ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология
ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ ӘДІСТЕРІ МЕН ҚҰРАЛДАРЫ
КІЛТТЕРДІ БАСҚАРУ
1-бөлім
Негізгі ережелер

Информационная технология
МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ
УПРАВЛЕНИЕ КЛЮЧАМИ
Часть 1
Основные положения

ҚР СТ ИСО/МЭК 11770-1-2008

(ИСО/ХЭТК 11770-1:1996 «Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Кілттерді басқару. 1-бөлім. Негізгі ережелер», IDT)

Ресми басылым

Қазақстан Республикасы Индустрия және сауда министрлігінің
Техникалық реттеу және метрология комитеті
(Мемстандарт)

Астана

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология

ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ ӘДІСТЕРІ МЕН ҚҰРАЛДАРЫ

КІЛТТЕРДІ БАСҚАРУ

1-бөлім
Негізгі ережелер

ҚР СТ ИСО/МЭК 11770-1-2008
(ИСО/ХЭТК 11770-1:1996 «Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Кілттерді басқару. 1-бөлім. Негізгі ережелер», IDT)

Ресми басылым

Қазақстан Республикасы Индустрия және сауда министрлігінің
Техникалық реттеу және метрология комитеті
(Мемстандарт)

Астана

Алғысөз

1 Қазақстан Республикасы Ақпараттандыру және байланыс агенттігі **ӘЗІРЛЕП ЕНГІЗДІ**.

2 Қазақстан Республикасы Индустрия және сауда министрлігінің Техникалық реттеу және метрология комитеті 2008 жылғы «25» ақпандағы №107-од бұйрығымен **БЕКІТІЛІП ҚОЛДАНЫСҚА ЕНГІЗІЛДІ**

3 Осы стандарт Қазақстан Республикасы экономикасының қажеттіліктерін көрсететін талаптар мәтін бойынша көлбеу қаріппен белгіленіп «Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Кілттерді басқару. 1-бөлім. Негізгі ережелер» ИСО/ХЭТК 11770-1:1996 халықаралық стандартына («Information technology. Security techniques. Key management. Part 1. Framework»), IDT сәйкес.

4 БІРІНШІ ТЕКСЕРУ МЕРЗІМІ 2013 жыл
ТЕКСЕРУ КЕЗЕҢДІЛІГІ 5 жыл

5 АЛҒАШ РЕТ ЕНГІЗІЛДІ

Мазмұны

Кіріспе

Ақпараттық технологияларда мәліметтерді заңсыз ашудан немесе өзгертуден қорғау үшін, сәйкестендіру үшін және бас тартпаушылықты қамтамасыз ету үшін криптографиялық тетіктерді пайдалануда әрдайым өсіп жатқан қажеттілік туындауда. Бұл тетіктердің қауіпсіздігі мен сенімділігі кілт секілді құпия шаманы басқару мен қорғауға тікелей байланысты. Кілттерді қауіпсіз басқару криптографиялық қызметтердің бір жүйеге шоғырлануы үшін күрделі, өйткені қауіпсіздіктің ең жақсы дамыған тұжырымдамасы кілттерді басқарудың әлсіз жүйесінде тиімсіз болып қалады. Кілттерді басқарудың мақсаты – симметриялық немесе асимметриялық криптографиялық әдістерде пайдаланылатын криптографиялық кілттік материалдармен жұмыс істеу барысында жасалынатын шараларды қамту.

Тіке және жанама пайдаланушылар үшін тегі, тұтастығы, өзектілігі және (құпия кілттер үшін) құпиялығы секілді қасиеттеріне кепілдік беріле алатын кілттік материалды жасау негізгі мәселе болып табылады. Кілттерді басқаруға кілттік материалдарды қауіпсіздік саясатына сәйкес (ГОСТ ИСО 7498-2) біріктіру, сақтау, тарату, жою және архивтеу қызметтері енеді.

Осы стандарт ашық жүйелер қауіпсіздігінің Негіздеріне ерекше қатысы бар (*ҚР СТ ИСО/МЭК 10181*). Осыны қоса, барлық Негіздер қауіпсіздіктің түрлі тұрғыларын қамтитын тетіктердің базалық тұжырымдамалары мен мінездемелерін белгілейді. Осы стандарт симметриялық және асимметриялық криптографиялық әдістер үшін негізгі болып табылатын кілттерді басқарудың жалпы үлгілерін іске енгізеді.

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология
ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ ӘДІСТЕРІ МЕН ҚҰРАЛДАРЫ
КІЛТТЕРДІ БАСҚАРУ
1-бөлім
Негізгі ережелер

Енгізілген күні 2008.07.01

1 Қолданылу саласы

Осы стандарт:

1. Кілттерді басқарудың мақсаттарын белгілейді.

2. Кілттерді басқарудың тетіктері негізделетін жалпы үлгіні суреттейді.

3. Осы стандарттың барлық бөліктеріне жалпы болып табылатын кілттерді басқарудың базалық тұжырымдамаларын белгілейді.

4. Кілттерді басқаруға көрсетілетін қызметтерді белгілейді.

5. Кілттерді басқару әдістерінің мінездемелерін белгілейді.

6. Кілттік материалдың өмірлік циклі бойы оны басқаруға қойылатын талаптарды белгілейді.

7. Кілттік материалдың өмірлік циклі бойы оны басқарудың құрылымын белгілейді.

Осы стандарт пайдаланылатын нақты криптографиялық алгоритмге қатысты емес кілттерді басқарудың жалпы үлгісін анықтайды. Бірақ кілттерді таратудың кейбір әдістері нақты алгоритмдердің қасиеттеріне мысалы, ассиметриялық алгоритмдердің қасиеттеріне қатысты болуы мүмкін. Ақпаратты криптографиялық қорғаудың нақты құралдарын таңдау және қолдану Қазақстан Республикасының заңнамасымен белгіленеді және осы стандарттың қарастыру объектісі болып табылмайды.

Кілттерді басқарудың нақты әдістері *ИСО/МЭК 11770* басқа бөлімдерінде қарастырылады. Симметриялық әдістер 2-бөлімде қарастырылады (*ҚР СТ ИСО/МЭК 11770-2, Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Кілттерді басқару. 2-бөлім. Симметриялық әдістерді қолданатын тетіктер*). Асимметриялық әдістер 3-бөлімде қарастырылады (ҚР СТ ИСО/МЭК 11770-3 Ақпараттық технология. Қауіпсіздікті қамтудың әдістері мен құралдары. Кілттерді басқару. 3-бөлім. Асимметриялық әдістерді қолданатын тетіктер).

Осы стандартта ҚР СТ ИСО/МЭК 11770-2 және *ҚР СТ ИСО/МЭК 11770-3* түсіну үшін қажетті материалдар бар. Кілттерді басқару тетіктерін пайдалану мысалдары *ИСО 8732* және *ИСО 11166* стандарттарында келтіріледі. Егер кілттерді басқару үшін жұмыс істемей қалмауы қажет болса, ИСО/МЭК 13888 қолдануға болады (оның ішінде *ҚР СТ ИСО/МЭК*

13888-2). Осы стандарт кілттерді басқаруға көрсетілетін қызметтерге қол жеткізу үшін пайдаланылатын операциялардың реттілігі мен деректер элементтерінің құрылымын қоса кілттерді автоматтық және қолмен басқару тұжырымдамаларын қарастырады. Бірақ бұл құжат қажет болуы мүмкін алмасу хаттамаларының бөлшектерін белгілемейді.

Қауіпсіздіктің басқа да қызметтері секілді, кілттерді басқару қауіпсіздіктің белгілі саясаты шеңберінде ғана ұсынылуы мүмкін. Қауіпсіздік саясатын белгілеу бұл стандарттың қарастырылуына енгізілмеген.

2 Нормативтік сілтемелер

Осы стандартта мынадай стандарттарға сілтемелер пайдаланылды:

ГОСТ ИСО 7498-2:2002 Ақпаратты өңдеу жүйелері. Ашық жүйелердің өзара байланысы. Базалық эталондық үлгі. 2-бөлім. Қауіпсіздік архитектурасы.

ҚР СТ ИСО/МЭК 10116-2006 Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. N-биттік блоктық шифрлердің жұмыс тәртібі.

ҚР СТ ИСО/МЭК 11770-2: 2006 Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Кілттерді басқару. 2-бөлім. Симметриялық әдістерді қолданатын тетіктер.

ҚР СТ ИСО/МЭК 9798-1-2008 Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Сәйкестендіру тетіктері. 1-бөлім. Негізгі ережелер.

ҚР СТ ИСО/МЭК 10181-1-2008 Ақпараттық технология. Ашық жүйелердің өзара байланысы. Ашық жүйелер үшін қауіпсіздік негіздері: Шолу.

3 Терминдер мен анықтамалар

Осы стандартта сәйкес анықтамаларымен мынадай терминдер қолданылды:

3.1 Асимметриялық криптографиялық әдіс (asymmetric cryptographic technique): Екі байланысты түбегейлі өзгерістерді пайдаланатын криптографиялық әдіс: ашық түбегейлі өзгеріс (ашық кілтпен белгіленеді) және жабық түбегейлі өзгеріс (құпия кілтпен белгіленеді). Осы түбегейлі өзгерістер жұбының бір қасиеті бар, бұл мәліметтер блогының ашық түбегейлі өзгерістерін ғана пайдалана отырып, есептеу жолымен сол мәліметтер блогының құпия түбегейлі өзгерістерін ала алмау.

3.2 Жабық кілт (private key): Мәндер кілттерінің асимметриялық жұбынан осы мән ғана пайдалана алатын кілт.

Ескертпе – Жабық кілт ашылуға қажетті емес.

3.3 Ашық кілт туралы ақпарат (public key information): Ең болмағанда, мәннің айырмашылық ұқсастығы бар, және де осы мәнге бір ашық кілті бар дербес мәнге қатысты ақпарат. Ашық кілт туралы ақпаратқа ашық кілттің қолданылу мерзімі, сәйкес құпия кілттің әрекет ету мерзімі немесе пайдаланылатын криптографиялық алгоритмдердің ұқсастығы секілді куәландырушы орталық, мән және ашық кілт туралы қосымша ақпараттар енгізілуі мүмкін.

3.4 Кілт (key): Криптографиялық түбегейлі өзгерістер операцияларын басқаратын (мысалы, шифрлау, шифрын ашу, тексеру криптографиялық функцияларын есептеу, қолды генерациялау немесе верификациялау) белгілердің жүйелілігі.

3.5 Кілттік материал (keying material): Криптографиялық қатынастарды орнатуға және қолдауға қажетті мәліметтер (мысалы, кілттер, бастапқы мағыналар).

3.6 Кілтті бақылау (key control): Кілтті есептеп шығару барысында кілтті немесе шамаларды таңдау мүмкіншілігі.

3.7 Уақыт таңбасы (time stamp): Уақыттың жалпы есебінде уақыт сәтін белгілейтін уақытқа тәуелді шама.

3.8 Ашық кілт (public key): Мәндер кілттерінің асимметриялық жұбынан жалпыға ашық бола алатын кілт.

3.9 Уақытқа тәуелді шама (time variant parameter): Хабарлама қайталанбағанын верификациялау үшін мәнді қолданатын кездейсоқ сан, реттік сан немесе уақыт таңбасы секілді мәліметтер элементі.

3.10 Кілтті растау (key confirmation): Бір мәннің екінші мәнде дұрыс кілті бар болуына кепілдік.

3.11 Реттік сан (sequence number): Уақыттың белгілі кезең шеңберінде қайталанбайтын, мәні тапсырылған реттіліктен таңдалатын уақытқа тәуелді шама.

3.12 Шифрын ашу (decipherment): Шифрлауға сәйкес қарама-қарсы іс.

3.13 Құпия кілт (secret key): Белгілі көптеген мәндер ғана қолданатын симметриялық криптографиялық әдістерде пайдаланылатын кілт.

3.14 Ашық кілт сертификаты (public key sertificate): Кейін жасанды емес ретінде қарастырылатын, куәландырушы орталықпен расталған мәннің ашық кілтінің ақпараты. Осы терминге балама Қазақстан Республикасы заңнамасында қолданылатын «тіркеу куәлігі» термині болып табылады.

3.15 Симметриялық криптографиялық әдіс (symmetric cryptographic technique): Бір ғана құпия кілтті жіберуші жағынан да, алушы жағынан да хабарламаны түбегейлі өзгерту үшін пайдаланылатын криптографиялық әдіс. Құпия кілтті білмей хабарламаны жіберуші немесе алушы жағынан түбегейлі өзгерістерді ашу мүмкін емес.

3.16 Кездейсоқ сан (random number): Мағынасы алдын ала болжамдалмайтын уақытқа тәуелді шама.

3.17 Кілтті қиыстыру (key agreement): Бірде біреуі кілттің мағынасын алдын ала жобалай алмайтын жолмен екі мәндердің жалпы құпия кілтін қалыптастыру ісі.

3.18 Куәландыратын орталық - КО (certification authority - CA): Ашық кілттердің сертификаттарын қалыптастыруға және таратуға уәкілді орган. Бұдан басқа, КО мәндерге кілттерді қалыптастырып, тарата алады.

3.19 Кілттерді басқару (key management): Қауіпсіздік саясатына сәйкес генерация, тіркеу, сертификаттау, тіркеуді жою, тарату, орнату, сақтау, архивтеу, жою процестерін басқару және пайдалану, туындыны қалыптастыру және кілттік материалдарды жою.

3.20 Кілттерді тарату орталығы (КТО) (key distribution center (KDC)): Әрбіреуінде КТО-ға бірдей кілті бар мәндердің арасында кілттерді қалыптастыруға немесе сұратуға және таратуға уәкілді мән.

3.21 Кілттерді трансляциялау орталығы (КТО) (key translation center (KTC)): Әрбіреуінде КТО-мен бірдей кілті бар мәндердің арасында кілттерді трансляциялауға уәкілді мән.

3.22 Шифрлау (encipherment): Шифрланған мәтінді алу үшін мәліметтерді криптографиялық алгоритммен түбегейлі өзгерту (қайтымды), яғни мәліметтердің ақпараттық мазмұнын жасыру үшін.

Осы стандартта *ИСО 7498-2* бойынша мына терминдер қолданылады:

- **мәліметтер дереккөзін сәйкестендіру** (data origin authentication);
- **мәліметтердің тұтастығы** (data integrity);
- **цифрлік қол** (digital signature).

Осы стандартта *ҚР СТ ИСО 9798-1* бойынша мынадай терминдер қолданылады:

- **мәнді сәйкестендіру** (entity authentication).

Осы стандартта *ҚР СТ ИСО 10181-1* бойынша мынадай терминдер қолданылады:

- **сенімді үшінші жақ** – СҮЖ (trusted third party – TTP);
- **қауіпсіздік домені** (security domain);
- **қауіпсіздік бойынша уәкілетті** (security authority);

4 Кілттерді басқарудың жалпы мәселелері

Кілтті басқару - бұл топтау, тіркеу, сертификаттау, тіркеуді жою, тарату, орнату, сақтау, архивтеу, жою, туындыны қалыптастыру және кілттік материалдарды жою қызметтерін басқару және қолдану.

Кілттерді басқару мақсаты – кілттерді басқару қызметтерін басқару және қолданудың қауіпсіздігін қамту және, сол себептен, кілттерді қорғау өте маңызды.

Кілттерді басқару істері қолданатын криптографиялық әдістерге, кілтті жорамалды қолдануға және ағымдағы қауіпсіздік саясатына байланысты. Кілттерді басқару ісіне криптографиялық жабдықтарда орындалатын қызметтер де енеді.

4.1 Кілттерді қорғау

Кілттер криптографиялық әдістерге тиісті, қауіпсіздіктің әрбір жүйесінің қиын бөлшегі болып табылады. Кілттердің қажетті қорғанысы кілттер қолданылатын қосымша түрі, оларда кездесетін қауіп-қатерлер, кілттерді пайдалануда кездесетін түрлі жағдайлар, т.б. секілді мәндер қатарына байланысты. Алдымен криптографиялық әдіске байланысты кілттер ашылудан, өзгертілуден, жойылудан және жаңғыртылудан қорғанылуға тиіс. Кілттерге жасалынуы мүмкін қауіп-қатерлер мысалдары А қосымшасында келтірілген. Кілттің жарамдылығы оны пайдалану мерзімі мен саны бойынша шектелуі қажет. Бұл шектеулер кілтті ашуға жасалынған шабуылды жүргізу үшін қажетті мәліметтер көлемімен және уақытымен, сонымен бірге қорғалатын ақпараттың құндылығымен белгіленеді. Басқа кілттерді генерациялау үшін қолданылатын кілттер генерациялайтын кілттерден гөрі үлкен қорғанысты қажет етеді. Кілттер қорғанысының басқа маңызды жағы оларды дұрыс емес қолдануға жол бермеу болып табылады, мысалы, кілттерді шифрлауға арналған кілттің мәліметтерін шифрлауға пайдалану.

4.1.1 Криптографиялық әдістермен қорғау

Криптографиялық әдістерді қолдану кейбір кілттік материалға қарсы тұруға мүмкіндік береді. Мысалы: шифрлау кілтті ашудан және заңсыз пайдаланудан қорғайды; мәліметтердің тұтастығын қамту әдістері өзгерістерден қорғайды; мәліметтер дереккөзінің сәйкестендіру әдістері, цифрлік қолдар және мәндерді сәйкестендіру әдістері ауыстыруға қарсы тұрады.

Криптографиялық әдістерді қолданудың бөлінісі оларды дұрыс емес пайдаланудан қорғайды. Мұндай атқарымдық қолданудың бөлінісі кілтпен кейбір ақпаратты байланыстыру жолы арқылы жетілуі мүмкін. Мысалы, басқару ақпаратының кілтке байлануы белгілі кілттің белгілі мақсаттар үшін пайдалана алатындығына кепілдік береді (мысалы, кілттерді шифрлау немесе мәліметтер тұтастығын қамту үшін); симметриялық әдістер қолданылса, кілтке бақылау жүргізу авторлықтан бас тартпауды қамту үшін қажет.

4.1.2 Криптографиялық емес әдістермен қорғау

Уақыт таңбалары кілтті белгілі уақыт мерзімі бойы қолданылуын шектеу үшін қолданылады. Олар реттік сандармен қатар кілтті келістіру процесінде ақпаратты жаңғыртудан қорғайды.

4.1.3 Физикалық деңгейде қорғау

Қауіпсіздік жүйесіндегі әрбір криптографиялық құрылғы өзі қолданатын кілттік материалды өзгертуден, жоюдан және, ашық кілттен басқа, ашудан қорғауды талап етеді. Кілтті сақтау және қолдану үшін құрылғының криптографиялық алгоритмдерді жүзеге асыру үшін қорғалатын саласы бар. Олар мыналарға құралдар ұсынылa алады:

– кілттік материалды кілтті сақтаудың басқа дербес құрылғысынан жүктеу;

– дербес «зияткерлік» құрылғыларда жүзеге асырылған криптографиялық алгоритмдермен өзара қатынас жасау (мысалы, смарт-карталарда, сақтау карталарында);

– кілттік материалды сыртқы тасымалдаушыларда сақтау (мысалы, дискетада).

Әдетте, қорғалған сала физикалық қорғау тетіктерінің көмегімен қалыптасады.

4.1.4 Ұйымдастырушылық әдістермен қорғау

Кілттерді қорғау құралдарының бірі оларды сатылық құрылыммен ұйымдастыру болып табылады. Иерархияның төменгі деңгейінен басқа, иерархияның бір деңгейіндегі кілттер бір деңгейге төмен кілттерді қорғау үшін ғана қолданылады. Тек қана иерархияның ең төменгі деңгейдегі кілттер қауіпсіздік қызметтерінде тікелей қолданылады. Мұндай тәсіл шабуылдардың жасалуын шектеп, олардың іске асырылуын қиындата отырып, әрбір кілттің пайдалану шеңберін шектеуге мүмкіндік береді. Мысалы, бір сессиялық кілттің ашылуы осы кілтпен ғана қорғалған ақпараттың ашылуына жол береді.

Қорғалған салалардың қолданысы уәкілді емес мәндермен кілтті ашу, өзгерту және жою қауіп-қатерлеріне қарама-қарсы тұруға бағытталған. Бірақ кілттерді басқару қызметтерінің бөлшектерін басқарудың белгілі функцияларын орындауда уәкілді жүйелік басшылары өз мүмкіндіктерінің ерекше артықшылықтарын дұрыс реттей алмауының қауіп-қатері бар. Жеке алғанда, олар негізгі кілтті алуға талпына алады (жоғарғы деңгей кілті кілттер иерархиясында). Негізгі кілтті ашу оның иесіне сол кілтпен қорғалған барлық басқа кілттерді алуға немесе өзгертуге мүмкіндік бере алады (яғни осы кілттер иерархиясындағы барлық басқа кілттер). Сондықтан бұл кілтке енуді шектеу қажет, мысалы, ешқандай пайдаланушы бір өзі ғана оған кіруге рұқсат алмайтындығын белгілеу арқылы. Мұны негізгі кілтті

бөлу (кілтті екі жақты басқару не болмаса n-жақты басқару) немесе арнайы криптографиялық сызбаларды қолдану (Құпия ақпаратты бірігіп қолдану сызбасы) арқылы жүзеге асыруға болады.

4.2 Кілттің өмірлік кезеңінің жалпы үлгісі

Криптографиялық кілт оның өмірлік кезеңі белгілеген түрлі жағдайлардан өтеді. Үш негізгі жағдайлар - бұл:

Белсендіру алдында: Бұл жағдайда кілт генерацияланады, бірақ қолдану үшін қарқындалған жоқ.

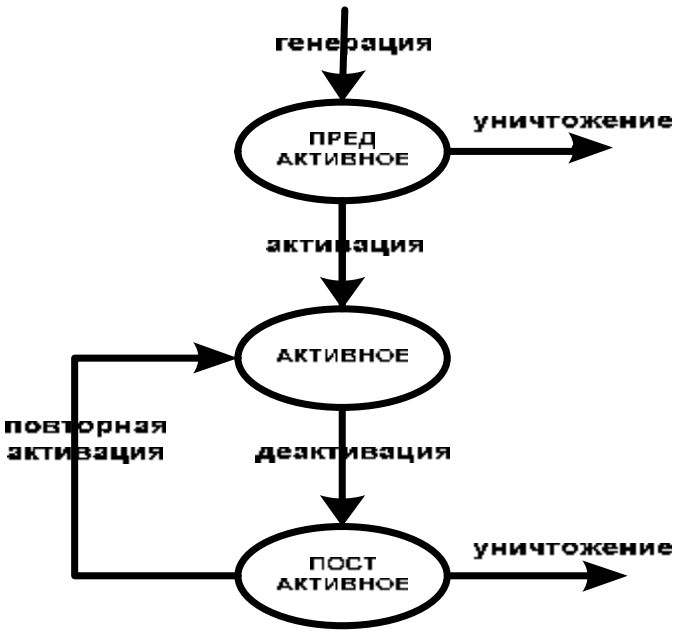
Белсенді: Бұл жағдайда кілт ақпаратты криптографиялық өндеу үшін қолданылады.

Белсендіруден кейін: Бұл жағдайда кілт шифрды ашу немесе верификациялау үшін қолданылады.

Ескертпе – белсендіруден кейінгі жағдайдағы кілттің пайдаланушысы кілт мәліметтер криптографиялық өңделген соң бұл жағдайға ауысқанына сенімді болуы қажет. Әдетінше, бұл сенімді уақыт шамасының көмегімен қамтылады.

