



**АДМІНІСТРАЦІЯ
ДЕРЖАВНОЇ СЛУЖБИ СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ
ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ
(АДМІНІСТРАЦІЯ ДЕРЖСПЕЦЗВ'ЯЗКУ)**

вул. Солом'янська, 13, м. Київ, 03110, тел. (044) 281-92-10, факс: (044) 281-94-83,
e-mail: info@dsszzi.gov.ua, сайт: www.dsszzi.gov.ua, код згідно з ЄДРПОУ 34620942

05.05.2021 № 04/05/02-1248

На № _____

від _____

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 29.04.2021

м. Київ

Виданий: Товариству з обмеженою відповідальністю «САЙФЕР ПРО»
(код ЄДРПОУ 42125815)

на підставі рішення Експертної комісії з питань проведення державної експертизи в сфері криптографічного захисту інформації Державної служби спеціального зв'язку та захисту інформації України, протокол від 29.04.2021 № 499.

Об'єкт експертизи: Програмне забезпечення «Система криптографічного захисту інформації «Шифр-Х.509» версії 2 ТЗ У 72.2-421258818-002:2020.

Розроблений (виготовлений): Товариством з обмеженою відповідальністю «САЙФЕР ПРО»
(код ЄДРПОУ 42125815).

Експертний заклад: Товариство з обмеженою відповідальністю «ДОЛЯ І КО. ЛТД»
(код ЄДРПОУ 01043342).

Висновки:

1. В об'єкті експертизи правильно реалізовано криптографічні алгоритми, визначені ДСТУ ГОСТ 28147:2009 (у режимах простої заміни, гамування, гамування зі зворотним зв'язком та обчислення імітовставки), ГОСТ 34.311-95, ДСТУ 4145-2002 (у поліноміальному базисі), ДСТУ 7624:2014 (у режимах ECB, OFB, CFB, CBC, CTR, CMAC), ДСТУ 7564:2014.
2. В об'єкті експертизи алгоритм генерації випадкових двійкових послідовностей відповідає додатку А ДСТУ 4145-2002.
3. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування TDEA визначений ДСТУ ISO/IEC 18033-3:2015 (в режимах ECB, OFB, CFB, CBC, CMAC, визначених ДСТУ ISO/IEC 10116:2019, в режимі CMAC, визначеному NIST SP 800-38B).
4. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування AES визначений ДСТУ ISO/IEC 18033-3:2015 (в режимах ECB, OFB, CFB, CBC, CTR, CMAC, визначених ДСТУ ISO/IEC 10116:2019, в режимі CMAC, визначеному NIST SP 800-38B).
5. В об'єкті експертизи правильно реалізовано криптографічний алгоритм шифрування RSA, визначений ДСТУ ISO/IEC 18033-2:2015.
6. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного підпису RSA, визначений IETF RFC 3447.
7. В об'єкті експертизи правильно реалізовано криптографічний алгоритм формування та перевіряння електронного підпису ECDSA, визначений ДСТУ ISO/IEC 14888-3:2019.

