WithGost34311m179(ONB)	1.2.804.2.1.1.1.3.1.2.2.1
Ступінь розширення основного поля стандартної еліптичної кривої $m=191$	Dstu4145WithGost34311m191(ONB)	1.2.804.2.1.1.1.3.1.2.2.2
Ступінь розширення основного поля стандартної еліптичної кривої $m=233$	Dstu4145WithGost34311m233(ONB)	1.2.804.2.1.1.1.3.1.2.2.3
Ступінь розширення основного поля стандартної еліптичної кривої $m=431$	Dstu4145WithGost34311m431(ONB)	1.2.804.2.1.1.1.3.1.2.2.4

кривої $m=431$		
Алгоритм підпису за ГОСТ 34.310-95 з геш-функцією за ГОСТ 34.311-95	Gost34310WithGost34311	1.2.804.2.1.1.1.3.2
Протокол узгодження ключа у циклічній групі поля з використанням геш-функції за ГОСТ 34.311-95	DH-ua	1.2.804.2.1.1.1.3.3
Протокол узгодження ключа в групі точок еліптичної кривої з використанням геш-функції за ГОСТ 34.311-95 (алгоритм з кофакторним множенням)	dhSinglePass-cofactorDH-gost34311kdf	1.2.804.2.1.1.1.3.4
Протокол узгодження ключа в групі точок еліптичної кривої з використанням геш-функції за ГОСТ 34.311-95 (алгоритм без кофакторного множення)	dhSinglePass-stdDH-gost34311kdf	1.2.804.2.1.1.1.3.5
Алгоритм підпису за ДСТУ 4145-2002 з геш-функцією за ДСТУ 7564-2014	Dstu4145WithDstu7564	1.2.804.2.1.1.1.3.6
Алгоритм підпису за ДСТУ 4145-2002 з геш-функцією за ДСТУ 7564-2014 у режимі «Купина-256»	Dstu4145WithDstu7564 (256)	1.2.804.2.1.1.1.3.6.1
Поліноміальний базис Формат кодування полів Little-Endian	Dstu4145WithDstu7564 (256)pb	1.2.804.2.1.1.1.3.6.1.1
Спеціальні еліптичні криві	Dstu4145WithDstu7564 (256)SpecialCurves(PB)	1.2.804.2.1.1.1.3.6.1.1.1
Формат кодування полів Big-Endian	Dstu4145WithDstu7564 (256)keyFormat(PB)	1.2.804.2.1.1.1.3.6.1.1.1.1
Стандартні еліптичні криві	Dstu4145WithDstu7564 (256)NamedCurves(PB)	1.2.804.2.1.1.1.3.6.1.1.2
Ступінь розширення основного поля стандартної еліптичної кривої $m=163$	Dstu4145WithDstu7564 (256)m163(PB)	1.2.804.2.1.1.1.3.6.1.1.2.0