Біреумен ашылған кілт туралы белгілі болған соң, ол сол бетте белсендіруден кейінгі жағдайға ауысуы қажет, және ерекше қатынасты талап етуі мүмкін. Егерде кілттің заңсыз ашылуы белгілі болса немесе мұндай жағдайына күмәнданса, кілт біреумен ашылған болып табылады.

1-суретте айтылған жағдайлар мен тиісті ауысымдар көрсетілген.



1-сурет – Кілттің өмірлік кезеңі

1-суретте кілттің өмірлік кезеңінің жалпы үлгісі көрсетілген. Өмірлік кезеңнің басқа үлгілері айтылған үш жағдайдың жағдай астары түрінде

қосымша бөлшектерден тұра алады. Кілттердің көптеген өмірлік кезеңдері архивтеу бойынша әрекеттерді талап етеді. Бұл әрекеттер өмірлік кезеңнің нақты бөлшегіне тәуелді түрлі жағдаймен байланысты болуы мүмкін.

4.2.1 Кілттің жағдайлары арасындағы ауысымдар

Кілттің бір жағдайдан екінші жағдайға түсуі мүмкіндігінше (ол 1-суретте көрсетілгендей) ауысымдардың біреуін жүзеге асырады:

- **Генерация** - кілттің қалыптасу процесі. Кілттің генерациясы осыған тиісті жазылған ережелерге сәйкес жүзеге асырылуы қажет. Бұл іске барлық ережелер сақталғандығының тексерісі енуі мүмкін.
- Кілттің **қарқындауы** оны криптографиялық шаралар үшін қолайлы етеді.
- **Қарқынды жою** кілттің қолданысын шектейді. Бұл кілттің пайдалану мерзімі аяқталған себебінен немесе кілттің жойылуынан болады.
- **Қайталап қарқындау** белсендіруден кейінгі кілтті криптографиялық операцияларда пайдалануға мүмкіндік береді.
- **Жою** кілттің өмірлік кезеңін аяқтайды. Бұл кілттің логикалық жойылуын, және оның физикалық жойылуын да білдіреді.

Ауысымдар жаңа кілтті қажет ету, қолдану мерзімнің аяқталуы және кілттің өмірлік кезеңінің аяқталуы секілді жағдайлармен шартталады. Барлық осы ауысымдар бірқатар кілтті басқару қызметтерін пайдаланады. Ауысымдар мен қызметтер арасындағы байланыстар 1-кестеде көрсетілген. Бұл қызметтер 5-бөлімде мазмұндалған.

Әрбір нақты криптографиялық әдіс 1 – кестеде көрсетілген қызметтердің кейбір астарлы көпшілігін талап етеді.

4.2.2 Ауысымдар, қызметтер мен кілттер

Нақты криптографиялық әдістердегі кілттер өзінің өмірлік кезеңінде түрлі қызметтер қисынын пайдаланады. Екі мысал төменде келтірілген.

Симметриялық криптографиялық әдістерде кілттің генерациясынан кейінгі белсендіру алдындағы жағдайдан белсенді жағдайға ауысымы кілттің орнатылуына әкеледі және кілтті тіркеу мен таратуға да алып келуі мүмкін. Кейбір жағдайларда кілттің орнатылуына бір кілттен туындаған кілттердің қалыптастырылуы кіреді. Кілттің өмір уақыты белгіленген кезеңмен шектелуі қажет. Қарқынды жою белсенді жағдайды аяқтайды, бұл кілттің пайдалану мерзімі аяқталған соң болады. Егер кілт белсенді жағдайда біреумен ашылса немесе осыда күмәнданса, оның мүлдем жойылуы да белсендіруден кейінгі жағдайға ауысуына әкеледі. Белсендіруден кейінгі жағдайдағы кілтті архивтеуге болады. Егер архивтелген кілт тағы да қажет болса, ол қайта архивтелінуі мүмкін, бұл оның толық белсендіруі алдында қайта орнатылуы мен таратылуын талап етуі мүмкін. Керісінше жағдайда,

кілттің белсенділігі жойылған соң оның тіркелуі өзгеріп, кілт мүлдем жойылады.

Асимметриялық криптографиялық әдістерде кілттердің жұбы генерацияланады (ашық және жабық), және екі кілт те белсендіру алдындағы жағдайға ауысады. Екі кілттің өмірлік кезеңдері байланысты, бірақ бірдей емес. Жабық кілт белсенді жағдайға көшер алдында, ол міндетті емес тәртіпте тіркелуі, және осы міндетті емес тәртіпте оның пайдаланушысына жеткізілуі мүмкін, бірақ әрқашан орнатылған күйде болуы қажет. Жабық кілт үшін белсенді және белсендіруден кейінгі жағдайлар арасындағы ауысым, қарқынды жою, қайта қарқындау және жойылу жағдайларын қоса, симметриялық кілттер үшін суреттелген ауысымға жақын. Ашық кілт сертификатталған кезде ашық кілті бар сертификат ашық кілттің шынайылығы мен иелігін растау үшін КО-мен қалыптастырылады. Ашық кілттің бұл сертификаты таратылу үшін каталогқа немесе ұқсас қызметке орналастырылуы мүмкін, немесе ол таратылуы үшін иесіне қайтарылуы мүмкін. Кілт иесі жабық кілтпен жазылған ақпаратты жіберген кезде, ол өзінің сертификатын қосып жіберуіне болады. Кілттер жұбы ашық кілт сертификатталған соң белсенді болады. Кілттер жұбы цифрлік жазба үшін қолданылған кезде ашық кілт тиісті жабық кілттің қарқыны жойылған соң немесе мүлдем жойылған соң, белгісіз уақыт белсенді немесе белсендіруден кейінгі жағдайда болуы мүмкін. Ашық кілтке ену ісі тиісті жабық кілттің қолдану мерзімі өткен соң ғана жасалған цифрлік жазбаның верификациясы үшін қажет. Асимметриялық әдістермен жасалынған шифрлау және шифрлауға пайдаланылған кілттің қарқыны жойылса немесе мүлдем жойылса, жұптың тиісті кілті шифрды ашу кезінде қолдану үшін белсенді немесе белсендіруден кейінгі жағдайда болуы мүмкін.

Кілттің қолданысы осы кілтке қажетті қызметтерді белгіле алады. Мысалы, жүйе сессиялық кілттерді тіркемеуге шешім қабылдай алады, өйткені тіркеу ісі кілттің өмірінен ұзақ болуы мүмкін. Керісінше, симметриялық әдістер цифрлік жазбалар үшін қолданылған кезде, құпия кілт тіркелуге тиіс.

1-кесте – Ауысымдар мен қызметтер

Ауысым	***Қызмет***	***Ескертпелер***
Генерация	Кілтті генерациялау	Міндетті
	Кілтті тіркеу	Міндетті емес немесе сол кезде немесе белсендіру кезінде
	Кілттің сертификатын қалыптастыру	Міндетті емес
	Кілтті тарату	Міндетті емес

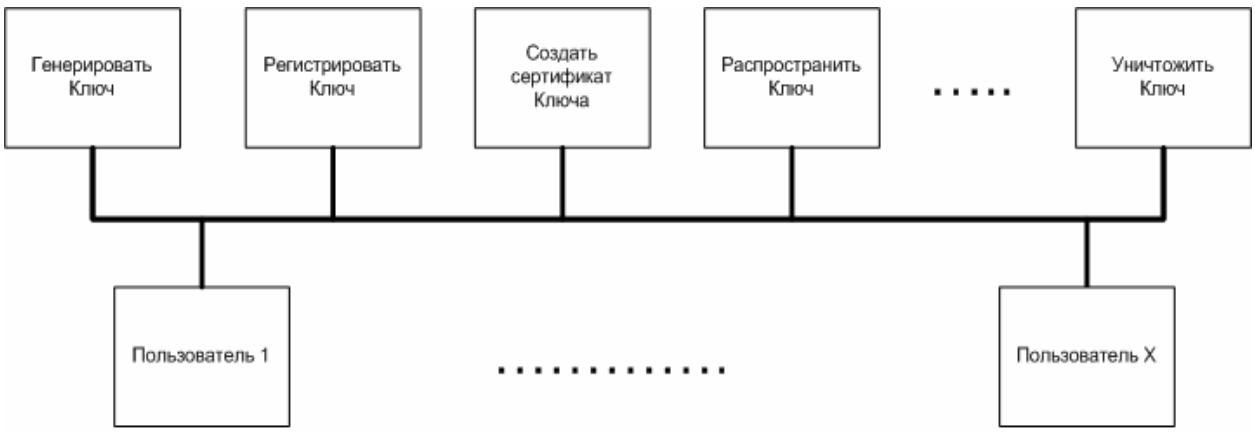
	Кілтті сақтау	Міндетті емес
Қарқындату	Кілттің сертификатын қалыптастыру	Міндетті емес
	Кілтті тарату	Міндетті емес
	Кілттің туындыларын қалыптастыру	Міндетті емес
	Кілтті орнату	Міндетті емес
	Кілтті сақтау	Міндетті емес
	Кілтті тіркеу	Міндетті емес немесе сол кезде, немесе генерация кезінде
Қарқынын жою	Кілтті сақтау	Міндетті емес
	Кілтті архивтеу	Міндетті емес немесе сол кезде, немесе жою кезінде
	Кілттің күшін жою	Міндетті емес
Қайта қарқындату	Кілттің сертификатын қалыптастыру	Міндетті емес
	Кілтті тарату	Міндетті емес
	Кілттің туындыларын қалыптастыру	Міндетті емес
	Кілтті орнату	Міндетті емес
	Кілтті сақтау	Міндетті емес
Мүлдем жою	Кілттің тіркелуін өзгерту	Кілт тіркелген кезде міндетті
	Кілтті мүлдем жою	Міндетті
	Кілтті архивтеу	Міндетті емес немесе сол кезде, немесе қарқындауды жою кезінде

5 Кілттерді басқарудың тұжырымдамалары

5.1 Кілтті басқару қызметтері

Бұл бөлім кілттерді басқарудың жалпы құрылымын суреттейді және кілттерді басқару қызметтерін, олардың өзара қарым-қатынастарын және оларға қандай қолдау көрсетілетіндігін түсіндіруге көмектеседі.

Кілттерді басқару ісі генерация, тіркеу, сертификаттау, тарату, орнату, сақтау, кілттің туындыларын қалыптастыру, архивтеу, күшін жою, тіркеуді өзгерту және жою базалық қызметтеріне негізделген. Бұл қызметтер кілттерді басқару жүйесінің бөлшегі бола алады немесе басқа қызмет көрсетушілерімен ұсынылa алады. Қызмет түріне байланысты қызмет көрсетуші оған барлық қатысушы жақтар сенуі үшін, қауіпсіздікті сақтаудың белгілі талаптарын орындауға тиіс (мысалы, қорғанған алмасу). Жеке алғанда, қызмет көрсетуші сенімді үшінші тарап болуы мүмкін. 2-суретте кілттерді басқару қызметтері бір деңгейде болып, олар түрлі пайдаланушылармен (адамдармен және процестермен) қолданылуы мүмкін екендігі көрсетілген. Бұл пайдаланушылар өздерінің мұқтаждықтарына сәйкес қызметтерді қолдана отырып, түрлі қосымшалардан кілттерді басқару қызметтеріне енуі мүмкін. Кілттерді басқару қызметтерінің тізімі 1-кестеде келтірілген.



2-сурет – Кілттерді басқару қызметтері

5.1.1 Кілтті генерациялау

Кілтті генерациялау – бұл нақты криптографиялық алгоритм үшін кілтті қауіпсіз түрде генерациялау үшін қолданылатын қызмет. Бұл кілттердің генерациясы амал-айла әрекетпен жасалуы мүмкін еместігін және кілттер кездейсоқ түрде және бөлінудің алдын ала заңына сәйкес қалыптастырылғандығын тұспалдайды. Бұл бөлу заңы қолданылатын криптографиялық алгоритммен және криптографиялық сақтаудың қажетті деңгейімен белгіленеді. Кейбір кілттердің, мысалы, негізгі кілттердің генерациясы, ерекше назарды талап етеді, өйткені бұл кілттерді білу барлық байланысты және туындаған кілттерге енуге рұқсат береді.

5.1.2 Кілтті-тіркеу

Кілтті-тіркеу қызметі кілтті мәнмен байланыстырады. Бұл қызмет тіркеу жөніндегі органмен ұсынылады және, әдетінше, симметриялық криптографиялық әдістер қолданған кезде пайдаланылады. Мән кілтті

тіркегісі келгенде, ол тіркеу органымен байланыс жасайды. Кілттің тіркеліміне тіркеуге сұраныс және тіркеуді растау кіреді.

Тіркеу органы тиісті қорғалған түрде кілттер тізімін және олармен байланысты ақпаратты қолдайды. В қосымшада кілттерді басқару бойынша толық ақпарат бар.

Тіркеу органы тіркеу және тіркеуді өзгерту операцияларын ұсынады.

5.1.3 Кілттің сертификатын қалыптастыру

Кілттің сертификатын қалыптастыру қызметі ашық кілттің мәнмен байланысын растайды және куәландыратын орталықпен ұсынылады. Егерде сертификаттауға сұраныс қабылданса, куәландыратын орталық кілттің сертификатын жасайды. Ашық кілттердің сертификаттары ИСО/МЭК 11770-3 –те нақты талқыланады.

5.1.4 Кілтті тарату

Кілтті тарату – бұл кілттерді басқарудың ақпараттық объекттерін авторланған мәндерге ұсыну үшін шаралардың жиынтығы (В қосымшасындағы мысалға қараңыз). Кілттерді таратудың ерекше жағдайы ретінде мәндер арасындағы кілттік материалмен алмасу кілттерді трансляциялау орталығын пайдалану арқылы жүзеге асырылғандағы кілттер трансляциясы болып табылады (6.2. - бөлігін қараңыз). *ҚР СТ ИСО/МЭК 11770-2* мәндер арасындағы кілттер келісуінің түрлі тетіктерін ұсынады. ИСО/МЭК 11770-3 -ге құпия кілттерді келістіру үшін тетіктер, сонымен бірге құпия және ашық кілттерді тасымалдау әдістері кіреді.

5.1.5 Кілтті-орнату

Кілтті-орнату қызметі әрқашан кілтті пайдалану алдында қажетті. Кілттің орнатылуы кілттің басқару жүйесіне оның біреумен ашылуын болдырмау үшін орналастырылуын білдіреді.

5.1.6 Кілтті-сақтау

Кілтті-сақтау қызметі ағымдағы қолданыс үшін және жақын кезге арналған, сонымен қатар резервтік сақтауға арналған кілттердің қауіпсіз сақталуын қамтиды. Әдетте кілттерді физикалық тәуелсіз сақтау орнын қамтудың мәні бар, бұл кілттік материалдың құпиялығын және тұтастығын, және де ашық кілттердің тұтастығын қамтиды. Сақтау кілттің өмірлік кезеңінің барлық жағдайларында қажет болуы мүмкін (яғни белсендіру алдында, белсендіру және белсендіруден кейінгі жағдайларда). Кілттердің маңыздылығына байланысты олар төменде келтірілген әдістердің біреуінің көмегімен қорғалуы мүмкін:

– физикалық қорғаныс (оларды заңсыз қолданудан қорғалған құрылғыларда немесе дискета не болмаса жады карталары секілді сыртқы тасымалдауыштарда сақтау);

– физикалық әдістермен қорғалған кілттермен шифрлау;

– кілттерге пароль немесе жеке код көмегімен енуді сақтау.

Барлық түйінді материалдар үшін әрбір біреумен ашу талпынысы сол кезде білінуі қажет.

5.1.7 Кілттің туындысын қалыптастыру

Кілттің туындысын қалыптастыру қызметі бастапқы кілт аталатын құпия кілтті, құпия емес ауыспалы мәліметтерді және кейбір түбегейлі өзгеріс процесті (ол да құпия емес болуы мүмкін) қолдана отырып, кілттердің үлкен санын шығару мүмкіндігін ұсынады. Бұл процестің нәтижесі туынды кілт болып табылады. Бастапқы кілт ерекше қорғанысты талап етеді. Туындаған кілттің біреумен ашылуы бастапқы кілттің немесе басқа туылған кілттердің ашылуына жол бермеуі үшін туынды кілтті қалыптастыру процесі қайтымсыз және оның нәтижесінің алдын алуға болмайды.

5.1.8 Кілтті-архивтеу

Кілтті-архивтеу қызметі кілттің қалыпты қолданысы аяқталған соң оның қауіпсіз ұзақ мерзім сақталу процесін қамтиды. Бұл үшін автономды сақтауды жүзеге асыру үшін түрлі өзгерістері бар кілттерді сақтау қызметін қолдануға болады. Архивтелген кілттер кілттің қалыпты қолданысы аяқталған соң, растау үшін немесе белгілі пікірлерді жоққа шығару үшін кешірек уақытта қажет болуы мүмкін.

5.1.9 Кілттің күшін жою

Кілттің біреумен ашылуы белгілі болса немесе осыған күмән болса, кілттің күшін жою қызметі кілт қарқынының қауіпсіз жойылуын қамтиды. Бұл қызмет пайдалану мерзімі аяқталған кілттер үшін қажетті. Кілт күшінің жойылуы оның иесінің жағдайлары өзгерген кезде де жүзеге асырылады. Кілттің күші жойылған соң, ол шифрларды ашуға және верификациялау үшін пайдаланылуы мүмкін. Кілттің күшін жою қызметі сертификаты бар сызбалар үшін жарамсыз, өйткені мұнда кілттің өмір уақыты оның сертификатының қолдану мерзімінің аяқталуымен белгіленеді.

Ескертпе – Кейбір қосымшалар осы қызмет үшін Кілтті жою деген атауды қолданады.

5.1.10 Кілттің тіркелуін өзгерту

Кілттің тіркелуін өзгерту қызметі кілттерді тіркеу органымен ұсынылып, кілттің мәнмен байланысын үзуді қамтиды. Бұл кілтті жою процесінің бөлігі болып табылады (5.1.11 бөлігін қараңыз). Мән кілт тіркелімін өзгерткісі келген жағдайда, ол тіркеу органына жүгінеді.

5.1.11 Кілтті мүлдем жою

Кілтті мүлдем жою қызметі керек емес кілттердің қауіпсіз жойылуын қамтиды. Кілттің мүлдем жойылуы - бұл осыдан кейін қалған қандай да болмасын ақпарат түрлі әдістермен жойылған кілтті жаңғырта алмайтын, кілтті басқарудың тиісті ақпараттық объектілерінің барлық жазбаларын жою дегенді білдіреді. Кілтті жоюға барлық оның мұрағаттық көшірмелерін жою кіреді. Бірақ архивтелген кілттерді жою алдында бұл кілттермен қорғалған қандай да болмасын материал кейін қажет болмайтындығына көз жеткізу қажет.

Ескертпе – Кейбір кілттер электронды құрылғыдан немесе жүйеден тыс сақталынуы мүмкін. Мұндай кілттердің жойылуы қосымша әкімшілік шараларды талап етеді.

5.2 Көмекші қызметтер

Кілттерді басқаруға көмекші қызметтер қажет болуы мүмкін.

5.2.1 Кілттерді басқаруды қамту қызметтері

Кілттерді басқару қызметтері қауіпсіздікпен байланысты басқа да қызметтерді пайдалана алады. Бұл қызметтерге мыналар кіреді:

- **Қол жеткізуді басқару:** бұл қызмет кілттерді басқару жүйесінің ресурстары авторланған мәндермен және ұйғарылған түрде қолданылуына кепілдік беру үшін пайдаланылады.

- **Аудит:** кілттерді басқару жүйесіндегі қауіпсіздік тұрғысынан маңызды әрекеттерді қадағалау. Аудит жазбалары ақпараттық қауіпсіздікті қамтудағы қауіп-қатерлер мен шығындарды сәйкестендіру үшін көмектесе алады.

Сәйкестендіру: бұл қызмет мәннің қауіпсіздік доменнің авторланған элементтеріне тәуелділігін растау үшін қолданылуы мүмкін.

Криптографиялық қызметтер: бұл қызметтер тұтастықты, құпиялықты, шынайылықты және істен шықпауды қамту үшін пайдаланылуы қажет.

Уақыт қызметі: бұл қызмет пайдалану мерзімі секілді уақыттық шамаларды генерациялау үшін қажет.

5.2.2 Пайдаланушыға бейімделген қызметтер

Криптографиялық жүйелер мен құрылғылар қалыпты жұмыс істеуге қажетті басқа да қызметтерді мысалы, пайдаланушыларды тіркеу қызметін талап ете алады. Бұл қызметтер жүзеге асырылуына тәуелді және осы стандартта қарастырылмайды.

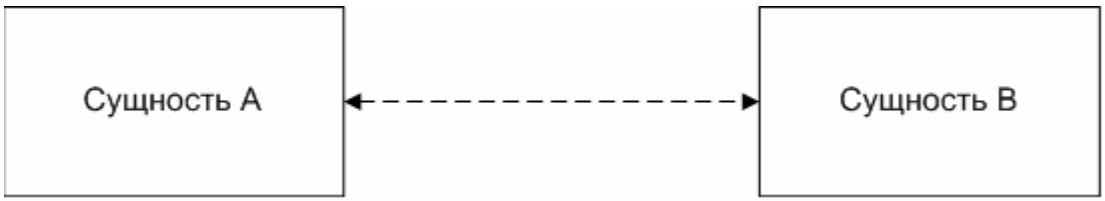
6 Кілттерді таратудың тұжырымдамалық үлгілері

Мәндер арасындағы кілттердің таралуы күрделі іс болуы мүмкін. Бұл байланыс құралдарымен, тараптар сенімділігінің қатынастарымен және қолданылатын криптографиялық әдістермен белгіленеді. Мәндер тікелей немесе жанама қатынаса алады, бір немесе түрлі қауіпсіздік домендеріне қатысты бола алады, уәкілді органдар қызметтерін қолданыла алады немесе қолданыла алмайды. Келесі тұжырымдамалық үлгілер осы түрлі жағдайлар кілттер мен ақпараттардың таратылуына қалай әсер ететіндігін суреттейді.

6.1 Хабарласатын мәндер арасындағы кілттердің таратылуы

Мәндердің қатынас жолдарының мүмкіндіктеріне олардың арасындағы байланыс жолы, мәндер арасындағы сенімділік және қолданылатын криптографиялық әдістер әсер етеді.

А және В мәндері арасында криптографиялық әдістерді қолдана отырып, ақпаратпен алмасқысы келетін байланыс бар. Осы коммуникациялық байланыс 3-суретте көрсетілген. Жалпы, кілттер жөнелту жолдарынан логикалық өзгешеленетін қауіпсіздік жолдары бойынша таратылады.



3-сурет – Екі мәндер арасындағы байланыс жолы

Мәндер арасындағы тікелей байланыс кілтті келістіру, кілтті бақылау және растау жағдайларында қолданылады. Бұл жағдайлар ИСО/МЭК 11770 стандартының 2-бөлімінде (*ҚР СТ ИСО/МЭК 11770-2, Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Кілттерді басқару. 2-бөлім. Симметриялық әдістерді қолданатын тетіктер.*) және 3-бөлімінде (*ИСО/МЭК 11770-3, Ақпараттық технология. Қауіпсіздік әдістері. Кілттерді басқару. 3-бөлім. Асимметриялық әдістерді қолданатын тетіктер.*) толық қарастырылған.