8. В об'єкті експертизи правильно реалізовано криптографічні алгоритми гешування SHA-224, SHA-256, SHA-384, SHA-512, визначені ДСТУ ISO/IEC 10118-3:2005.
9. В об'єкті експертизи правильно реалізовано криптографічні алгоритми гешування SHA-512/224, SHA-512/256, визначені ДСТУ ISO/IEC 10118-3:2018.
10. В об'єкті експертизи правильно реалізовано криптографічний протокол автономного узгодження ключів типу Діффі-Гелмана (KANIDH), визначений п. 8.2 ДСТУ ISO/IEC 15946-3:2006.
11. Формат та вміст статусів сертифікатів та запитів на їх отримання відповідає вимогам IETF RFC 6960 «Internet Public Key Infrastructure Online Certificate Status Protocol».
12. Формат та вміст сертифікатів і списків відкликаних сертифікатів відповідають вимогам ДСТУ ETSI EN 319 412:2016 (ETSI EN 319 412:2016, IDT) «Електронні підписи й інфраструктури (ESI). Профілі сертифікатів».
13. Формат та вміст підписаних даних (криптографічних повідомлень типу «signed-data») відповідають вимогам ДСТУ ETSI EN 319 122:2016 (ETSI EN 319 122:2016, IDT). Електронні підписи й інфраструктури (ESI). Цифрові підписи CAdES».
14. Формат та вміст позначок часу TSP та запитів на їх отримання відповідають вимогам ДСТУ ETSI EN 319 422:2016 (ETSI EN 319 422:2016, IDT). Електронні підписи й інфраструктури. Протокол мітки часу та профілі токенів мітки часу».
15. В об'єкті експертизи алгоритм формування початкових значень генератора випадкових двійкових послідовностей відповідає вимогам документа «Методика ініціалізації генератора випадкових двійкових послідовностей. UA.33349855.00001 – 01 94 01».
16. В об'єкті експертизи механізми зберігання особистих ключів електронного підпису відповідають вимогам документа «Система криптографічного захисту інформації «Шифр-Х.509» версії 2. Методика захисту особистого ключа».
17. Об'єкт експертизи відповідає вимогам технічного завдання ТЗ У 72.2-421258818-002:2020 в частині реалізації функцій криптографічних перетворень.
18. Методи захисту, реалізовані в об'єкті експертизи, відповідають вимогам до засобів криптографічного захисту інформації класу В2 (захист від порушника першого та нульового рівнів), визначеним в Положенні про порядок розроблення, виробництва та експлуатації засобів криптографічного захисту інформації, затвердженому наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20.07.2007 № 141, зареєстрованим в Міністерстві юстиції України 30.07.2007 за №862/14129 (зі змінами).
19. Об'єкт експертизи може бути використаний для криптографічного захисту інформації з обмеженим доступом (крім службової інформації та інформації, що становить державну таємницю) та відкритої інформації, вимога щодо захисту якої встановлена законом.
20. Об'єкт експертизи при спільному застосуванні із криптомодулем мережним «Шифр-НСМ» МКМ 42125815.ТД-01, що має експертний висновок за результатами державної експертизи у сфері криптографічного захисту інформації № 04/03/02-1762 від 08.07.2020 може бути використаний у якості засобу кваліфікованого електронного підпису чи печатки для надання електронних довірчих послуг.

Особливі умови (рекомендації): дія експертного висновку поширюється на зразки об'єкта експертизи, у яких криптографічні перетворення здійснюються програмними модулями, значення геш-функцій яких наведено в додатку до цього експертного висновку.

Термін дії експертного висновку – до 08.07.2025.

Голова Служби



Юрій ЩИГОЛЬ

**ЗНАЧЕННЯ ГЕШ-ФУНКЦІЙ
програмних модулів програмного забезпечення «Система криптографічного захисту
інформації «Шифр-Х.509» версії 2»**