Ступінь розширення основного поля стандартної еліптичної кривої $m=167$	Dstu4145WithDstu7564 (256)m167(PB)	1.2.804.2.1.1.1.1.3.6.1.1.2.1
Ступінь розширення основного поля стандартної еліптичної кривої $m=173$	Dstu4145WithDstu7564 (256)m173(PB)	1.2.804.2.1.1.1.1.3.6.1.1.2.2
Ступінь розширення основного поля стандартної еліптичної кривої $m=179$	Dstu4145WithDstu7564 (256)m179(PB)	1.2.804.2.1.1.1.1.3.6.1.1.2.3
Ступінь розширення основного поля стандартної еліптичної кривої $m=191$	Dstu4145WithDstu7564 (256)m191(PB)	1.2.804.2.1.1.1.1.3.6.1.1.2.4
Ступінь розширення основного поля стандартної еліптичної кривої $m=233$	Dstu4145WithDstu7564 (256)m233(PB)	1.2.804.2.1.1.1.1.3.6.1.1.2.5
Ступінь розширення основного поля стандартної еліптичної кривої $m=257$	Dstu4145WithDstu7564 (256)m257(PB)	1.2.804.2.1.1.1.1.3.6.1.1.2.6
Ступінь розширення основного поля стандартної еліптичної кривої $m=307$	Dstu4145WithDstu7564 (256)m307(PB)	1.2.804.2.1.1.1.1.3.6.1.1.2.7
Ступінь розширення основного поля стандартної еліптичної кривої $m=367$	Dstu4145WithDstu7564 (256)m367(PB)	1.2.804.2.1.1.1.1.3.6.1.1.2.8
Ступінь розширення основного поля стандартної еліптичної кривої $m=431$	Dstu4145WithDstu7564 (256)m431(PB)	1.2.804.2.1.1.1.1.3.6.1.1.2.9
Оптимальний нормальний базис Формат кодування полів Little-Endian	Dstu4145WithDstu7564 (256)onb	1.2.804.2.1.1.1.1.3.6.1.2
Спеціальні еліптичні криві	Dstu4145WithDstu7564 (256)SpecialCurves(ONB)	1.2.804.2.1.1.1.1.3.6.1.2.1
Формат кодування полів Big-Endian	Dstu4145WithDstu7564 (256)keyFormat(ONB)	1.2.804.2.1.1.1.1.3.6.1.2.1.1
Стандартні еліптичні криві	Dstu4145WithDstu7564 (256)NamedCurves(ONB)	1.2.804.2.1.1.1.1.3.6.1.2.2
Ступінь розширення основного поля стандартної еліптичної кривої $m=173$	Dstu4145WithDstu7564 (256)m173(ONB)	1.2.804.2.1.1.1.1.3.6.1.2.2.0

Ступінь розширення основного поля стандартної еліптичної кривої $m=179$	Dstu4145WithDstu7564 (256)m179(ONB)	1.2.804.2.1.1.1.3.6.1.2.2.1
Ступінь розширення основного поля стандартної еліптичної кривої $m=191$	Dstu4145WithDstu7564 (256)m191(ONB)	1.2.804.2.1.1.1.3.6.1.2.2.2
Ступінь розширення основного поля стандартної еліптичної кривої $m=233$	Dstu4145WithDstu7564 (256)m233(ONB)	1.2.804.2.1.1.1.3.6.1.2.2.3
Ступінь розширення основного поля стандартної еліптичної кривої $m=431$	Dstu4145WithDstu7564 (256)m431(ONB)	1.2.804.2.1.1.1.3.6.1.2.2.4
Алгоритм підпису за ДСТУ 4145-2002 з геш-функцією за ДСТУ 7564-2014 у режимі «Купина-384»	Dstu4145WithDstu7564 (384)	1.2.804.2.1.1.1.3.6.2
Поліноміальний базис Формат кодування полів Little-Endian	Dstu4145WithDstu7564 (384)pb	1.2.804.2.1.1.1.3.6.2.1
Спеціальні еліптичні криві	Dstu4145WithDstu7564 (384)SpecialCurves(PB)	1.2.804.2.1.1.1.3.6.2.1.1
Формат кодування полів Big-Endian	Dstu4145WithDstu7564 (384)keyFormat(PB)	1.2.804.2.1.1.1.3.6.2.1.1.1
Стандартні еліптичні криві	Dstu4145WithDstu7564 (384)NamedCurves(PB)	1.2.804.2.1.1.1.3.6.2.1.2
Ступінь розширення основного поля стандартної еліптичної кривої $m=163$	Dstu4145WithDstu7564 (384)m163(PB)	1.2.804.2.1.1.1.3.6.2.1.2.0
Ступінь розширення основного поля стандартної еліптичної кривої $m=167$	Dstu4145WithDstu7564 (384)m167(PB)	1.2.804.2.1.1.1.3.6.2.1.2.1
Ступінь розширення основного поля стандартної еліптичної кривої $m=173$	Dstu4145WithDstu7564 (384)m173(PB)	1.2.804.2.1.1.1.3.6.2.1.2.2
Ступінь розширення основного поля стандартної еліптичної кривої $m=179$	Dstu4145WithDstu7564 (384)m179(PB)	1.2.804.2.1.1.1.3.6.2.1.2.3