6.2 Бір қауіпсіздік доменнің ішінде кілттерді тарату

Келесі үлгі *ҚР СТ ИСО/МЭК 10181-1-ге* сәйкес қауіпсіздік доменінің қауіпсіздік жөніндегі уәкілеттігі мен тұжырымдамасына негізделген. Қауіпсіздік жөніндегі уәкілетті кілттерді басқару қызметтерін мысалы, кілттер трансляциясын ұсынып алады. Мәндер асимметриялық әдісті ақпаратпен қауіпсіз алмасу үшін қолданған кезде, келесі жағдайларды бөліп көрсетуге болады:

– мәліметтер тұтастығын тексеру немесе олардың дереккөзін сәйкестендіру үшін алушы жіберушінің ашық кілтінің тиісті сертификатын талап етеді;

– құпиялықты сақтау үшін жіберуші алушының ашық кілтінің қолданыстағы сертификатын талап етеді;

– сәйкестендіруді, құпиялықты және тұтастықты қамту үшін әрбір серіктес басқаның ашық кілтінің сертификатын талап етеді. Бұл бас тартпауды өзара қамту үшін құралдарын қамтиды.

Әрбір мән өзінің қауіпсіздік бойынша уәкілеттігіне ашық кілттің қажетті сертификатын алу үшін жүгіне алады. Егер серіктестер бір-біріне сеніп, ашық кілттерінің сертификаттарын көрсете алса, қауіпсіздік жөніндегі уәкілеттікке жүгіну қажет емес.

Ескертпе – Уәкілетті қолданбайтын қауіпсіздік жөніндегі криптографиялық қосымшалар бар. Бұл жағдайларда серіктестер ашық кілттер сертификаттарымен емес, белгілі ашық ақпаратпен алмасуы мүмкін.

Егер екі осындай серіктес симметриялық криптографияны пайдаланса, кілттің генерациясы екі тәсілдің бірімен ынталанады:

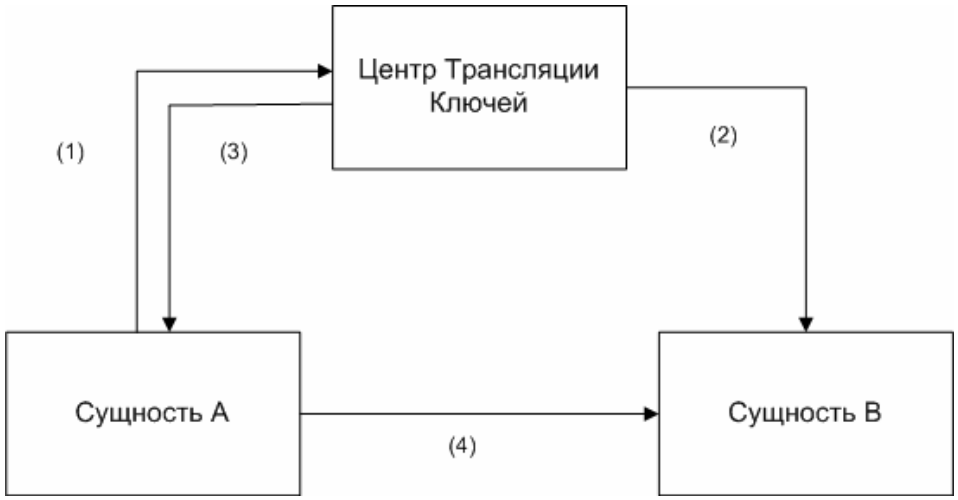
1. Мәндердің бірі кілтті генерациялап, оны Кілттерді Трансляциялау Орталығына (КТО) жібереді.

2. Мәндердің бірі Кілттерді Тарату Орталығын кейінгі тарату үшін кілтті генерациялауды сұрайды.

Егер кілт генерациясы мәндердің бірімен жүзеге асырылса, бұл кілттің қауіпсіз таратылуы, 4-суретте көрсетілгендей, Кілттерді Трансляциялау Орталығымен жүргізілуі мүмкін. Сандар алмасу кезеңдерін көрсетеді. КТО А мәнінен (1) шифрланған кілтті алады, оның шифрын ашады және оны В мәнімен бөліскен кілттің көмегімен шифрлайды. Кейін ол:

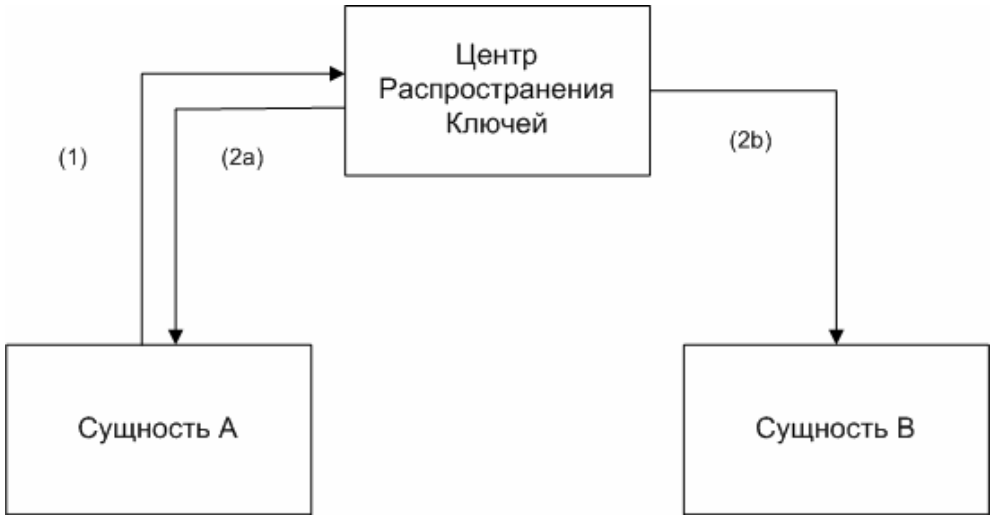
– шифрланған кілтті В (2) мәніне жібере алады;

– оны А мәнінің (3) В мәніне (4) беруі үшін қайтара алады.



4-сурет – Кілттерді Трансляциялау Орталығы

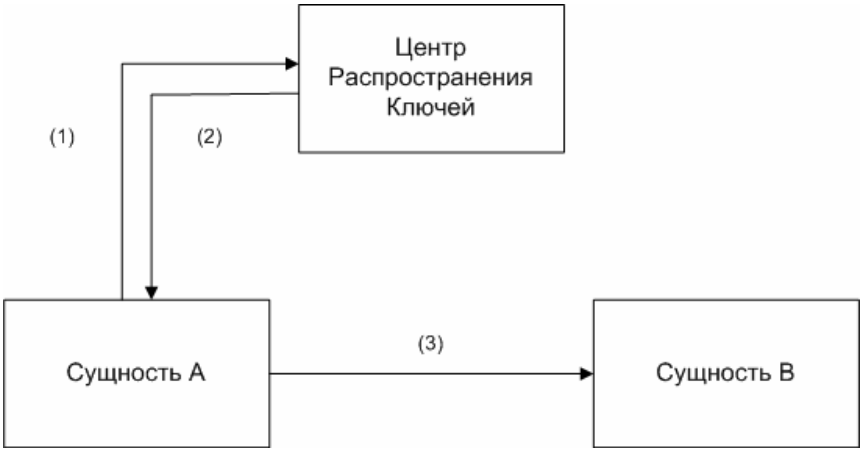
Егер кілт генерациясы сенімді үшінші тараппен жүзеге асырылса, кейін байланыс жасайтын серіктестерге кілтті таратудың екі амалы бар. Бұл жағдайлар «Кілттерді Тарату Орталығының тұжырымдамалық үлгісі» 5-суретте және «А мәнінен В мәніне кілттерді жөнелту арқылы тарату» 6-суретте көрсетілген.



5-сурет – Кілттерді Тарату Орталығының тұжырымдамалық үлгісі

5-сурет Кілттерді Тарату Орталығы екі мәндермен қауіпсіз байланыс жасай алу жағдайын көрсетеді. Бұл жағдайда кілт мәндердің бірімен генерацияланған соң, Кілттерді Тарату Орталығы екі мәндер арасындағы кілттің қауіпсіз жағдайына жауапты. Жалпы кілттің сұранысы (1) деп белгіленген, ал байланыс жасайтын серіктестер арасында кілттің таратылуы (2a) және (2b) деп белгіленген.

А және В мәндері арасына бөлінген құпия кілтті А мәні сұраған кезде, орталық екі түрлі тәсілді қолдана алады. Егер ол екі мәнмен қауіпсіз қарым-қатынас жасай алса, ол құпия кілтті жоғарыда көрсетілгендей олардың арасына тарата алады. Егер орталық А мәнімен ғана қарым-қатынас жасай алса, А мәні кілтті В мәніне беруге жауапты болып табылады. 6-суретте кілтті таратудың осы түрі көрсетілген. Жалпы кілт сұранысы (1) деп белгіленген, оның А мәніне берілуі (2) деп белгіленген. Кілттің А-дан В-ға жөнелтілуі (3) деп белгіленген.



6-сурет – А мәнінен В мәніне кілттерді жөнелту арқылы тарату

6.3 Домендер арасында кілттерді тарату

Бұл үлгіде бір жалпы криптографиялық әдісті қолданатын (симметриялық немесе асимметриялық), екі түрлі қауіпсіздік домендерге тиесілі А және В мәндері пайдаланылады. Әрбір қауіпсіздік доменінің өзінің қауіпсіздік жөніндегі уәкілеттігі бар: бірінде – А мәні сенетін, және екіншісінде – В мәні сенетін. Егер А және В мәндері бір-біріне сенсе, немесе олардың әрбіреуі басқа доменнің уәкілеттігіне сенсе, кілттер 6.1 немесе 6.2 бөліктеріне сәйкес таратылады.

А және В мәндерімен кілттерді алу кезінде екі жағдай қарастырылуы мүмкін:

– В ашық кілтінің сертификатын алу (бұл мүмкін болған кезде);

– А және В мәндерінің жалпы құпия кілтін қалыптастыру.

Бұл бөлшектер арасында түрлі қатынастар болуы мүмкін. Осы қатынастар бөлшектер арасындағы сенімділікті бейнелейді.

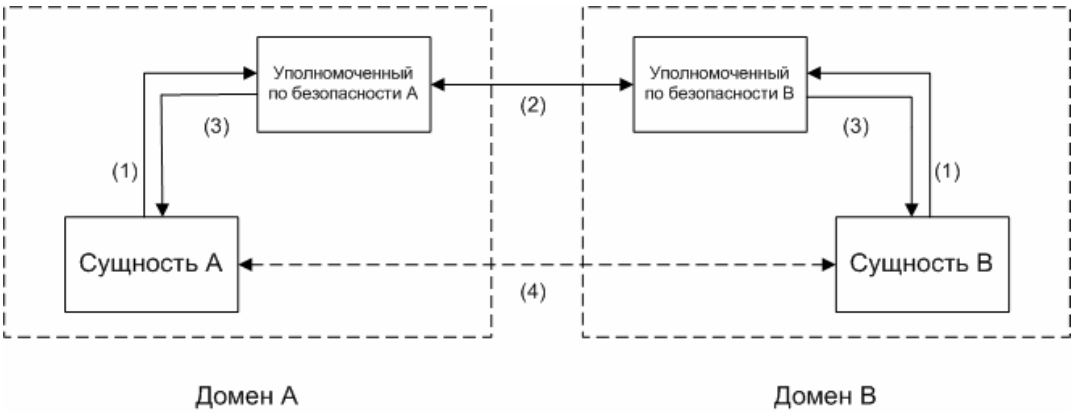
Мәндер ақпаратпен алмасу үшін асимметриялық әдісті қолданғанда және ашық кілттер сертификаттарын ұсынатын каталогтың жалпы қызметіне ене алмағанда, олардың әрқайсысы қауіпсіздік жөніндегі уәкілдікке серіктесінің ашық кілтінің сертификатын алу үшін жүгінеді (7-суретті қараңыз (1)). А және В домендерінің қауіпсіздігі жөніндегі уәкілеттіктер А және В (2) мәндерінің ашық кілттерінің сертификаттарымен алмасады және оларды А және В мәндеріне жібереді. Кейін А және В мәндері тікелей және қауіпсіз қарым-қатынас жасай алады (4).

Ашық кілттердің сертификаттарымен алмасу үшін басқа әдіс – қиылысқан сертификаттау (Г Қосымшасын қараңыз).

Мәндер симметриялық әдістерді қолдану арқылы қатынас жасағанда, әрбір мән тиісті уәкілеттікке (1) олардың қатынас жасауына мүмкіндік беретін құпия кілтті алу үшін қауіпсіз тәсілмен жүгіне алады. Уәкілеттіктер мәндер қолданатын жалпы құпия кілт туралы (2) келіседі. Бір уәкілетті тұлға

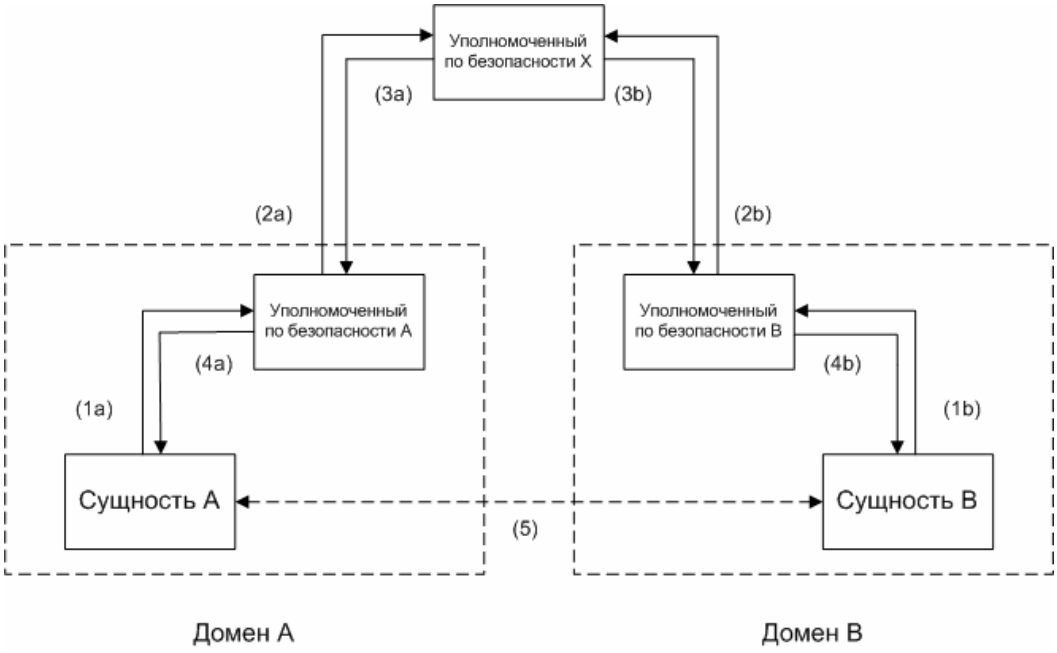
басқа уәкілетті тұлғаны тарату орталығы ретінде пайдалана отырып, екі мәндер арасында құпия кілтті таратады. Соңғысы кілттердің трансляциясын ((2) және (3)) қамтиды.

А мәні В мәнімен байланыс жасау үшін құпия кілтті сұраған кезде уәкілетті екі жолмен әрекет жасай алады. Егер оның екі мәнмен қатынас жасауға мүмкіндігі болса, ол екі мәндер арасында құпия кілтті, жоғарыда көрсетілгендей, тарата алады. Егер уәкілетті тек бір мәнмен ғана қатынас жасай алса, кілтті алатын мән екінші мәнге кілттің жөнелтілуіне жауапты.



7-сурет – Екі домен арасында кілтті тарату

Кей кезде А және В уәкілеттіктерінің өзара сенімді қатынастары да, тікелей байланыс жолы да болмайды. Бұл жағдайда олар, 8-суретте көрсетілгендей, екеуі де сенім артатын Х қауіпсіздік жөніндегі уәкілеттіні пайдаланады ((2a) және (2b) көрсеткіштері). Х уәкілетті кілтті генерациялап, оны А және В уәкілеттілер арасында таратады ((3a) және (3b) көрсеткіштері) (8-суретті қараңыз). Х уәкілетті алынған құпия кілтті немесе ашық кілттің сертификатын (мысалы, 2a) А уәкілеттіден В уәкілеттіге (3b) жөнелтеді. Кейін уәкілеттілер ақпаратпен қауіпсіз алмаса алатын тиісті мәндерге ((4a) және (4b) (8-суретте)) алынған кілтті жөнелтулері тиіс. Сенімдік тізбегі құрастырылғанға дейін қосымша уәкілеттілер ізденісі қажет болуы мүмкін.



8-сурет – Қауіпсіздік жөніндегі уәкілеттілер арасындағы сенімдік тізбегі

7 Арнайы қызмет көрсетушілер

Кілттерді басқару жүйесіндегі кейбір қызметтер сыртқы қызмет көрсетушілерімен ұсынылуы мүмкін. Қызмет көрсетушілер ретінде мыналар бола алады:

– Уәкілетті тіркеу органы немесе куәландыратын орталық;

– ИСО/МЭК 8732 стандартында белгіленгендей, кілтті тарату орталығы;

– ИСО/МЭК 8732 стандартында белгіленгендей, кілтті трансляциялау орталығы.

А қосымшасы
(анықтамалық)
Кілттерді басқарудағы қауіп-қатерлер

Кілтті басқару бірқатар қауіп-қатерлерге душар болады, оның ішінде:

Кілттік материалды ашу: кілттік материал шифрланбаған түрінде сақталады, қорғанбаған және оған енуге рұқсат қажет, не болмаса шифрланған және шифры ашылуы мүмкін.

Кілттік материалды түрлендіру: кілттік материал ол бағытталған түрде жұмыс істемейтіндей түрлендірілген.

Кілттік материалды рұқсатсыз жою: Кілтті немесе онымен байланысты мәліметтерді жою.

Кілттік материалды толық емес түрінде жою: бұл ағымдағы немесе болашақ кілттердің біреумен ашылуына әкеледі.

Рұқсатсыз күшін жою: қолданыстағы кілтті немесе кілттік материалды тікелей немесе жанама жою.

Ауыстыру: авторланған пайдаланушы немесе мән ретінде көрсету.

Кілттерді басқару функцияларын орындаудағы кідірістер: кілтті генерациялау, тарату, күшін жою, тіркеу мүмкіндіктері болмауында, кілттер сақтау орындарын жаңарту мүмкіндігі болмауында, пайдаланушы өкілеттік деңгейін қолдауда мүмкіндік болмауында және т.б. түрде білінеді. Кідіріс қауіп-қатері жоғарыда көрсетілген себептер салдарынан немесе тиісті жабдықтың іс жүзінде істемей қалуынан пайда болуы мүмкін.

Кілттердің дұрыс емес пайдаланылуы:

– кілтті ол бағытталмаған мақсаттарда жұмсау, мысалы, кілттерді шифрлауға бағытталған кілт мәліметтерін шифрлауға пайдалану;

– кілттің басқару құралдарын жарамсыз мақсаттарда пайдалану, мысалы, заңсыз шифрлау немесе мәліметтердің шифрын ашу;

– әрекет ету мерзімі өткен кілтті пайдалану;

– кілтті шектен тыс пайдалану;

– кілтті авторланбаған пайдаланушыларға ұсыну.

Б қосымшасы
(анықтамалық)
Кілттерді басқарудың ақпараттық объектілері

Кілтті басқарудың ақпараттық объекттері кілттен немесе кілттерден және, мүмкін, кілтті (кілттерді) қалай қолдануға болатындығын белгілейтін басқа ақпараттан тұрады. Басқарушы ақпарат тек қана анық түрде емес, кілттерді басқарудың ақпараттық объектілерін пайдалануды реттейтін келісімдерден де шығуы мүмкін. Мысалы, асимметриялық жұптың бір кілтін пайдалану екіншіні келісімді пайдаланумен реттеледі: біреуі – шифрлау үшін, екіншісі – шифрын ашу үшін.

Басқарушы ақпарат мыналарды қадағалайды:

– сол кілтпен қорғалатын объекттің түрі (мысалы, кілттерді басқарудың мәліметтері немесе ақпараттық объекті);

– мүмкін болатын операциялар (мысалы, шифрлеу, шифрын ашу);

– мүмкін болатын пайдаланушылар;

– кілтті пайдаланатын орта;

– кілтті басқарудың ақпараттық объектін пайдаланатын басқарудың нақты әдісіне немесе қосымшасына тән басқа да аспекттер.

Кілтті басқарудың ақпараттық объектісінің нақты мысалы ретінде кілттің сертификаты болып табылады. Оның куәландыратын орталықпен жазылған мынадай мәліметтері бар:

– кілттік материал;

– кілтті басқарудың тиісті ақпараттық объектісін қолданатын пайдаланушының сәйкестендірушісі;

– кілтті басқарудың тиісті ақпараттық объектісі орындайтын операциялар (анық емес берілуі мүмкін);

– кілттің қолданылу кезеңі;

– куәландыратын орталықтың сәйкестендірушісі.

ASN.1 форматындағы мынадай анықтама кілтті басқарудың ақпараттық объектісінің мысалы болып табылады, бірақ кілтті басқарудың ақпараттық объектісінде басқа да жүзеге асыруға тәуелді шамалар болуы мүмкін:

```
Key ::=          PROTECTED {KeyContents protectionType};
KeyContents::=   SEQUENCE {
                    keyID          [0] Key_ldentity,
                    keyValue       [1] Key_Value,
                    checkValue     [2] Check_Value,
                    cryptoMethod   [3] Cryptographic_
                                       Method,
                    timeStamp      [4] Time_Stamp,
                    generAuthority [5] Generating_Auth
                                       ority,
```

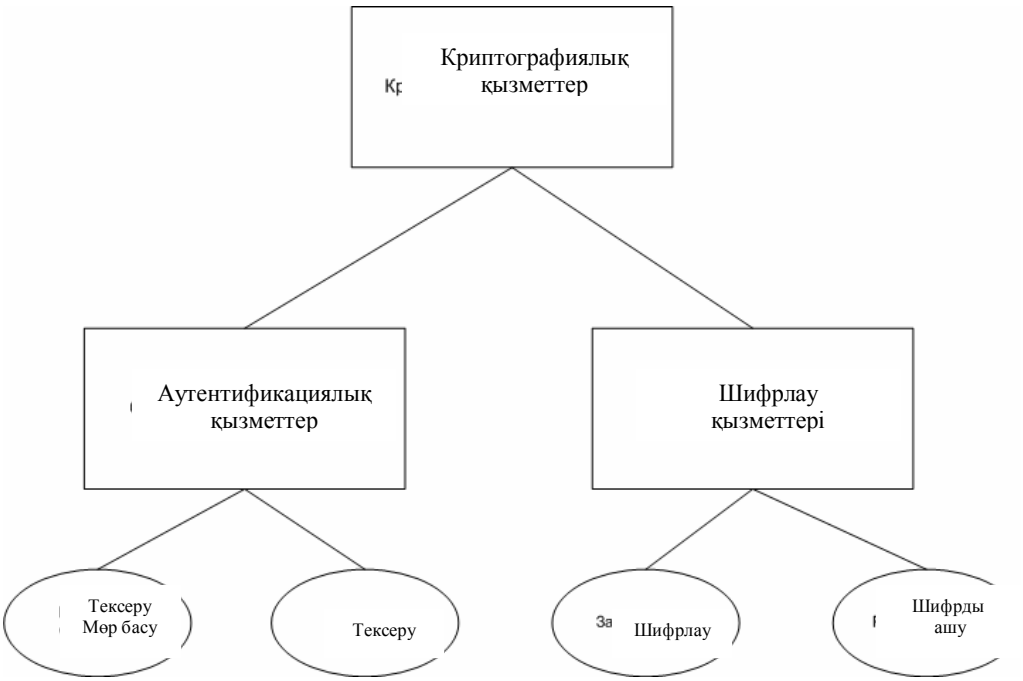
```
certiAuthority   [6] Certification_Au
                     thority,
issuer           [7] Issuer,
validity         [8] Validity_of_Key
                     };
```

Бұл анықтамада Key_ldentity (кілттің бірігей сәйкестендірушісі), Key_Value (кілттің мазмұны) және Check_Value (кілттің толықтылығын растау үшін тексеру сомасы) шамалары бар, мұнда Key_Value ғана міндетті шама болып табылады. Cryptographic_Method (криптографиялық әдіс), Issuer (шығарушы) және Validity_of_Key (кілттің шынайылығы) шамалары кілтті белгілі алгоритмдермен, уақытпен және пайдаланушымен шектей отырып, оның қолданылуын реттейді. Бұл шамалар кілтті пайдалануды реттеу үшін маңызды, бірақ міндетті емес. Generating_Authority (генерациялау органы), Certification_Authority (куәландыратын орталық) және Time_Stamp (уақыт таңбасы) шамалары кілттің дереккөзін растау үшін және оның жасын белгілеу үшін маңызды, бірақ бұлар да міндетті емес болып табылады. Кілттің сертификаты үшін Issuer (шығарушы) шамасы міндетті болып табылады.