Каталог CiX509_CA									
CiX509API.dll*	01B79814	69321B05	C3C5804F	D63F9C1D	0B66A532	66BB28C2	B7238A31	1FBE320A	
CiX509Core.dll*	E4CA8761	EE850B48	82737158	E0106BFC	F6D9C0E9	4C81C081	5EE1817F	B35EE820	
CiX509Server.dll*	93E107EE	2C3C25F0	6FCFB9F1	BA88C541	5B131157	6F079423	35678495	54C71446	
cixCSP_API.dll*	3A1B6A38	9C8DB668	3A59E990	344B2F1D	CDFBEF00	E414BD05	B792C563	D42C07E7	
cphpki.dll*	28620C7A	BC4A5193	5DBFD29D	E1858CC2	1F1D3054	93B07B61	F8FE7BD8	300571A4	
cx509pki.dll*	EA57FEA3	33C0D400	33C0290E	5047BBC9	E2AD6AA4	C4E79B06	72E696A1	BB7B3653	
dstu4145.dll*	3AE2BCF5	06F7D107	1D88B3C8	EEA3F0C5	871FAF67	1F55C0D8	33636D69	B9B45D95	
Каталог CiX509_CAdm									
CiX509API.dll*	01B79814	69321B05	C3C5804F	D63F9C1D	0B66A532	66BB28C2	B7238A31	1FBE320A	
CiX509Core.dll*	E4CA8761	EE850B48	82737158	E0106BFC	F6D9C0E9	4C81C081	5EE1817F	B35EE820	
CiX509Server.dll*	93E107EE	2C3C25F0	6FCFB9F1	BA88C541	5B131157	6F079423	35678495	54C71446	
cixCSP_API.dll*	3A1B6A38	9C8DB668	3A59E990	344B2F1D	CDFBEF00	E414BD05	B792C563	D42C07E7	
cx509pki.dll*	EA57FEA3	33C0D400	33C0290E	5047BBC9	E2AD6AA4	C4E79B06	72E696A1	BB7B3653	
dstu4145.dll*	3AE2BCF5	06F7D107	1D88B3C8	EEA3F0C5	871FAF67	1F55C0D8	33636D69	B9B45D95	
Каталог CiX509_CAServer									
CiX509API.dll*	01B79814	69321B05	C3C5804F	D63F9C1D	0B66A532	66BB28C2	B7238A31	1FBE320A	
CiX509Core.dll*	E4CA8761	EE850B48	82737158	E0106BFC	F6D9C0E9	4C81C081	5EE1817F	B35EE820	
CiX509Server.dll*	93E107EE	2C3C25F0	6FCFB9F1	BA88C541	5B131157	6F079423	35678495	54C71446	
cixCSP_API.dll*	3A1B6A38	9C8DB668	3A59E990	344B2F1D	CDFBEF00	E414BD05	B792C563	D42C07E7	
cx509pki.dll*	EA57FEA3	33C0D400	33C0290E	5047BBC9	E2AD6AA4	C4E79B06	72E696A1	BB7B3653	
dstu4145.dll*	3AE2BCF5	06F7D107	1D88B3C8	EEA3F0C5	871FAF67	1F55C0D8	33636D69	B9B45D95	
Каталог CiX509_chk									
CiX509API.dll*	01B79814	69321B05	C3C5804F	D63F9C1D	0B66A532	66BB28C2	B7238A31	1FBE320A	
CiX509Core.dll*	E4CA8761	EE850B48	82737158	E0106BFC	F6D9C0E9	4C81C081	5EE1817F	B35EE820	
cixCSP_API.dll*	3A1B6A38	9C8DB668	3A59E990	344B2F1D	CDFBEF00	E414BD05	B792C563	D42C07E7	
cx509pki.dll*	EA57FEA3	33C0D400	33C0290E	5047BBC9	E2AD6AA4	C4E79B06	72E696A1	BB7B3653	
dstu4145.dll*	3AE2BCF5	06F7D107	1D88B3C8	EEA3F0C5	871FAF67	1F55C0D8	33636D69	B9B45D95	
Каталог CiX509_CtxViewer									
CiX509API.dll*	01B79814	69321B05	C3C5804F	D63F9C1D	0B66A532	66BB28C2	B7238A31	1FBE320A	
CiX509Core.dll*	E4CA8761	EE850B48	82737158	E0106BFC	F6D9C0E9	4C81C081	5EE1817F	B35EE820	
cixCSP_API.dll*	3A1B6A38	9C8DB668	3A59E990	344B2F1D	CDFBEF00	E414BD05	B792C563	D42C07E7	
cx509pki.dll*	EA57FEA3	33C0D400	33C0290E	5047BBC9	E2AD6AA4	C4E79B06	72E696A1	BB7B3653	