Ступінь розширення основного поля стандартної еліптичної кривої $m=191$	Dstu4145WithDstu7564 (384)m191(PB)	1.2.804.2.1.1.1.1.3.6.2.1.2.4
Ступінь розширення основного поля стандартної еліптичної кривої $m=233$	Dstu4145WithDstu7564 (384)m233(PB)	1.2.804.2.1.1.1.1.3.6.2.1.2.5
Ступінь розширення основного поля стандартної еліптичної кривої $m=257$	Dstu4145WithDstu7564 (384)m257(PB)	1.2.804.2.1.1.1.1.3.6.2.1.2.6
Ступінь розширення основного поля стандартної еліптичної кривої $m=307$	Dstu4145WithDstu7564 (384)m307(PB)	1.2.804.2.1.1.1.1.3.6.2.1.2.7
Ступінь розширення основного поля стандартної еліптичної кривої $m=367$	Dstu4145WithDstu7564 (384)m367(PB)	1.2.804.2.1.1.1.1.3.6.2.1.2.8
Ступінь розширення основного поля стандартної еліптичної кривої $m=431$	Dstu4145WithDstu7564 (384)m431(PB)	1.2.804.2.1.1.1.1.3.6.2.1.2.9
Оптимальний нормальний базис Формат кодування полів Little-Endian	Dstu4145WithDstu7564 (384)onb	1.2.804.2.1.1.1.1.3.6.2.2
Спеціальні еліптичні криві	Dstu4145WithDstu7564 (384)SpecialCurves(ONB)	1.2.804.2.1.1.1.1.3.6.2.2.1
Формат кодування полів Big-Endian	Dstu4145WithDstu7564 (384)keyFormat(ONB)	1.2.804.2.1.1.1.1.3.6.2.2.1.1
Стандартні еліптичні криві	Dstu4145WithDstu7564 (384)NamedCurves(ONB)	1.2.804.2.1.1.1.1.3.6.2.2.2
Ступінь розширення основного поля стандартної еліптичної кривої $m=173$	Dstu4145WithDstu7564 (384)m173(ONB)	1.2.804.2.1.1.1.1.3.6.2.2.2.0
Ступінь розширення основного поля стандартної еліптичної кривої $m=179$	Dstu4145WithDstu7564 (384)m179(ONB)	1.2.804.2.1.1.1.1.3.6.2.2.2.1
Ступінь розширення основного поля стандартної еліптичної кривої $m=191$	Dstu4145WithDstu7564 (384)m191(ONB)	1.2.804.2.1.1.1.1.3.6.2.2.2.2
Ступінь розширення основного поля	Dstu4145WithDstu7564	1.2.804.2.1.1.1.1.3.6.2.2.2.3