В Қосымшасы
(анықтамалық)
Криптографиялық қосымшалардың дәрежелері

Криптографиялық жүйелердің жалпы жіктелуі екі негізгі криптографиялық әдістерді қолданумен белгіленеді – бұл симметриялық және асимметриялық әдістер. Кілтті басқару екі әдісті де қамтуы үшін басқа тәсіл қажет. Сондықтан бұл бөлім криптографиялық жүйелерді әдістермен ұсынылатын мүмкіндіктерге сәйкес жіктейді.

Жалпы алғанда криптографиялық жүйе екі түрлі криптографиялық қызметтерді: сәйкестендіру қызметін және шифрлау қызметін ұсынады. Шифрлау қызметтері ақпаратты криптографиялық қорғау үшін пайдаланылады, яғни олар мәліметтердің құпиялығын қамтиды. Сәйкестендіру қызметтері мәндерді, мәліметтер дереккөздерін сәйкестендіру үшін, мәліметтердің толықтылығына кепілдік беру үшін және бас тартпауды қамту үшін пайдаланылады. Криптографиялық жүйелер түрлері мен тиісті операциялар С-1 суретінде көрсетілген.



В-1 суреті – Криптографиялық қызметтер мен тиісті әдістер.

В.1 Сәйкестендіру қызметтері мен кілттер

Сәйкестендіру қызметтері өзара қатынас жасайтын мәндерді сәйкестендіру үшін (мәндердің сәйкестендірілуі), мәліметтердің шығуын сәйкестендіру (мәліметтер дереккөзін сәйкестендіру), бас тартпаушылықты сәйкестендіру үшін және мәліметтер тұтастығын қамту үшін қызмет етеді.

мәліметтер блогын бекітіп қою	бұған мәліметтер үшін олардың тұтастығын бақылау мақсатымен криптографиялық қадағалау мазмұнын есептеу кіреді, мысалы, симметриялық алгоритм көмегімен хабарламаны сәйкестендіру кодын генерациялау (MAC)

мәліметтер блогын жазу	бұған мәліметтер дереккөзін сәйкестендіру үшін, олардың тұтастығына кепілдік беру және/немесе бас тартпаушылықты қамту үшін цифрлік жазбаны қалыптастыру кіреді
бекітіліп қойылған блокты верификация-лау	бұған цифрлік жазба мәлімдеушімен және/немесе мәліметтер тұтастығын растау үшін қалыптастырылды ма екендігін анықтау үшін оны верификациялау кіреді

Сәйкестендіру қызметтерінде жазу және бекітіп қою процестері дереккөзде бар жабық ақпаратты (яғни бірігей және құпия) немесе дереккөз бен алушыға мәлім құпия ақпаратты қолданады. Верификация процесі дереккөздің жабық ақпаратын алуға мүмкіндік жоқ бәріне мәлім шаралар мен ақпаратты қолданады немесе дереккөз бен алушыға жалпы құпия ақпаратты пайдаланады. Жазудың маңызды мінездемесі бұл жазуды дереккөздің жабық ақпаратын – оның жабық кілтін пайдалану арқылы қалыптастыру. Осылайша, егер жазу дереккөздің ашық кілтімен расталса, кейін бұл жазуды жабық ақпарат иесі жасағандығы туралы үшінші тарапқа дәлелдеуге болады (мысалы, нотариалды органға).

Сәйкестендіру қызметтері үш кілт түрлерінен екеуін пайдаланады:

– бекітіп қою үшін кілт – жалпы құпия кілт

– жазу үшін кілт – дереккөзбен байланысты бірігей,жабық кілт

– верификациялау үшін кілт – немесе ашық, немесе құпия кілт.

Симметриялық әдістерде сәйкестендіру қызметі бір құпия кілтпен ұсынылған бекітіп қою кілтін және верификациялау кілтін қолданады. Асимметриялық әдістерде бұл қызмет ашық және жабық кілттерден тұратын кілттер жұбымен ұсынылған жазу кілтін және верификациялау кілтін қолданады.

В.2 Шифрлау қызметтері мен кілттер

Шифрлау қызметтері негізінде ақпараттың құпиялығын қамту үшін, және де мәліметтер тұтастығын қамту үшін қолданылады. Қолданылатын әдістерге байланысты сәйкестендіру және бас тартпаушылық секілді қауіпсіздік қызметтері де ұсынылуы мүмкін. Бұл жағдайда екі негізгі тетік пайдаланылады:

– шифрланған мәтінді бастапқы мәліметтерден шығаратын *шифрлау операциясы;*

– ашық мәтінді тиісті шифрланған мәтіннен шығаратын *шифрды ашу операциясы.*

Шифрлау қызметі қолданылатын криптографиялық, яғни симметриялық және асимметриялық әдістерімен мінезделеді. Симметриялық әдіс қолданылғанда, шифрлау және шифрды ашу операциялары бір кілтті (жалпы құпия кілтті) пайдаланады. Асимметриялық әдіс қолданылғанда, шифрлау және шифрды ашу операциялары екі түрлі өзара байланысты, яғни ашық және жабық кілттерді пайдаланады.

Г қосымшасы
(анықтамалық)
Сертификаттың өмірлік кезеңін басқару

Бұл қосымшада ашық кілттер сертификатының өмірлік кезеңін басқаруда қолданылатын талаптар мен шаралар берілген.

Г.1 Куәландыратын орган

Абоненттер өзінің Куәландыратын орталығына «сенеді». Мұндай сенім тиісті криптографиялық әдістерді және жабдықтарды қолдануға, және де кәсіби басқару мен бақылау қызметіне негізделген. Бұл сенім тәуелсіз аудитпен расталады (ішкі, сыртқы немесе екеуімен де) және аудит қорытындыларымен абоненттердің танысуына болады.

КО мыналарға жауапты:

1. Сертификаттауға ұсынылған кілттер жұбының мәндерін сәйкестендіру.

2. Ашық кілт сертификатын өндеу үшін қолданылатын асимметриялық кілттер жұбының сапасын қамтамасыз ету.

3. Ашық кілт ақпаратын жазу үшін қолданылатын жабық кілт пен сертификаттау процесінің қауіпсіздігін қамтамасыз ету.

4. Ашық кілт туралы ақпаратқа енгізілуге міндетті ашық кілттің сертификаты, куәландыратын орталықтың сәйкестендірушісі және т.б. секілді арнайы мәліметтерді басқару.

5. Әрекет мерзімін белгілеу және тексеру.

6. Ашық кілттің сертификаты шығарылғандығы жөнінде ашық кілт туралы ақпаратта көрсетілген мәнді хабардар ету. Хабарламаны жіберуге қолданылған құралдар КО-ға ашық кілт туралы ақпаратты беру үшін қолданылған әдістен тәуелсіз болуға тиіс.

7. Екі түрлі мәндер бір сәйкестендірушіге ие болмағандығы, яғни олар елеулі өзгеше екендігіне кепілдік беру.

8. Күші жойылған сертификаттардың тізімін қолдау және шығару.

9. Ашық кілт сертификатын генерациялау процесінде қолданылатын барлық қадамдарын тіркеу.

Ашық кілт сертификатын алу үшін бір КО екінші КО-ның ашық кілт туралы ақпаратын сертификаттай алады. Сондықтан сәйкестендіру ашық кілттер сертификаттарының тізбегін қолдана алады. Бұл тізбектегі ашық кілттің бірінші сертификаты алынуы және ашық кілттің сертификатталуынан ерекше әдіспен расталуы қажет.

Г.1.1 КО-ның кілттерінің асимметриялық жұбы

КО-ның өзін пайдалану арқылы кілттердің асимметриялық жұбын генерациялайтын кілттерді қауіпсіз басқарудың құралдары болуға тиіс. Генерация процесі кілттік материалдың болжамсыздығын қамтуы қажет. Ешкім генерация процесін білуден артықшылық алуға тиіс емес.

КО-ның жабық кілті мәндердің ашық кілттерінің ақпаратын жазу үшін қолданылады. Мұндай кілтке ие болу КО ретінде көрсетілуге және ашық кілттерінің жасанды сертификаттарын генерациялау мүмкіндіктерін беретіндіктен, бұл кілтті қорғаудың жоғары дәрежесі қамтылуы қажет. Осылайша, КО-ның жабық кілті оны кілттерді басқару құралдарында пайдалану кезінде жақсы қорғалуға тиіс. Кілт кілттерді басқару құралдарына қорғалған әдіспен және КО бақылауымен енуі және одан шығуы қажет.

КО ашық кілтінің верификация үшін толықтылығы ашық кілттер сертификаттау жүйесінің қауіпсіздігі үшін маңызды болып табылады. Егер КО-ның ашық кілті ашық кілттің сертификатында болмаса, оның сәйкестендірудің таратылуын қамту үшін арнайы шаралар жасалуға тиіс. Пайдаланушылар жағынан КО ашық кілтінің сақталынған көшірмесінің түпнұсқаға барабарлығына кепілдік беру үшін шаралар қолданылуы керек.

КО-ның верификация үшін ашық кілті басқа пайдаланушылардың ашық кілттер сертификаттарын тексеру үшін пайдаланылады. КО ашық кілтін әрбір қолдану алдында пайдаланушы верификация үшін кілттің сол сәтке дұрыстығына көзі жеткізуі керек.

Г.2 Сертификаттау процесі

Бұл бөлім сертификаттау процесінде қолданылатын талаптар мен шараларды бейнелейді.

Г.2.1 Ашық кілтті сертификаттау үлгісі

Бұл бөлім ашық кілттерді сертификаттаудың негізгі үлгісін белгілейді. Бұл үлгіде негізгі функциялар логикалық мәндер арасында бөлінеді (Г-1 суретін қараңыз):

1. КО (куәландыратын орталық): пайдаланушылық мәннің ашық кілті туралы ақпаратын сертификаттауға жауапты мән.

2. Каталог (DIR): ашық кілттер сертификаттарына пайдаланушылық мәндердің жедел түрде кіруді ұсынуға жауапты мән.

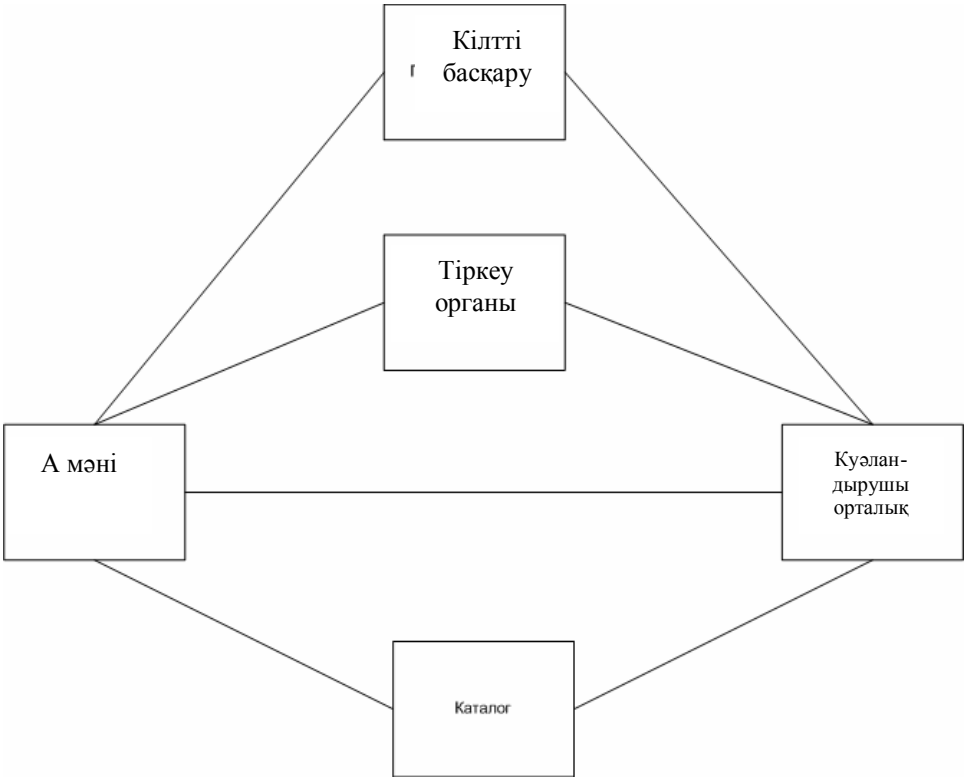
3. Кілттер генерациясы (КГ): асимметриялық кілттер жұптардың генерациясына жауапты мән.

4. Тіркеу органы (ТО): КО-ға пайдаланушылардың тексерілген сәйкестендірушілерін ұсынуға жауапты мән.

5. Пайдаланушылық мән (А).

Бұл бөлімде осы үлгінің логикалық мәндері мен осы қатынастарға қойылатын қауіпсіздік талаптар арасындағы қатынастар талқыланады. Логикалық мәндер бірігулері мүмкін. Мысалы, пайдаланушылық мән асимметриялық кілттер жұбын өзі генерацияласа, А және КГ бірігулері мүмкін. КО пайдаланушылық мәндер атынан жұптарды генерацияласа, КО және КГ бірігулері мүмкін.

Ескертпе – біріккен ТО және КО-мен жасалған сертификат дербес ТО мен КО жасаған сертификатқа сәйкес екендігіне көз жеткізу қажет.



Г-1 сурет – Ашық кілттерді сертификаттаудың базалық үлгісі

Г.2.1.1 Сертификаттау үлгісіндегі байланыстар

Бұл бөлім базалық үлгідегі кейбір байланыстарды және тиісті қауіпсіздік талаптарын бейнелейді. Жүйенің нақты жүзеге асыруында барлық байланыстар болуы міндетті емес. Мысалы, ТО, КО және КГ функциялары бірігуі мүмкін.

А-КГ

А мәні КГ кілттер генераторын асимметриялық кілттер жұбын генерациялауды сұрайды. КГ асимметриялық жұптар генерациясында жақсы сапалы кілттерге сенім білдіреді. КГ кілттер жұбын генерациялайды (Sa, Va), мұнда Sa – жазу үшін кілт, Va – верификация үшін кілт, және оны А мәніне жөнелтеді. Бұл жөнелту қауіпсіз және құпия әдіспен жасалуы қажет. КГ және А жөнелту уақытында асимметриялық кілттер жұбын үшінші тарап өзгертпегендігіне және кілттердің мазмұнын ашпағандығына көздері жетуі қажет.

А-ТО

А мәні Тіркеу орталығында (ТО) тіркелуді сұрайды. А ТО-ға сәйкестендірілген ақпарат ұсынуы тиіс. ТО бұл ақпараттың шынайылығын тексеріп, оған қажетті арнайы мәліметтерді қосуына болады. Осындай қауіпсіз түрде ақпарат ТО-ға жіберіледі.

А-КО

А мәні КО-ны ашық кілт пен оның бірігей атын қоса, ашық кілт ақпаратын (немесе оның астарлы көпшілігін) сертификаттауды сұрайды. КО-ға ашық кілт ақпаратын ұсыну ісі оның толықтылығы мен шынайылығына кепілдік беру арқылы жасалуы қажет. КО А мәнінің ашық кілт ақпаратының шынайылығын тексеріп, мүмкін болса, арнайы жүйелік мәліметтерді қосып, кейін ашық кілт туралы толық ақпаратты А мәнінің ашық кілт

сертификатын өндеу үшін құптайды. Енді ашық кілт сертификаты А мәніне жөнелтілуіне болады.

Берілген ашық кілт сертификатын алған соң А куәландыратын орталықтың $v_{УЦ}$ верификациялау үшін кілтінің көмегімен оның шынайылығын тексереді. Осы $v_{УЦ}$ верификациялау үшін ашық кілт А мәніне шынайылық кепілдігімен ұсынылуы қажет. Осы сәттен А мәнінің ашық кілті ашық кілт сертификаты ретінде таратылуына болады және КО-ны верификациялау үшін кілтке енуге рұқсаты барлармен қолданыла алады.

Бірақ, егер, КО КГ-ны А мәніне асимметриялық кілттер жұбын генерациялауды сұраса, кілттер жұбы КГ-дан А мәніне жіберілуі мүмкін. Бұл жөнеліске құпиялық, толықтылық және түпнұсқаға барабарлық талаптары қойылады. Бұған қоса КО өндеу және сақтау кезінде барлық асимметриялық жұптардың құпиялығын, толықтылығын және түпнұсқаға барабарлығын сақтауға тиіс. КО жабық кілтті А мәніне кілттің жіберілген мазмұны үшінші тараппен өзгертілмеуіне немесе оқыла алынбайтынына көзі жеткен соң ғана жіберуге тиіс.

А - DIR

А мәні өзінің ашық кілт сертификатын DIR каталогына беріп, оны осы каталогта тіркейді. Каталогта ашық кілт сертификатын тіркеу үшін мәннің сәйкестендірілуі және оған енуге құқықтардың тексерісі қажет. А және DIR мәндері арасында каталогтағы мәліметтерді кім басқаруға уәкілді болатындығына келісім болуы қажет. Бір сценарий бойынша DIR каталогтағы барлық ақпараттарды басқарады, ал екіншісі бойынша - әрбір мән каталогтағы өз ақпаратын өзі басқарады.

ТО-КО

ТО КО-ны А мәнінің ашық кілті туралы ақпаратын сертификаттауды сұрайды. А ашық кілті туралы ақпараттың ТО-дан КО-ға жөнелісі сәйкес әдіспен болуы қажет. КО А ашық кілті туралы ақпараттың шынайылығын тексеріп, арнайы жүйелік мәліметтерді мүмкін болса қосып, кейін ашық кілт сертификатын алу үшін ашық кілт туралы толық ақпаратты құптайды. КО ТО-ны сертификатталуы туралы хабардар етеді.

КО-КГ

Куәландыратын орталық КГ кілттер генераторын А мәні үшін асимметриялық кілттер жұбын генерациялауды сұрайды. КГ асимметриялық жұптар генерациясында жақсы сапалы кілттерге сенім білдіреді. КГ кілттер жұбын генерациялап, оны КО-ға жібереді. Бұл жөнеліс қауіпсіз және құпия әдіспен жүзеге асырылуы тиіс. КГ және КО жөнелту уақытында асимметриялық кілттер жұбын үшінші тарап өзгертпегендігіне және кілттердің мазмұнын алмағандығына көздері жетуі қажет. КО өндеу және сақтау кезінде барлық асимметриялық кілттер жұбының құпиялығын, толықтылығын және шынайылығын сақтауға тиіс.

КО- DIR

КО алынған ашық кілттер сертификатын тікелей DIR Каталогына жіберіп, оларды каталогта тіркейді. Ашық кілт сертификатын каталогта тіркеу үшін мәннің аутентификациясы және оның енуге құқығының бар болуы тексерілуі қажет.

Г.2.2 Тіркеу

Мәннің кілтін тіркеуге мәнге сертификатты беру туралы арыз және оның ТО-мен немесе КО-мен тексерілуі кіреді. Келесі бөліктерде сертификатты беру туралы арызды ұсынуға қойылатын талаптар келтірілген. Сертификатты беру туралы арызда ашық кілттің мазмұны болуы да, болмауы да мүмкін.

Г.2.2.1 Жеке тұлғалардың арыз беруі

Аз ғана қауіп-қатері бар қосымшалар үшін сертификатты беру туралы арызды қанағаттау ашық кілт сертификатын алушы тұлғаны сәйкестендіруге негізделуге тиіс. Сертификатты беру туралы арызды жеке тұлға беруге тиісті емес, бірақ тұлғаны куәландырудың іскерлік тәртібі пайдаланылуы қажет.

Жоғары қауіп-қатері бар қосымшалар үшін сертификатты беру туралы арызды қанағаттау ашық кілт сертификатын алуға тілек білдіргеннің жеке жүгінісіне (немесе уәкілді агент арқылы) және сертификатқа жүгінушіні (және, қажет болса, оның агентін) сәйкестендіру үшін коммерциялық стандарттарды пайдалануға негізделуі қажет. Бұл тұлғаның үшінші сенімді тараппен куәландырылуын қажет етуі мүмкін.

Г.2.2.2 Заңды тұлғалардың арыз беруі

Сертификат беру туралы арызды қанағаттандыру туралы бұл арыз, кем дегенде, заңды тұлғаның бір өкілімен жеке жеткізілуіне және мыналарға негізделуі қажет:

1. Ашық кілт сертификатын беру туралы арыздағы қол мен мөрге.

2. Заңды тұлғаның қолы мен мөрінің шынайылығын растау үшін коммерциялық тәжірибені пайдалануға.

3. Сертификатты беру туралы арызды жеткізген өкілдердің шынайылығын растау үшін коммерциялық тәжірибені пайдалануға.

Г.2.3 Заңды тұлғалар арасындағы қатынастар

Заңды тұлғалар үшін басқа заңды тұлғалармен байланыс орнату қажеттілігі туындауы мүмкін. Бұл түрлі әдістермен жүзеге асырылады:

1. Компания қызметкерлерінде жеке асимметриялық кілт жұптары бар. Заңды тұлға өз компаниясының қызметкерлері үшін КО ретінде болады. Мәмілелер қызметкерлердің компания КО-сымен сертификатталған жеке кілттерінің көмегімен куәландырылады. Алушылар жіберушілерде компания сертификаты бар екендігін тексереді, ал олардың ашық кілті жоғарыда тұрған кейбір КО-мен сертификатталады.

2. Компания қызметкерлерінде жеке асимметриялық кілттер жұбы жоқ. Тек заңды тұлғада ғана бір немесе бірнеше асимметриялық кілттер жұптары бар. Алушылар жіберуші компаниясындағы қауіпсіздік саясаты мен енуге рұқсат деңгейіне алаңдамауы тиіс.

Г.2.4 Сертификаттарды генерациялау

Ашық кілттің сертификатын генерациялау процесі асимметриялық кілттер жұбын пайдалануға дейін жүзеге асырылуы қажет.

Келесі қадамдар сертификатты генерациялау процесінде қажетті:

1. Ашық кілт ақпаратында қатенің бар болуына тексеру.

2. Ашық кілт туралы ақпаратты қабылдау. Ашық кілт туралы ақпаратты қабылдауға қойылатын талаптар жоғарыдағы тіркеу туралы бөлікте белгіленген.

3. Ашық кілттер сертификаттарын басқару үшін қажетті мәліметтерді дайындау және қосу. Қосымша, бірақ міндетті емес түрде КО асимметриялық кілттер жұбын (жұптарын) генерациялай алады.

4. Хэш-функцияны пайдалана алатын ашық кілт сертификаты үшін жазуды есептеп шығару.

