



ДЕРЖАВНА СЛУЖБА СПЕЦІАЛЬНОГО ЗВ'ЯЗКУ ТА ЗАХИСТУ ІНФОРМАЦІЇ УКРАЇНИ

вул. Солом'янська, 13, м. Київ, 03680,
тел. (044) 281-92-10, факс: (044) 281-94-83, e-mail: info@dsszzi.gov.ua

27.07.2015 № 05/02/02-3146

ЕКСПЕРТНИЙ ВИСНОВОК

Дата видачі: 27.07.2015

м. Київ

Виданий: Товариству з обмеженою відповідальністю "САЙФЕР БІС" (код ЄДРПОУ 33349855)

на підставі рішення Експертної комісії з питань проведення державної експертизи у сфері криптографічного захисту інформації Державної служби спеціального зв'язку та захисту інформації України, протокол від 27.07.2015 № 202.

Об'єкт експертизи: Система криптографічного захисту інформації "Шифр-Х.509" ТЗ У 72.2 23154898 002:2007.

Розроблений (виготовлений): Товариством з обмеженою відповідальністю "САЙФЕР БІС" (код ЄДРПОУ 33349855).

Експертний заклад: Інститут спеціального зв'язку та захисту інформації НТУУ "КПІ" (код ЄДРПОУ 34979237).

Висновки:

1. Програмні криптографічні примітиви, реалізовані в об'єкті експертизи відповідають вимогам технічного завдання "Виріб програмний "Шифр+". Бібліотека функцій криптографічних перетворень. Версія 1.0. ТЗ У 72.2 23154898 001:2007".
2. Формат заявок на формування сертифікатів відкритих ключів, що створюються та обробляються об'єктом експертизи, відповідає вимогам PKCS#10.
3. Механізми зберігання особистих ключів електронного цифрового підпису, реалізовані в об'єкті експертизи, відповідають вимогам документу "Методика захисту особистого ключа ЦСК" (до вх. № 4787 від 13.12.2012).
4. Об'єкт експертизи відповідає вимогам технічного завдання ТЗ У 72.2 23154898 002:2007, доповнення № 1 ТЗ У 72.2 23154898 002:2007-1 та доповнення № 2 ТЗ У 72.2 23154898 002:2007-2 до нього, в частині реалізації функцій криптографічних перетворень.
5. Формат посиленого сертифіката відкритого ключа, структура об'єктних ідентифікаторів для криптоалгоритмів, що є державними стандартами, формат списку відкликаних сертифікатів, формат підписаних даних, протокол фіксування часу, протокол визначення статусу сертифіката, які реалізовані та використовуються в об'єкті експертизи, відповідають вимогам наказу Міністерства юстиції України та Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 20.08.2012 № 1236/5/453 "Про затвердження вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису".
6. Формати криптографічних повідомлень та протоколи розподілу ключів, які реалізовані та використовуються в об'єкті експертизи, відповідають вимогам наказу Адміністрації Державної служби спеціального зв'язку та захисту інформації України від 18.12.2012 № 739 "Про затвердження Вимог до форматів, криптографічних повідомлень", зареєстрованого в Міністерстві юстиції України 14.01.2013 за № 108/22640.
7. 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.

8. Об'єкт експертизи може бути використаний для побудови акредитованих центрів сертифікації ключів.

Особливі умови (рекомендації): дія експертного висновку поширюється на зразки об'єкта експертизи зі значеннями геш-функцій програмних модулів, що наведені в додатку до цього експертного висновку.

Термін дії експертного висновку – до 27.07.2020.

Голова Служби



Л.О.Свдоченко

Значення геш-функцій програмних модулів системи криптографічного захисту інформації
«Шифр-Х.509»

Каталог CiX509 CA

CiX509API.dll*	8E148B0C	01FE1348	49BCC30C	931B70C5	2EA94EAC	22782A75	737DCB05	C5DEA660
CiX509Core.dll*	94C1557F	8760DD69	685B418E	A5E4AD9B	E512C21F	71FFEA65	5392F698	0FA4BA00
CiX509Server.dll*	BB24A299	E1AD9F9E	120DB7F4	A737763B	39D202B9	F1661DF4	DE8F49E6	B4CBA8B8
cixCSP_API.dll*	C04F593E	9D69BA11	B4F34C34	F15BF056	5E2CDED2	88F091DA	5861A43D	92FA097B
dstu4145.dll*	2C044E31	3AA74559	1FF522D9	23085CD9	50EFAEEE	D527D179	915E81C9	A171CACE

