ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология
АШЫҚ ЖҮЙЕЛЕРДІҢ ӨЗАРА БАЙЛАНЫСЫ
Ашық жүйелерге арналған қауіпсіздік негіздері
2-бөлім
Сәйкестендіру негіздері

Информационная технология
ВЗАИМОДЕЙСТВИЕ ОТКРЫТЫХ СИСТЕМ
Основы безопасности для открытых систем
Часть 2
Основы аутентификации

ҚР СТ ИСО/МЭК 10181-2-2008

(ИСО/МЭК 10181-2:1996 «Ақпараттық технология. Ашық жүйелердің өзара әрекеті. Ашық жүйелерге арналған қауіпсіздік негіздері. Сәйкестендіру негіздері», IDT)

Ресми басылым

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

Астана

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология

АШЫҚ ЖҮЙЕЛЕРДІҢ ӨЗАРА БАЙЛАНЫСЫ

Ашық жүйелерге арналған қауіпсіздік негіздері
2-бөлім
Сәйкестендіру негіздері

ҚР СТ ИСО/МЭК 10181-2-2008
(ИСО/МЭК 10181-2:1996 «Ақпараттық технология. Ашық жүйелердің өзара әрекеті. Ашық жүйелерге арналған қауіпсіздік негіздері. Сәйкестендіру негіздері », IDT)

Ресми басылым

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

Астана

Алғысөз

1 «Инфосистемы Джет» ЖАҚ **ӘЗІРЛЕДІ**

Қазақстан Республикасының Ақпараттандыру және байланыс агенттігі **ЕНГІЗДІ**

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

3 Осы стандарт Қазақстан Республикасы экономикасының қажеттіліктерін көрсететін қосымша талаптар мәтін бойынша көлбеу қаріппен белгіленіп ИСО/МЭК 10181-2:1996 «Ақпараттық технология. Ашық жүйелердің өзара әрекеті. Ашық жүйелерге арналған қауіпсіздік негіздері. Сәйкестендіру негіздері» («Information technology. Open Systems Interconnection. Security frameworks for open systems. Authentication framework») халықаралық стандартына балама, IDT

4 БІРІНШІ ТЕКСЕРУ МЕРЗІМІ 2013 жыл
ТЕКСЕРУ КЕЗЕҢДІЛІГІ 5 жыл

5 АЛҒАШ РЕТ ЕНГІЗІЛДІ

Мазмұны

Кіріспе

«Ақпараттық технология. Ашық жүйелердің өзара әсерлері. Ашық жүйелерге арналған қауіпсіздік негіздері» жалпы тақырыпқа ие ҚР СТ ИСО/МЭК 10181 мына бөлімдерден тұрады:

– 1 бөлім. Шолу
– 2 бөлім. Сәйкестендіру негіздері
– 3 бөлім. Қол жеткізуді басқару негіздері
– 4 бөлім. Авторлықтан бас тартпау негіздері
– 5 бөлім. Құпиялық негіздері
– 6 бөлім. Тұтастық негіздері
– 7 бөлім. Қауіпсіздік және жедел хабарлауды есепке алу негіздері.

Осы стандарт қосымшалары анықтамалық болып табылады.

Көптеген қосымшаларға ақпаратты өткізу кезіндегі қатерлерге қарсы тұру мақсатында қауіпсіздікті қамтамасыз ету талаптары қойылады. Кейбір белгілі қауіпсіздік қатерлері, сонымен қатар қауіпсіздік тетіктері мен сервистері ГОСТ ИСО 7498-2:2002 сипатталған.

Осы стандарт сәйкестендіру сервистерін көрсетудің жалпы негіздерін ұсынады.

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология
АШЫҚ ЖҮЙЕЛЕРДІҢ ӨЗАРА БАЙЛАНЫСЫ
Ашық жүйелерге арналған қауіпсіздік негіздері
2-бөлім
Сәйкестендіру негіздері

Енгізілген күні 2008.07.01

1 Қолданылу саласы

Осы стандарт ашық жүйелер ортасында қауіпсіздік сервистерін қолдану мәселелерін шешуге арналған Қауіпсіздік негіздерін белгілейді. «Ашық жүйелер» термині бойынша мәліметтер базасы, бекітілген қосымшалар, ашық таралған өңдеу және ашық жүйелер өзара әрекеттері деген салаларды білдіреді.

Қауіпсіздіктің негізгі ережелері мәліметтер элементтерімен қатар арнайы қауіпсіздік сервистерін алу мақсатында қолданылатын кезекті әрекеттерімен (хаттама элементтерінен басқа) жұмыс жасайды. бұл қауіпсіздік сервистері өзара әрекеттесу жүйелер мәндеріне қатысты, сонымен қатар жүйелер арасында мәлімет алмасуға, және жүйені басқаратын мәліметтерге қатысты қолдануы мүмкін.

Осы стандарт:

– Сәйкестендірудің негізгі ұғымдарын;

– Сәйкестендіру тетіктерінің мүмкін сыныптарын;

– Сәйкестендіру тетігінің осы класына сервисті;

– Сәйкестендірудің осы тетіктерін қолдауға арналған хаттамаларға қойылатын атқарымдық талаптарды;

– Сәйкестендіруді басқаруға қойылатын жалпы талаптарды белгілейді.

Осы стандарт мыналарды қоса стандарттардың әртүрлі типтеріне қатысты қолданыла алады:

1) Сәйкестендіру ұғымдары көрсетілген стандарттар;

2) Сәйкестендіру сервисін көрсететін стандарт;

3) Сәйкестендіру сервисін қолдану стандарттары;

4) ашық жүйелер архитектурасында сәйкестендіруді ұсыну әдістері мен құралдар ерекшелендіретін стандарттары;

5) Сәйкестендіру тетіктерін мамандандыратын стандарттары. [атап өтетін жайт, 2), 3) және 4) жағдайлар құрамында сәйкестендіру болуы мүмкін, алайда мақсаттары басқа болады]

Ресми басылым

Бұл стандарттар осы стандарттарды мынадай үлгіде қолдана алады:

– 1), 2), 3), 4) және 5) түрдегі стандарттар осы стандарт терминологиясын қолдануы мүмкін;

– 2), 3), 4) және 5) стандарт түрлері осы стандарттың 7-бөлімінде көрсетілген сервистерді қолдануы мүмкін;

– 5) түрдегі стандарт осы стандарттың 8-бөлімінде көрсетілген тетіктерге негізделуі мүмкін.

Басқа қауіпсіздік сервистері сияқты сәйкестендіру де белгілі бір қосымшаға арналған арнайы қауіпсіздік саясаты контекстінде ғана ұсынылады. Қауіпсіздік саясатын анықтау осы стандарттар шеңберіне кірмейді.

Осы стандарттар аясы хаттамалық айырбас сәйкестендіруді жүзеге асыруға қажетті бөліктерінің спецификациясын қамтымайды.

Осы стандарт сәйкестендіру сервистерін қолдау жөніндегі арнайы механизмдерді анықтамайды. Басқа стандарттарда (*ҚР СТ ИСО/МЭК 9798 сияқты*) сәйкестендірудің толық әдістері толығырақ өңделген. Одан басқа, осындай әдістердің мысалдары стандарттарда (*ҚР СТ ИСО/МЭК 9594-8 сияқты*) сәйкестендірудің арнайы талаптарын көрсету үшін қолданылады.

Осы стандартта сипатталған бірқатар процедуралар криптографиялық әдістерді қолдану арқылы қауіпсіздікті қамтамасыз етеді. Осы Негіздер арнайы криптографиялық немесе басқа алгоритмдерді қолдануға байланысты емес, сәйкестендірудің кейбір тетіктері арнайы алгоритм қасиеттеріне байланысты болуы мүмкін, мысалы, ассиметриялық қасиеттер. *Ақпаратты криптографиялық қорғаудың нақты құралдарын таңдау және қолдану Қазақстан Республикасының заңнамасымен регламенттеледі және осы стандарттың қарастыратын заты болып табылмайды.*

2 Нормативтік сілтемелер

Осы стандартта мынадай стандарттарға сілтемелер пайдаланылды:

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

ҚР СТ ИСО/МЭК 9798-2-2008 Ақпараттық технология. Қауіпсіздікті қамтамасыз етудің әдістері мен құралдары. Сәйкестендіру тетіктері. 2-бөлім. Симметриялық шифрлеу алгоритмдерін қолданатын тетіктер.

ҚР СТ ИСО/МЭК 9798-3-2008 Қауіпсіздікті қамтамасыз етудің әдістері мен құралдары. Сәйкестендіру тетіктері. 3-бөлім. Цифрлік қолтаңба әдісін қолданатын тетіктер.

ҚР СТ ИСО/МЭК 10116-2008. Ақпараттық технология. Қауіпсіздікті қамтамасыз етудің әдістері мен құралдары. n-биттік блок шарттарымен жұмыс жасау режимі.

ҚР СТ ИСО/МЭК 10181-1-2008. Ақпараттық технология. Ашық жүйелердің өзара әрекеттері. Ашық жүйелерге арналған қауіпсіздік негіздері: 1-бөлім. Шолу.

ГОСТ ИСО 7498-2:2002 Ақпараттық технология. Ашық жүйелердің өзара әрекеттері. Негіздік эталондық модель. 2-бөлім. Ақпаратты қорғау архитектурасы.

ИСО/МЭК 8348-2002 Ақпараттық технологиялар. Ашық жүйелердің өзара әрекеті. Желілік қызметті анықтау.

ИСО/МЭК 8824-2002 (4 бөлікте) Ақпараттық технология. Бір нұсқасында синтаксисті белгілеудің абстрактілі жүйесі (ASN.1).

ИСО/МЭК 9545-1994 Ақпараттық технологиялар. Ашық жүйелердің өзара әрекеті. Анықтамалық. Ашық кілтпен шифрлеу және сапалы сертификаттық құрылымдар.

ИСО/МЭК 9979-1991. Криптографиялық әдістер. Криптографиялық алгоритмдерді тіркеу процедурасы.

3 Терминдер мен анықтамалар

Осы стандартта *ҚР СТ ИСО/МЭК 10116-2008, ҚР СТ ИСО/МЭК 10181-1-2008,* ГОСТ ИСО 7498-2 бойынша терминдер, сондай-ақ сәйкес анықтамаларымен мынадай терминдер қолданылады:

3.1 Автономды сәйкестендіру сертификаты (off-line authentication certificate): Барлық мағыналарға бірдей қол жеткізерлік бола алатын айырым идентификаторын байланыстыратын сәйкестендіру сертификаты.

3.2 Сәйкестендірудің ассиметриялық әдісі (asymmetric authentication method): барлық ақпараты екі мән аралығында бөліне бермейтін Сәйкестендіру әдісі.

3.3 Сәйкестендірулік айырбас (authentication exchange): Сәйкестендіруді жүзеге асыру мақсатында сәйкестендіру ақпараттың бір немесе одан да көп кездегі айырбас ақпараты.

3.4 Сәйкестендіру сертификаты (authentication certificate): Сәйкестендіру жөніндегі уәкілетті растаған қауіпсіздік сертификаты, ол сертификат бірқатар мән түпнұсқасын растау мақсатында қолдануы мүмкін.

3.5 Сәйкестендіру (authentication): бірқатар мәндердің мәлімделген түпнұсқасын кепілдендіруді қамтамасыз ету.

3.6 Сәйкестендірілген мән (authenticated identity): Сәйкестендіру процессі барысында куәландырылған принципиалдың айырым идентификаторы (Сәйкестендіру объектісі).

3.7 Верификатор (verifier): түпнұсқаны растайтын өзі болатын немесе оның өкілі болып табылатын мән. Верификатор сәйкестендіру процессінде

мәліметтердің ақпараттық айырбасын жүзеге асыру атқарымдығына ие болып табылады.

3.8 Сәйкестендірудің верификациялық ақпараты (верификациялық ИА) (verification authentication information, verification AI): Верификатордың айырбастық ИА да мәлімделген мәнді верификациялау мақсатында қолданатын ақпарат.

3.9 Сұраныс (challenge): верификатор жасайтын уақыт жөнінде ауыспалы параметр.

3.10 Мәлімдеуші (claimant): Сәйкестендіру мақсатында принципиал немесе өкілі болып табылатын маңыз. Мәлімдеуші принципиал атынан сәйкестендірулік айырбасқа қатысуға қажетті қызметтерді қосады.

3.11 Сәйкестендірудің мәлімдеуші ақпараты (мәлімдеуші ИА) (claim authentication information, claim ИА): Мәлімдеушінің принципиал сәйкестендірілуіне қажетті айырбас ИА туындауға қолданатын ақпараты.