dstu4145.dll*	3AE2BCF5	06F7D107	1D88B3C8	EEA3F0C5	871FAF67	1F55C0D8	33636D69	B9B45D95	
Каталог CiX509_CVR									
CiX509API.dll*	01B79814	69321B05	C3C5804F	D63F9C1D	0B66A532	66BB28C2	B7238A31	1FBE320A	
CiX509Core.dll*	E4CA8761	EE850B48	82737158	E0106BFC	F6D9C0E9	4C81C081	5EE1817F	B35EE820	
CiX509_CVR.exe*	931EA593	6110698E	C39CEA6F	BB5E1866	9A71724C	B9F48AF5	663B63FF	E1ED4118	
cixCSP_API.dll*	3A1B6A38	9C8DB668	3A59E990	344B2F1D	CDFBEF00	E414BD05	B792C563	D42C07E7	
cphpki.dll*	28620C7A	BC4A5193	5DBFD29D	E1858CC2	1F1D3054	93B07B61	F8FE7BD8	300571A4	
cx509pki.dll*	EA57FEA3	33C0D400	33C0290E	5047BBC9	E2AD6AA4	C4E79B06	72E696A1	BB7B3653	
dstu4145.dll*	3AE2BCF5	06F7D107	1D88B3C8	EEA3F0C5	871FAF67	1F55C0D8	33636D69	B9B45D95	
Каталог CiX509_Java_lib									
ccx509auth.jar*	52EC8E9E	E8E9F25E	0D7B3924	CCB9072F	2C99D404	F850F03D	86C9FECC	E2F2C26D	
ccx509v1.20.jar*	0FC563A9	DD22B2CD	1F430269	A1BF5C7D	5DC55C14	2A71B946	C1F980C3	79EDAFDB	
ccx509v1.22.jar*	3C802A5D	50C9353C	EE49B8F8	97A9FC8F	1A73ADF6	EF167402	096574B1	947EAC58	
cipherplus.jar*	8FB24B43	27208537	E3B901E3	D15362BD	F7A083EF	233553A2	CDDC2B53	05299D4C	
Каталог CiX509_KCC									
CiX509_KCC.exe*	D1208942	6684633E	4E094758	8CD7DD91	E3A1BBB0	41687F9A	762BBD71	580BE3D9	
Каталог CiX509_LogViewer									
CiX509API.dll*	01B79814	69321B05	C3C5804F	D63F9C1D	0B66A532	66BB28C2	B7238A31	1FBE320A	
CiX509Core.dll*	E4CA8761	EE850B48	82737158	E0106BFC	F6D9C0E9	4C81C081	5EE1817F	B35EE820	
cixCSP_API.dll*	3A1B6A38	9C8DB668	3A59E990	344B2F1D	CDFBEF00	E414BD05	B792C563	D42C07E7	
cx509pki.dll*	EA57FEA3	33C0D400	33C0290E	5047BBC9	E2AD6AA4	C4E79B06	72E696A1	BB7B3653	
dstu4145.dll*	2C044E31	3AA74559	1FF522D9	23085CD9	50EFAEEE	D527D179	915E81C9	A171CACE	
Каталог CiX509_OCC									
CiX509API.dll*	01B79814	69321B05	C3C5804F	D63F9C1D	0B66A532	66BB28C2	B7238A31	1FBE320A	
CiX509Core.dll*	E4CA8761	EE850B48	82737158	E0106BFC	F6D9C0E9	4C81C081	5EE1817F	B35EE820	
cixCSP_API.dll*	3A1B6A38	9C8DB668	3A59E990	344B2F1D	CDFBEF00	E414BD05	B792C563	D42C07E7	
cx509pki.dll*	EA57FEA3	33C0D400	33C0290E	5047BBC9	E2AD6AA4	C4E79B06	72E696A1	BB7B3653	
dstu4145.dll*	3AE2BCF5	06F7D107	1D88B3C8	EEA3F0C5	871FAF67	1F55C0D8	33636D69	B9B45D95	
Каталог CiX509_OCSPServer									
CiX509API.dll*	01B79814	69321B05	C3C5804F	D63F9C1D	0B66A532	66BB28C2	B7238A31	1FBE320A	
CiX509Core.dll*	E4CA8761	EE850B48	82737158	E0106BFC	F6D9C0E9	4C81C081	5EE1817F	B35EE820	
cixCSP_API.dll*	3A1B6A38	9C8DB668	3A59E990	344B2F1D	CDFBEF00	E414BD05	B792C563	D42C07E7	
cx509pki.dll*	EA57FEA3	33C0D400	33C0290E	5047BBC9	E2AD6AA4	C4E79B06	72E696A1	BB7B3653	
dstu4145.dll*	3AE2BCF5	06F7D107	1D88B3C8	EEA3F0C5	871FAF67	1F55C0D8	33636D69	B9B45D95	