Каталог CiX509 CAdm

CiX509API.dll*	8E148B0C	01FE1348	49BCC30C	931B70C5	2EA94EAC	22782A75	737DCB05	C5DEA660
CiX509Core.dll*	94C1557F	8760DD69	685B418E	A5E4AD9B	E512C21F	71FFEA65	5392F698	0FA4BA00
CiX509Server.dll*	BB24A299	E1AD9F9E	120DB7F4	A737763B	39D202B9	F1661DF4	DE8F49E6	B4CBA8B8
cixCSP_API.dll*	C04F593E	9D69BA11	B4F34C34	F15BF056	5E2CDED2	88F091DA	5861A43D	92FA097B
dstu4145.dll*	2C044E31	3AA74559	1FF522D9	23085CD9	50EFAEEE	D527D179	915E81C9	A171CACE

Каталог CiX509 CAServer

CiX509API.dll*	8E148B0C	01FE1348	49BCC30C	931B70C5	2EA94EAC	22782A75	737DCB05	C5DEA660
CiX509Core.dll*	94C1557F	8760DD69	685B418E	A5E4AD9B	E512C21F	71FFEA65	5392F698	0FA4BA00
CiX509Server.dll*	BB24A299	E1AD9F9E	120DB7F4	A737763B	39D202B9	F1661DF4	DE8F49E6	B4CBA8B8
cixCSP_API.dll*	C04F593E	9D69BA11	B4F34C34	F15BF056	5E2CDED2	88F091DA	5861A43D	92FA097B
dstu4145.dll*	2C044E31	3AA74559	1FF522D9	23085CD9	50EFAEEE	D527D179	915E81C9	A171CACE

Каталог CiX509 chk

CiX509API.dll*	8E148B0C	01FE1348	49BCC30C	931B70C5	2EA94EAC	22782A75	737DCB05	C5DEA660
CiX509Core.dll*	94C1557F	8760DD69	685B418E	A5E4AD9B	E512C21F	71FFEA65	5392F698	0FA4BA00
CiX509Server.dll*	BB24A299	E1AD9F9E	120DB7F4	A737763B	39D202B9	F1661DF4	DE8F49E6	B4CBA8B8
cixCSP_API.dll*	C04F593E	9D69BA11	B4F34C34	F15BF056	5E2CDED2	88F091DA	5861A43D	92FA097B
dstu4145.dll*	2C044E31	3AA74559	1FF522D9	23085CD9	50EFAEEE	D527D179	915E81C9	A171CACE

Каталог CiX509 CtxViewer

CiX509API.dll*	8E148B0C	01FE1348	49BCC30C	931B70C5	2EA94EAC	22782A75	737DCB05	C5DEA660
CiX509Core.dll*	94C1557F	8760DD69	685B418E	A5E4AD9B	E512C21F	71FFEA65	5392F698	0FA4BA00
cixCSP_API.dll*	C04F593E	9D69BA11	B4F34C34	F15BF056	5E2CDED2	88F091DA	5861A43D	92FA097B
dstu4145.dll*	2C044E31	3AA74559	1FF522D9	23085CD9	50EFAEEE	D527D179	915E81C9	A171CACE

Каталог CiX509 CVR

CiX509_CVR.exe*	8B2EE3C6	20D289A5	E6F73277	70389113	D7C3E53A	D5484381	1F16D048	3F22A5E2
CiX509API.dll*	8E148B0C	01FE1348	49BCC30C	931B70C5	2EA94EAC	22782A75	737DCB05	C5DEA660
CiX509Core.dll*	94C1557F	8760DD69	685B418E	A5E4AD9B	E512C21F	71FFEA65	5392F698	0FA4BA00
cixCSP_API.dll*	E987EB70	D814CB35	970A966D	EB9FABEC	9C53C950	D8EEB363	1F5DD222	F1EC936F
cphpki.dll*	A285720A	21C47E88	9DA62421	6FBE5BF2	37A3BC73	3E34BA57	429A8B94	CFB53592
dstu4145.dll*	2C044E31	3AA74559	1FF522D9	23085CD9	50EFAEEE	D527D179	915E81C9	A171CACE