5. Ашық кілт сертификатын генерациялау процесінде КО әрекеттерін хаттамалау.

Жоғары қауіп-қатері бар қосымшалар үшін (1) түрлі криптографиялық құралдарын (түрлі жабық кілттермен) қолдану арқылы бір КО-мен ашық кілт сертификатының бірнеше жазуларын қалыптастыруды талап ету, немесе (2) түрлі КО-мен жасалынған ашық кілт туралы ақпараттардың бірнеше жазуларын талап ету дұрыс болар.

Г.2.5 Жаңғырту/Өмір уақыты

Жабық кілттің сертификатында ашық кілт сертификатында көрсетілген пайдалану мерзімімен немесе КО-мен белгіленген басқа түрдегі өмір уақыты бар.

Г.3 Ашық кілттер сертификаттарын тарату және қолдану

Бұл бөлім ашық кілт сертификатын тарату мен пайдалануда қолданылатын талаптар мен шараларды суреттейді.

Г.3.1 Ашық кілттер сертификаттарын тарату және сақтау

Ашық кілт сертификаты жасалынған кезде, оның құпиялығы мен толықтылығын сақтау үшін арнайы шаралар қажет емес. Ашық кілт сертификаты бәріне жалпы каталогта сақталады.

Г.3.2 Ашық кілттердің сертификаттарын верификациялау

Ашық кілт сертификатының шынайылығын тексеру үшін, тексеріп жатқан В мәні, кем дегенде, ашық кілт сертификатының КО қолын тексеруге тиіс. Егер ашық кілт сертификатының пайдалану мерзімі белгіленсе, В А мәнінің ашық кілт ақпараты сол уақытқа дұрыс екендігіне көзі жетуі керек (Г.5. Сертификаттардың күшін жоюды қараңыз). Ашық кілт сертификатын верификациялау үшін тексерушіде верификациялау үшін КО кілтінің қолданыстағы көшірмесі болуға тиіс.

Г.4 Сертификаттық тізбектер

КО-дан қалған барлық КО-ларды білу және олардың сертификаттары қажет етілмейді. КО-ның қатал иерархиясында да қажеттілік жоқ. Бірақ КО-да ашық кілттер сертификаттарымен икемді пайдалану және алмасу мүмкіндіктері бар болуы үшін бірін бірі сертификаттауына болады (қиылысқан сертификаттау жүргізу). Бұл қиылысқан сертификаттау жоғары дәрежедегі қорғаныспен және тиісті ойластырылған шаралар арқылы жүзеге асырылуы қажет. Қиылысқан сертификаттау жүйесі болған кезде, ашық кілт сертификатының шынайылығын тексеруге жолдар табуға болады. Пайдаланушының КО-ның біреуін верификациялау үшін кілтке ғана сенімділігі болуы тиіс. Бұл сенімділік белгісіз КО-мен берілген серіктестің ашық кілтіне дейін тізбек бойынша таратылуы мүмкін.

Г.5 Сертификаттың күшін жою

Сертификаттың пайдалану мерзімі аяқталғанға дейін күші жойылуы мүмкін. Бұл бірнеше себептер салдарынан болады, оған келесі кіреді:

1. Мәннің ашық кілтінің біреумен ашылуы.
2. Мәннен кілтті өзгертуді сұрау.
3. Мәннің қосылу жағдайларын өзгерту.
4. Мән қызметінің аяқталуы.
5. Мәннің дұрыс емес сәйкестендірілуі.
6. КО жабық кілтінің біреумен ашылуы.
7. КО-ны толығымен жою.

Сондықтан, келесіні жеңіл және қауіпсіз болдырмау үшін, мүдделі жақтарды тез хабардар ету шаралары мен құралдары болуы қажет:

1. Бір немесе бірнеше мәндердің бір немесе бірнеше ашық кілттер сертификаттары.

2. Ашық кілттер туралы ақпаратты құптау үшін КО-мен пайдаланылатын бір асимметриялық кілттер жұбына негізделген, КО-мен берілген барлық ашық кілттер сертификаттарының жиынтығы.

3. Пайдаланылатын асимметриялық кілттер жұбының функцияларына тәуелсіз, КО-мен берілген ашық кілттердің барлық сертификаттары.

Екі соңғы талаптар КО жабық кілті біреумен ашылғанда немесе осыда күмданғанда, немесе ашық кілттер сертификаттарын жазу үшін қолданылған асимметриялық кілттер жұбы өзгертілген кезде ашық кілттер сертификаттар күшін жою мүмкіндігін қамтиды. Ашық кілттер сертификаттарының күші жойылғанда немесе олардың пайдалану мерзімі аяқталғанда, олардың көшірмесі сенімді үшінші тараппен іскерлік тәжірибемен, заңмен және нормативті құжаттармен белгіленген уақытқа сақталуға тиіс.

Мәннің немесе КО-ның жабық кілті түрлі жағдайлармен өзгертілген кезде, осы ашық кілт сертификатын берген КО барлық тиісті ашық кілт сертификаттарының күші жойылғандығы жөнінде жүйедегі барлық мәндерді жедел түрде хабардар етуі қажет. Бұл КО-мен расталған және барлық мәндерге таратылған хабарлама түрінде болуы мүмкін; басқа КО-мен расталған хабарлама түрінде; сенімді үшінші тараппен қолданылатын онлайндық тізімге ашық кілттердің күші жойылған сертификаттарын енгізу немесе ашық кілттердің шынайы немесе күші жойылған сертификаттарының тізімін басып шығару түрінде.

Ашық кілт сертификаты белгілі болғандығынан немесе тиісті жабық кілтті біреу ашқандықтан күші жойылса, жабық кілт ендігі қолданылмайды. Ашық кілт сертификаты, мәліметтер сертификаттың күші жойылғанына дейін құпталу шартымен, верификациялау мақсатында ғана пайдаланылады. Осы ашық кілт сертификатын пайдалану арқылы шифрленген қандай да болмасын кілттік материалдың қолданысы (түріне тәуелсіз) сол сәтте тоқталуына тиіс.

Кілттің пайдалану мерзімі аяқталған кезде, немесе, күмәнді не болмаса шынайы біреумен ашылуынан басқа, түрлі себептермен оның күші жойылса, жабық кілт ендігі қолданылмайды. Ашық кілт сертификаты верификациялау және шифрды ашу үшін әлі де пайдаланылуына болады. Ашық кілттің осы сертификатын қолдану арқылы таратылған және қорғалған барлық кілттік материал (түріне тәуелсіз) барынша жылдам ауыстырылуы қажет.

Г.5.1 Күші жойылған сертификаттардың тізімі

Күші жойылған сертификаттардың тізімінде КО-мен күші жойылған сериялық нөмірлер немесе ашық кілттердің сертификаттар сәйкестендірушілер тізімінің уақытша белгілері бар. Күші жойылған сертификаттар тізімінде екі уақытты белгілеу түрі қолданылады:

1. КО сертификаттың күшін жойған күні мен уақыты;

2. Белгілі немесе күмәнді біреумен ашылудың күні мен уақыты.

Соңғы уақыттық белгі, егер шынайы болса, сезікті хабарламалардың тексерісін жеңілдетеді. Ашық кілт сертификаты күші жойылған сертификаттар тізімінде, кем дегенде, оның пайдалану мерзімі аяқталғанына дейін қалады. Уақыт белгілері өте маңызды, өйткені олар мәннің ашық кілті мен мән арасындағы байланыс қай уақытта жойылғандығын белгілеуі мүмкін.

Егер күштің жойылуы белгілі немесе күмәнді біреумен ашылу себебінен болса, қол біреумен ашылған күннен соң қойылса немесе қол қою күні сенімді белгіленбесе, тиісті жабық кілтпен құпталған ақпарат анық деп есептелмейді. Ақпарат күші жойылған ашық кілттің көмегімен шифрленбеуі тиіс.

Күші жойылған сертификаттар тізімінде:

1. Мәндер тізімнің толықтылығын және оны тарату уақытын тексеру үшін КО-ның қолы мен күні болуға тиіс.

2. Соңғы басып шығарудан кейін ешқандай өзгерістер болмаса да, КО-мен уақытылы басылып шығарылуы қажет.

3. Заңмен, нормативтік құжаттармен немесе сот шешімімен тыйым салынбаған жағдайлардан басқа, жүйенің барлық мәндері үшін ашық болуға тиіс.

Күші жойылған сертификаттардың тізімін тарату үшін түрлі тетіктерді қолданысы мүмкін, бұған кіретін:

– әрбір пайдаланушыға сенімді үшінші тараппен хабарлама түрінде жеткізу;

– пайдаланушының сенімді үшінші тараптан ашық кілттің осы сертификатының ағымдағы мәртебесі жөнінде сұрау;

– КО-ның күштері жойылған сертификаттардың ағымдағы тізімі туралы сұрату.

КО күші жойылған сертификаттардың жаңа тізімін мерзімді басып шығаруға және таратуға тиіс.

Д қосымшасы
(анықтамалық)
Библиография

[1] ИСО 8732: 1988 Банктік іс. Кілттерді басқару (шолу)

[2]ИСО/МЭК 9594-8: 1990 Ақпараттық технологиялар. Ашық жүйелердің өзара қарым-қатынастары. Анықтамалық. 8-Бөлім. Сәйкестендіру құрылымы.

[3]ИСО 11166-1: 1994 Банктік іс. Кілттерді асимметриялық алгоритмдердің көмегімен басқару. 1-Бөлім. Қағидаттар, шаралар мен форматтар.

[4]ИСО 11568-1: 1994 Банктік іс. Кілттерді басқару (бөлшектер). 1-Бөлім. Кілттерді басқаруға кіріспе.

[5]ИСО 11568-2: 1994 Банктік іс. Кілттерді басқару (бөлшектер). 2-Бөлім. Симметриялық шифрлер үшін кілттерді басқару әдістері.

[6]ИСО 11568-3: 1994 Банктік іс. Кілттерді басқару (бөлшектер). 3-Бөлім. Симметриялық шифрлер үшін кілттің өмірлік кезеңі.

[7]ИСО 11568-4: 1994 Банктік іс. Кілттерді басқару (бөлшектер). 4-Бөлім. Ашық кілті бар криптожүйелер үшін кілттерді басқару әдістері.

[8]ИСО 11568-5: 1994 Банктік іс. Кілттерді басқару (бөлшектер). 5-Бөлім. Ашық кілті бар криптожүйелер үшін кілттің өмірлік кезеңі.

[9]ИСО/МЭК 11770-3: Ақпараттық технологиялар. Қауіпсіздік әдістері. Кілттерді басқару. 3-Бөлім. Асимметриялық әдістерді қолданатын тетіктер.

[10]ИСО/МЭК 13888: Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Бас тартпаушылық (барлық бөлімдер).

ӘОЖ 681.324:006.354 **МСЖ 13.040**

Түйінді сөздер: мәліметтерді өндеу, ақпараттық алмасу, қорғау әдістері, кілттерді басқару, криптография.

Ескертулер үшін

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

УПРАВЛЕНИЕ КЛЮЧАМИ

Часть 1
Основные положения

СТ РК ИСО/МЭК 11770-1-2008
(ИСО/МЭК 11770-1:1996 «Информационная технология. Методы и средства обеспечения безопасности. Управление ключами. Часть1. Основные положения», IDT)

Издание официальное

Комитет по техническому регулированию и метрологии Министерства индустрии и торговли Республики Казахстан (Госстандарт)

Астана

Предисловие

1 ПОДГОТОВЛЕН И ВНЕСЕН Агентством Республики Казахстан по информатизации и связи.

2 УТВЕРЖДЕН И ВВЕДЕН В ДЕЙСТВИЕ приказом Комитета по техническому регулированию и метрологии Министерства индустрии и торговли Республики Казахстан № 107-од от 25.02.2008.

3 Настоящий стандарт идентичен международному стандарту ИСО/МЭК 11770-1:1996 «Информационная технология. Методы и средства обеспечения безопасности. Управление ключами. Часть1. Основные положения» («Information technology. Security techniques. Key management. Part 1. Framework»), IDT, с дополнительными требованиями, отражающими потребности экономики Республики Казахстан, которые выделены курсивом.

4 СРОК ПЕРВОЙ ПРОВЕРКИ 2013 год
ПЕРИОДИЧНОСТЬ ПРОВЕРКИ 5 лет

5 ВВЕДЕН ВПЕРВЫЕ

Содержание

Введение

В информационных технологиях существует постоянно увеличивающаяся потребность в использовании криптографических механизмов для защиты данных от несанкционированного раскрытия или изменения, для аутентификации и обеспечения неотказуемости. Безопасность и надежность этих механизмов непосредственно зависит от защиты и управления таким параметром, как ключ. Безопасное управление ключами критично для интеграции криптографических функций в систему, т.к. самая развитая концепция безопасности будет неэффективной при слабой системе управления ключами. Цель управления ключами – обеспечить процедуры для работы с криптографическим ключевым материалом, который используется в симметричных или асимметричных криптографических методах.

Фундаментальной проблемой является создание ключевого материала, чье происхождение, целостность, актуальность и (для секретных ключей) конфиденциальность могут быть гарантированы для прямых и косвенных пользователей. Управление ключами включает в себя функции генерации, хранения, распространения, уничтожения и архивирования ключевого материала в соответствии с политикой безопасности (ГОСТ ИСО 7498-2).

Настоящий стандарт имеет особое отношение к основам безопасности открытых систем *(СТ РК ИСО/МЭК 10181-2008).* Все стандарты, включая этот, определяют базовые концепции и характеристики механизмов, охватывающие различные аспекты безопасности. Настоящий стандарт вводит общие модели управления ключами, которые являются фундаментальными для симметричных и асимметричных криптографических методов.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология
МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ
УПРАВЛЕНИЕ КЛЮЧАМИ
ЧАСТЬ 1
Основные положения

Дата введения 2008.07.01

1 Область применения

Настоящий стандарт:

1 Определяет цели управления ключами.

2 Описывает общую модель, на которой базируются механизмы управления ключами.

3 Определяет базовые концепции управления ключами, общие для всех частей данного стандарта.

4 Определяет сервисы управления ключами.

5 Определяет характеристики методов управления ключами.

6 Задает требования к управлению ключевым материалом в течение его жизненного цикла.

7 Определяет структуру управления ключевым материалом в течение его жизненного цикла.

Настоящий стандарт определяет общую модель управления ключами, которая не зависит от конкретного используемого криптографического алгоритма. Однако некоторые методы распространения ключей могут зависеть от свойств конкретных алгоритмов, например, свойств асимметричных алгоритмов. Выбор и применение конкретных средств криптографической защиты информации регламентируется законодательством Республики Казахстан и не является предметом рассмотрения настоящего стандарта.

Конкретные методы управления ключами рассматриваются в других частях *СТ РК ИСО/МЭК 11770-2008. Симметричные методы* рассматриваются в части 2 (*СТ РК ИСО/МЭК 11770-2-2008, Информационная технология. Методы и средства обеспечения безопасности. Управление ключами. Часть 2. Механизмы, использующие симметричные методы*). Асимметричные методы рассматриваются в части 3 (ИСО/МЭК 11770-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Управление ключами. Часть 3. Механизмы, использующие асимметричные методы).

Настоящий стандарт содержит материал, необходимый для понимания *СТ РК ИСО/МЭК 11770-2-2008* и ИСО/МЭК 11770-3-2008. Примеры использования механизмов управления ключами приводятся в

ИСО 8732 и ИСО 11166. Если для управления ключами требуются функции неотказуемости, следует использовать ИСО/МЭК 13888 (в том числе *СТ РК ИСО/МЭК 13888-2-2008)*. Настоящий стандарт рассматривает аспекты автоматического и ручного управления ключами, включая структуру элементов данных и последовательности операций, которые используются для получения доступа к сервисам управления ключами. Однако данный стандарт не определяет детали протоколов обмена, которые могут потребоваться.

Как и другие сервисы безопасности, управление ключами может быть предоставлено только в контексте определенной политики безопасности. Определение политики безопасности не входит в рассмотрение данного стандарта.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

ГОСТ ИСО 7498-2-2002 Системы обработки информации. Взаимодействие открытых систем. Базовая эталонная модель. Часть 2. Архитектура безопасности.

СТ РК ИСО/МЭК 10116-2006 Информационная технология. Методы и средства обеспечения безопасности. Режимы работы n-битовых блочных шифров.

СТ РК ИСО/МЭК 11770-2-2006 Информационная технология. Методы и средства обеспечения безопасности. Управление ключами. Часть 2. Механизмы, использующие симметричные методы.

СТ РК ИСО/МЭК 9798-1-2008 Информационная технология. Методы и средства обеспечения безопасности. Механизмы аутентификации. Часть 1. Общие положения.

СТ РК ИСО/МЭК 10181-1-2008 Информационная технология. Взаимодействие открытых систем. Основы безопасности для открытых систем: Обзор.

3 Термины и определения

В настоящем стандарте используются следующие термины с соответствующими определениями:

3.1 Асимметричный криптографический метод (asymmetric cryptographic technique) - криптографический метод, который использует два связанных преобразования: открытое преобразование (определяемое открытым ключом) и закрытое преобразование (определяемое секретным ключом). Данная пара преобразований обладает свойством, благодаря которому, используя только открытое преобразование блока данных,

неосуществимо вычислительным путем получить секретное преобразование того же блока данных.

3.2 Закрытый ключ (private key) - тот ключ из асимметричной пары ключей сущности, который должен использоваться только этой сущностью.

Примечание. Закрытый ключ обычно не должен раскрываться.

3.3 Информация об открытом ключе (public key information) - информация, относящаяся к отдельной сущности, которая содержит, по крайней мере, отличительный идентификатор сущности, а также, по крайней мере, один открытый ключ для этой сущности. В информацию об открытом ключе могут быть включены дополнительные сведения об удостоверяющем центре, сущности и открытом ключе, такие, как срок действия открытого ключа, срок действия соответствующего секретного ключа или идентификатор используемых криптографических алгоритмов.

3.4 Ключ (key) - последовательность символов, которая управляет операцией криптографического преобразования (например, шифрованием, расшифрованием, вычислением контрольных криптографических функций, генерацией подписи или верификацией подписи).

3.5 Ключевой материал (keying material) - данные (например, ключи, начальные значения), необходимые для установления и поддержания криптографических отношений.

3.6 Контроль над ключом (key control) - возможность выбрать ключ или параметры, используемые при вычислении ключа.

3.7 Метка времени (time stamp) - зависящий от времени параметр, который обозначает момент времени в общем отсчете времени.

3.8 Открытый ключ (public key) - тот ключ из асимметричной пары ключей сущности, который может быть сделан общедоступным.

3.9 Параметр, зависящий от времени (time variant parameter) - элемент данных, такой как случайное число, последовательное число или метка времени, который используется сущностью для верификации того, что сообщение не было повторено.

3.10 Подтверждение ключа (key confirmation) - гарантия для одной из сущностей, что другая сущность обладает правильным ключом.

3.11 Последовательное число (sequence number) - зависящий от времени параметр, значение которого выбирается из заданной последовательности, которая не повторяется в пределах определенного периода времени.

3.12 Расшифрование (decipherment) -обратный процесс соответствующего шифрования.

3.13 Секретный ключ (secret key) - ключ, применяемый в симметричных криптографических методах, который может использоваться только определенным множеством сущностей.

3.14 Сертификат открытого ключа (public key sertificate) - информация открытого ключа сущности, подписанная удостоверяющим центром, вследствие чего рассматривается как неподдельная. Эквивалентным этому термину является термин «регистрационное свидетельство», применяемый в законодательстве Республики Казахстан.

3.15 Симметричный криптографический метод (symmetric cryptographic technique) - криптографический метод, который использует один и тот же секретный ключ как для преобразования со стороны отправителя, так и для преобразования со стороны получателя сообщения. Без знания секретного ключа невозможно раскрыть преобразование со стороны отправителя или получателя сообщения.

3.16 Случайное число (random number) - зависящий от времени параметр, значение которого непредсказуемо.

3.17 Согласование ключа (key agreement)- процесс создания общего секретного ключа двумя сущностями таким образом, что ни одна из них не может заранее предсказать значение данного ключа.

3.18 Удостоверяющий центр; **УЦ** (certification authority; CA) - орган, уполномоченный создавать и распространять сертификаты открытых ключей. Кроме того, УЦ может создавать и распространять ключи сущностям.

3.19 Управление ключами (key management) - администрирование и использование процессов генерации, регистрации, сертификации, отмены регистрации, распространения, установки, хранения, архивирования, аннулирования, создания производного и уничтожения ключевого материала в соответствии с политикой безопасности.

3.20 Центр распространения ключей (ЦРК) (key distribution center (KDC)) - сущность, уполномоченная создавать или запрашивать и распространять ключи между сущностями, каждая из которых имеет общий ключ с ЦРК.

3.21 Центр трансляции ключей (ЦТК) (key translation center(KTC)) - сущность, уполномоченная транслировать ключи между сущностями, каждая из которых имеет общий ключ с ЦТК.

3.22 Шифрование (encipherment) - (обратимое) преобразование данных криптографическим алгоритмом для получения зашифрованного текста, т.е. для сокрытия информационного содержания данных.

В настоящем стандарте применяются следующие термины по ГОСТ *ИСО 7498-2:*

- **Аутентификация источника данных** (data origin authentication);
- **Целостность данных** (data integrity);
- **Цифровая подпись** (digital signature).

В настоящем стандарте применяется следующий термин по *СТ РК ИСО 9798-1*:

– **Аутентификация сущности** (entity authentication).

В настоящем стандарте применяются следующие термины по *СТ РК ИСО 10181-1*:

– **Доверенная третья сторона** (ДТС) (trusted third party; TTP);
– **Домен безопасности** (security domain);
– **Уполномоченный по безопасности** (security authority).

4 Общие вопросы управления ключами

Управление ключами – это администрирование и использование сервисов генерации, регистрации, сертификации, отмены регистрации, распространения, установки, хранения, архивирования, аннулирования, порождения производного и уничтожения ключевого материала.

Цель управления ключами – обеспечение безопасности администрирования и использования сервисов управления ключами и, следовательно, защита ключей чрезвычайно важна.

Процедуры управления ключами зависят от используемых криптографических методов, предполагаемого использования ключа и текущей политики безопасности. Управление ключами также включает функции, которые выполняются в криптографическом оборудовании.

4.1 Защита ключей

Ключи являются критичной частью любой системы безопасности, которая полагается на криптографические методы. Необходимая защита ключей зависит от ряда факторов, таких как тип приложения, в котором используются ключи, угрозы, с которыми они сталкиваются, различные состояния, в которых могут находиться ключи и т.д. Прежде всего, в зависимости от криптографического метода, ключи должны быть защищены от раскрытия, изменения, уничтожения и воспроизведения. Примеры возможных угроз ключам даны в приложении А. Действительность ключа должна быть ограничена по времени и по количеству его использования. Эти ограничения определяются временем и объемом данных, необходимых для проведения атаки раскрытия ключа, и ценностью защищаемой информации. Ключи, которые используются для генерации других ключей, нуждаются в большей защите, чем генерируемые ключи. Другим важным аспектом защиты ключей является пресечение их неправильного использования, например, использования для шифрования данных ключа, предназначенного для шифрования ключей.

4.1.1 Защита криптографическими методами

Использование криптографических методов позволяет противостоять некоторым угрозам ключевому материалу. Например, шифрование

защищает ключ от раскрытия и несанкционированного использования; методы обеспечения целостности данных защищают от модификации; методы аутентификации источника данных, цифровые подписи и методы аутентификации сущностей противостоят подменам.