ocspsrv.exe*	89210265	AE316DF7	60279CEC	53CAF2B4	AB1A2793	D79814D4	F0B924B9	92A92D17
Каталог CiX509_Office_Addin								
AddinCommon.dll*	78080D08	A2276F82	FB9C5AE0	36A1C405	52705BFF	F521DA3B	8EF62554	74B4BDCD
CiX509API.dll*	01B79814	69321B05	C3C5804F	D63F9C1D	0B66A532	66BB28C2	B7238A31	1FBE320A
CiX509Core.dll*	E4CA8761	EE850B48	82737158	E0106BFC	F6D9C0E9	4C81C081	5EE1817F	B35EE820
CiX509Server.dll*	93E107EE	2C3C25F0	6FCFB9F1	BA88C541	5B131157	6F079423	35678495	54C71446
CiXCSP_API.dll*	3A1B6A38	9C8DB668	3A59E990	344B2F1D	CDFBEF00	E414BD05	B792C563	D42C07E7
cphpki.dll*	28620C7A	BC4A5193	5DBFD29D	E1858CC2	1F1D3054	93B07B61	F8FE7BD8	300571A4
cx509pki.dll*	EA57FEA3	33C0D400	33C0290E	5047BBC9	E2AD6AA4	C4E79B06	72E696A1	BB7B3653
dstu4145.dll*	3AE2BCF5	06F7D107	1D88B3C8	EEA3F0C5	871FAF67	1F55C0D8	33636D69	B9B45D95
Excel2010Crypto.dll*	3069D17B	18DFCE8B	78ED69B0	C975B53B	24273BB5	43D1C077	847AB0F9	14A34967
LibAdapter.dll*	4E2B2555	D81FDDE7	F7EB483E	DE25E952	F00815D0	BF4920D8	332938DE	F9E84BB1
Outlook2010Crypto.dll*	A99AF69B	E1340D77	D5E68667	434592A2	9F70DE4B	897BAAF0	DF9211FF	E128BDC4
PowerPoint2010Crypto.dll*	B2473905	972888E6	A77E5BA4	EEDCC886	8E55F999	3748C785	1670281F	A31E37C4
Word2010Crypto.dll*	C5AC091C	61E034C5	D3DDB9C6	8CFACED3	C071D5B4	C65E50EA	2B5F5529	D3A4786E
Каталог CiX509_Opr								
CiX509API.dll*	01B79814	69321B05	C3C5804F	D63F9C1D	0B66A532	66BB28C2	B7238A31	1FBE320A
CiX509Core.dll*	E4CA8761	EE850B48	82737158	E0106BFC	F6D9C0E9	4C81C081	5EE1817F	B35EE820
CiXCSP_API.dll*	3A1B6A38	9C8DB668	3A59E990	344B2F1D	CDFBEF00	E414BD05	B792C563	D42C07E7
cx509pki.dll*	EA57FEA3	33C0D400	33C0290E	5047BBC9	E2AD6AA4	C4E79B06	72E696A1	BB7B3653
dstu4145.dll*	3AE2BCF5	06F7D107	1D88B3C8	EEA3F0C5	871FAF67	1F55C0D8	33636D69	B9B45D95
Каталог CiX509_PW								
careport1.dll*	E11506B7	5B6AFC2A	FBCAD643	3603DEE3	B7CC816B	54168D93	239C5254	0D1F59DB
careport2.dll*	7FE99056	4D56A345	0CDC1820	6A6DF353	8D9E6DFD	A5D40EF6	92E3F941	FC996700
CiX509-PW.exe*	28B227F8	E424C14B	744E45DA	E997AD64	0573A2AC	D91BB7AF	00FC9C63	7D9881DB
CiX509API.dll*	01B79814	69321B05	C3C5804F	D63F9C1D	0B66A532	66BB28C2	B7238A31	1FBE320A
CiX509Core.dll*	E4CA8761	EE850B48	82737158	E0106BFC	F6D9C0E9	4C81C081	5EE1817F	B35EE820
CiXCSP_API.dll*	3A1B6A38	9C8DB668	3A59E990	344B2F1D	CDFBEF00	E414BD05	B792C563	D42C07E7
cixtsa.dll*	F4C05B10	D2E3513F	4FF1DC33	44CA9B07	5968B62F	CBF21A05	E9FB19EB	7C2E7788
cphpki.dll*	28620C7A	BC4A5193	5DBFD29D	E1858CC2	1F1D3054	93B07B61	F8FE7BD8	300571A4
cx509pki.dll*	EA57FEA3	33C0D400	33C0290E	5047BBC9	E2AD6AA4	C4E79B06	72E696A1	BB7B3653
dstu4145.dll*	3AE2BCF5	06F7D107	1D88B3C8	EEA3F0C5	871FAF67	1F55C0D8	33636D69	B9B45D95
tsareport1.dll*	2B71C753	A5529222	40FA5F50	9158D075	06F012E5	D9E0230A	D196D7AD	9D8621A1
tsareport2.dll*	70F4C3FB	1D865F70	B884C4A9	BF90BAFF	D0815BC3	847CBE3B	FD3D54B7	F2011514
Каталог CiX509_RA								
CiX509API.dll*	01B79814	69321B05	C3C5804F	D63F9C1D	0B66A532	66BB28C2	B7238A31	1FBE320A