3.12 Сәйкестендіру бастамашысы (authentication initiator): Сәйкестендірулік айырбасты бастайтын мән.

3.13 Сәйкестендіру ақпараты (authentication information): Сәйкестендіру мақсатында қолданылатын ақпарат.

3.14 Айырбастық сәйкестендіру ақпараты (айырбастық ИА) (exchange authentication information, exchange ИА): Принципиал сәйкестендірілуі процессі кезінде мәлімдеуші мен верификатор айырбастайтын ақпарат.

3.15 Оперативті сәйкестендіру сертификаты (on-line authentication certificate): Сәйкестендірулік айырбаста қолдануға мақсатталған, уәкілетті мәліметшіден тікелей алынатын сәйкестендіру сертификаты.

3.16 Айырым идентификаторы (distinguishing identifier): Сәйкестендіру процессінде мәнді бір жақты идентификациялайтын мәліметтер. Осы стандарт осындай ең жоқ дегенде қауіпсіздік доменінің шеңберінде бірегей болуын талап етеді.

3.17 Уақыт бойына құбылмалы болып келетін параметр (time variant parameter)**:** хабарламаның қайта жаңғыртудың нәтижесі еместігін растау үшін мәндік қолданатын мәліметтер элементі.

3.18 Принципиал (Сәйкестендіру объектісі) (principal): түпнұсқасы расталуы мүмкін мағына

3.19 Сәйкестендірудің симметриялық әдісі (symmetric authentication method): Екі мән де жалпы сәйкестендіру ақпаратын бөлісетін сәйкестендіру әдісі.

3.20 Бірегей нөмір (unique number): Мәлімдеуші арқылы туындалып уақыт бойына құбылмалы болып табылатын параметр.

4 Сәйкестендіру туралы жалпы мәліметтер

4.1 Сәйкестендірудің негізгі ұғымдары

Сәйкестендіру мәлімделген мәнге сенімді қамтамасыз етеді. Сәйкестендіру тек принципиал мен верификатор арасындағы өзара әрекет контекстінде ғана маңызға ие болады. Екі маңызды жағдай бар: верификатормен ерекше коммуникациялық өзара әрекетке ие мәлімдеуші ұсынған принципиал (мән сәйкестендірілуі) және верификатордың қол жеткізерлік мәліметтер элементінің көзі болып табылады (мәліметтер көзінің сәйкестендірілуі).

Осы стандарт сәйкестендірудің екі түрін айырады. Мән сәйкестендірілуі коммуникациялық өзара байланыс контексіндегі принципиал түпнұсқасын растауды қамтамасыз етеді (сәйкестендіру объектісі). Принципиалдың сәйкестендірілген маңызы тек ол сервис қосылғанда ғана куәландырады. 4..2.7. тармақта көрсетілгендей сәйкестендіру үздіксіздігіне қол жеткізу мүмкін. Оған ГОСТ ИСО 7498-2 де суреттелген бір дәрежелі ВОС Сәйкестендірілуі мысал бола алады.

Дерекқорлардың сәйкестендірілуі арнайы нақты деректер блогіне жауапты принципиалды растауын қамтамасыз етеді.

Ескертпелер

1 Деректер көзін сәйкестендіру кезінде мәліметтердің өзгертілмегені туралы балама сенімге ие болу қажет. Оған тұтастық сервисін қолдану арқылы қол жеткізуге болады, мысалы:

а) деректер өзгеруіне болмайтын ортаны қолдану;

б) алынған мәліметтердің жіберілген мәліметтердің сандық таңбасына сәйкестігі туралы верификациясы;

в) сандық қол қою тетігін қолдану;

г) симметриялық криптографиялық алгоритмді қолдану;

2 Сәйкестендірулік мәнді анықтауда қолданылған коммуникациялық өзара байланыс термині кең интерпретацияға жол береді және қайта қосылу, процесс аралық коммуникация немесе қолданушы мен терминал арасындағы қатынасқа да жатуы мүмкін.

4.1.1 Сәйкестендіру және баламалау

Принципиал — дегеніміз белгіленуі (сәйкестендіру) мүмкін мағына, түпнұсқа болып табылады. Принципиал бір немесе бірнеше айырым сәйкестендіргіштерге ие. Сәйкестендіру сервистері принципиалды верификациялау мақсатында мәндер арқылы қолданылады. Осылайша расталған принципиал түнұсқасы Сәйкестендірулік мән деп аталады.

Сәйкестендіріліп және баламаланатын принципиал мысалдары:

– Қолданушы-адамдар;

– процесстер;

– шынайы ашық жүйелер;

– ВОС деңгейінің маңыздары;

– Кәсіпорындар.

Айырым идентификаторлардың қауіпсіздік домені аясында бірегей болуы талап етіледі. Айырым идентификаторлары принципиалды сол домендегі басқалардан екі әдістің бірімен ерекшеленеді:

– Нақтылаудың төменгі деңгейінде — сәйкестендіру мақсаттарына теңдес болып саналатын маңыздар тобына жатуы арқылы (бұл жағдайда топ толығымен бір принципиал ретінде қарастырылады және бір айырым идентификаторына ие);

– Нақтылаудың ең жоғарғы деңгейі – бір ғана мағынаны сәйкестендіру.

Түрлі қауіпсіздік домендері арасында сәйкестендіру орын алғанда, мағынаны біржақты баламалауға айырым идентификаторы жеткіліксіз болады, себебі түрлі қауіпсіздік домендерге құзыретті бірдей айырым идентификаторын қолданулары мүмкін. Бұл жағдайда айырым идентификаторлары мағынаның бірегей идентификаторымен қамтамасыз ету үшін қауіпсіздік доменінің идентификаторымен қолданылуы қажет:

– каталогтар аттары(ИСО/МЭК 9594-8);

– тораптық мекен жайлар (ИСО/МЭК 8348);

– қолданбалы процесстер мен қолданбалы деңгейдегі маңыздар аттары (ИСО/МЭК 9545);

– объект идентификаторлары (ИСО/МЭК 8824);

– адамдар аттары (домен контекстегі бірегейлер);

– төлқұжат нөмірлері мен әлеуметтік сақтандыру нөмірлері.

4.1.2 Сәйкестендіру мәні

Мәлімдеуші термині сәйкестендіру мақсатында принципиал болып табылатын немесе өкілі болып табылатын мағынаны сипаттауға қолданады. Мәлімдеуші принципиал атынан сәйкестендірулік айырбасқа қатысу үшін қажетті қызметті қосады.

Верификатор термині өзі түпнұсқаны растайтын мән болып табылатын немесе олардың өкілін сипаттауға қолданылады. Верификатор сәйкестендіру процесінде мәліметтерді ақпараттық айырбасты жүзеге асыруға қажетті қабілетке ие.

Екі жақты сәйкестендіруге тартылған мән, (5.2.4 қараңыз), мәлімдеуші және верификатор ролін қабылдайды.

Сенім артылған үшінші тарап термині қауіпсіздік жөнінде уәкілеттік берілген немесе қауіпсіздікпен байланысты әрекеттерге қатысты басқа мағыналардың сеніміне ие оның агентін сипаттау үшін қолданылады, осы стандарт контекстінде сенім артылған үшінші тарап сәйкестендіру мақсатында мәлімдеуші және/немесе верификатор сеніміне ие болады.

Ескертпе – Мәлімдеуші немесе верификатор бірнеше атқарымдық құрамбірліктер түрінде сипатталуы мүмкін, олар түрлі ашық жүйелерде орналасуы мүмкін.

4.1.3 Сәйкестендіру ақпараты

Төменде сәйкестендіру ақпаратының түрлері берілген:

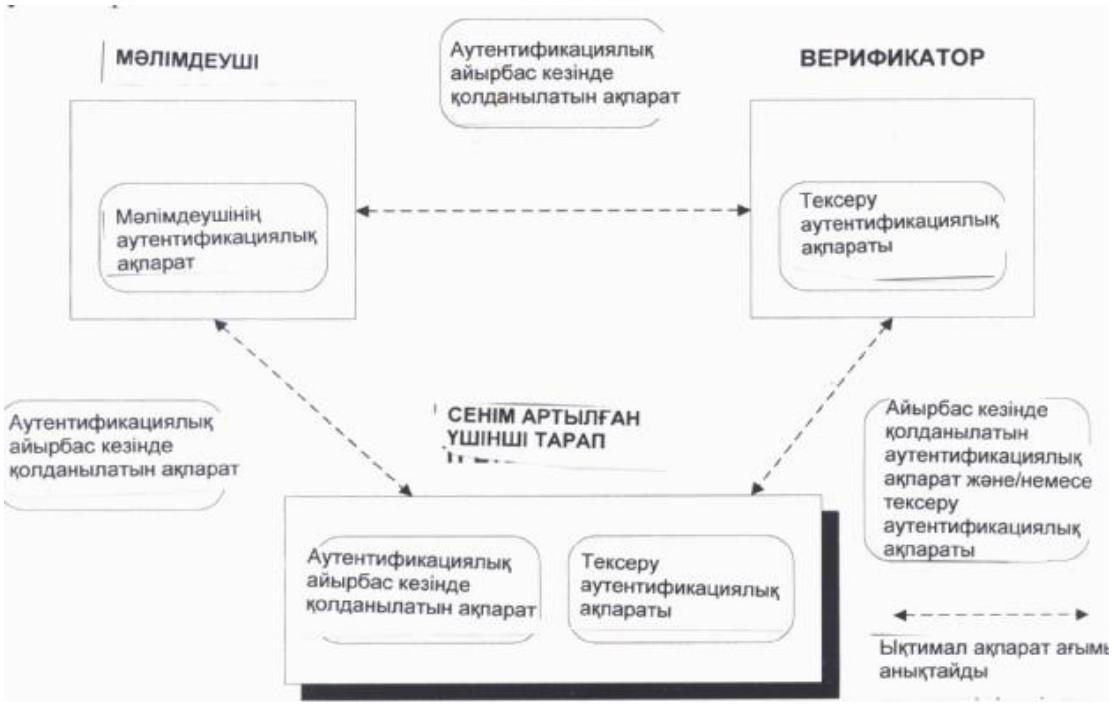
– сәйкестендіру айырбас кезінде қолданылатын ақпарат (ИА айырбас);

– айтылатын сәйкестендіру ақпараты (айтылатын ИА);

– сәйкестендірудің верификаторлық ақпараты (верификаторлық ИА).

Сәйкестендірулік айырбас термині сәйкестендіру мақсатына жету үшін жүзеге асырылатын бір немесе бірнеше ақпарат берілуін сипаттау мақсатында қолданылады.

1-сурет. мәлімдеуші мен верификатор және сенім артылған үшінші тарап арасындағы қатынасты сипаттайды, сонымен қатар сәйкестендіру ақпаратының үш түрін сипаттайды.



1. сурет – Мәлімдеуші, верификатор және сенім артылған үшінші тарап арасындағы қатынас, сонымен қатар сәйкестендірілетін ақпараттың үш түрі

Ескертпе:

1 Кейбір сценарийлерде сенім артылған үшінші тараптарды сәйкестендірулер қолданылмайды.

2 Верификатордың сәйкестендіру ақпаратын принципиал немесе сенім артылған үшінші тарап арқылы берілуі мүмкін (ол туралы толығырақ . 4.5 тармақта көрсетілген).

Кейбір жағдайда ИА айырбасын туындау үшін мәлімдеушіге сенім артылған үшінші тараппен өзара қатынас қажет болады. Осылайша верификатор ИА айырбасын тексеру мақсатында сондай-ақ сенім артылған үшінші тараппен өзара қатынас қажет болуы мүмкін.Бұндай жағдайларда, сенім артылған үшінші тарап Заңсыз қол сұғумен байланысты қатерлерге

қарсы әрекеттер кезінде сәйкестендіруге тұтастық бақылау қызметінің қандай да бір формасымен бірге қолданылуы мүмкін, ол сәйкестендіруге ұқсастықты әрекетпен байланыстырады.

Қайта жасау құқығынсыз нәтиже алу үшін ИА айырбасын қайта қолдану қажет. Қайта жасау әдетте шабуылдың басқа түрлеріне қолданылады, мысалы, мәліметтердің өзгерісі. Сәйкестендіру тетіктердің қайта жасау, алайда біркелкі қарсы тұра алмайды. Қайта жасау қауіпсіздіктің басқа қызметтеріне қауіп төндіреді. Сәйкестендіру қайта жасауға қарсы қолданылуы мүмкін, себебі ол ақпарат көзін орнату құралдарын қолданады.