Разделение применения криптографических методов защищает от их неправильного использования. Такое разделение функционального использования может быть достигнуто путем связывания с ключом некоторой информации. Например, привязка управляющей информации к ключу гарантирует, что определенный ключ используется только для определенных задач (например, для шифрования ключей или обеспечения целостности данных); контроль над ключом требуется для обеспечения неотказуемости от авторства, если используются симметричные методы.

4.1.2 Зашита некриптографическими методами

Метки времени могут использоваться для ограничения использования ключей в течение определенного периода времени их действия. Вместе с последовательными числами они также защищают от воспроизведения информации в процессе согласования ключа.

4.1.3 Защита на физическом уровне

Каждое криптографическое устройство в системе безопасности обычно требует защиты ключевого материала, который оно использует, от модификации, удаления и, кроме открытых ключей, раскрытия. Устройство, как правило, имеет защищенную область для хранения и использования ключей и для реализации криптографических алгоритмов. Оно может предоставлять средства для:

– загрузки ключевого материала из отдельного устройства хранения ключей;

– взаимодействия с криптографическими алгоритмами, реализованными в отдельных «интеллектуальных» устройствах (например, смарт-картах, картах памяти);

– хранения ключевого материала на внешних носителях (например, на дискете).

Обычно, защищенная область создается с помощью применения механизмов физической защиты.

4.1.4 Защита организационными методами

Одним из средств защиты ключей является организация их иерархической структуры. Кроме низшего уровня иерархии, ключи на одном уровне иерархии используются исключительно для защиты ключей, находящихся на уровень ниже. Только ключи на самом нижнем уровне иерархии используются непосредственно в сервисах безопасности. Такой подход позволяет ограничивать использование каждого ключа, ограничивая

его проявления и затрудняя осуществление атак. Например, компрометация одного сессионного ключа компрометирует только информацию, защищенную этим ключом.

Использование защищенных областей направлено на противодействие угрозам раскрытия, изменения и удаления ключа неуполномоченными сущностями. Однако существует угроза того, что системные администраторы, уполномоченные выполнять определенные функции управления компонентами сервисами управления ключами, могут неправильно распорядиться своими особыми привилегиями доступа. В частности, они могут попытаться получить главный ключ (ключ верхнего уровня в иерархии ключей). Раскрытие главного ключа может позволить его обладателю получить или изменить все остальные ключи, защищаемые главным ключом (т.е. все остальные ключи в данной иерархии ключей). Следовательно, желательно минимизировать доступ к этому ключу, может быть, установив, что никакой пользователь не может в одиночку получить к нему доступ. Это можно реализовать путем разделения главного ключа (двухстороннее управление или даже n-стороннее управление ключом) или использование специальных криптографических схем (Схем совместного использования секретной информации).

4.2 Общая модель жизненного цикла ключа

Криптографический ключ проходит через серию состояний, которые определяют его жизненный цикл. Тремя основными состояниями являются:

– **Предактивное.** В этом состоянии ключ был сгенерирован, но не был активирован для использования.

– **Активное.** В активном состоянии ключ используется для криптографической обработки информации.

– **Постактивное.** В этом состоянии ключ может использоваться только для расшифрования или верификации.

Примечание. Пользователь ключа, находящегося в постактивном состоянии, должен быть уверен, что данные были криптографически обработаны до того, как ключ перешел в постактивное состояние. Это, как правило, обеспечивается с помощью доверенного временного параметра.

Ключ, про который известно, что он скомпрометирован, должен немедленно перейти в постактивное состояние, и может потребовать особого отношения. Ключ является скомпрометированным, если известно или подозревается его несанкционированное использование.

На рисунке 1 показаны описанные состояния и соответствующие переходы.

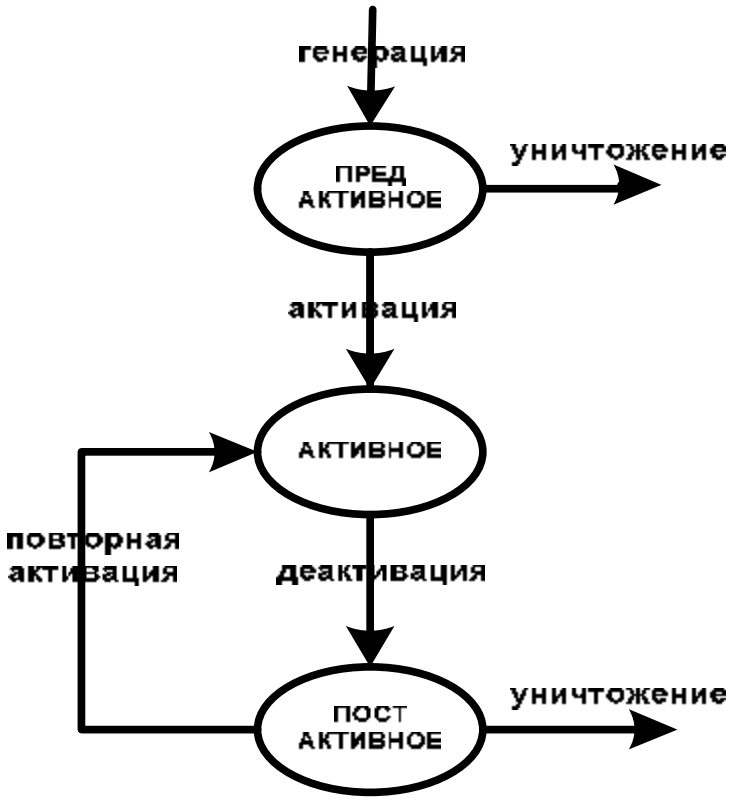


Рисунок 1. Жизненный цикл ключа

Рисунок 1 представляет общую модель жизненного цикла ключа. Другие модели жизненного цикла могут иметь дополнительные детали в виде подсостояний трех представленных состояний. Большинство жизненных циклов ключей требует действий по архивации. Эти действия могут быть связаны с любым состоянием, в зависимости от конкретных деталей жизненного цикла.

4.2.1 Переходы между состояниями ключа

По мере того, как ключ продвигается из одного состояния в другое, он осуществляет один из переходов, изображенных на рисунке 1:

– **Генерация –** процесс создания ключа. Генерация ключа должна проводиться в соответствии с предписанными правилами генерации ключей. Этот процесс может включать проверку того, что все правила были соблюдены.

– **Активация** делает ключ доступным для криптографических процедур.

– **Деактивация** ограничивает использование ключа. Это может происходить из-за того, что завершился срок действия ключа, или ключ был аннулирован.

– **Повторная активация** позволяет использовать постактивный ключ в криптографических операциях.

– **Уничтожение** завершает жизненный цикл ключа. Это означает логическое уничтожение ключа, но может включать и его физическое уничтожение.

Переходы могут быть вызваны такими событиями, как потребность в новом ключе, компрометация, окончание срока действия и завершение жизненного цикла ключа. Все эти переходы используют ряд сервисов управления ключами. Связи между переходами и сервисами показаны в таблице 1. Эти сервисы описаны в разделе 5.

Каждый конкретный криптографический метод требует только некоторого подмножества сервисов, указанных в таблице 1.

4.2.2 Переходы, сервисы и ключи

Ключи в конкретном криптографическом методе во время своего жизненного цикла используют различные комбинации сервисов. Два примера приведены ниже.

В симметричных криптографических методах переход из предактивного в активное состояние после генерации ключа приводит к установке ключа и может привести к регистрации и распространению ключа. В некоторых случаях установка ключа может включать в себя создание ключей, производных от данного. Время жизни ключа должно быть ограничено фиксированным периодом. Деактивация завершает активное состояние, как правило, после окончания срока действия ключа. Если известно или подозревается, что ключ скомпрометирован в активном состоянии, его аннулирование также вызывает его переход в постактивное состояние. Постактивный ключ можно архивировать. Если архивированный ключ потребуется снова, он может быть повторно активирован, что может потребовать его повторную установку и распространение перед полной активацией. В противном случае, после деактивации ключа, его регистрация может быть отменена, и ключ может быть уничтожен.

В асимметричных криптографических методах генерируется пара ключей (закрытый и открытый), и оба ключа переходят в предактивное состояние. Следует отметить, что жизненные циклы двух ключей связаны, но не одинаковы. Перед тем, как закрытый ключ переходит в активное состояние, он может быть в необязательном порядке зарегистрирован и, также в необязательном порядке доставлен его пользователю, но всегда должен быть установлен. Переход между активным и постактивным состояниями для закрытого ключа, включая деактивацию, повторную активацию и уничтожение, близок тому, который описан выше для симметричных ключей. Когда открытый ключ сертифицируется, обычно сертификат, содержащий открытый ключ, создается УЦ, чтобы подтвердить

действительность и принадлежность открытого ключа. Этот сертификат открытого ключа может быть помещен в каталог или подобную службу для распространения, или он может быть возвращен владельцу для распространения. Когда владелец ключа отсылает информацию, подписанную его закрытым ключом, он может добавить свой сертификат. Пара ключей становится активной, когда открытый ключ становится сертифицированным. Когда пара ключей используется для цифровой подписи, открытый ключ может оставаться в активном или постактивном состоянии неопределенное количество времени, после того как соответствующий закрытый ключ был деактивирован или уничтожен. Доступ к открытому ключу может быть необходим для верификации цифровой подписи, сделанной до истечения срока действия соответствующего закрытого ключа. Когда производится шифрование асимметричными методами, и ключ, используемый для шифрования, был деактивирован или уничтожен, соответствующий ключ из пары может оставаться в активном или постактивном состоянии для использования при расшифровании.

Использование ключа может определить сервисы, необходимые для этого ключа. Например, система может решить не регистрировать сессионные ключи, т.к. процесс регистрации может длиться дольше, чем время жизни ключа. Напротив, совершенно необходимо регистрировать секретный ключ, когда симметричные методы используются для цифровой подписи.

Таблица 1. Переходы и сервисы

Переход	Сервис	Замечания
Генерация	Генерировать-ключ	обязательный
	Регистрировать-ключ	необязательный или здесь, или при Активации
	Создать-сертификат-ключа	необязательный
	Распространить-ключ	необязательный
	Хранить-ключ	необязательный
Активация	Создать-сертификат-ключа	необязательный
	Распространить-ключ	необязательный
	Создать-производные-ключи	необязательный
	Установить-ключ	обязательный
	Хранить-ключ	необязательный
	Регистрировать-ключ	необязательный или здесь, или при Генерации
Деактивация	Хранить-ключ	Необязательный

	Архивировать-ключ	необязательный или здесь, или при Уничтожении
	Аннулировать-ключ	необязательный
Повторная активация	Создать-сертификат-ключа	необязательный
	Распространить-ключ	необязательный
	Создать-производные-ключи	необязательный
	Установить-ключ	обязательный
	Хранить-ключ	необязательный
Уничтожение	Отменить-регистрацию-ключа	обязательный, если ключ зарегистрирован
	Уничтожить-ключ	обязательный
	Архивировать-ключ	необязательный или здесь, или при Деактивации

5 Концепции управления ключами

5.1 Сервисы управления ключами

Этот раздел описывает общую структуру управления ключами и помогает понять сервисы управления ключами, их взаимодействие друг с другом и как они поддерживаются.

Управление ключами основывается на базовых сервисах генерации, регистрации, сертификации, распространения, установки, хранения, создания производных ключей, архивирования, аннулирования, отмены регистрации и уничтожения. Эти сервисы могут быть частью системы управления ключами или обеспечиваться другими поставщиками услуг. В зависимости от типа сервиса поставщик услуг должен выполнять определенный минимум требований обеспечения безопасности (например, защищенный обмен), чтобы ему доверяли все участвующие стороны. В частности, поставщик услуг может быть доверенной третьей стороной. На рисунке 2 показано, что сервисы управления ключами находятся на одном уровне и могут использоваться различными пользователями (людьми и процессами). Эти пользователи могут обращаться к функциям управления ключами из различных приложений, используя сервисы, соответствующие их потребностям. Список сервисов управления ключами приведен в таблице 1.

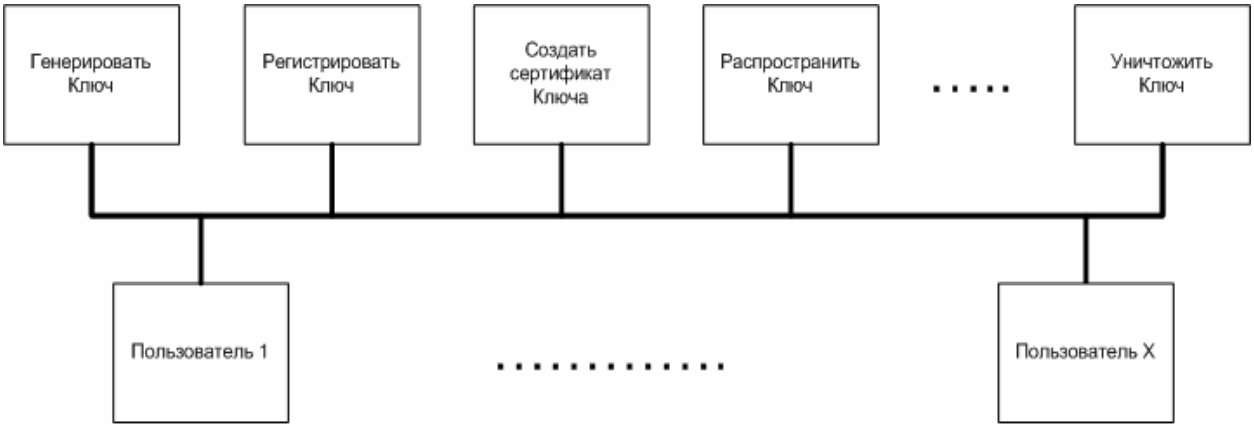


Рисунок 2. Сервис управления ключами

5.1.1 Генерировать-ключ

Генерироватъ-ключ – это сервис, который используется для генерации ключа безопасным образом для конкретного криптографического алгоритма. Это подразумевает, что генерацией ключей невозможно манипулировать, и ключи создаются случайным образом и в соответствии с предписанным законом распределения. Этот закон распределения определяется криптографическим алгоритмом, для которого он будет использован, а также требуемым уровнем криптографической защиты. Генерация некоторых ключей, например, главных ключей, требует особого внимания, т.к. знание этих ключей дает доступ ко всем связанным и порожденным ключам.

5.1.2 Регистрировать-ключ

Сервис *Регистрировать-ключ* связывает ключ с сущностью. Этот сервис предоставляется органом по регистрации и обычно применяется, если используются симметричные криптографические методы. Когда сущность хочет зарегистрировать ключ, она должна связаться с органом регистрации. Регистрация ключа включает в себя запрос на регистрацию и подтверждение регистрации.

Орган регистрации поддерживает реестр ключей и связанной с ними информации соответствующим защищенным образом. Приложение В содержит детальную информацию по управлению ключами.

Орган регистрации предоставляет операции регистрации и отмены регистрации.

5.1.3 Создать-сертификат-ключа

Сервис *Создать-сертификат-ключа* заверяет связь открытого ключа с сущностью и предоставляется удостоверяющим центром. Если запрос на сертификацию принимается, то удостоверяющий центр создает сертификат ключа. Сертификаты открытых ключей более подробно обсуждаются в ИСО/МЭК 11770-3-2008.

5.1.4 Распространить-ключ

Распространение ключа – это набор процедур для предоставления защищенным образом информационных объектов управления ключами (см. пример в Приложении В) авторизованным сущностям. Особым случаем распространения ключей является трансляция ключей, когда обмен ключевым материалом между сущностями происходит с использованием центра трансляции ключей (см. 6.2). *СТ РК ИСО/МЭК 11770-2-2008* предлагает различные механизмы согласования ключей между сущностями. ИСО/МЭК 11770-3-2008 включает механизмы для согласования секретных ключей и методы транспортировки секретных и открытых ключей.

5.1.5 Установить-ключ

Сервис *Установить-ключ* всегда необходим перед использованием ключа. Установка ключа означает помещение ключа в систему управления ключами таким образом, чтобы исключить его компрометацию.

5.1.6 Хранить-ключ

Сервис *Хранить-ключ* обеспечивает безопасное хранение ключей, предназначенных для текущего использования и в ближайшем будущем, а также для резервного хранения. Обычно имеет смысл обеспечить физически независимое хранилище ключей, что обеспечивает конфиденциальность и целостность ключевого материала, а также целостность открытых ключей. Хранение может потребоваться во всех состояниях (т.е. Предактивном, Активном и Постактивном) жизненного цикла ключа. В зависимости от важности ключей они могут быть защищены с помощью одного из следующих методов:

– физическая защита (например, хранение их в устройствах, защищенных от несанкционированного использования или на внешних носителях, таких как дискеты или карты памяти);

– шифрование ключами, которые в свою очередь защищены физическими методами;

– защита доступа к ключам с помощью пароля или персонального кода.

Для всех ключевых материалов должна быть обнаруживаемой любая попытка их компрометации.

5.1.7 Создать-производный-ключ

Сервис *Создать-производный-ключ* предоставляет возможность порождения большого количества ключей, используя секретный ключ, называемый исходным ключом, несекретные переменные данные и некоторый процесс преобразования (который также может быть не секретным). Результатом этого процесса является производный ключ.

Исходный ключ требует особой защиты. Процесс создания производного ключа должен быть необратимым и его результат непредсказуемым, чтобы компрометация порожденного ключа не раскрыла исходный ключ или другие порожденные ключи.

5.1.8 Архивировать-ключ

Сервис *Архивировать-ключ* обеспечивает процесс безопасного долговременного хранения ключей после окончания их нормального использования. Для этого может использоваться сервис хранения ключей с возможными изменениями для реализации автономного хранения. Архивированные ключи могут потребоваться в более позднее время, чтобы подтвердить или опровергнуть определенные утверждения, после того как прекратилось нормальное использование ключа.

5.1.9 Аннулировать-ключ

Когда известна или подозревается компрометация ключа, сервис *Аннулировать-ключ* обеспечивает безопасную деактивацию ключа. Этот сервис необходим для ключей, у которых достигнут срок окончания их действия. Аннулирование ключа происходит и при изменении обстоятельств у его владельца. После того, как ключ аннулирован, он может использоваться только для расшифрования и верификации. Сервис Аннулировать-ключ не пригоден для схем с сертификацией, где время жизни ключа определяется окончанием срока действия его сертификата.

Примечание. Некоторые приложения используют название Удалить-ключ для этого сервиса.

5.1.10 Отменить-регистрацию-ключа

Сервис *Отменить-регистрацию-ключа* предоставляется органом по регистрации ключей и обеспечивает удаление связи ключа с сущностью. Это является частью процесса уничтожения ключа (см. 5.1.11). Когда сущность хочет отменить регистрацию ключа, она обращается к органу по регистрации.

5.1.11 Уничтожить ключ

Сервис *Уничтожитъ-ключ* обеспечивает безопасное уничтожение ненужных ключей. Уничтожение ключа означает удаление всех записей соответствующего информационного объекта управления ключами, таким образом, чтобы любая информация, оставшаяся после удаления, не могла привести к восстановлению уничтоженного ключа любыми средствами. Уничтожение ключа должно включать уничтожение всех его архивных копий. Однако перед уничтожением архивированных ключей нужно убедиться, что никакой материал, защищенный этими ключами, не потребуется впоследствии.

Примечание. Некоторые ключи могут храниться вне электронного устройства или системы. Уничтожение таких ключей требует дополнительных административных мер.

5.2 Вспомогательные сервисы

Для управления ключами могут потребоваться вспомогательные сервисы.

5.2.1 Сервисы обеспечения управления ключами

Сервисы управления ключами могут пользоваться другими сервисами, связанными с безопасностью. Эти сервисы включают:

– **Управление доступом.** Этот сервис может использоваться для гарантии того, что ресурсы системы управления ключами используют только авторизованные сущности и только предписанным образом.

– **Аудит.** Отслеживание действий, важных с точки зрения безопасности, которые происходят в системе управления ключами. Записи аудита могут помочь идентифицировать риски и бреши в обеспечении информационной безопасности.

– **Аутентификация.** Этот сервис может быть использован для подтверждения принадлежности сущности к авторизованным элементам домена безопасности.

– **Криптографические сервисы.** Эти сервисы должны использоваться сервисами управления ключами для обеспечения целостности, конфиденциальности, подлинности и неотказуемости.

– **Служба времени.** Эта служба необходима для генерации временных параметров, таких как сроки действия.

5.2.2 Сервисы, ориентированные на пользователя

Криптографические системы и устройства могут потребовать других сервисов, которые необходимы для нормального функционирования, например, сервиса регистрации пользователей. Эти сервисы зависят от реализации и не рассматриваются в настоящем стандарте.

6 Концептуальные модели распространения ключей

Распространение ключей между сущностями может быть достаточно сложной процедурой. Это определяется природой средств связи, отношениями доверия сторон и используемыми криптографическими методами. Сущности могут общаться непосредственно или косвенно, могут принадлежать к одному или к разным доменам безопасности, могут использовать или не использовать сервисы уполномоченных органов. Следующие концептуальные модели иллюстрируют, как эти различные случаи влияют на распространение ключей и информации.

6.1 Распространение ключей между сообщающимися сущностями

На возможности коммуникации сущностей влияет канал связи между ними, доверие между сущностями и используемые криптографические методы.

Существует соединение между сущностями А и В, которые хотят обменяться информацией, используя криптографические методы. Это коммуникационное соединение показано на рисунке 3. В общем случае распространение ключей должно происходить по безопасным каналам, которые логически отличаются от транспортных каналов.

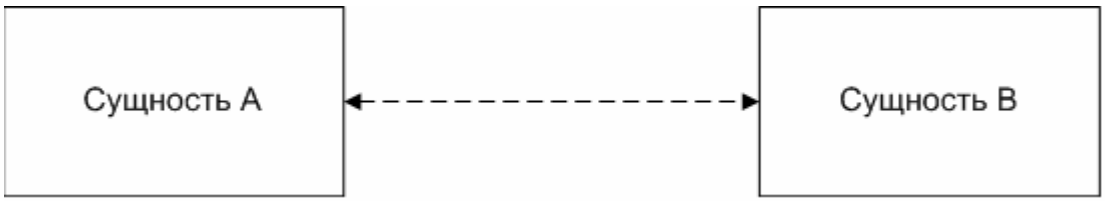


Рисунок 3. Канал связи между двумя сущностями

Прямое соединение между сущностями используется в случаях согласования ключа, контроля над ключом и подтверждения ключа. Подробнее эти случаи рассмотрены в Части 2 (*СТ РК ИСО/МЭК 11770-2-2008, Информационная технология. Методы и средства обеспечения безопасности. Управление ключами. Часть 2. Механизмы, использующие симметричные методы)* и Части 3 (ИСО/МЭК 11770-3, *Информационные технологии. Методы безопасности. Управление ключами. Часть 3. Механизмы, использующие асимметричные методы*) стандарта ИСО/МЭК 11770-2008.

6.2 Распространение ключей внутри одного домена безопасности

Следующая модель основана на концепции домена безопасности с уполномоченным по безопасности в соответствии с *СТ РК ИСО/МЭК 10181-1-2008*. Уполномоченный по безопасности может предоставлять сервисы управления ключами, например, трансляцию ключей. Когда сущности используют асимметричный метод для безопасного обмена информацией, можно выделить следующие случаи:

– для проверки целостности данных или аутентификации их источника получатель требует соответствующий сертификат открытого ключа отправителя;

– для соблюдения конфиденциальности отправитель требует действующий сертификат открытого ключа получателя;

– для аутентификации, обеспечения конфиденциальности и целостности каждый партнер требует сертификат открытого ключа другого. Это обеспечивает средства для взаимного обеспечения неотказуемости.