CiX509Core.dll*	E4CA8761	EE850B48	82737158	E0106BFC	F6D9C0E9	4C81C081	5EE1817F	B35EE820
CiXCSP_API.dll*	3A1B6A38	9C8DB668	3A59E990	344B2F1D	CDFBEF00	E414BD05	B792C563	D42C07E7
cx509pki.dll*	EA57FEA3	33C0D400	33C0290E	5047BBC9	E2AD6AA4	C4E79B06	72E696A1	BB7B3653
dstu4145.dll*	3AE2BCF5	06F7D107	1D88B3C8	EEA3F0C5	871FAF67	1F55C0D8	33636D69	B9B45D95
Каталог CiX509_RA_CM								
CiX509API.dll*	01B79814	69321B05	C3C5804F	D63F9C1D	0B66A532	66BB28C2	B7238A31	1FBE320A
CiX509Core.dll*	E4CA8761	EE850B48	82737158	E0106BFC	F6D9C0E9	4C81C081	5EE1817F	B35EE820
CiXCSP_API.dll*	3A1B6A38	9C8DB668	3A59E990	344B2F1D	CDFBEF00	E414BD05	B792C563	D42C07E7
cx509pki.dll*	EA57FEA3	33C0D400	33C0290E	5047BBC9	E2AD6AA4	C4E79B06	72E696A1	BB7B3653
dstu4145.dll*	3AE2BCF5	06F7D107	1D88B3C8	EEA3F0C5	871FAF67	1F55C0D8	33636D69	B9B45D95
Каталог CiX509_RRA								
CiX509API.dll*	01B79814	69321B05	C3C5804F	D63F9C1D	0B66A532	66BB28C2	B7238A31	1FBE320A
CiX509Core.dll*	E4CA8761	EE850B48	82737158	E0106BFC	F6D9C0E9	4C81C081	5EE1817F	B35EE820
CiXCSP_API.dll*	3A1B6A38	9C8DB668	3A59E990	344B2F1D	CDFBEF00	E414BD05	B792C563	D42C07E7
cx509pki.dll*	EA57FEA3	33C0D400	33C0290E	5047BBC9	E2AD6AA4	C4E79B06	72E696A1	BB7B3653
dstu4145.dll*	3AE2BCF5	06F7D107	1D88B3C8	EEA3F0C5	871FAF67	1F55C0D8	33636D69	B9B45D95
Каталог CiX509_SA								
CiX509-SA.exe*	9D0C1659	68183E69	C5C9165A	E6389F63	8559AB60	11D22F1D	B3760398	2B5D985A
CiX509API.dll*	01B79814	69321B05	C3C5804F	D63F9C1D	0B66A532	66BB28C2	B7238A31	1FBE320A
CiX509Core.dll*	E4CA8761	EE850B48	82737158	E0106BFC	F6D9C0E9	4C81C081	5EE1817F	B35EE820
CiX509Server.dll*	93E107EE	2C3C25F0	6FCFB9F1	BA88C541	5B131157	6F079423	35678495	54C71446
CiXCSP_API.dll*	3A1B6A38	9C8DB668	3A59E990	344B2F1D	CDFBEF00	E414BD05	B792C563	D42C07E7
cphpki.dll*	28620C7A	BC4A5193	5DBFD29D	E1858CC2	1F1D3054	93B07B61	F8FE7BD8	300571A4
cx509pki.dll*	EA57FEA3	33C0D400	33C0290E	5047BBC9	E2AD6AA4	C4E79B06	72E696A1	BB7B3653
dstu4145.dll*	2C044E31	3AA74559	1FF522D9	23085CD9	50EFAEEE	D527D179	915E81C9	A171CACE
Каталог CiX509_TSPServer								
CiX509API.dll*	01B79814	69321B05	C3C5804F	D63F9C1D	0B66A532	66BB28C2	B7238A31	1FBE320A
CiX509Core.dll*	E4CA8761	EE850B48	82737158	E0106BFC	F6D9C0E9	4C81C081	5EE1817F	B35EE820
CiXCSP_API.dll*	3A1B6A38	9C8DB668	3A59E990	344B2F1D	CDFBEF00	E414BD05	B792C563	D42C07E7
cx509pki.dll*	EA57FEA3	33C0D400	33C0290E	5047BBC9	E2AD6AA4	C4E79B06	72E696A1	BB7B3653
dstu4145.dll*	3AE2BCF5	06F7D107	1D88B3C8	EEA3F0C5	871FAF67	1F55C0D8	33636D69	B9B45D95
tssvc.exe*	1CABEA3F	FF2BB733	5E7ACAAE	93EEE83C	4812C472	A4B28C39	9FB7E82D	12D77189
Каталог CiX509_Win32_lib								
CiX509API.dll*	01B79814	69321B05	C3C5804F	D63F9C1D	0B66A532	66BB28C2	B7238A31	1FBE320A
CiX509Core.dll*	E4CA8761	EE850B48	82737158	E0106BFC	F6D9C0E9	4C81C081	5EE1817F	B35EE820
CiXCSP_API.dll*	3A1B6A38	9C8DB668	3A59E990	344B2F1D	CDFBEF00	E414BD05	B792C563	D42C07E7
cphpki.dll*	28620C7A	BC4A5193	5DBFD29D	E1858CC2	1F1D3054	93B07B61	F8FE7BD8	300571A4
cx509pki.dll*	EA57FEA3	33C0D400	33C0290E	5047BBC9	E2AD6AA4	C4E79B06	72E696A1	BB7B3653