Принципиалға жататын тексеру ИА ұстаушысы болуы мүмкін. Сенім артылған үшінші тарапты ИА айырбасын беруге қолданылуы мүмкін.

Сәйкестендіру ақпараттың үш түрінің мысалы 6.1. тармағында көрсетілген.

Ескертпе – Куәлік термині барлық жағдайда дұрыс үйлесімді қолданылмағандықтан бұл құжатта ол термин қолданылмайды. *ГОСТ ИСО 7498-2* анықталған *куәлік* термині АІ айырбасы мысалы ретінде қолданылады.

4.2 Сәйкестендіру қызметінің түрлі аспектілері

4.2.1 Сәйкестендіру қауіптері

Сәйкестендіру мақсаты принципиал ұқсастығының кепілдігін қамтамасыз ету болып табылады. Сәйкестендіруді қамтамасыз ету тетіктері заңсыз кіру және көшіру қатерлерін жоюлары қажет.

Заңсыз кіру дегеніміз объектінің басқа бір объект ретінде болуы, яғни басқаша түрмен верификатормен байланысты (мысалы, мәліметтердің шығу тег немесе коммуникациялық өзара әрекет арқылы) басқа объект екендігін білдірмеу. Бұған қайта жасау, жасырын ауыстыру немесе мәлімдеуші компроментациясы жатады.

Заңсыз ену қатерімен әрекет ету барысында беттеседі (мәліметтер шығуымен немесе коммуникациялық өзара қатынас арқылы), оны мәлімдеуші немесе верификатор бастаулары мүмкін. Заңсыз енуден қорғану тұтастықты бақылау қызметін талап етеді, ол осы мәліметтер элементтерін сәйкестендірулік айырбаспен байланыстырады.

Заңсыз енумен байланысты қатерлерге қарсы әрекеттер кезінде сәйкестендіру тұтастықты бақылау қызметінің қандай да бір нысанымен бірге қолданылуы мүмкін, ол сәйкестендіруді ұқсастық әрекетімен байланыстырады.

Қайта жасау құқығынсыз нәтиже алу үшін АІ айырбасын қайта қолдану жатады. Қайта жасау әдетте шабуылдың басқа түрлерімен қолданылады, мысалы, мәліметтерді өзгерту. Сәйкестендіру тетіктерді қайта жасауға біркелкі қарсы тұра алмайды. Қайта жасау қауіпсіздіктің басқа қызметтеріне қауіп төндіреді. Сәйкестендіру қайта жасауға қарсы қолданылуы мүмкін, себебі ол ақпарат көзін орнату құралдарын қолданады.

4.2.2 Сәйкестендіруді өткізу

Кей жағдайларда принципиалдың жүйемен жанаса өзара қатынасқа түсуін талап етілуі мүмкін. Бұндай жағдайларда жүйеде принципиалдың өкілдігі жасалады. Жүйеде өкілдікті жасамас бұрын, принципиал сәйкестендірілуі тиіс.

Принципиал атынан әрекет ете отырып, өкіл принципиалмен бірге сәйкестендірілуі мүмкін. Өкіл өзі принципиал болғандай әрекет етеді, жүйедегі принципиалдың әрекеттері оның тікелей қатысуынсыз орын алуы мүмкін, А қосымшасын қараңыз, онда мысалдар келтірілген.

Егер принципиал болып мәлімдеуші адам табылса, өкілдің әрекет ету уақытының ұзақтығын шектеу тетігі қолданылуы мүмкін, ал қолданушы арнайы бір орында болуы мүмкін.

4.2.3 Бір жақты және өзара сәйкестендіру

Сәйкестендіру бір жақты немесе екі жақты болуы мүмкін. Біржақты сәйкестендіру бір ғана принципиалдың ұқсастығына сенімділікті қамтамасыз етеді. Екі жақты сәйкестендіру екі принципиалдың да ұқсастығын кепілдендіруді қамтамасыз етеді.

Объекттер сәйкестендірілуі бір жақты да екі жақты да бола алады. Сәйкестендіру өз табиғатының шығу тегі жағынан үнемі бір жақты болады.

4.2.4.Сәйкестендірулік айырбасты бастау

Сәйкестендірулік айырбасты мәлімдеуші де верификатор да бастай алады. Сәйкестендірулік айырбасты бастайтын объект сәйкестендіру бастамашысы болып табылады.

4.2.5 Сәйкестендіру ақпаратын жою

Сәйкестендіру ақпаратын жою тексерулік сәйкестендіру ақпараттың үнемі дұрыс болмауымен байланысты. Арнайы жағдайларда қауіпсіздік стратегиясы сәйкестендірілген ақпаратты жоюды талап етуі мүмкін. Сәйкестендірілген ақпаратты жою туралы шешім қауіпсіздікті бұзу жағдайының ашылуымен шартты болуы мүмкін, стратегия өзгеруімен немесе басқа да шешімдермен байланысты болуы мүмкін. Сәйкестендіруші ақпаратты жою қол жеткізуді немесе басқа әрекетке түрткі болуы мүмкін (түрткі болмауы да мүмкін).

Бұдан басқа басқаруға қатысты мына әрекеттер қолданылуы мүмкін:

а) жағдайды тіркеу журналына жазу;

б) жағдай туралы жергілікті деңгейде хабарлау;

в) жағдай туралы алысқа хабарлау;

г) коммуникациялық өзара әрекетті тоқтату.

Әр жағдайға байланысты қабылданатын ерекше шара қауіпсіздік стратегиясына және коммуникациялық өзара әрекетке жататын басқа да

факторларға байланысты немесе принципиал жүйеге тіркелген кезде өзгерістер болғаны немесе активті болуы.

4.2.6 Сәйкестендіру үздіксіздігін қамтамасыз ету

Объект сәйкестендірілуі оның ұқсастығын тек бір белгілі уақытта ғана қамтамасыз етеді. Сәйкестендірудің үздіксіздігін қамтамасыз етуші сәйкестендіру қызметін мәліметтер тұтастығын қамтамасыз ететін қызметпен байланыстыруды қамтамасыз етудің бір жолы болып табылады.

Сәйкестендіру қызметі мен мәліметтер тұтастығын қамтамасыз ету қызметі байланысты, принципиал ең алдымен принципиал сәйкестендіру қызметінің көмегімен сәйкестендіріледі, содан кейін принципиал атынан жіберілетін мәліметтер ИА айырбасымен толықтырылады, ал мәліметтерді өткізу кезінде мәліметтер тұтастығының қызметі қолданылады. Ол ақпараттың басқа объекті арқылы өзгертілмеуін кепілдендіреді және бастапқы сәйкестендірілген принципиалдан шығады. Маңыздысы, мәліметтер тұтастығы ақпараттың принципиалдан верификаторға дейінгі жолдың барлығында мәліметтер тұтастығы қамтамасыз етілуі қажет. Мысалы, егер ақпараттың бір бөлігі сәйкестендірілгеннен басқа принципиал туындаған болса, онда заңсыз ену мүмкін болар еді.

Жойылған объектінің әлі орын алуының кепілдігін алудың басқа жолы әр кезде сәйкестендірулік айырбасты жүзеге асыру болып табылады. Бірақ ол сәйкестендірулік айырбас арасында енуден сақтамайды, және сәйкестендіру үздіксіздігіне кепілдік бермейді.

Мысалы, шабуылдың келесі түрі орын алуы мүмкін: «қаскүнем» кезектегі сәйкестендіруге сұраныс жасағанда, заңды қатысушыға сәйкестендіру жөнінде әрекеттерді орындау мүмкіндігін береді, содан кейін «қаскүнем» қайта басшылықты қолына алады.

Егер тұтастықты тексеру тетігі кілтті талап етсе, онда ол кілт Сәйкестендірулік айырбас кезінде берілген параметрлерден шығуы мүмкін. Ол кілт пен сәйкестендірулік принципиалмен байланысты қамтамасыз етеді, және өз кезегінде екі қызметтің өзара байланысын қамтамасыз етеді.

Тұтастық қызметінің кілт алу жолы келесі түрде жасалуы мүмкін: Сәйкестендіру параметрлерінің негізінде сәйкестендірулік айырбас процессінде қолданылатын әдістер мен алгоритмдер таңдалады

Ескертпе – қауіпсіздік қызметін қолданған кезде, қажетті ақпаратты сәйкестендірулік айырбас яғни құпия кілт кезінде берілетін параметрлерден алу мүмкін.

4.2.7 Бірнеше домен арасында сәйкестендіргіш құрамбірліктерді тарату

Қауіпсіздік домендері егер мәлімдеуші бір доменге, ал верификатор басқа жатса қатынасқа түсуі мүмкін. Қауіпсіздік доменінің келесі түрі мүмкін:

– сәйкестендіру процесінің бастамашысы орналасқан қауіпсіздік домені;

– верификатор орналасқан қауіпсіздік домені; сенім артылған үшінші тараптар орналасқан қауіпсіздік домені;

Жоғарыда көрсетілген домендердің барлығы түрлі болуы тиісті емес.

Қауіпсіздіктің түрлі домендері арасында сәйкестендіру мүмкін болуы үшін қауіпсіз өзара әрекет ету саясатын белгілеу керек.

4.3. Сәйкестендіру кезінде қолданылатын көздер

Жалпы жағдайда сәйкестендіру әдісін таңдау болжамдар тіркесіне немесе келесі бір немесе одан да көп қағидаларға негізделген мүмкіндіктерге байланысты:

бұл қағидалар қатарына мыналар жатады:

а) белгілі бір нәрсе, мысалы, пароль

б) қолда бар бір нәрсе, мысалы, магнитті немесе смарт карточка ;

в) бірқатар өзгермейтін параметрлер, мысалы, биометрлік;

г) сәйкестендіруді жүзеге асыруға сенім артылған үшінші тараптарды жіберу;

д) контекст, мысалы, принципиал мекен жайы

Жоғарыда аталған принциптардың барлығының бөлінбес кемшіліктерін атап өту қажет. Мысалы, белгілі бір нәрсеге негізделген сәйкестендіру, ол иесінің емес қолда бар нәрсенің сәйкестендірілуі болып табылады. Кейбір жағдайларда, кемшіліктер бірнеше принциптер комбинациялары арқылы жойылулары мүмкін. Мысалы, зияткерлік карталарды қолданғанда (қолда бар нәрсе) кемшілік *жеке сәйкестендіру кодын* (белгісіз бір нәрсе) қолданумен жасала алады. Бұдан басқа д) қағидасы ең сезімтал болып табылады, үнемі басқа принциптармен бірге қолданылады.

Атап өтетін жайт, г) қағидасы рекурсияның екі түрін қолданады:

– үшінші тарапты сәйкестендіру үшін баламалау қажет;

– үшінші тараптар жүргізетін сәйкестендіру төртінші тарапты тартуды талап етуі мүмкін, және әрі қарай жалғасады.

Аталып өткен қағидаларды қолданатын шынайы әдістердің сараптамасы онда қатысып отырған объектілер мен құралдары тура анықтауы қажет.

4.4. Сәйкестендіру сатылары

Сәйкестендіру процессі мына сатыларға бөлінеді:

– орнату сатысы;

– сәйкестендірулік ақпаратты өзгерту сатысы;

– тарату сатысы;

– алу сатысы;

– өткізу сатысы;
– тексеру сатысы;
– блоктау сатысы;
– блоктан шешу сатысы;
– құрастырылымды бұзу сатысы.

Аталған сатылар міндетті түрде уақыттарға бөлінбейді, олар бір уақытта жүре берулері мүмкін.

Сәйкестендірудің тура сызбасына барлық кезең міндетті болып табылмайды. Сонымен қатар, бірқатар жағдайларда сатылар кезектілігі келтірілген сипаттан ауытқуы мүмкін.

4.4.1 Орнату сатысы

Орнату сатысында мәлімдеуші мен сәйкестендірілетін ақпараттың верификаторы анықталады.

4.4.2 Сәйкестендіру ақпаратының өзгеру сатысы

Сәйкестендіру ақпараты өзгерту сатысында принципиал немесе менеджер мәлімдеуші немесе верификатордың (мысалы, парольдің өзгеруі) сәйкестендіру ақпаратының өзгеруіне түрткі болады.

4.4.3 Тарату сатысы

Сәйкестендіру ақпаратын тарату сатысында объектілерге ақпараттың сәйкестендіру айырбасына қолдану үшін объектілерге (мәлімдеушіге, верификаторға) жеткізіледі.