Каждая сущность может обратиться к своему уполномоченному по безопасности для получения необходимого сертификата открытого ключа. Если партнеры доверяют друг другу и могут взаимно удостоверить свои сертификаты открытых ключей, то обращение к уполномоченному по безопасности не требуется.

Примечание. Существуют криптографические приложения, которые не используют уполномоченного по безопасности. В этих ситуациях партнеры могут безопасно обмениваться только определенной открытой информацией, а не сертификатами открытых ключей.

Если два таких партнера используют симметричную криптографию, то генерация ключа инициируется одним из двух способов:

1. Одна из сущностей генерирует ключ и отсылает его в Центр Трансляции Ключей (ЦТК).

2. Одна из сущностей просит Центр Распространения Ключей сгенерировать ключ для последующего распространения.

Если генерация ключа осуществлена одной из сущностей, безопасное распространение этого ключа может быть проведено Центром Трансляции Ключей, как показано на рисунке 4. Числа представляют этапы обмена. ЦТК получает зашифрованный ключ от сущности А (1), расшифровывает его и зашифровывает с помощью ключа, который он разделяет с сущностью В. Затем он может:

- переслать зашифрованный ключ сущности В (2);
- отослать его назад сущности А (3), которая перешлет его сущности В (4).

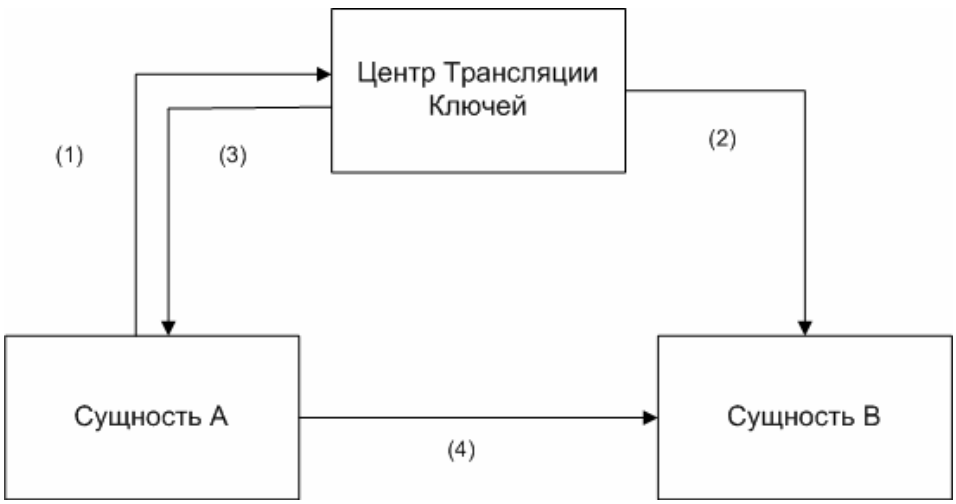


Рисунок 4. Центр Трансляции Ключей

Если генерация ключа осуществляется доверенной третьей стороной, существует два пути последующего распространения ключа общающимся партнерам. Эти случаи показаны на рисунке 5 «Концептуальная модель

Центра распространения ключей» и рисунок 6 «Распространение ключа пересылкой от сущности А сущности В».

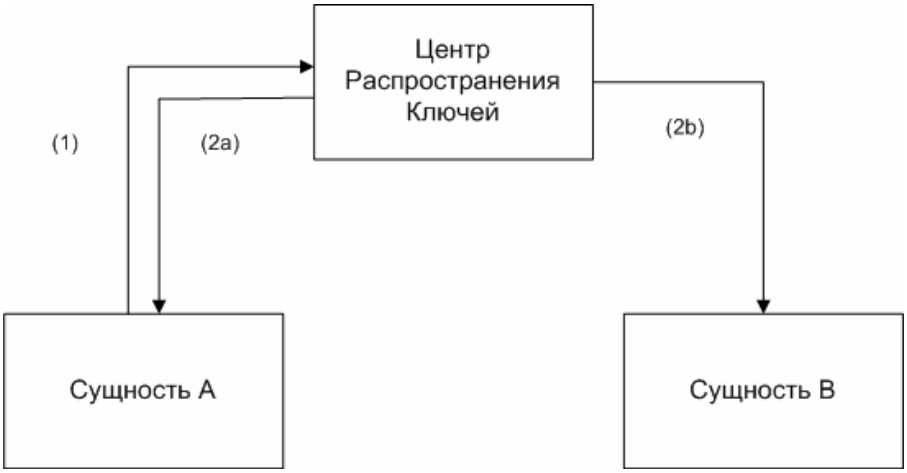


Рисунок 5. Концептуальная модель Центра распространения ключей

Рисунок 5 иллюстрирует случай, в котором Центр Распространения Ключей может безопасно общаться с обеими сущностями. В этом случае, после того как ключ сгенерирован по запросу одной из сущностей, Центр распространения ключей отвечает за безопасное распространение ключа между обеими сущностями. Запрос общего ключа обозначен (1), а распространение ключа между общающимися партнерами обозначен (2a) и (2b).

Когда только сущность А запрашивает секретный ключ, разделяемый сущностями А и В, центр может действовать двумя различными способами. Если он имеет возможность безопасно общаться с обеими сущностями, он может распространить секретный ключ между ними, как показано выше. Если центр может общаться только с сущностью А, сущность А отвечает за передачу ключа сущности В. На рисунке 6 показан этот тип распространения ключа. Запрос общего ключа обозначен (1), передача его сущности А обозначена (2). Пересылка ключа от А к В обозначена (3).

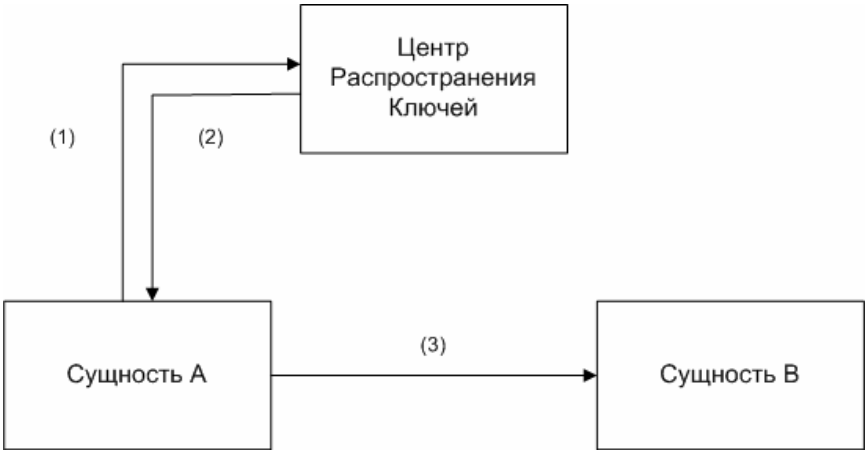


Рисунок 6. Распространение ключа пересылкой его
от сущности А сущности В

6.3 Распространение ключей между доменами

В этой модели используются две сущности А и В, принадлежащие двум различным доменам безопасности, которые используют хотя бы один общий криптографический метод (т.е. симметричный или асимметричный). Каждый домен безопасности имеет своего уполномоченного по безопасности: в одном, - которому доверяет сущность А, и в другом, - которому доверяет сущность В. Если А и В доверяют друг другу, или каждый из них доверяет уполномоченному другого домена, то ключи распространяются в соответствии с 6.1 или 6.2.

При получении ключа сущностями А и В могут быть рассмотрены два случая:

– получение сертификата открытого ключа В (когда это возможно);

– создание общего секретного ключа сущностями А и В.

Различные отношения возможны между этими компонентами. Эти отношения отражают природу доверия между компонентами.

Когда сущности используют асимметричные методы для обмена информацией и не имеют доступа к общей службе каталогов, которая предоставляет сертификаты открытых ключей, каждый из них должен обратиться к своему уполномоченному по безопасности для получения сертификата открытого ключа партнера (см. рисунок 7 (1)). Уполномоченные по безопасности доменов А и В обмениваются сертификатами открытых ключей сущностей А и В (2) и переправляют их сущностям А и В (3). Затем А и В могут общаться непосредственно и безопасно (4).

Другой подход для обмена сертификатами открытых ключей - перекрестная сертификация (см. Приложение Г).

Когда сущности общаются с использованием симметричных методов, каждая сущность также должна обратиться безопасным способом к соответствующему уполномоченному (1), чтобы получить секретный ключ, который позволит им общаться. Уполномоченные договариваются об общем секретном ключе (2), который будут использовать сущности. Один уполномоченный распространяет секретный ключ между обеими сущностями, используя другого уполномоченного в качестве центра распространения. Последний может также обеспечивать трансляцию ключей ((2) и (3)).

Когда только сущность А запрашивает секретный ключ для связи с сущностью В, уполномоченный может действовать двумя способами. Если он имеет возможность общаться с обеими сущностями, он может распространить секретный ключ между обеими сущностями, как описано выше. Если уполномоченный может общаться только с одной сущностью, сущность, получающая ключ, отвечает за пересылку ключа другой сущности.

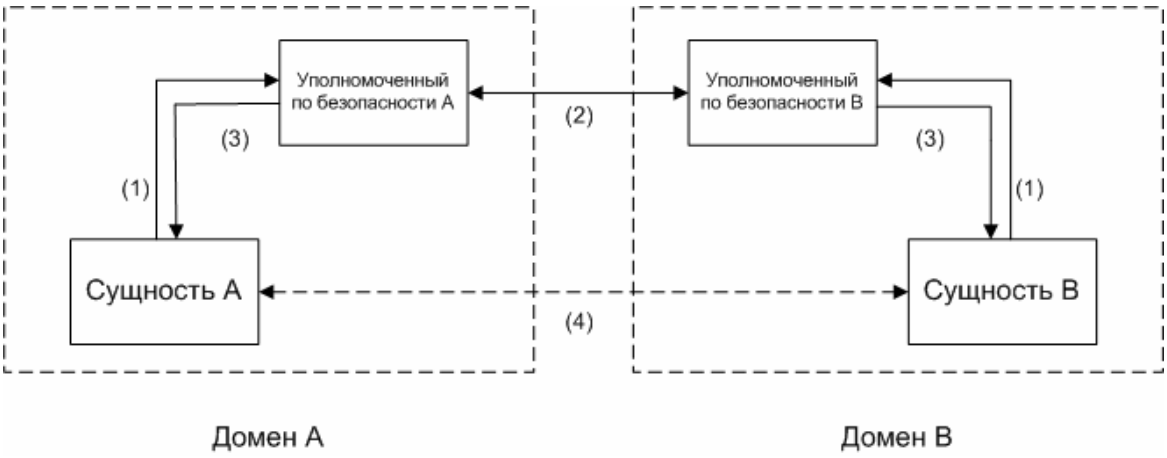


Рисунок 7. Распространение ключа между двумя доменами

Иногда уполномоченные А и В не имеют ни взаимных доверительных отношений, ни прямой линии связи. В этом случае они используют уполномоченного по безопасности Х, которому они оба доверяют, как показано на рисунке 8 (стрелки (2a) и (2b)). Уполномоченный Х может сгенерировать ключ и распространить его между уполномоченными А и В (стрелки (3a) и (3b) на рисунке 8). Уполномоченный Х может также переправить полученный секретный ключ или сертификат открытого ключа (например, (2a)) от уполномоченного А уполномоченному В (3b). Уполномоченные затем должны переправить полученный ключ соответствующим сущностям ((4a) и (4b) на рисунке 8), которые затем смогут безопасно обмениваться информацией. Может потребоваться поиск дополнительных уполномоченных, пока не будет получена цепочка доверия.

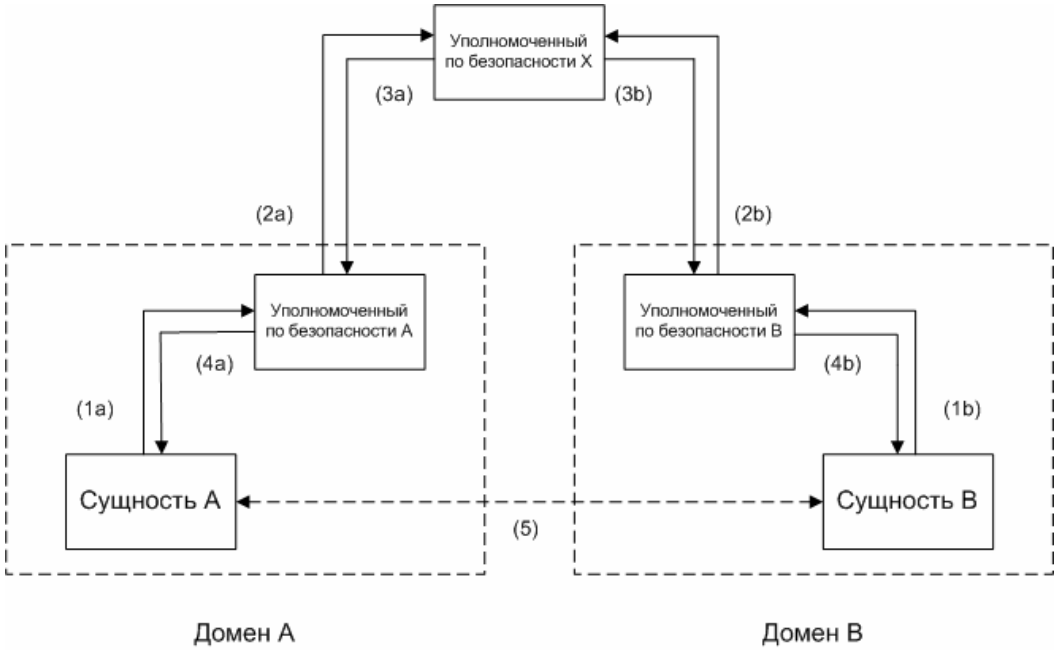


Рисунок 8. Цепочка доверия между уполномоченными по безопасности

7 Специальные поставщики услуг

Некоторые сервисы, требуемые в системе управления ключами, могут быть предоставлены внешними поставщиками услуг. Возможными поставщиками сервисов являются:

- уполномоченный орган регистрации или удостоверяющий центр;
- центр распространения ключей, как определено в ИСО/МЭК 8732;
- центр трансляции ключей, как определено в ИСО/МЭК 8732.

Приложение А
(справочное)
Угрозы управлению ключами

Управление ключами подвержено ряду угроз, которые включают следующее.

Раскрытие ключевого материала: либо ключевой материал хранится в незашифрованном виде, не защищен и к нему может быть получен доступ, либо зашифрован и может быть расшифрован.

Модификация ключевого материала: изменение ключевого материала таким образом, что он не работает так, как ему предназначено.

Несанкционированное удаление ключевого материала: удаление ключа или связанных с ним данных.

Неполное уничтожение ключевого материала: это может привести к компрометации текущего или будущих ключей.

Несанкционированное аннулирование: прямое или косвенное удаление действующего ключа или ключевого материала.

Подмена: выступление в роли авторизованного пользователя или сущности.

Задержка в выполнении функций управления ключами: может выразиться в невозможности генерации, распространении, аннулировании или регистрации ключа, невозможности вовремя обновить хранилище ключей, невозможности поддерживать уровень полномочий пользователя и т.д. Угроза задержки может возникать из-за указанных выше угроз или из-за физического отказа соответствующего оборудования.

Неправильное использование ключей:

– использование ключа в целях, для которых он не предназначен, например, использование для шифрования данных ключа, предназначенного для шифрования ключей;

– использование средств управления ключами в недопустимых целях, например, несанкционированное шифрование или расшифровывание данных;

– использование ключа, у которого истек срок действия;

– чрезмерное использование ключа;

– предоставление ключей неавторизованным получателям.

Приложение Б
(справочное)
Информационные объекты управления ключами

Информационный объект управления ключами состоит из ключа или ключей и, возможно, другой информации, которая определяет, каким образом можно использовать ключ(и). Управляющая информация может быть задана не только явно, но и вытекать из соглашений, регулирующих использование информационных объектов управления ключами. Например, использование одного ключа из асимметричной пары регулируется согласованным использованием другого: один – для шифрования, другой – для расшифрования.

Управляющая информация может контролировать следующее:

– тип объекта, который может быть защищен данным ключом (например, данные или информационный объект управления ключами);

– допустимые операции (например, шифрование, расшифрование);

– допустимые пользователи;

– среда, в которой ключ может быть использован;

– другие аспекты, специфические для конкретного метода управления или приложения, которое использует информационный объект управления ключами.

В целях оптимизации информационный объект управления ключами может частично или целиком создаваться в процессе генерации ключа.

Конкретным примером информационного объекта управления ключами является сертификат ключа. Он содержит, как минимум, следующие данные, подписанные удостоверяющим центром:

– ключевой материал;

– идентификатор пользователя, который может использовать соответствующий информационный объект управления ключами;

– операции, которые выполняет соответствующий информационный объект управления ключами (могут быть заданы неявно);

– период действия ключа;

– идентификатор удостоверяющего центра.

Следующее определение в формате ASN.1 является примером информационного объекта управления ключами, однако информационный объект управления ключами может содержать и другие параметры, зависящие от реализации:

```
Key ::=            PROTECTED {KeyContents protectionType};
KeyContents::=     SEQUENCE {
                     keyID          [0] Key_Identity,
                     keyValue       [1] Key_Value,
                     checkValue     [2] Check_Value,
                     cryptoMethod   [3] Cryptographic_Method,
                     timeStamp      [4] Time_Stamp,
                     generAuthority [5] Generating_Authority,
                     certiAuthority [6] Certification_Authority,
```

```
issuer          [7] Issuer,
validity        [8] Validity_of_Key};
```

Это определение содержит параметры Key_ldentity (уникальный идентификатор ключа), Key_Value (значение ключа) и Check_Value (контрольная сумма для подтверждения целостности ключа), где только Key_Value является обязательным параметром. Параметры Cryptographic_Method (криптографический метод), Issuer (издатель) и Validity_of_Key (действительность ключа) регулируют использование ключа, ограничивая его определенными алгоритмами, временем и пользователями. Эти параметры важны для регулирования использования ключа, но являются необязательными. Параметры Generating_Authority (орган генерации), Certification_Authority (удостоверяющий центр) и Time_Stamp (метка времени) важны для подтверждения источника ключа и его возраста, но также являются необязательными. Для сертификата ключа обязателен параметр Issuer (издатель).

Приложение В
(справочное)
Классы криптографических приложений

Общая классификация криптографических систем определяется использованием двух основных криптографических методов - симметричного и асимметричного. Так как управление ключами должно удовлетворять обоим методам, необходим другой подход. Поэтому данный раздел классифицирует криптографические системы в соответствии с возможностями, предоставляемыми методами.

В общем случае криптографическая система предлагает два различных типа криптографических сервисов: сервисы аутентификации и сервисы шифрования. Сервисы шифрования используются для криптографической защиты информации, т.е. они обеспечивают конфиденциальность данных. Сервисы аутентификации используются главным образом для аутентификации сущностей, аутентификации источника данных, гарантии целостности данных и обеспечения неотказуемости. Типы криптографических систем и соответствующие операции представлены на рисунке В.1.

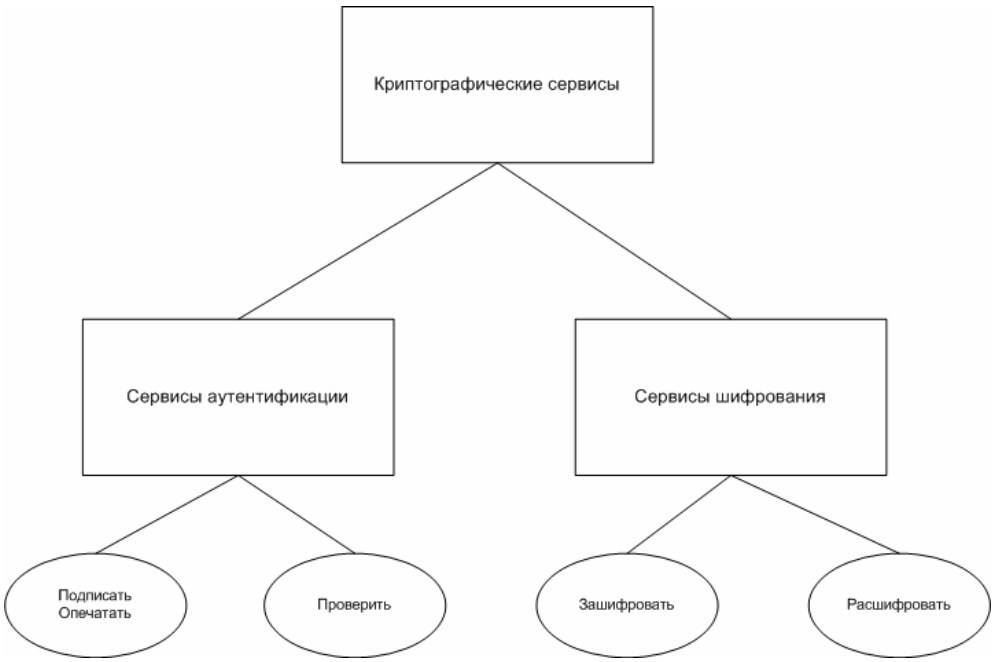


Рисунок В.1. Криптографические сервисы и соответствующие методы

В.1 Сервисы аутентификации и ключи

Сервисы аутентификации служат для аутентификации взаимодействующих сущностей (аутентификация сущностей), аутентификации происхождения данных (аутентификация источника данных), обеспечения неотказуемости и для гарантии целостности данных.

опечатывание блока данных	которое содержит вычисление криптографического контрольного значения для данных с целью контроля их целостности, например, генерация кода аутентификации сообщений (MAC) с помощью симметричного алгоритма

подписывание блока данных	которое содержит создание цифровой подписи для аутентификации источника данных, гарантии их целостности и/или обеспечения неотказуемости
верификация опечатанного блока	которая содержит вычисление криптографического контрольного значения для данных и сравнение его с соответствующим контрольным значением (подтверждение целостности данных).
верификация подписанного блока данных	которая содержит верификацию цифровой подписи для определения того, была ли она создана заявителем, и/или для подтверждения целостности данных

В сервисах аутентификации процессы подписывания и опечатывания используют закрытую информацию, которая имеется только у источника (т.е. уникальная и конфиденциальная), или секретную, известную источнику и получателю. Процесс верификации использует либо общедоступные процедуры и информацию, из которых невозможно получить закрытую информацию источника, либо секретную информацию, разделяемую источником и получателем. Существенной характеристикой подписывания является тот факт, что подпись может быть создана только с использованием закрытой информацию источника - его закрытого ключа. Таким образом, если подпись подтверждена с помощью открытого ключа источника, впоследствии можно доказать третьей стороне (например, нотариальному органу), что только владелец закрытой информации мог создать данную подпись.

Сервисы аутентификации используют два из трех типов ключей:

– ключ для опечатывания - общий секретный ключ;

– ключ для подписи - уникальный, закрытый ключ, связанный с источником;

– ключ для верификации - либо открытый, либо секретный ключ.

В симметричных методах сервис аутентификации использует ключ для опечатывания и ключ для верификации, которые представлены одним и тем же секретным ключом. В асимметричных методах этот сервис использует ключ для подписывания и ключ для верификации, которые представлены парой ключей, состоящей из открытого и закрытого ключей.

B.2 Сервисы шифрования и ключи

Сервисы шифрования служат, главным образом, для обеспечения конфиденциальности информации, но могут использоваться и для обеспечения целостности данных. В зависимости от используемых методов могут предоставляться и такие сервисы безопасности, как аутентификация и обеспечение неотказуемости. При этом используются два основных механизма:

–*шифрование*, которое вырабатывает зашифрованный текст из исходных данных;

–*расшифрование*, которое вырабатывает открытый текст из соответствующего зашифрованного текста.