dstu4145.dll*	3AE2BCF5 06F7D107 1D88B3C8 EAA3F0C5 871FAF67 1F55C0D8 33636D69 B9B45D95
Каталог CiX509_Win32_lib_RA	
CiX509API.dll*	01B79814 69321B05 C3C5804F D63F9C1D 0B66A532 66BB28C2 B7238A31 1FBE320A
CiX509Core.dll*	E4CA8761 EE850B48 82737158 E0106BFC F6D9C0E9 4C81C081 5EE1817F B35EE820
CiX509Server.dll*	93E107EE 2C3C25F0 6FCFB9F1 BA88C541 5B131157 6F079423 35678495 54C71446
CiXCSP_API.dll*	3A1B6A38 9C8DB668 3A59E990 344B2F1D CDFBEF00 E414BD05 B792C563 D42C07E7
cx509pki.dll*	EA57FEA3 33C0D400 33C0290E 5047BBC9 E2AD6AA4 C4E79B06 72E696A1 BB7B3653
dstu4145.dll*	3AE2BCF5 06F7D107 1D88B3C8 EAA3F0C5 871FAF67 1F55C0D8 33636D69 B9B45D95

Розрахунок геш-функцій здійснено відповідно до ГОСТ 34.311-95 з урахуванням значення нульового стартового вектора та ДКЕ № 1 з додатка № 1 до Інструкції про порядок постачання і використання ключів до засобів криптографічного захисту інформації, затвердженої наказом Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 12.06.2007 № 114, зареєстрованої в Міністерстві юстиції України 25.06.2007 за № 729/13996.

Голова Служби



Юрій ШИГОЛЬ