Мысалы, автономды әдістерді қолдануда объектілер осы сатыда сәйкестендіру сертификаттарды, жойылған сертификаттар тізімін, жойылған құзыреттер тізімін алады. Тарату сатысы өткізу сатысының алдында, бір уақытта, өткеннен соң болуы мүмкін.

4.4.4 Жинау сатысы

Қабылдау сатысы кезінде мәлімдеуші немесе верификатор сәйкестендіруді жүргізуге қажетті арнайы сәйкестендіру ақпаратын тудыруға қажетті ақпаратты алады. Түрлі процедуралар сенім артылған үшінші тараптан AI айырбасын алады немесе сәйкестендіру процесіне қатысушы объектілер арасында ақпараттар алмасуы арқылы жүзеге асырылады.

Мысалы, кілттерді тарату оперативті орталығын қолданған кезде мәлімдеуші мен верификатор бірқатар ақпарат мысалы сәйкестендіру сертификатын алады. (6.1.3. тармағын қараңыз).

4.4.5 Өткізу сатысы

Өткізу сатысында мәлімдеуші мен верификатор арасында сәйкестендіру ақпаратымен алмасу жүзеге асырылады.

4.4.6 Тексеру сатысы

Тексеру сатысына ИА айырбасы ИА тексеруімен салыстырылады. Осы сатыда объект өздігімен ИА айырбасын жүзеге асыра алма Тексеруін жасайтын сенім артылған үшінші тарапқа барады. Бұл жағдайда сенім артылған үшінші тарап оң немесе теріс жауап қайырады.

4.4.7 Блоктау сатысы

Блоктау сатысында бұрын сәйкестендірілуі мүмкін принципиал уақытша сәйкестендірілмеуі мүмкін жағдайын белгілейді.

4.4.8 Блоктан шешу сатысы

Блоктан шешу сатысында блоктау сатысында басталған іс аяқталады.

4.4.9 Бұзу сатысы

Құрастырылымды бұзу сатысында принципиал қағидалар бірлестігінен жойылады.

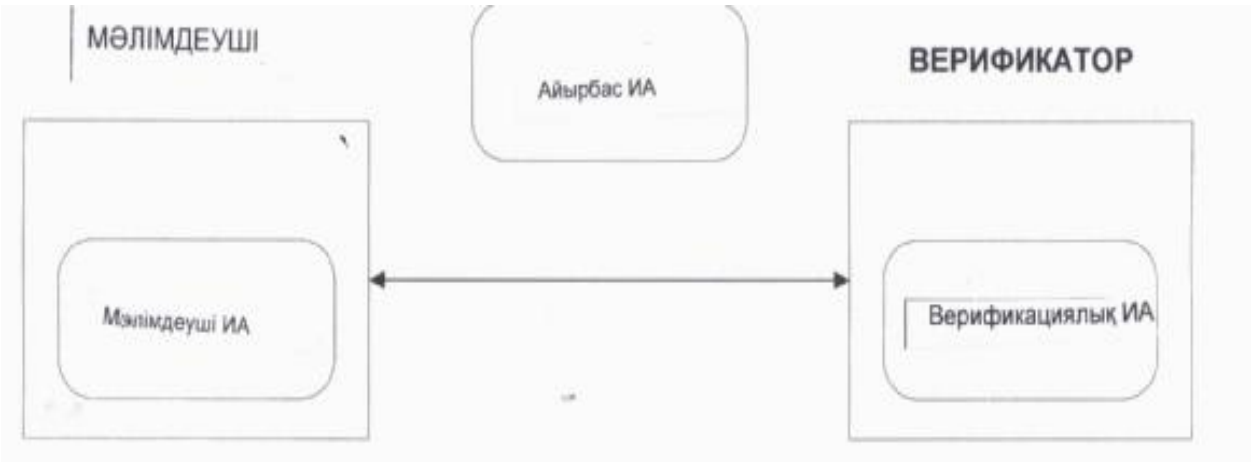
4.5 Сенім артылған үшінші тараптың қатысуы

Сәйкестендіру тетіктерін сәйкестендіруге қатысқан сенім артылған үшінші тараптар санымен сипаттауға болады.

4.5.1 Сенім артылған үшінші тараптың қатысуынсыз жүргізілетін сәйкестендіру

Ең қарапайым жағдайда, АІ айырбасы және айырбас верификациясы кезінде мәлімдеуші де верификатор да басқа объектілерді қолданбайды. Бұндай жағдайда, принципиалға арналған тексеру сәйкестендіру ақпаратын верификаторда орнатуы қажет.

Бұндай әдіс ірі масштабты коммуникациялық ортада шектелген күйде және объектілердің көбісінде екі жақты әрекет жөнінде әріптестерінің саны шектелген болса ғана қолданыла алады. Ең нашар жағдайда әр верификатор қауіпсіздік доменінің барлық принципиалдарына арналған тексеру АІ ие болулары қажет, осыған байланысты ақпараттың жалпы көлемі бар объектілердің сандарының екі дәрежесіне тең.(2 суретті қараңыз)



.

2 сурет – Сенім артылған үшінші тарапсыз сәйкестендіру

4.5.2 Сенім артылған үшінші тараптың қатысуымен сәйкестендіру

Тексеру ИА сенім артылған үшінші тараппен өзара қатынасқа түсу нәтижесінде пайда болады. Ол ақпараттың тұтастығы кепілдендірілуі қажет. Сонымен қатар мәлімделген ИА мен тексеру ИА сенім артылған үшінші тарапқа кепілдік ету қажет, егер мәлімдеуші ИА оның негізінде енгізілуі мүмкін.

Сәйкестендіруде бір сенім артылған тарап немесе 5.3. тармақтағы г) қағидасында сенім артылған үшінші тараптардың тізбегі қатыса алады. Қосымша сенім артылған үшінші тараптарды енгізу үлкен объектілердің жиынтығын сәйкестендіру мүмкіндігін береді, сенім артылған әр тарап тек шектелген объект (барлық объектілер туралы емес) сандары туралы ғана ақпаратты қолдайды. Осылайша, ақпараттың жалпы көлемі объектілер санынан желілік түрде өседі.

Мультиобъектік қатынасты объектілер (объектілер арасындағы актив байланыстар саны) өзара қатынастарының талабына сай сипатталуы мүмкін, сонымен қатар сәйкестендіруді басқаруда қандай құзыретке ие екендеріне қарай, мысалы, сәйкестендірілетін ақпаратты жоққа шығаруды ұстау мүмкіндігі.

4.5.2.1 Кірістірілген сәйкестендіру

Кірістірілген сәйкестендіру жағдайында сенім артылған үшінші тарап сәйкестендірулік айырбас кезінде мәлімдеуші мен верификатор арасында делдал қызметін атқарады. Принципиал делдал арқылы сәйкестендіріледі, ол содан кейін оның келесі кірістірілген сәйкестендіру айырбастағы ұқсастығын растайды.

Орнатылған сәйкестендіруде верификатордың делдалға принципиалды дұрыс сәйкестендірілуіне сенім артуын талап етеді, сонымен қатар сәйкестендіру арқылы делдалдың ұқсастығына көзі жетті.

Кей жағдайда сәйкестендірудің бұндай сызбасы сенім артылған делдалдар тізбегіне дейін кеңейтіледі. Жүзеге асырылып жатқан қауіпсіздік стратегиясына байланысты соңғы сенім тізбектегі артылған үшінші тарап делдалдар тізбегінің туралығын тексеруге жауапты.

3 сурет – Орнатылған Сәйкестендіру

4.5.2.2 Оперативті сәйкестендіру

Оперативті сәйкестендіру жағдайында бір немесе бірнеше сенім артылған тараптар сәйкестендірулік айырбастың әр жағдайына қатысады. Алайда орнатылған сәйкестендіруден айырмашылығы оперативті сәйкестендіру жағдайында сенім артылған үшінші тараптар мәлімдеуші мен верификатор арасындағы сәйкестендірулік айырбастың жолында тікелей орналаспаған. Оперативті сәйкестендіру кезінде сенім артылған үшінші тараптарды ИА айырбасын құру үшін және ИА айырбасын тексеруде верификаторға жәрдемдесу үшін сұралуы мүмкін.

Оперативті сенім артылған үшінші тарап оперативті түрде қол жеткізерлік сәйкестендіру сертификаттарды құра алады (6.1.3 тармақты қара).

Оперативті сәйкестендіру верификатор мен сенім артылған үшінші тараптар арасында АІ айырбасын туындауға ат салысатын кезінде сенім артылған үшінші тараптар тізбегі болуы қажет. Бұл тізбек мәлімделген АІ принципиалының дұрыстығын тексеруге қабілетті болулары қажет. Ең қарапайым жағдайда мәлімдеушімен немесе верификатормен тікелей байланыстағы тек бір ғана сенім артылған үшінші тарап қана қажет болады. Бұл жағдай алайда мәлімдеуші немесе верификатормен тікелей немесе жанама әрекет етуші сенім артылған үшінші тараптардың тізбегіне дейін үлкеюі мүмкін.

Сәйкестендіру мүмкіндіктерін жоққа шығару сәйкестендірулік талпыныстарда түбегейлі бақылануы мүмкін.

Оперативті түрде қол жеткізерлік сенім артылған үшінші тараптар сәйкестендіру серверлері мен кілтті тарату орталықтары болып табылады.

4 сурет – Оперативті Сәйкестендіру

Ескертпе – Суреттегі үш түрлі объектілер арасында қолданылатын ИА айырбасы ортақ біреу болуы мүмкін емес.

4.5.2.3 Автономды сәйкестендіру

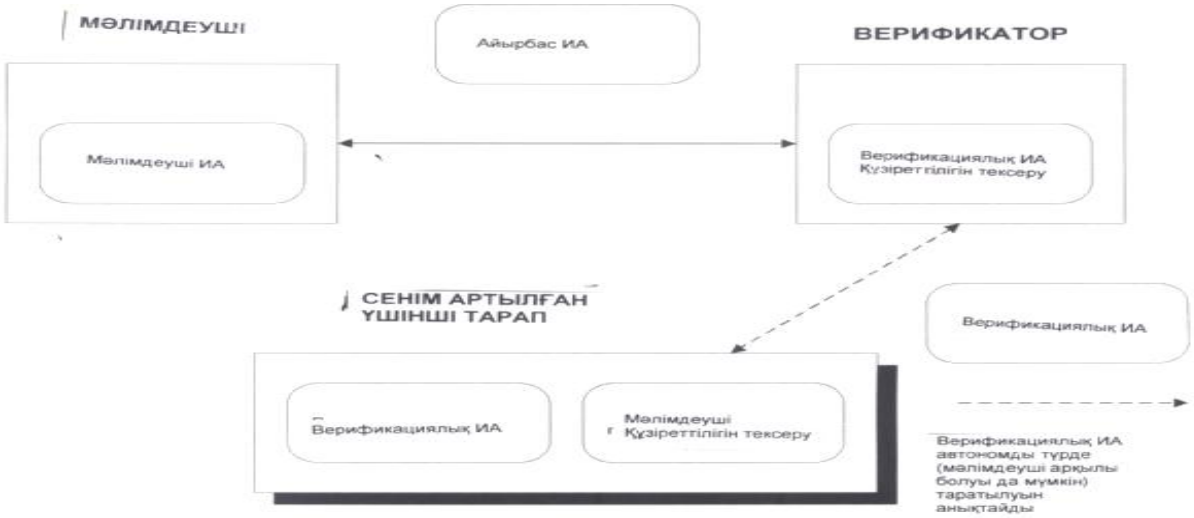
Автономды сәйкестендіру жойылған сертификаттардың расталған тізімін қолдану қажеттілігімен сипатталады, онымен қатар сертификаттар жарамдылық уақыты немесе шұғыл реакцияны талап етпейтін сәйкестендіру ақпаратты жоюдың басқа жолдары есепке алынады.

Автономды сәйкестендіру жағдайында бір немесе бірнеше сенім артылған үшінші тараптар сәйкестендіруді әр бөлек процесінде оған араласусыз қолдайды.

Автономды сенім артылған үшінші тараптар уақытынан бұрын автономды сәйкестендіру сертификаттарын жасап, таратады, оларды соңынан верификатор сәйкестендірулік айырбас дұрыстығын тексереді. Осылайша, сәйкестендіру процесі автономды түрде қауіпсіздік органының қатысуынсыз жүзеге асырады.

Сенім артылған үшінші тараптарға сәйкестендіру процесінде мәлімдеушімен де верификатормен де тікелей әрекет ету қажеттілігі жоқ болғандықтан, бұл әдіс өзара әрекет санына қатысты тиімдірек болып табылады.