Каталог CiX509 Java lib

ccx509auth.jar*	52EC8E9E	E8E9F25E	0D7B3924	CCB9072F	2C99D404	F850F03D	86C9FECC	E2F2C26D
ccx509v1.20.jar*	0FC563A9	DD22B2CD	1F430269	A1BF5C7D	5DC55C14	2A71B946	C1F980C3	79EDA FDB
cipherplus.jar*	F130DA95	73241FFD	A24FB77B	C95A4959	68257274	1ACCB4FF	3B01EFC2	80CF1111

Каталог CiX509 KCC

CiX509_KCC.exe*	B8D4C7FA	D4FB550B	E2D0966E	C525E929	98B5B3FD	0EF50141	B059B924	74BDD607
-----------------	----------	----------	----------	----------	----------	----------	----------	----------

Каталог CiX509 LogViewer

CiX509API.dll*	8E148B0C	01FE1348	49BCC30C	931B70C5	2EA94EAC	22782A75	737DCB05	C5DEA660
CiX509Core.dll*	94C1557F	8760DD69	685B418E	A5E4AD9B	E512C21F	71FFEA65	5392F698	0FA4BA00
cixCSP_API.dll*	C04F593E	9D69BA11	B4F34C34	F15BF056	5E2CDED2	88F091DA	5861A43D	92FA097B
dstu4145.dll*	2C044E31	3AA74559	1FF522D9	23085CD9	50EFAEEE	D527D179	915E81C9	A171CACE

Каталог CiX509 OCC

CiX509API.dll*	8E148B0C	01FE1348	49BCC30C	931B70C5	2EA94EAC	22782A75	737DCB05	C5DEA660
CiX509Core.dll*	94C1557F	8760DD69	685B418E	A5E4AD9B	E512C21F	71FFEA65	5392F698	0FA4BA00
cixCSP_API.dll*	C04F593E	9D69BA11	B4F34C34	F15BF056	5E2CDED2	88F091DA	5861A43D	92FA097B
dstu4145.dll*	2C044E31	3AA74559	1FF522D9	23085CD9	50EFAEEE	D527D179	915E81C9	A171CACE

Каталог CiX509 OCSPServer

CiX509API.dll*	8E148B0C	01FE1348	49BCC30C	931B70C5	2EA94EAC	22782A75	737DCB05	C5DEA660
CiX509Core.dll*	94C1557F	8760DD69	685B418E	A5E4AD9B	E512C21F	71FFEA65	5392F698	0FA4BA00
cixCSP_API.dll*	C04F593E	9D69BA11	B4F34C34	F15BF056	5E2CDED2	88F091DA	5861A43D	92FA097B
dstu4145.dll*	2C044E31	3AA74559	1FF522D9	23085CD9	50EFAEEE	D527D179	915E81C9	A171CACE
ocspsrv.exe*	BDAD17C7	511A3739	E75AFA1D	1424BA9D	74234366	B6005813	907F50AA	01A8AC7F

Каталог CiX509 Office Addin

AddinCommon.dll*	78080D08	A2276F82	FB9C5AE0	36A1C405	52705BFF	F521DA3B	8EF62554	74B4BDCD
CiX509API.dll*	8E148B0C	01FE1348	49BCC30C	931B70C5	2EA94EAC	22782A75	737DCB05	C5DEA660
CiX509Core.dll*	94C1557F	8760DD69	685B418E	A5E4AD9B	E512C21F	71FFEA65	5392F698	0FA4BA00
cixCSP_API.dll*	06FEC480	CCD2F5D9	9E4D7BB5	38D378A8	61136FA7	5D0916A4	82C7E23D	9BB392DA
cphpki.dll*	A285720A	21C47E88	9DA62421	6FBE5BF2	37A3BC73	3E34BA57	429A8B94	CFB53592

dstu4145.dll*	2C044E31	3AA74559	1FF522D9	23085CD9	50EFAEEE	D527D179	915E81C9	A171CACE
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*	8E148B0C	01FE1348	49BCC30C	931B70C5	2EA94EAC	22782A75	737DCB05	C5DEA660
CiX509Core.dll*	94C1557F	8760DD69	685B418E	A5E4AD9B	E512C21F	71FFEA65	5392F698	0FA4BA00
cixCSP_API.dll*	C04F593E	9D69BA11	B4F34C34	F15BF056	5E2CDED2	88F091DA	5861A43D	92FA097B
dstu4145.dll*	2C044E31	3AA74559	1FF522D9	23085CD9	50EFAEEE	D527D179	915E81C9	A171CACE