стандартної еліптичної кривої $m=233$	(384)m233(ONB)	
Ступінь розширення основного поля стандартної еліптичної кривої $m=431$	Dstu4145WithDstu7564 (384)m431(ONB)	1.2.804.2.1.1.1.1.3.6.2.2.2.4
Алгоритм підпису за ДСТУ 4145-2002 з геш-функцією за ДСТУ 7564-2014 у режимі «Купина-512»	Dstu4145WithDstu7564 (512)	1.2.804.2.1.1.1.1.3.6.3
Поліноміальний базис Формат кодування полів Little-Endian	Dstu4145WithDstu7564 (512)pb	1.2.804.2.1.1.1.1.3.6.3.1
Спеціальні еліптичні криві	Dstu4145WithDstu7564 (512)SpecialCurves(PB)	1.2.804.2.1.1.1.1.3.6.3.1.1
Формат кодування полів Big-Endian	Dstu4145WithDstu7564 (512)keyFormat(PB)	1.2.804.2.1.1.1.1.3.6.3.1.1.1
Стандартні еліптичні криві	Dstu4145WithDstu7564 (512)NamedCurves(PB)	1.2.804.2.1.1.1.1.3.6.3.1.2
Ступінь розширення основного поля стандартної еліптичної кривої $m=163$	Dstu4145WithDstu7564 (512)m163(PB)	1.2.804.2.1.1.1.1.3.6.3.1.2.0
Ступінь розширення основного поля стандартної еліптичної кривої $m=167$	Dstu4145WithDstu7564 (512)m167(PB)	1.2.804.2.1.1.1.1.3.6.3.1.2.1
Ступінь розширення основного поля стандартної еліптичної кривої $m=173$	Dstu4145WithDstu7564 (512)m173(PB)	1.2.804.2.1.1.1.1.3.6.3.1.2.2
Ступінь розширення основного поля стандартної еліптичної кривої $m=179$	Dstu4145WithDstu7564 (512)m179(PB)	1.2.804.2.1.1.1.1.3.6.3.1.2.3
Ступінь розширення основного поля стандартної еліптичної кривої $m=191$	Dstu4145WithDstu7564 (512)m191(PB)	1.2.804.2.1.1.1.1.3.6.3.1.2.4
Ступінь розширення основного поля стандартної еліптичної кривої $m=233$	Dstu4145WithDstu7564 (512)m233(PB)	1.2.804.2.1.1.1.1.3.6.3.1.2.5
Ступінь розширення основного поля стандартної еліптичної кривої $m=257$	Dstu4145WithDstu7564 (512)m257(PB)	1.2.804.2.1.1.1.1.3.6.3.1.2.6

Ступінь розширення основного поля стандартної еліптичної кривої $m=307$	Dstu4145WithDstu7564 (512)m307(PB)	1.2.804.2.1.1.1.1.3.6.3.1.2.7
Ступінь розширення основного поля стандартної еліптичної кривої $m=367$	Dstu4145WithDstu7564 (512)m367(PB)	1.2.804.2.1.1.1.1.3.6.3.1.2.8
Ступінь розширення основного поля стандартної еліптичної кривої $m=431$	Dstu4145WithDstu7564 (512)m431(PB)	1.2.804.2.1.1.1.1.3.6.3.1.2.9
Оптимальний нормальний базис Формат кодування полів Little-Endian	Dstu4145WithDstu7564 (512)onb	1.2.804.2.1.1.1.1.3.6.3.2
Спеціальні еліптичні криві	Dstu4145WithDstu7564 (512)SpecialCurves(ONB)	1.2.804.2.1.1.1.1.3.6.3.2.1
Формат кодування полів Big-Endian	Dstu4145WithDstu7564 (512)keyFormat(ONB)	1.2.804.2.1.1.1.1.3.6.3.2.1.1
Стандартні еліптичні криві	Dstu4145WithDstu7564 (512)NamedCurves(ONB)	1.2.804.2.1.1.1.1.3.6.3.2.2
Ступінь розширення основного поля стандартної еліптичної кривої $m=173$	Dstu4145WithDstu7564 (512)m173(ONB)	1.2.804.2.1.1.1.1.3.6.3.2.2.0
Ступінь розширення основного поля стандартної еліптичної кривої $m=179$	Dstu4145WithDstu7564 (512)m179(ONB)	1.2.804.2.1.1.1.1.3.6.3.2.2.1
Ступінь розширення основного поля стандартної еліптичної кривої $m=191$	Dstu4145WithDstu7564 (512)m191(ONB)	1.2.804.2.1.1.1.1.3.6.3.2.2.2
Ступінь розширення основного поля стандартної еліптичної кривої $m=233$	Dstu4145WithDstu7564 (512)m233(ONB)	1.2.804.2.1.1.1.1.3.6.3.2.2.3
Ступінь розширення основного поля стандартної еліптичної кривої $m=431$	Dstu4145WithDstu7564 (512)m431(ONB)	1.2.804.2.1.1.1.1.3.6.3.2.2.4