Жою кезінде жарамдылық мерзімі өту, сертификаттарды жаңарту, жойылған сертификаттардың куәландырған тізімі секілді қосымша шаралар көзделуі қажет.



5 сурет – Автономдық сәйкестендіру

Сертификаттарды беру органдары ретіндегі мысалдар 6.1.3. тармақта келтірілген.

4.5.3 Мәлімдеушінің верификаторға сенім артуы

Верификаторға сенім арту қажетті тетіктер егер барлық мүмкін верификаторларға сенім артуға болмайтын болса онда балама болмай шығады. Бұл верификатор ұқсастығының сәйкестендірмегенімен және оған деген сенім деңгейінің белгісіз болуымен байланысты. Мысалы, сәйкестендіру үшін қарапайым парольдерді қолдану кезінде верификатор парольді екінші рет қолдануға сақтамағанына сену қажет.

4.6 Принципиал түрлері

Принципиалдар санаттар бойынша мына түрге бөлінеді:

а) пассив қасиеттерге ие мысалы, сәйкестендіру белгісі, биометрикалық сипаттама;

б) ақпараттық айырбас пен мәліметтер өңдеу құралдарына ие;

в) ақпаратты сақтау мүмкіншілігі бар;

г) бірегей және белгіленген орында орналасқандар.

Принципиалдар бір санаттан көбіне жатқызылуы мүмкін [мысалы, адамдар а), б), с) категориялар талаптарын қанағаттандырулары мүмкін]. Онымен қатар сәйкестендірудің түрлі әдістері қолданылады:

а) пассив сипаттамаларды өлшеу;

б) сұраныс/жауап секілді күрделі процедуралар;

в) құпия ақпаратты еске сақтау (мысалы, пароль);

г) орналасқан жерін анықтау.

4.7 Қолданушы адамдарды сәйкестендіру

Сәйкестендірудің жеке жағдайы болып адам атынан қызмет атқаратын процесс емес адамды сәйкестендіру болып табылады.

Қолданушы адамдар сәйкестендіру әдістері экономикалық жақтан мақсаты бар және сенімді адамдарға қатысты ыңғайлы болып табылады. Ыңғайсыз әдістер қолданушыларды сәйкестендіру процедурасынан аулақ болатын жолдарды іздестіруге түрткі болады, және ол заңсыз ену қатерін ұлғайтады.

Адамдар сәйкестендірілу әдістері 5.3. тармақта көрсетілген қағидаларға негізделген. Қолданушы адамдардың сәйкестендірулері 5.4. тармақта көрсетілген сатыларға негізделген.

А қосымшасы қолданушы адамдар сәйкестендірілуі жайында, олардың атынан қызмет ететін процесстер туралы ақпаратқа ие.

4.8 Сәйкестендіруге шабуыл түрлері

Шабуылдың үш түрі сөз болады:

– *қайта жасау шабуылдары,* ИА айырбасы оқылады, ал соңынан қайта жасалады;

– *«қаскүнемнің» бастаған өткізу шабуылдары;*

– *«қаскүнем» жауаптылар болып табылатын өткізу шабуылдары.*

АІ айырбасын өткізу шабуылдарында жедел береді

4.8.1 Қайта жасау шабуылдары

Қарастыруды қажет ететін қайта жасау шабуылдарының екі жағдайы бар, оған АІ қайта жасау жатады; сол верификаторға; басқа верификаторға жатады.

Соңғы оқиға бір принципиалдың верификаторлық ақпараты бірнеше верификаторларға белгілі болған жағдайда ғана орын алуы мүмкін. Сәтті қайта құру заңсыз кірудің ерекше жағдайы болып табылады.

Қайта жасау шабуылының екі түріне де төтеп беру шақырулар арқылы жүзеге асырылады. Шақыруларды верификаторлар жасайды. Бір шақыруды верификатор екі рет жасамайды. Оған бірнеше жолдар арқылы қол жеткізуге болады. (С қосымшасын қараңыз).

4.8.1.1 Сол верификаторға қайта жасау

Бір верификаторға төтеп беру тек бірегей номерлерді немесе шақыруларды қолдану арқылы ғана мүмкін болады. Бірегей номерлерді мәлімдеуші жасайды. Бір бірегей номер бір верификатормен екі рет қолданылмайды. Оған бірнеше жолдар арқылы қол жеткізуге болады. (В қосымшасын қараңыз).

4.8.1.2 Верификаторға қайта жасау

Басқа верификаторға қайта жасауға шақырулар арқылы төтеп беруге болады. Бұдан басқа бұл шабуыл түріне AI айырбасы кезінде верификаторға бірегей болып табылатын есептеу кезіндегі кез келген параметрді қолдану арқылы қарсы тұруға болады. Бұндай сипатқа верификатор аты немесе оның тораптық аты болады, жалпы жағдайда верификаторға бірегей болып табылатын кез келген белгіні тексеру сәйкестендіру ақпараты қолданады.

4.8.2 Өткізу шабуылдары

5.8.2.1 Қаскүнемдер бастаған өткізу шабуылдары

Шабуылдың бұл түрінде «қаскүнемдер» сәйкестендіру бастамашысы болып табылады. Бұл шабуыл тек егер мәлімдеуші мен верификатор сәйкестендіруді бастай алса ғана мүмкін болады. Шабуыл жасау процесінде мәлімдеуші мен верификатор ол туралы білместен «қаскүнем» арқылы аутентификациялық ақпарат айырбасын жүзеге асырады, яғни «қаскүнем» мәлімдеуші алдында верификатор, ал верификатор алдында мәлімдеуші болып алдайды.

Мысалы, С «қаскүнем» В верификаторы алдында А мәлімдеуші болғансыса, С әсерін А мен В-дан бастайды. С А-ға В-мын деп хабарлайды, А В-ға қатысты сәйкестендіруді сұрайды, сонымен қатар В-ға А-мын деп айтып өзін сәйкестендірілуін сұрайды.

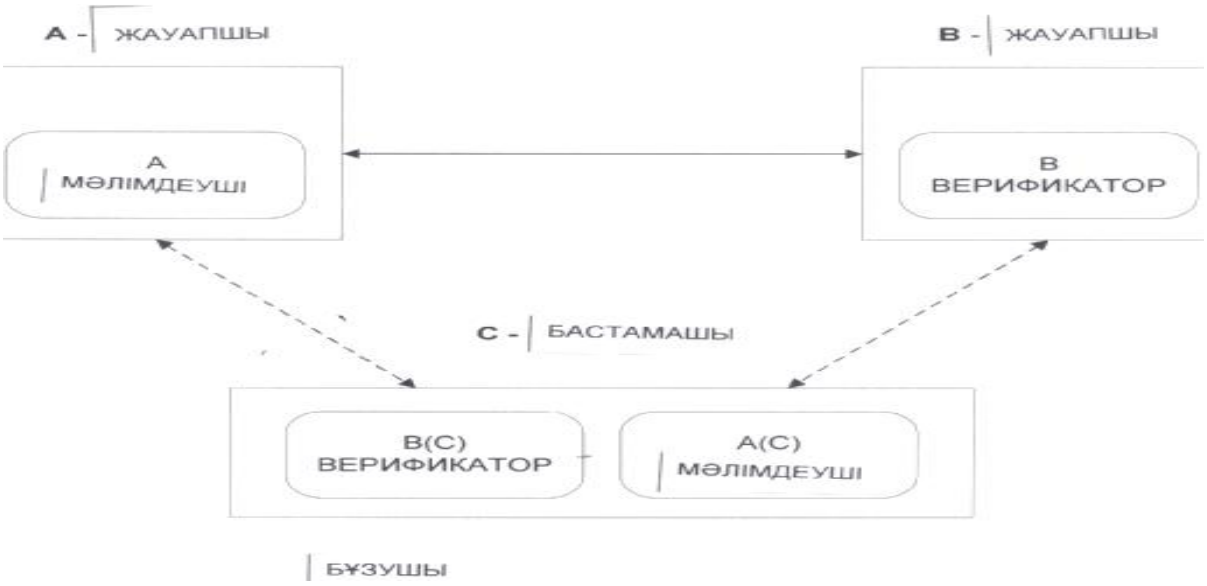
4.8.2. Қайта бағыттау шабуылдар

4.8.2.2 Қаскүнем жауап беретін өткізу шабуылдары

Шабуылдың бұл түрінде «қаскүнем» Сәйкестендірулік айырбасқа тікелей қатысады, Сәйкестендірулік ақпаратты қамтып, өзі бастамашы рөліне енеді. Шабуылдың бұл түрі «қаскүнемді» байқаусызда жауапты ретінде қабылданып немесе жүйелік түрде жауапты ретінде әрекет ету (мысалы, ресурстарды орналастыру орталық кестесі) шабуылға жағымды жағдайлардың тууына ғана байланысты.

Аталған шабуыл түріне төтеп беру және ары қарай мәліметтерді айырбастау мақсатында қосымша қызметтерді (мәліметтер тұтастығы немесе қауіпсіздік) қолдануды талап етеді. AI айырбасы басқаша ақпаратпен біріктіріледі егер мәлімдеуші мен верификатор Сәйкестендірудің заңды қатысушылары болса кілттер жасау мүмкіндігін береді. Бұл кілттер соңынан криптографиялық тетіктерде тұтастық пен қауіпсіздік бақылауы үшін қолданылады.

Бұл шабуылға қарсы тұруға мәліметтер беру торабында мәліметтерді ұстап қалу мүмкіндігі болмаған жағдайда пайда болады, яғни мәліметтер үнемі өзгертілмейтін дұрыс мекен жайға жіберіледі. Бұл жағдайда AI айырбасына (яғни тораптық мекен жайды қол ретінде қолдану) тораптық мекен жайды енгізу арқылы төтеп беруге болады



6 сурет – Бұзушының бастаған қайта бағытталған шабуылы

Сәйкестендіру барысында А В-ға қатысты мәліметші ретінде әрекет етеді, (шын мәнінде В рөлінде С ойнайды) сондықтан С В-ға қатысты сәйкестендіру мақсатында қолданатын ақпаратты алады. В верификатор рөлін орындайды сондай ақ С ақпаратын береді, оны соңғысы верификатор ролін ойнауға қажет етеді. Сәйкестендіруден кейін «қаскүнем» С В алдында сәйкестендірілген А секілді көрінеді.

Аталған шабуыл түріне қарсы тұру әдістері түрлі верификаторларға арналған қайта жасаудан сақталады:

а) Сәйкестендіруді бастаған объект үнемі мәлімдеуші болады (аталатын жадай, екі жақты сәйкестендіру кезінде мүмкін емес болады) немесе;

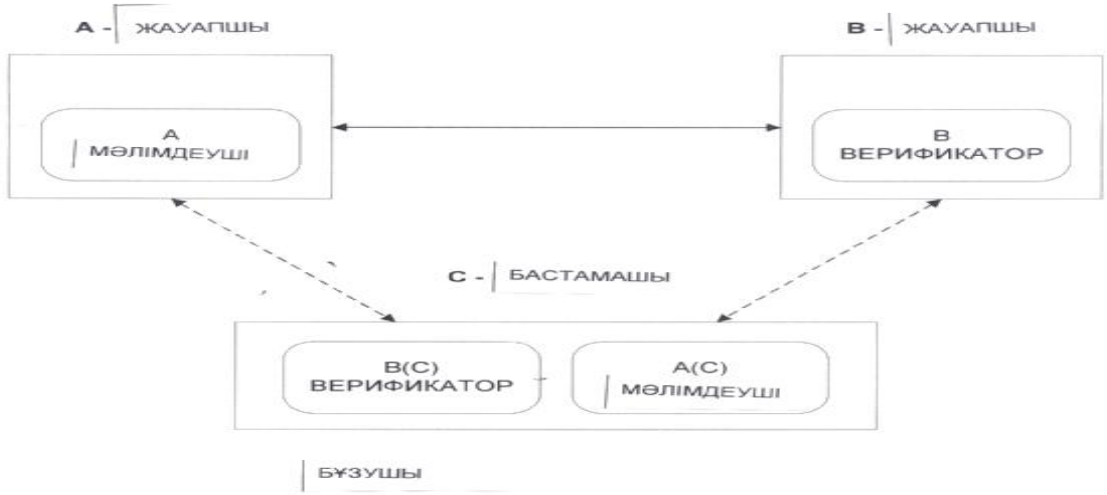
б) айырбас кезінде қолданылатын және оны мәлімдеуші берген аутентификациялық сұраныс бастамашысы немесе сәйкестендіру шақыруына жауапты ретіндегі рөліне байланысты болады. Бұл айырмашылық верификаторға жоғарыда қарастырылған шабуыл түрін анықтауға мүмкіндік береді. Бұл Г қосымшасында толығырақ көрсетілген.