Каталог CiX509 PKM

CiX509API.dll*	8E148B0C	01FE1348	49BCC30C	931B70C5	2EA94EAC	22782A75	737DCB05	C5DEA660
CiX509Core.dll*	94C1557F	8760DD69	685B418E	A5E4AD9B	E512C21F	71FFEA65	5392F698	0FA4BA00
cixCSP_API.dll*	C04F593E	9D69BA11	B4F34C34	F15BF056	5E2CDED2	88F091DA	5861A43D	92FA097B
dstu4145.dll*	2C044E31	3AA74559	1FF522D9	23085CD9	50EFAEEE	D527D179	915E81C9	A171CACE

Каталог CiX509 PW

careport1.dll*	0A2725D2	0486B790	973CF8CB	60E6A6E8	F9CFA9DB	C800E38D	A24037BB	0150E1BF
careport2.dll*	99C3B69F	0E66C932	27C9CED1	C67476EB	386B5769	4D8BC567	4A899EE3	85AD6812
CiX509API.dll*	8E148B0C	01FE1348	49BCC30C	931B70C5	2EA94EAC	22782A75	737DCB05	C5DEA660
CiX509Core.dll*	94C1557F	8760DD69	685B418E	A5E4AD9B	E512C21F	71FFEA65	5392F698	0FA4BA00
CiX509-PW.exe*	71FF5312	BDB984BB	8A58DBFD	D09B45BF	27FA42F2	69973D23	1390E4B2	B6022735
cixCSP_API.dll*	E987EB70	D814CB35	970A966D	EB9FABEC	9C53C950	D8EEB363	1F5DD222	F1EC936F
cixtsa.dll*	F4C05B10	D2E3513F	4FF1DC33	44CA9B07	5968B62F	CBF21A05	E9FB19EB	7C2E7788
cphpki.dll*	A285720A	21C47E88	9DA62421	6FBE5BF2	37A3BC73	3E34BA57	429A8B94	CFB53592
dstu4145.dll*	2C044E31	3AA74559	1FF522D9	23085CD9	50EFAEEE	D527D179	915E81C9	A171CACE
tsareport1.dll*	0D56D98A	A6127A19	E532C2CC	5BF5355A	33DA2E89	7F60B862	38CC2D50	039D4536
tsareport2.dll*	03B2F588	57DF4938	A86214FF	EBFE5719	E32BE233	FA61663B	A4661EF0	14F94175

Каталог CiX509 RA

CiX509API.dll*	8E148B0C	01FE1348	49BCC30C	931B70C5	2EA94EAC	22782A75	737DCB05	C5DEA660
CiX509Core.dll*	94C1557F	8760DD69	685B418E	A5E4AD9B	E512C21F	71FFEA65	5392F698	0FA4BA00
cixCSP_API.dll*	C04F593E	9D69BA11	B4F34C34	F15BF056	5E2CDED2	88F091DA	5861A43D	92FA097B
dstu4145.dll*	2C044E31	3AA74559	1FF522D9	23085CD9	50EFAEEE	D527D179	915E81C9	A171CACE

Каталог CiX509 RA CM

CiX509API.dll*	8E148B0C	01FE1348	49BCC30C	931B70C5	2EA94EAC	22782A75	737DCB05	C5DEA660
CiX509Core.dll*	94C1557F	8760DD69	685B418E	A5E4AD9B	E512C21F	71FFEA65	5392F698	0FA4BA00
cixCSP_API.dll*	C04F593E	9D69BA11	B4F34C34	F15BF056	5E2CDED2	88F091DA	5861A43D	92FA097B
dstu4145.dll*	2C044E31	3AA74559	1FF522D9	23085CD9	50EFAEEE	D527D179	915E81C9	A171CACE