Таблиця 3

Об'єктні ідентифікатори політики сертифікації

Опис	Скорочена назва	Значення
Політики сертифікації	cp	1.2.804.2.1.1.1.2
Ознака відповідності Закону	-	1.2.804.2.1.1.1.2.1

України «Про електронний цифровий підпис»		
Ознака того, що сертифікат сформовано як посилений	-	1.2.804.2.1.1.1.2.2
Політика формування позначок часу	TSPpolicy	1.2.804.2.1.1.1.2.3
Відповідь TSP з ЕЦП за ДСТУ 4145-2002 (поліноміальний базис) з геш-функцією за ГОСТ 34.311-95	TSPpolicyDstu4145WithGost34311(PB)	1.2.804.2.1.1.1.2.3.1
Відповідь TSP з ЕЦП за ДСТУ 4145-2002 (оптимальний нормальний базис) з геш-функцією за ГОСТ 34.311-95	TSPpolicyDSTU4145WithGost34311(ONB)	1.2.804.2.1.1.1.2.3.3
Відповідь TSP з ЕЦП за ДСТУ 4145-2002 з геш-функцією за ДСТУ 7564-2014	TSPpolicyDstu4145WithDstu7564	1.2.804.2.1.1.1.2.3.4
Відповідь TSP з ЕЦП за ДСТУ 4145-2002 з геш-функцією за ДСТУ 7564-2014 у режимі «Купина-256»	TSPpolicyDstu4145WithDstu7564(256)	1.2.804.2.1.1.1.2.3.4.1
Відповідь TSP з ЕЦП за ДСТУ 4145-2002 (поліноміальний базис) з геш-функцією за ДСТУ 7564-2014 у режимі «Купина-256»	TSPpolicyDstu4145WithDstu7564(256)PB	1.2.804.2.1.1.1.2.3.4.1.1
Відповідь TSP з ЕЦП за ДСТУ 4145-2002 (оптимальний нормальний базис) з геш-функцією за ДСТУ 7564-2014 у режимі «Купина-256»	TSPpolicyDstu4145WithDstu7564(256)ONB	1.2.804.2.1.1.1.2.3.4.1.2
Відповідь TSP з ЕЦП за ДСТУ 4145-2002 з геш-функцією за ДСТУ 7564-2014 у режимі «Купина-384»	TSPpolicyDstu4145WithDstu7564(384)	1.2.804.2.1.1.1.2.3.4.2
Відповідь TSP з ЕЦП за ДСТУ 4145-2002 (поліноміальний базис) з геш-функцією за ДСТУ 7564-2014 у режимі «Купина-384»	TSPpolicyDstu4145WithDstu7564(384)PB	1.2.804.2.1.1.1.2.3.4.2.1
Відповідь TSP з ЕЦП за ДСТУ 4145-2002 (оптимальний нормальний базис) з геш-функцією за ДСТУ 7564-2014 у режимі «Купина-384»	TSPpolicyDstu4145WithDstu7564(384)ONB	1.2.804.2.1.1.1.2.3.4.2.2
Відповідь TSP з ЕЦП за ДСТУ 4145-2002 з геш-функцією за ДСТУ 7564-2014 у режимі «Купина-512»	TSPpolicyDstu4145WithDstu7564(512)	1.2.804.2.1.1.1.2.3.4.3
Відповідь TSP з ЕЦП за ДСТУ 4145-2002 (поліноміальний базис) з геш-функцією за ДСТУ 7564-2014 у режимі	TSPpolicyDstu4145WithDstu7564(512)PB	1.2.804.2.1.1.1.2.3.4.3.1

«Купина-512»		
Відповідь TSP з ЕЦП за ДСТУ 4145-2002 (оптимальний нормальний базис) з ґеш-функцією за ДСТУ 7564-2014 у режимі «Купина-512»	TSPpolicyDstu4145With Dstu7564(512)ONB	1.2.804.2.1.1.1.2.3.4.3.2

».

**Директор Департаменту
приватного права Міністерства
юстиції України**

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



Олена ФЕРЕНС



Андрій ПУШКАРЬОВ