4.8.2.2 «Қаскүнем» жауап беретін өткізу шабуылдары

Шабуылдың бұл түрінде «қаскүнем» сәйкестендірулік айырбасқа тікелей қатысады, сәйкестендір ақпаратты қамтып, өзі бастамашы рөліне енеді. Шабуылдың бұл түрі «қаскүнемді» байқаусызда жауапты ретінде қабылданып немесе жүйелік түрде жауапты ретінде әрекет ету (мысалы, ресурстарды орналастыру орталық кестесі) шабуылға жағымды жағдайлардың тууына ғана байланысты.

Аталған шабуыл түріне төтеп беру және ары қарай мәліметтерді айырбастау мақсатында қосымша қызметтерді (мәліметтер тұтастығы немесе қауіпсіздік) қолдануды талап етеді. АІ айырбасы басқаша ақпаратпен біріктіріледі егер мәлімдеуші мен верификатор сәйкестендірудің заңды қатысушылары болса кілттер жасау мүмкіндігін береді. Бұл кілттер соңынан криптографиялық тетіктерде тұтастық пен қауіпсіздік бақылауы үшін қолданылады.

Бұл шабуылға қарсы тұруға мәліметтер беру торабында мәліметтерді ұстап қалу мүмкіндігі болмаған жағдайда пайда болады, яғни мәліметтер үнемі өзгертілмейтін дұрыс мекен жайға жіберіледі. Бұл жағдайда АІ айырбасына (яғни тораптық мекен жайды қол ретінде қолдану) тораптық мекен жайды енгізу арқылы төтеп беруге болады.



7 сурет – Бұзақылық жасаушы қайта бағытталған шабуылдар үшін жауапты

Ескертпелер

1 «қаскүнем» бастаған шабуылдарға жауап ретінде 5.8.2.1 тармағындағы а) немесе б) әдістерін қолдану арқылы контршаралар қолданса да, Сәйкестендіру әдісі «қаскүнем» жауабы кезінде Сәйкестендіру әдісі әлсіз болып табылады.

2 X(Y) жазуы X өзін Y деп танытатынды білдіреді.

5 Сәйкестендіру ақпараты мен құралдары

5.1 Сәйкестендіру ақпараты

5.1.1 Мәлімденген сәйкестендіру ақпараты

Мәлімделген ИА–принципиал сәйкестендірілуіне қажетті АІ айырбасының пайда болуына түрткі болады.

Мәлімделген сәйкестендіру ақпараттар мысалы:

а) **пароль;**

б) **құпия кілт**. *Бұл құрал симметриялық алгоритмді қолданатын*

сәйкестендірулік тетіктерді қолдануға қажетті;

в*)* **жабық кілт.** *Бұл құрал асимметриялық алгоритмді қолданатын сәйкестендірулік тетіктерді қолдануға қажетті;*

5.1.2 Тексерілетін сәйкестендіру ақпараты

Тексерілетін ИА - ИА айырбасы көмегімен мәлімденген ұқсастықты тексеруге қолданылатын ақпарат болып табылады.

Тексерілетін сәйкестендіру ақпаратының мысалдары:

а) **Пароль** принципиал ұқсастығымен байланысты;

б*)* **Құпия кілт** принципиал ұқсастығымен немесе қауіпсіздік органы симметриялық алгоритмдер қолданатын Сәйкестендірулік тетіктеріне арналған.;

в**) ашық кілт,** принципиал ұқсастығымен немесе қауіпсіздік органы асимметриялық алгоритмдер қолданатын Сәйкестендірулік тетіктеріне арналған.;

Тексеру ИА сәйкестендіру кестесі және/немесе автономды сәйкестендіру сертификаты ретінде көрсетілген (6.1.4.2 тармағын қара).

Сәйкестендірулік қасиет верификаторға тікелей қол жеткізерлік объектілер кешені болып табылады. Кестеге қол жеткізуге қолданатын әдіс тұтастық қорғанысын және симметриялық алгоритмдерге қосымша қауіпсіздік қорғанысын қамтамасыз ету қажет.

Сәйкестендіру кестеге кіруге болатын элементтер мысалдары:

– Принципиал ұқсастығы;

– Тексеру ИА, мысалы, пароль, құпия немесе жалпы кілт; кестеге ену жарамдылық мерзімі;

– Кестеге кіруге қолданылатын қауіпсіздік стратегиясы, кестеге кіруге жауапты қауіпсіздік органы;

5.1.3 Айырбас кезінде қолданылатын сәйкестендіру ақпараты

ИА айырбасы –принципиал сәйкестендірілуі кезінде мәлімдеуші мен верификатор арасында айырбасталатын ақпарат.

ИА айырбас мысалдары:

– мәлімденген бірегей идентификаторы;

– пароль;

– шақыру;

– шақыру жауабы;

– бірегей номері;

– тексеру бірегей сәйкестендіргіші;

– мәлімденген ИА мен басқа мәліметтерге (яғни уақытша белгіге, кездейсоқ санға, есепшіге, шақыруға, верификатор атына, сандық идентификациялық белгіге, мәлімдеуші атына) айналу қызметін қолдану

нәтижесі: түрлену қызметтерінің мысалдары болып біржақты түрлену қызметтері, шарттанудың симметриялық қызметтері бола алады;

– оперативті түрде қол жеткізерлік сәйкестендіру сертификаты;

– автономды сәйкестендіру сертификаты.

ИА айырбасының бөлігі немесе толығымен бір ретте берілетін қауіпсіздік белгісі нысанында болады.

5.1.4 Сәйкестендіру сертификаты

Сәйкестендірілетін ақпараттың қарапайым нысаны сәйкестендіру сертификаты болады. Сәйкестендіру сертификаты сенім сенімді қауіпсіздік органы куәландырған және сәйкестендіру кезінде қолданылатын ақпарат.

Сәйкестендіру сертификаттардың түрлі типтері:

– оперативті түрде қол жеткізерлік сәйкестендіру сертификаты;

– автономды сәйкестендіру сертификаты;

– сәйкестендіруді жою сертификаты;

– жойылған сәйкестендіру сертификаттарының тізімі.

Автономды сәйкестендіру сертификаттары (6.1.4.2 тармағын қара) жалпы кілтпен біріктірілген ИА тексеруіне қатысты қолданылады. Автономды сәйкестендіру сертификатын жою сертификаты немесе жойылған сертификаттар тізімі көмегімен жойылуы мүмкін.

Төменде кез келген сәйкестендіру сертификат құрамында болатын элементтермен мысалдар келтірілген:

– Криптографиялық бақылау белгісін жасау мақсатында қолданылатын әдіс және/немесе кілтті анықтау.

– Сертификат берген сәйкестендіру органы және/немесе агентінің ұқсастығы (орган бірнеше агенттермен өкілдік еткен кезде агент ұқсастығы агенттік қай кілті қолданғандығын анықтау мүмкіндігін береді).

– Сәйкестендіру сертификатын жасау уақыты (құру уақыты тексеру үшін қолданылады, сонымен қатар сәйкестендіру сертификаттың жарамдылық уақыты көрсетілмеген жағдайда және қауіпсіздік стратегиясына сәйкес өте ескі сертификаттар қайтарылып берілуі мүмкін.

– Сәйкестендіру сертификаттың (жарамдылық уақыты алушыға қауіпсіздік стратегиясы оны жасауға мүмкіндік бергенде қолданылады, басқаша жағдайда сертификаттың жарамдылық мерзімінің өтуі алушының қауіпсіздік стратегиясын жасау уақытына негізделеді) жарамдылық уақыты (сертификат жарамдылық мерзімінен бұрын да, соңынан да қолданыла алмайды)

– Сәйкестендіру сертификатпен бірге қолданатын қауіпсіздік стратегиясы.

– Аталған әкімшілік агентіне бірегей болып табылатын сертификаттың сілтеме нөмірі.

– Сертификат түрі.

– Сәйкестендіру сертификаты арналып жасалған верификатордың ұқсастығы немесе белгілері (объектілер көрсетілген егер бар болса көрсетілген мағыналарды тексере алады және мәліметі дұрыс емес сертификаттарды жоққа шығара алады. Ұқсастық/белгілер, мысалы, қолданушы адамның аттары, процесстердің және/немесе физикалық машиналар сәйкестендіргіш аттары бола алады).

Түрлі сәйкестендіру сертификаттарға қосымша элементтері түрлі қосалқы класстарға жатқызылады. Арнайы стандарттарда қандай элементтер міндетті, қандай міндетті емес болып табылатындығы көрсетілген пішіндер берілуі мүмкін.

5.1.4.1 Шұғыл түрде қол жеткізерлік сәйкестендіру сертификаттары

Шұғыл түрде қол жеткізерлік сәйкестендіру сертификаттар мәлімдеушінің сұранысы бойынша сенім артылған үшінші тарап арқылы жасалады. Оперативті түрде қол жеткізерлік сәйкестендіру сертификаты әдетте верификаторға ИА айырбасының бөлігі ретінде беріледі.

Төменде сәйкестендіру сертификатында орын алуы мүмкін қосымша элементтер мысалдары келтірілген:

– Принципиалдың бірегей сәйкестендіргіші.

– Мәліметтердің шығу тегінің сәйкестендірілуі қолданған кездегі сандық сәйкестендіру белгі.

– Кілтпен қоса қолдануға қажетті алгоритмді көрсету арқылы сәйкестендіруді жүзеге асыру үшін принципиалға берілген симметриялық кілт. Бұл жағдайда ақпараттың құпиялығын қамтамасыз ету қажет.

– Аталған сәйкестендіру сертификатын алуға қолданылатын балама әдіс.

– Сәйкестендіру сертификаты бірге қолданылатын сәйкестендіру әдістер (тер).

– Өткізу кезінде сәйкестендіру сертификатын қорғау мақсатында қолданылатын әдісті көрсету, сонымен қатар осындай қорғанысты қамтамасыз етуге қажетті әдістермен байланысты параметрлер жиынтығы. (Бұндай параметрлердің мысалдары болып шақыру, бірегей номер және қорғаныс кілті бола алады).

5.1.4.2 Автономды сәйкестендіру сертификаты

Автономды сәйкестендіру сертификаты нысанды криптографиялық кілтпен байланыстырады**.**

Сертификатты орган жасайды, және бұл жерде мәлімдеуші мен верификатордың осы органмен тікелей өзара қатынасқа түсуінің қажеттілігі жоқ. Автономды сертификаттар әдетте ассиметриялық алгоритмдерді қолданатын сәйкестендіру тетіктермен қолданылады. Сәйкестендіру

сертификаты айырбас кезінде қолданылатын сәйкестендіру ақпаратының бөлігі ретінде верификаторға беріледі.

Төменде автономды сәйкестендіру сертификаты құрамында болатын элементтер мысалдары келтірілген:

– Принципиалдың бірегей сәйкестендіргіш;

– принципиалға сәйкестендіру органы берген жалпы кілт және жалпы кілтпен қолданылатын алгоритмді көрсеткен.

Автономды сәйкестендіру сертификатын жою сертификаты немесе жойылған сертификаттар тізімі көмегімен уақытынан ерте тоқтатуға болады.

5.1.4.3 Жою сертификаттары

Жою сертификаттары қауіпсіздік органдарының осы сәйкестендіру сертификатының жойылғанын білдіру мақсатында берген қауіпсіздік сертификаты болып табылады. Ақпарат сақталып, аталған сәйкестендіру сертификаты жарамды екенін анықтау мақсатында қолданылады.

Төменде жою сертификатында жою сертификатының құрамында болуы мүмкін қосымша элементтер мысалдары көрсетілген:

– принципиал, принципиалдар тобы немесе уәкілеттінің сәйкестендіргіш деректері;

– автономды сәйкестендіру сертификаты шақырылған күн мен уақыты;

– жойылған сертификаттың сілтеме нөмірі.

5.1.4.4 Жойылған сертификаттар тізімі

Жойылған сертификаттар тізімі дегеніміз аталған қауіпсіздік органдары жойған куәландырған сертификаттар тізімі, уақыты мен күні көрсетілген тізім. Бұл ақпарат сақталады және қолдағы бар сертификаттарға қатысты, сонымен қатар сәйкестендіру сертификатының жарамдылығын анықтайды. Жойылған сертификаттар тізімі мыналарды қамтуы мүмкін:

– жою сертификаттары;

– жою сертификаттарының сілтемелік идентификаторы;

– сәйкестендіру сертификаттарын жою;

– жойылған сертификаттардың сілтеме идентификаторлары;

– тізімнің шығарылған күні;

– келесі тізімнің шығарылған күні.