Каталог CiX509 RRA

CiX509API.dll*	8E148B0C	01FE1348	49BCC30C	931B70C5	2EA94EAC	22782A75	737DCB05	C5DEA660
CiX509Core.dll*	94C1557F	8760DD69	685B418E	A5E4AD9B	E512C21F	71FFEA65	5392F698	0FA4BA00
cixCSP_API.dll*	C04F593E	9D69BA11	B4F34C34	F15BF056	5E2CDED2	88F091DA	5861A43D	92FA097B
dstu4145.dll*	2C044E31	3AA74559	1FF522D9	23085CD9	50EFAEEE	D527D179	915E81C9	A171CACE

Каталог CiX509 SA

CiX509API.dll*	8E148B0C	01FE1348	49BCC30C	931B70C5	2EA94EAC	22782A75	737DCB05	C5DEA660
CiX509Core.dll*	94C1557F	8760DD69	685B418E	A5E4AD9B	E512C21F	71FFEA65	5392F698	0FA4BA00
CiX509-SA.exe*	EBD0256F	6D746724	45048AD0	2486847E	983F8983	F92CBD58	91371DEA	92E85362
CiX509Server.dll*	BB24A299	E1AD9F9E	120DB7F4	A737763B	39D202B9	F1661DF4	DE8F49E6	B4CBA8B8
cixCSP_API.dll*	C04F593E	9D69BA11	B4F34C34	F15BF056	5E2CDED2	88F091DA	5861A43D	92FA097B
dstu4145.dll*	2C044E31	3AA74559	1FF522D9	23085CD9	50EFAEEE	D527D179	915E81C9	A171CACE

Каталог CiX509 TSPServer

CiX509API.dll*	8E148B0C	01FE1348	49BCC30C	931B70C5	2EA94EAC	22782A75	737DCB05	C5DEA660
CiX509Core.dll*	94C1557F	8760DD69	685B418E	A5E4AD9B	E512C21F	71FFEA65	5392F698	0FA4BA00
CiXCSP_API.dll*	C04F593E	9D69BA11	B4F34C34	F15BF056	5E2CDED2	88F091DA	5861A43D	92FA097B
dstu4145.dll*	991A8A8D	E0C87CAD	AF84D956	10E26683	F67DDA2D	49CC7731	2E4EDC49	F397CCEE
tssvc.exe*	8FDA272C	62513B60	40EECEF0	DFA29412	BA18910B	BF5B394F	C59D6EE2	034E14AB

Каталог CiX509 Win32 lib

CiX509API.dll*	8E148B0C	01FE1348	49BCC30C	931B70C5	2EA94EAC	22782A75	737DCB05	C5DEA660
CiX509Core.dll*	94C1557F	8760DD69	685B418E	A5E4AD9B	E512C21F	71FFEA65	5392F698	0FA4BA00
CiXCSP_API.dll*	C04F593E	9D69BA11	B4F34C34	F15BF056	5E2CDED2	88F091DA	5861A43D	92FA097B
cphpki.dll*	A285720A	21C47E88	9DA62421	6FBE5BF2	37A3BC73	3E34BA57	429A8B94	CFB53592
dstu4145.dll*	2C044E31	3AA74559	1FF522D9	23085CD9	50EFAEEE	D527D179	915E81C9	A171CACE

Каталог CiX509 Win32 lib RA

CiX509API.dll*	8E148B0C 01FE1348 49BCC30C 931B70C5 2EA94EAC 22782A75 737DCB05 C5DEA660
CiX509Core.dll*	94C1557F 8760DD69 685B418E A5E4AD9B E512C21F 71FFEA65 5392F698 0FA4BA00
CiX509Server.dll*	BB24A299 E1AD9F9E 120DB7F4 A737763B 39D202B9 F1661DF4 DE8F49E6 B4CBA8B8
CiXCSP_API.dll*	C04F593E 9D69BA11 B4F34C34 F15BF056 5E2CDED2 88F091DA 5861A43D 92FA097B
dstu4145.dll*	2C044E31 3AA74559 1FF522D9 23085CD9 50EFAEEE D527D179 915E81C9 A171CACE

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



Л.О. Євдоченко