Сервис шифрования может характеризоваться используемым криптографическим методом, т.е. симметричным или асимметричным. Когда применяется симметричный метод, операции шифрования и расшифрования используют один и тот же ключ (общий секретный ключ). Когда применяется асимметричный метод, операции шифрования и расшифрования используют два различных взаимосвязанных ключа, т.е. открытый и закрытый ключи.

Приложение Г
(справочное)
Управление жизненным циклом сертификата

Это приложение описывает требования и процедуры, применяемые в управлении жизненным циклом сертификатов открытых ключей.

Г.1 Удостоверяющий центр

Абоненты «доверяют» своему Удостоверяющему центру. Такое доверие основано на использовании соответствующих криптографических методов и оборудования, а также на профессиональной управленческой и контролирующей деятельности. Это доверие должно быть подтверждено независимым аудитом (внутренним, внешним или тем и другим), и результаты аудита должны быть доступны абонентам.

УЦ отвечает за:

1. Идентификацию сущностей, чьи пары ключей представлены для сертификации.

2. Обеспечение качества асимметричной пары ключей, используемой для выработки сертификата открытого ключа.

3. Обеспечение безопасности процесса сертификации и закрытого ключа, используемых для подписывания информации открытого ключа.

4. Управление специфическими данными, которые должны быть включены в информацию об открытом ключе, такими, как серийный номер сертификата открытого ключа, идентификатор удостоверяющего центра и т.д.

5. Установление и проверку периодов действия.

6. Уведомление сущности, указанной в информации об открытом ключе, что сертификат открытого ключа был издан. Средства, используемые для передачи уведомления, должны быть независимыми от метода, используемого для передачи информации об открытом ключе в УЦ.

7. Гарантирование того, чтобы две различные сущности не получили один идентификатор, т.е. чтобы они были существенно различимы.

8. Поддержание и издание списков аннулированных сертификатов.

9. Регистрацию всех шагов, используемых в процессе генерации сертификата открытого ключа.

Один УЦ может сертифицировать информацию об открытом ключе другого УЦ для получения сертификата открытого ключа. Следовательно, аутентификация может использовать цепь сертификатов открытых ключей. Первый сертификат открытого ключа в этой цепи должен быть получен и удостоверен способом, отличным от сертификации открытого ключа.

Г.1.1 Асимметричная пара ключей УЦ

УЦ должен иметь средства безопасного управления ключами, которые могут генерировать асимметричные пары ключей для использования этим УЦ. Процесс генерации должен обеспечивать непредсказуемость ключевого материала. Никто не должен получать преимуществ от знания процесса генерации.

Закрытый ключ УЦ используется для подписи информации открытых ключей сущностей. Так как обладание таким ключом позволяет выступать в роли УЦ и генерировать поддельные сертификаты открытых ключей, этому ключу должна быть обеспечена высокая степень защиты. Таким образом, закрытый ключ УЦ должен быть хорошо защищен при его использовании в средствах управления ключами. Ключ должен

поступать и покидать средство управления ключами защищенным способом и под контролем УЦ.

Целостность открытого ключа УЦ для верификации является существенной для безопасности системы сертификации открытых ключей. Если открытый ключ УЦ не содержится в сертификате открытого ключа, то должны быть предприняты специальные меры для обеспечения его аутентифицированного распространения. Со стороны пользователей должны быть предприняты меры для гарантирования аутентичности хранимой копии открытого ключа УЦ.

Открытый ключ УЦ для верификации используется для проверки сертификатов открытых ключей других пользователей. Перед каждым использованием открытого ключа УЦ пользователь должен убедиться в действительности на данный момент ключа для верификации.

Г.2 Процесс сертификации

Этот раздел описывает требования и процедуры, применяемые в процессе сертификации.

Г.2.1 Модель сертификации открытого ключа

Этот раздел определяет базовую модель сертификации открытых ключей. В этой модели основные функции разделяются между логическими сущностями (см. рисунке Г.l):

1. Удостоверяющий центр (УЦ): сущность, отвечающая за сертификацию информации об открытом ключе пользовательской сущности.

2. Каталог (DIR): сущность, отвечающая за предоставление оперативного доступа пользовательским сущностям к сертификатам открытых ключей.

3. Генератор ключей (ГК): сущность, отвечающая за генерацию асимметричной пары ключей.

4. Орган регистрации (ОР): сущность, отвечающая за предоставление УЦ проверенных идентификаторов пользователей.

5. Пользовательская сущность (А).

В этом разделе обсуждаются отношения между логическими сущностями этой модели и требованиями безопасности к этим отношениям. Логические сущности могут быть объединены. Например, А и ГК могут быть объединены, если пользовательская сущность сама генерирует асимметричную пару ключей. УЦ и ГК могут быть объединены, если УЦ генерирует пары ключей от имени пользовательских сущностей.

Примечание. Необходимо убедиться, что сертификат, созданный объединенными ОР и УЦ, идентичен созданному раздельными ОР и УЦ.

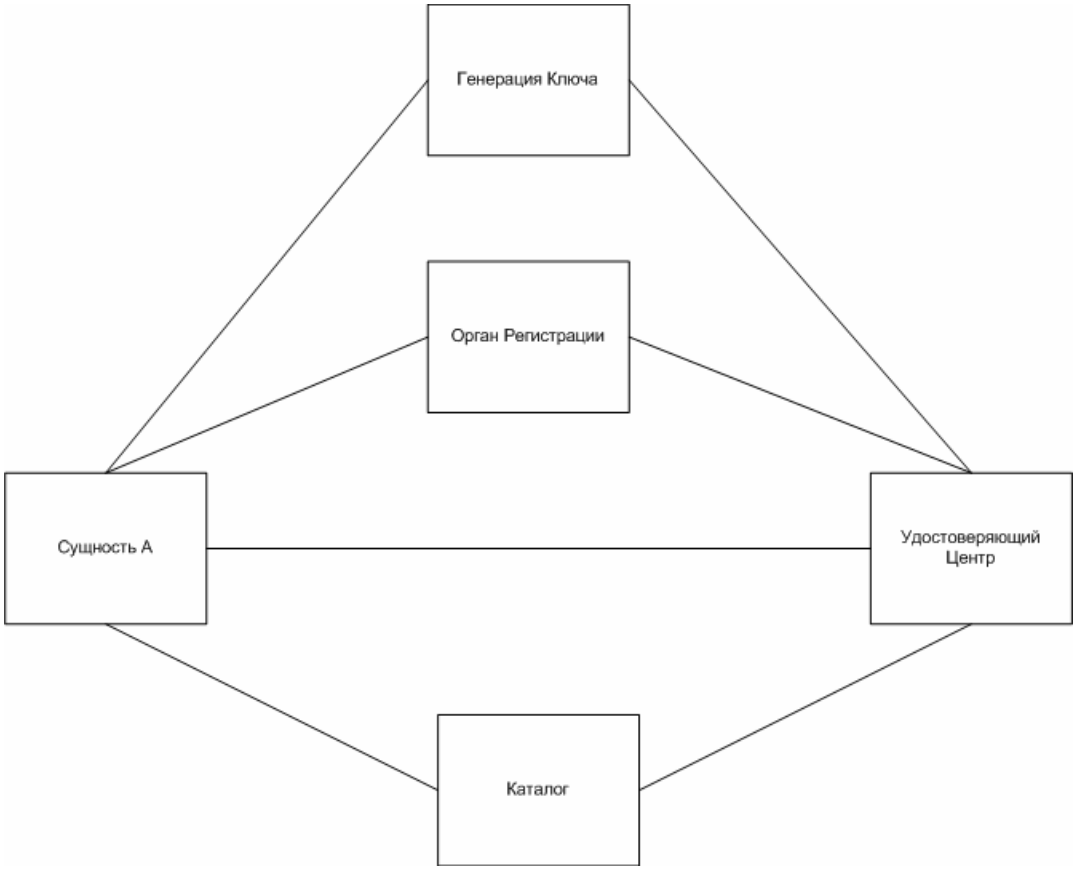


Рисунок Г.1. Базовая модель сертификации открытых ключей

Г.2.1.1 Связи в модели сертификации

Этот раздел описывает некоторые связи в базовой модели и соответствующие требования безопасности. Не все связи должны присутствовать в конкретной реализации системы. Например, функции ОР, УЦ и ГК могут быть объединены.

А - ГК

Сущность А просит генератор ключей ГК сгенерировать асимметричную пару ключей. ГК доверяют в генерации асимметричных пар ключей хорошего качества. ГК генерирует пару ключей (Sa, Va), где Sa - ключ для подписывания, Va - ключ для верификации, и передает ее А. Эта передача должна происходить безопасным и конфиденциальным способом. ГК и А должны быть абсолютно уверены, что никакая третья сторона не изменила асимметричную пару ключей и не получила значения ключей во время передачи.

А - ОР

Сущность А запрашивает регистрацию в Органе регистрации (ОР). А должен предоставить ОР идентификационную информацию. ОР проверяет подлинность этой информации и, возможно, добавляет специфические данные. Информация затем пересылается безопасным образом в ОР.

А - УЦ

Сущность А просит удостоверяющий центр сертифицировать информацию открытого ключа (или ее подмножество), включая открытый ключ и свое уникальное имя. Предоставление информации открытого ключа в УЦ должно происходить таким образом, чтобы гарантировать ее подлинность и целостность. УЦ проверяет подлинность информации открытого ключа сущности А, добавляет, возможно, специфические

системные данные и затем подписывает полную информацию об открытом ключе для выработки сертификата открытого ключа сущности А. Сертификат открытого ключа может затем быть передан сущности А.

При получении выданного сертификата открытого ключа А проверяет его правильность с помощью ключа для верификации $v_{УЦ}$ удостоверяющего центра. Этот открытый ключ для верификации $v_{УЦ}$ должен быть предоставлен сущности А с гарантией подлинности. С этого момента открытый ключ сущности А может распространяться как сертификат открытого ключа и использоваться всеми, кто имеет доступ к ключу для верификации УЦ.

Если, Удостоверяющий центр просит ГК сгенерировать асимметричную пару ключей для сущности А, то пара ключей будет передана от ГК сущности А. К этой передаче предъявляются требования конфиденциальности, целостности и аутентичности. В дополнение УЦ должен сохранять конфиденциальность, целостность и аутентичность всех асимметричных пар ключей во время обработки и хранения. Наконец, УЦ должен передать закрытый ключ сущности А, будучи абсолютно уверенным, что никакая третья сторона не сможет изменить или прочитать передаваемое значение ключа.

А - DIR

Сущность А передает свой сертификат открытого ключа в Каталог DIR и регистрирует его в этом каталоге. Для регистрации сертификата открытого ключа в каталоге требуется аутентификация сущности и проверка ее прав доступа. Между сущностью А и DIR должно быть соглашение по поводу того, кто уполномочен управлять данными сущности в каталоге. По одному сценарию DIR управляет всей информацией в каталоге, по другому - каждая сущность управляет своей информацией в каталоге.

ОР - УЦ

ОР просит УЦ сертифицировать информацию об открытом ключе сущности А. Передача информации об открытом ключе А от ОР к УЦ должна происходить аутентичным способом. УЦ проверяет подлинность информации об открытом ключе А, добавляет, возможно, специфические системные данные и затем подписывает полную информацию об открытом ключе для получения сертификата открытого ключа. УЦ уведомляет ОР о сертификации.

УЦ - ГК

Удостоверяющий центр просит генератор ключей ГК сгенерировать асимметричную пару ключей для сущности А. ГК доверяют в генерации асимметричных пар ключей хорошего качества. ГК генерирует пару ключей и передает ее в УЦ. Эта передача должна происходить безопасным и конфиденциальным образом. ГК и УЦ должны быть абсолютно уверены, что никакая третья сторона не изменила асимметричную пару ключей и не получила значения ключей во время передачи. УЦ должен сохранять конфиденциальность, целостность и подлинность всех асимметричных пар ключей во время обработки и хранения.

УЦ - DIR

УЦ передает полученные сертификаты открытых ключей непосредственно в Каталог DIR и регистрирует их в каталоге. Для регистрации сертификата открытого ключа в каталоге требуется аутентификация сущности и проверка ее прав доступа.

Г.2.2 Регистрация

Регистрация ключа сущности включает подачу заявления о выдаче сертификата сущности и его проверку ОР или УЦ. Следующие подразделы приводят требования, предъявляемые к подаче заявления о выдаче сертификата. Заявление о выдаче сертификата может содержать или не содержать значение открытого ключа.

Г.2.2.1 Подача заявления физическими лицами

Для приложений с небольшим риском, удовлетворение заявления о выдаче сертификата должно базироваться на идентификации личности, обращающейся за сертификатом открытого ключа. Заявление о выдаче сертификата может не подаваться персонально, однако должен быть использован разумный деловой порядок удостоверения личности.

Для приложений с высоким риском удовлетворение заявления о выдаче сертификата должно основываться на личном (или через уполномоченного агента) обращении желающего получить сертификат открытого ключа и на использовании разумных коммерческих стандартов для идентификации обращающегося за сертификатом (и его агента, если потребуется). Это может потребовать удостоверение личности третьей доверенной стороной.

Г.2.2.2 Подача заявления юридическими лицами

Удовлетворение заявления о выдаче сертификата должно основываться на том, что заявление о выдаче сертификата будет доставлен лично, как минимум, одним представителем юридического лица и, кроме того, основан на:

1. Подписи и печати на заявлении о выдаче сертификата открытого ключа.

2. Использовании разумной коммерческой практики для удостоверения подписи и печати юридического лица.

3. Использовании разумной коммерческой практики для удостоверения подлинности представителей, передающих заявление о выдаче сертификата.

Г.2.3 Отношения между юридическими лицами

Для юридических лиц может возникнуть необходимость установить контакты с другими юридическими лицами. Это может быть достигнуто различными способами:

1. Служащие компании имеют персональные асимметричные пары ключей. Юридическое лицо выступает в качестве УЦ для служащих своей компании. Сделки заверяются сотрудниками с помощью их персональных ключей, сертифицированных УЦ компании. Получатели проверяют, что отправитель имеет сертификат компании, чей открытый ключ, в свою очередь, сертифицирован некоторым вышестоящим УЦ.

2. Служащие компании не имеют персональных асимметричных пар ключей. Только юридическое лицо имеет одну или несколько асимметричных пар ключей. Получатели проверяют состоятельность сделки с помощью открытого ключа компании. Получателям не нужно беспокоиться об уровнях доступа и политики безопасности в компании отправителя.

Г.2.4 Генерация сертификатов

Процесс генерации сертификата открытого ключа должен происходить до использования асимметричной пары ключей.

Следующие шаги необходимы в процессе генерации сертификата:

1. Проверка информации открытого ключа на наличие ошибок.

2. Принятие информации об открытом ключе. Требования к принятию информации об открытом ключе определены выше в подразделе о регистрации.

3. Подготовка и добавление данных, необходимых для управления сертификатами открытых ключей. Дополнительно, но не в обязательном порядке УЦ может сгенерировать асимметричную(ые) пару(ы) ключей.

4. Вычисление подписи для сертификата открытого ключа, которое может использовать хэш-функцию.

5. Протоколирование действий УЦ в процессе генерации сертификата открытого ключа.

Для приложений с высоким риском может быть желательным (1) потребовать создания нескольких подписей сертификата открытого ключа одним УЦ с применением различных криптографических средств (с разными закрытыми ключами), или (2) потребовать несколько подписей информации об открытом ключе, сделанных различными УЦ.

Г.2.5 Возобновление/Время жизни

Сертификат открытого ключа имеет время жизни, которое определено сроком действия, указанным в сертификате открытого ключа, или другим образом определено УЦ.

Г.3 Распространение и использование сертификатов открытых ключей

Этот раздел описывает требования и процедуры, применяемые к распространению и использованию сертификата открытого ключа.

Г.3.1 Распространение и хранение сертификатов открытых ключей

Когда сертификат открытого ключа создан, не требуется специальных мер для сохранения его конфиденциальности и целостности. Сертификат открытого ключа может храниться в общедоступном каталоге.

Г.3.2 Верификация сертификатов открытых ключей

Чтобы проверить действительность сертификата открытого ключа, проверяющая сущность В должна, как минимум, проверить подпись УЦ сертификата открытого ключа. Если у сертификата открытого ключа определен срок действия, В должна убедиться, что информация открытого ключа сущности А действительна в настоящее время (см. Г.5 Аннулирование сертификатов). Для верификации сертификата открытого ключа проверяющий должен иметь действующую копию ключа УЦ для верификации.

Г.4 Сертификационные цепочки

От УЦ не требуется знания и сертификации всех остальных УЦ. Также нет необходимости в строгой иерархии УЦ. Однако УЦ могут сертифицировать друг друга (проводить перекрестную сертификацию), чтобы иметь возможность гибкого использования и обмена сертификатами открытых ключей. Эта перекрестная сертификация должна производиться с максимальной защищенностью и в соответствии с тщательно продуманной процедурой. Когда существует система перекрестных сертификатов, можно построить пути для проверки действительности сертификатов открытого ключа. Пользователь должен иметь доверие только к ключу для верификации одного из УЦ. Это доверие может быть распространено по цепочке до открытого ключа партнера, выданного неизвестным УЦ.

Г.5 Аннулирование сертификата

Сертификат может быть аннулирован до истечения его срока действия. Это может произойти по нескольким причинам, включая следующие:

1. Компрометация закрытого ключа сущности.
2. Запрос отмены ключа от сущности.
3. Изменение обстоятельств присоединения сущности.
4. Окончание деятельности сущности.
5. Неверная идентификация сущности.
6. Компрометация закрытого ключа УЦ.
7. Ликвидация УЦ.

Следовательно, должны существовать процедуры и средства быстрого оповещения заинтересованных сторон для того, чтобы легко и безопасно отменить:

1. Один или несколько сертификатов открытого ключа одного или нескольких сущностей.

2. Набор всех сертификатов открытых ключей, выданных УЦ, основанных на одной асимметричной паре ключей, используемой УЦ для подписи информации об открытых ключах.

3. Все сертификаты открытых ключей, выданные УЦ, независимо от используемых функций асимметричной пары ключей.

Два последних требования обеспечивают возможность аннулирования сертификатов открытых ключей, когда произошла или подозревается компрометация закрытого ключа УЦ, или когда асимметричная пара ключей, используемая для подписи сертификатов открытых ключей, была изменена. Когда сертификаты открытых ключей аннулируются или у них завершается срок действия, их копии должны сохраняться доверенной третьей стороной на время, определяемое разумной деловой практикой, законом и нормативными документами.

Когда закрытый ключ сущности или УЦ отменяется по любой причине, УЦ, выдавший сертификат этого открытого ключа, должен немедленно проинформировать все сущности в системе, что все соответствующие сертификаты открытого ключа были аннулированы. Это может, например, иметь форму сообщения, удостоверенного УЦ, и разосланного всем сущностям; сообщения, удостоверенного другим УЦ; внесения в онлайновый список, поддерживаемого доверенной третьей стороной, аннулированных сертификатов открытых ключей, или даже публикации списка аннулированных или действительных сертификатов открытых ключей.

Когда сертификат открытого ключа аннулирован из-за того, что известна или подозревается компрометация соответствующего закрытого ключа, закрытый ключ не должен больше использоваться. Сертификат открытого ключа должен использоваться только в целях верификации при условии, что данные были подписаны до аннулирования сертификата. Более того, использование любого ключевого материала, зашифрованного с использованием этого сертификата открытого ключа (независимо от типа), должно быть немедленно прекращено.

Когда прекращается срок действия ключа, или он аннулирован по любой причине, кроме подозреваемой или действительной компрометации, закрытый ключ не должен больше использоваться. Сертификат открытого ключа все еще может быть использован для верификации и расшифрования. Весь ключевой материал, отосланный и защищенный с использованием этого сертификата открытого ключа (независимо от типа) должен быть заменен настолько быстро, насколько это возможно.

Г.5.1 Списки аннулированных сертификатов

Список аннулированных сертификатов содержит имеющий временные отметки перечень серийных номеров или идентификаторов сертификатов открытых ключей, которые были аннулированы УЦ. В списках аннулированных сертификатов используются два типа отметок времени:

1. Дата и время, когда УЦ аннулировал сертификат.

2. Дата и время известной или подозреваемой компрометации.

Последняя временная отметка, если она известна, облегчает проверку подозрительных сообщений. Сертификат открытого ключа остается в списке аннулированных сертификатов, как минимум, до окончания срока своего действия. Отметки времени очень важны, т.к. они позволяют определить, в какое время связь между открытым ключом сущности и сущностью была ликвидирована.

Если аннулирование произошло из-за известной или подозреваемой компрометации, информация, подписанная соответствующим закрытым ключом, больше

не будет признана достоверной, если подпись была поставлена после даты компрометации, или дата подписи не может быть надежно установлена. Информация не должна шифроваться с помощью аннулированного открытого ключа.

Список аннулированных сертификатов должен:

1. Иметь дату и подпись УЦ, чтобы сущности могли проверить целостность списка и время его распространения.

2. Регулярно публиковаться УЦ, даже если не произошло никаких изменений со времени последней публикации.

3. Быть доступным для всех сущностей системы, кроме случаев, когда это запрещено законом, нормативными документами или решением суда.

Для распространения списка аннулированных сертификатов возможно использование различных механизмов, включая:

– доставку каждому пользователю в виде сообщения доверенной третьей стороной;

– запрос пользователя доверенной третьей стороне о текущем статусе данного сертификата открытого ключа;

– запросы УЦ о текущем списке аннулированных сертификатов.

УЦ должен периодически публиковать и распространять новый список аннулированных сертификатов.

Приложение
(справочное)
Библиография

[1] ИСО 8732: 1988 Банковское дело. Управление ключами (обзор).

[2] ИСО/МЭК 9594-8: 1990 Информационные технологии. Взаимодействие открытых систем. Справочник. Часть 8. Структура аутентификации.

[3] ИСО 11166-1: 1994 Банковское дело. Управление ключами с помощью асимметричных алгоритмов. Часть 1. Принципы, процедуры и форматы.

[4] ИСО 11568-1: 1994 Банковское дело. Управление ключами (детали). Часть 1. Введение в управление ключами.

[5] ИСО 11568-2: 1994 Банковское дело. Управление ключами (детали). Часть 2. Методы управления ключами для симметричных шифров.

[6] ИСО 11568-3: 1994 Банковское дело. Управление ключами (детали). Часть 3. Жизненный цикл ключа для симметричных шифров.

[7] ИСО 11568-4: Банковское дело. Управление ключами (детали). Часть 4. Методы управления ключами для криптосистем с открытым ключом.

[8] ИСО 11568-5: Банковское дело. Управление ключами (детали). Часть 5. Жизненный цикл ключа для криптосистем с открытым ключом.

[9] ИСО/МЭК 11770-3: Информационные технологии. Методы безопасности. Управление ключами. Часть 3. Механизмы, использующие асимметричные методы.

[10] ИСО/МЭК 13888: Информационная технология. Методы и средства обеспечения безопасности. Неотказуемость (все части).

УДК 681.324:006.354 **МКС 35.040**

Ключевые слова: обработка данных, информационный обмен, методы защиты, управление ключами, криптография.

Басуға _____ж. қол қойылды Пішімі 60х84 1/16
Қағазы офсеттік. Қаріп түрі «KZ Times New Roman»,
«Times New Roman»
Шартты баспа табағы 1,86. Таралымы ____ дана. Тапсырыс ____

«Қазақстан стандарттау және сертификаттау институты»
республикалық мемлекеттік кәсіпорны
010000, Астана қаласы Орынбор көшесі, 11 үй,
«Эталон орталығы» ғимараты
Тел.: 8 (7172) 240074