5.1.4.5 Сертификаттар тізбектері

Сәйкестендіру сертификаттары мәліметтердің шығу тегін үшінші тараптан сәйкестендірілуін қамтамасыз ететіндей болып қорғалған.

Егер верификатордың сертификаттың шығу тегін тексеру үшін тексеретін АІ болмаса, сертификаттар тізбектері қолданылуы мүмкін. Басқа қауіпсіздік органынан алынған бірінші сертификат тексеруші ИА-ны растау мақсатында қолданылған.

Сертификаттар тізбегі рекурсивті түрде қолданылулары мүмкін, осы сертификаттың тексеруші сәйкестендіру ақпаратын алдыңғы сертификат шығу тегін растау үшін қолданылуы мүмкін. Тізбек верификатордан мәлімдеушіге дейін сертификаттық кезекті қамтамасыз етеді. Верификатор тізбектегі әр сертификаттың ішіндегі немесе сенім артылған үшінші тараптардан алынатын ақпарат негізінде оларға сену немесе сенбеу туралы өздігімен шешім қабылдауы қажет.

5.2 Құралдар

Осы бөлімде ортақтастырылған құралдар терминдеріндегі сәйкестендірудің жалпы моделі қарастырылады.

5.2.1 Сәйкестендіру жағдайы туралы ақпарат

Сәйкестендіру жағдайы туралы ақпарат сәйкестендіру қызметтерін шақырулары арасында сақталған сәйкестендіру жағдайы болып табылады. Сәйкестендіру жағдайы туралы ақпарат өзіне мыналарды қамти алады:

– сеанстық криптографиялық кілттері;

– хабарлама реттік номерлері.

Сәйкестендіру жағдайы туралы ақпарат қорғалған күйде сақталуы қажет. Ол ақпарат осы қызметтердің провайдерлері арқылы сақталады.

5.2.2 Басқаруға қатысты қызметтер

Басқаруға қатысты сәйкестендіру құралдары сипаттама ақпарат жиынтығын, парольдерді, сәйкестендіруді орындау талап етілетін объектілерге арналған кілттерді (кілттерді басқаруды қолданғанда) қамтулары мүмкін. Бұл құралдар сәйкестендірілетін нысандар арасында және басқа сәйкестендірілетін ақпарат араларындағы өзара әрекет хаттамаларын қамтуы мүмкін. Сәйкестендіруді басқару сонымен қатар сәйкестендіру ақпаратын жоюды да қамтуы мүмкін.

5.2.2.1 Орнату

Орнату құралдары мәлімдеуші ИА мен тексеруші ИА іске қосады. Бұл құрал тіркеу, дұрыстықты тексеру, растау құралдары көмегімен толығымен сипатталуы мүмкін.

5.2.2.1.1 Тіркеу

Тіркеу құралдары қауіпсіздік органына принципиалмен байланысты бірқатар тексеру ИА жазуға мүмкіндік береді. Бұл ақпарат құрамында принципиал немесе қауіпсіздік органы беретін бірегей идентификатор бар. Бұл құрал принципиал, басқа объект немесе қауіпсіздік органы арқылы іске қосылады (тіркеу қауіпсіздік органы принципиалдан тіркеу дұрыстығын қолдау кепілдігін талап етуі мүмкін.) бұл кезде принципиал қауіпсіздік доменіне кіру кандидаты болып табылады, бірақ әлі қауіпсіздік доменінің

мүшесі болып тағайындалмаған. Осы уақытта сәйкестендіру ақпаратының айырбасы мүмкін емес.

5.2.2.1.2 Бекіту

Дұрыстықты бекіту құралы қауіпсіздік органы атынан орындалады және принципиалды қауіпсіздік доменіне енгізеді.

Принципиалмен байланысты тексерулік ИА дұрыстығын тексеру қауіпсіздік органы мен басқа объектілер арасында өзара қатынасты талап ету мүмкін, оны OSI құралдары арқылы жүзеге асыру міндетті емес.

5.2.2.1.3 Растау

Растау құралы дұрыстығын тексеру құралы соңынан іске қосылады. Ол принципиал мен басқа объектілерге арнайы ақпаратты қайтарады. Қайтарылған ақпараттың ең қарапайым түрі орнатуды растау немесе одан бас тарту болып табылады. Ақпараттың басқа түрлеріне мыналар жатады:

– автономды сәйкестендіру сертификаты;

– қабылданған бірегей идентификатор;

– мәлімделген ИА.

Растау негізінде принципиал сәйкестендірілуі мүмкін.

5.2.2.2 ИА өзгерту

ИА өзгерту құралы принципиал немесе әкімгер атынан іске қосылады және сәйкестендіру ақпаратын өзгертуді шақыруды талап етеді .

5.2.2.3 Тарату

Тарату құралы кез келген объектіге жеткілікті тексеру АІ алу мүмкіндігін береді, оның негізінде АІ айырбасын тексеруге болады.

5.2.2.4 Блоктау

Қауіпсіздік органы атынан шақырылатын *блоктау* құралы принципиалдың уақытша сәйкестендіріле алмау жайын анықтайды.

5.2.2.5 Жаңарту

Қауіпсіздік органы атынан шақырылатын *жаңарту* құралы блоктау құралы орнатқан жағдайын тоқтатады.

5.2.2.6 Деинсталляция

Деинсталляция құралы принципиалды көптеген сәйкестендірулік принципиалдар арасынан жою шартын құрайды. Бұл құрал заңды күшін жою, хабарлау, тіркеуден шығару құралдары көмегімен толық түсіндірілуіне болады.

5.2.2.6.1 Заңды күшін жою

Заңды күшін жою құралы қауіпсіздік органы әрекеті болып табылады, ол тексеру сәйкестендіру ақпаратын және/немесе принципиалмен байланысты жағдайды өзгерту туралы ақпаратты жою болып табылады.

Заңды күшін жою құралы принципиал сәйкестендірілуінің алдын алады.

5.2.2.6.2 Хабарлау

Хабарлау құралы қауіпсіздік органы арқылы заңды күшін жою құралынан кейін іске қосылады. Ол принципиалды оның жарамсыздығы туралы хабарлайды және қайтадан қалай тіркелу туралы хабарлайды.

5.2.2.6.3 Тіркеуден шығару

Тіркеуден шығару құралы принципиалды қауіпсіздік доменінен шығаруды көздейді. Ол принципиал идентификаторын және онымен байланысты тексеру ИА жоюға байланысты. Құралы қауіпсіздік органы арқылы іске қосылады.

5.2.3 Операцияларды жүргізуге қатысты құралдар

5.2.3.1 Жинау

Сұраныс құралы мәлімдеуші мен верификаторға арнайы ИА айырбасын туындауға қажетті ақпаратты алуға мүмкіндік береді. Ол үшін сенім артылған үшінші тараппен (мысалы, сәйкестендіру сервері) өзара әрекет ету талар етілуі мүмкін. Кіру мәліметтерінің мүмкін түрлері:

– сәйкестендірудің айырбас түрі;
– принципиалдың бірегей идентификаторы;
– верификатор ұқсастығы;
– мәлімделген ИА түрі (мысалы, кілт, пароль);
– мәлімделген ИА (пароль мағынасы);
– ИА айырбасының түрі;
– негіздеме (жарамдылық мерзімінің басы/аяғы).

Кіріс мәліметтерінің мүмкін түрлері:

– жағдайы (сәттілік немесе сәтсіздік);
– ИА айырбасын туындауға қажетті ақпараттар.

5.2.3.2 Туындау құралдары

Туындау құралын мәлімдеуші ИА айырбасын туындау және/немесе алынған ИА айырбасын өңдеу мақсатында мәлімдеуші арқылы іске қосылады.

– Төменде мүмкін болатын кіріс мәліметтері көрсетілген;
– Принципиалдың бірегей идентификаторы;
– ИА айырбасын сұраныс құралының кіріс мәліметтері секілді туындау мақсатында қажет ақпарат;
– Сәйкестендіру жағдайы туралы сақталған ақпаратқа сілтеме;
– Верификатордан алынған ИА айырбасы;
– ИА айырбасының түрлері;
– верификатор ұқсастығы;
– мәлімделген ИА.

Шығыс мәліметтерінің мүмкін түрлері:

– күйі (сәттілік немесе сәтсіздік);

– сәйкестендіру жағдайы туралы сақталған ақпаратқа сілтеме;

– верификаторға өткізу үшін ИА айырбасы.

Сәйкестендірулік айырбас түрі сәйкестендірулік айырбас туындау құралдарын шақырған кезде кіріс мәліметі ретінде берілуі мүмкін, онда мәліметші сәйкестендіру бастамашысы болып әрекет етеді.

Сол шақыруда шығыс мәліметтері ретінде сәйкестендіру күйі туралы сақталған ақпарат сілтемесі қайтып оралады. Сол сәйкестендірулік айырбасқа қатысты туындау құрал үшін келесі шақыруларда аталған кіру шығу мәліметтердің болмауы да мүмкін, бірақ Сәйкестендіру жағдайы туралы сақталған ақпаратқа сілтеме кіру мәліметі ретінде қолданылады.

«Айырбас жалғастыруы талап етуі мүмкін» нәтижесі қайтарылған болса, мәлімдеуші басқа объектінің АІ айырбасын алғаннан соң туындау құралын шақыру қажет. Бұл процесс сәтті не сәтсіз болып аяқтамайынша мәлімдеушіден осындай операциялардың бірнешеуін орындау талап етілуі мүмкін (яғни Сәйкестендіру жағдайы мен қабылданған АІ айырбасы туралы алдағы ақпаратпен қатар туындау құралдарының шақырулары). Осылайша қолданушы-қатысушылармен сұраныс жауапты, арнайы «нөлдік білімді» талап ететін сызбаларда қолданылатын айырбастарды қоса туындау құралы барлық сызбаларға бейімделген.

5.2.3.3 Тексеру құралы

Верификатор мәлімдеушіден алған АІ айырбасын тексеру мен/немесе мәлімдеушіге беру үшін АІ айырбасын туындау мақсатында тексеру құралын іске қосады.

Төменде кіру мәліметтерінің мүмкін түрлері келтірілген:

– сәйкестендірудің айырбас түрі;

– сұраныс құралының шығу ақпаратының негізінде ИА айырбасын туындау мақсатында талап етілетін ақпарат;

– сәйкестендіру жағдайы туралы ақпаратқа сілтеме;

– мәлімдеушіден алынған айырбас ИА; тексеру ИА.

Шығыс мәліметтерінің мүмкін түрлері:

– күйі (сәттілік, қосымша ақпарат қажет, сәтсіздік) ;

– сәйкестендіру жағдайы туралы сақталған ақпаратқа сілтеме;

– ИА айырбасы («қосымша ақпаратты жөнелту талап етіледі» жағдайында);

– принципиалдың бірегей идентификаторы («сәттілік» жағдайында);

– негіздеме (жарамдылық мерзімінің басталу/аяқталу сәті);

– жалпы сәйкестендіру белгісі;

Сәйкестендірулік айырбас түрі сәйкестендірулік айырбас туындау құралдарын шақырған кезде кіріс мәліметі ретінде берілуі мүмкін, онда мәліметші сәйкестендіру бастамашысы болып әрекет етеді.

Осы іске қосылған күйінде сәйкестендіру күйі туралы ақпаратқа сақталған сілтеме шығу мәліметі ретінде қайтарылады. Сол сәйкестендірулік айырбас үшін тексеру құралдарын келесі жолы іске қосқан кезде аталған кіріс және шығыс ақпараттардың болуы міндетті емес, алайда сәйкестендіру жағдайы туралы ақпаратқа сақталған сілтеме кіріс мәліметі ретінде қолданыла алады.

Сәйкестендірулік ақпарат күйі жайлы ақпарат құралдың ішінде келесі қолданғанға дейін және сәттілік пен сәтсіздік қайтып оралғанға дейін сақталады.

Егер сәттілік жағдайы қайтып келсе, сондай ақ принципиалдың сәйкестендірілген ұқсастығы оралады.

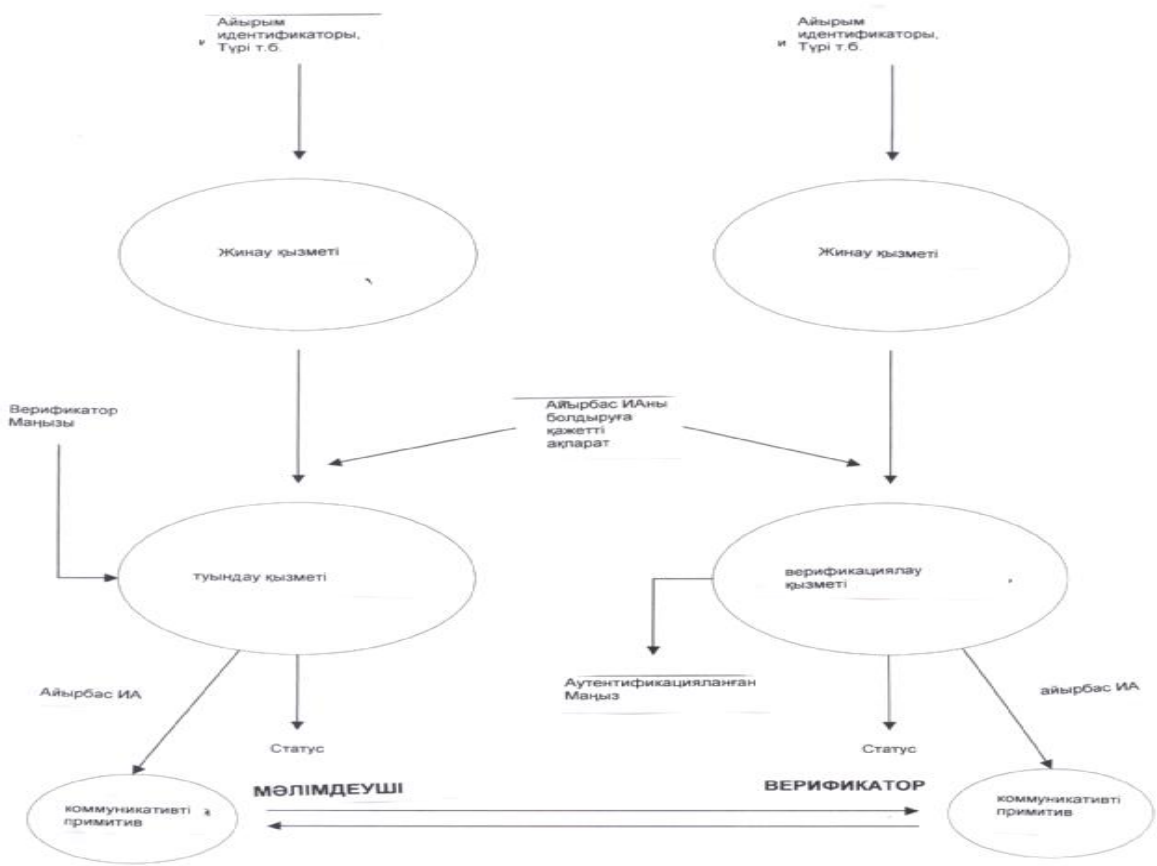
5.2.3.4 Туындау және тексеру құралдары

Екі жақты сәйкестендіру жағдайында туындау және тексеру құралдары бір құралға біріктірілуіне болады. Біріктірілген құралдың кіру және шығыс мәліметтері осы екі құралдардың ұқсас мәліметтерінің бірігуі болып табылады.

Ескертпе – Туындау және тексеру құралдары мәліметтерді өткізбейді. Мәліметтерді өткізу сәйкестендіру жүзеге асырылып жатқан ортаға байланысты. осы таралу аясынан кірмейді.

5.2.3.5 Ақпараттық ағымдар мысалы

8 суретте сәйкестендіруді өткізуге қолданылатын сұраныс, туындау және тексеру құралдарын іске қосумен байланысты ақпараттық ағымдар мысалы келтірілген (бұл жерде қолданбалы процесс ретінде қарастырылады).



8 -сурет– Қолданумен байланысты сервистердегі ақпараттар ағымының мысалдары

Ескертпе – Бұл мысалда *жинау сервисінің* мәлімдеуші арқылы да, верификатор арқылы да іске қосылатындығы көрсетілген. Тәжірибеде ол осы объектілерінің бірімен ғана немесе ешбірімен іске қосылмайтынды. *Туындау және тексеру* құралдарының арасында ақпараттық ағымдарының орын алғандығына байланысты, ол қызметтің бірде біреуі де коммуникациялық примитивтерді іске қоспайды.

6. Сәйкестендіру тетіктерінің сипаттамасы

Осы стандарттың таралу аясындағы сәйкестендіру тетіктері 5.3. тармақта көрсетілген а), г) және д) қағидаларына негізделген. г) қағидасы 5.5.2. тармақта көрсетілгендей сенім артылған үшінші тараптың болуын көздейді 5.5.2, алайда ол тетіктер нәтижесінде а) және д) қағидаларына негізделеді. Басқаша айтқанда, ашық жүйелерде жойылған Сәйкестендіру принципиалды көп жағдайларда а) қағидасына негізделген, және ол кілт немесе пароль түріндегі құпия түрлерді қолдануды көздейді.

6.1 Симметрия/ассимметрия

Сәйкестендіру принципиалы көп жағдайларда а) қағидасына негізделген, және ол кілт немесе пароль түріндегі құпия түрлерді қолдануды

көздейді. Сәйкестендіру осы аталған құпия түрлерді білуді көрсетеді. Демонстрация әдістерін мейлінше жалпы екі санатқа бөліп тастауға болады:

– *симметриялық,* ол кезде екі объекті де бірігіп сәйкестендіру ақпаратын қолданады;

– *асимметриялық кезде* сәйкестендіру ақпараты толығымен екі объектімен қолданылмайды.

Төменде симметриялық сәйкестендіру мысалдары келтірілген:

– симметриялық кілт арқылы шарттау әдісі арқылы шартталады;

– ассиметриялық сәйкестендіру әдістерін қолдану мысалдары;

– шарттаудың ассиметриялық әдістерін қолданатын әдістер;

– ақпараттың бөлігін ашу қажетінсіз ақпараттың бар екенін тексеру мүмкіндігі бар әдістер.

6.2 Криптографиялық/криптографиялық емес технологияларды пайдалану

Сәйкестендіру объектілеріне белгілі мағыналарға негізделген сәйкестендіру тетіктері (4.3 тармақшаны қараңыз) сәйкестендіру ақпаратын қорғау үшін криптографиялық алгоритмдерді қолданумен қосымша сипатталады. Тұтастықты, кей жағдайларда сәйкестендіру ақпаратының құпиялығын қамтамасыз ету үшін шарттаудың симметриялық, ассиметриялық және гибридтік технологиялары қолдануы мүмкін.

Криптографияны қолданбайтын технологиялар парольдер мен сұраныс – жауап кестелерін қолдануды көздейді. Криптографиялық технологиялар өткізу кезінде парольдерді қорғау үшін шарттауды қолдануды көздейді.

6.3 Сәйкестендіру түрлері

Сәйкестендіру екі объектінің орын алуын көздейді. Бір жақта сәйкестендіру кезінде бір объект мәлімдеуші, ал екіншісі верификатор ретінде қолданылады.

Екі жақты сәйкестендіру кезінде объектінің әрқайсысы бір уақытта мәлімдеуші мен верификатор ретінде әрекет етеді. Екі жақты сәйкестендіру бір немесе екі бағыттағы түрлі сәйкестендіру тетіктерін қолдану кезінде алынуы мүмкін.

6.3.1 Бір жақты сәйкестендіру

Бір жақты сәйкестендіру мыналар арқылы жүзеге асырылуы мүмкін:

– жалғыз сәйкестендіру ақпаратын өткізу, мысалы, бірегей номерлерді қолданғанда;

– шақыруды қолданғанда сәйкестендіру ақпаратын үш мәрте қолдану;

– сәйкестендіру ақпаратын үштен көп рет өткізілген кезде;

– бұл жағдай «нөлдік білімді» талап ететін сызбаларды қолданатын арнайы тетіктерді қолдануға жатады;

Жоғарыда көрсетілген жағдайларды қарастыру мәлімдеушінің сәйкестендіру бастамашысы болып табылатындығын жобалайды. Егер верификатор сәйкестендіру бастамашы болса, онда өткізу саны басқа болады; толығырақ 7.2.тармақта көрсетілген.

6.3.2 Екі жақты сәйкестендіру

Екі жақты сәйкестендіру міндетті түрде мәліметтер өткізу санын, бір сәйкестендіру тетігін екі бағытта қолдануды да екі еселенгенін білдірмейді.

Біржақты ақпаратқа арналған сәйкестендіру ақпараты үш өткізуін қолданатын сәйкестендіру ақпараты үшін, екі жақты сәйкестендіру үшін қосымша айырбастар талап етілмейді; шақыру сұранысы верификатор қолданатын (мәліметші ретінде әрекет ететін) басқа шақыруды жіберумен біріктірілуі мүмкін.

6.3.3 Сәйкестендіруді растау

Кейбір жағдайларда объект сәйкестендіруден өткені немесе сәйкестендіруден өтпегені туралы хабарлауы маңызды болып табылады. Хабарлама үшін шынайылық кепілдендірілуі қажет немесе ол шынайылыққа кепілдіксіз қарапайым «иә» немесе «жоқ» болуы мүмкін. Ол ақпараттың қосымша айырбасын талап етеді.

7 Сәйкестендіру тетіктері

7.1 Осалдық бойынша жіктеу

Сәйкестендіру тетіктері өздігінен шабуылдарға осал болулары мүмкін, ол өз кезегінде қолдануды шектейді. (5.8 тармақты қараңыз).

Сәйкестендіру тетіктері қосалқы клас мәліметтер өткізу сатысында сәйкестендіруді қолдау үшін қолданылады, өз кезегінде олар төтеп бере алатын қатерлерге қатысты жіктеледі. Барлық қарастырылған сәйкестендіру тетіктері «белгілі маңыз» қағидасына негізделген [5.3 а) тармағын қараңыз]. Барлық қарастырылған тетіктер объектілер сәйкестендірілуіне қатысты қолданылады, ал кейбірі мәліметтердің шығу тегін сәйкестендіруге де қатысты қолданылады, мысалы, сәйкестендіру айырбас кезінде мәліметтерге сандық идентификациялық белгілер жасау:

сәйкестендіру тетіктерінің келесі түрлері белгіленді:

– 0 сынып. Қорғалмаған.

– 1. сынып. Ашылудан қорғалған

– 2. сынып. Ашылудан және түрлі верификатор арқылы қайта жаңғыртудан қорғалған.

– 3. сынып. Ашылудан және сол верификатор арқылы қайта жаңғыртудан қорғалған.

– 4. сынып. Ашылудан, сол және түрлі верификатор арқылы қайта жаңғыртудан қорғалған.

Ескертпе – 1—4 сыныптарда «ашылудан қорғау» дегеніміз мақсатты сәйкестендіру ақпаратын ашылудан сақтайды.

Қажет болған жағдайда қосымша сыныптар анықталуы мүмкін. Осылайша кейбір тетіктер сыныптары үшін қосалқы кластар анықталуы мүмкін. Қосалқы кластардың толық болуы міндетті емес.

Әр сынып тетігі үшін АІ айырбасы диаграммада көрсетілген.

Шарттау қызметі туындау құралы бөлігі ретінде қолданған кезде, мәлімделген сәйкестендіру ақпараты басқа да ақпаратпен бірге кілтті құрау мақсатында қолданылады.

Төменде сәйкестендірулік айырбастар мәлімдеуші көзқарасынан сипатталады және әрқашан мәлімдеуші арқылы басталады. Верификатор бастайтын айырбастар 8.2. тармақта көрсетілген. Қарастырылған айырбастар бір жақты сәйкестендіруге қосымша бола алады. Екі жақты сәйкестендіру кезінде қолданылатын айырбастар қатысты 8.4. тармақты қараңыз. Кей жағдайларда сәйкестендірудің сәтті немесе сәтсіз болу дерегі туралы хабарлама алу өте қажет. Ол бұл бөлімде сипатталмаған. Осы бөлімге қатысты құралдар 6.2. тармақта сипатталған.

Диаграммаларда екі төрт бұрыш жақша түріндегі [] нотация өткізілген ақпараттың тек арнайы жағдайларда қамтылатын міндетті емес құрамбірліктері үшін қолданылады.

Міндетті емес құрамбірлік [сандық баламалау белгі] мәліметтердің шығу тегін сәйкестендіру кезінде ғана болады, басқа жағдайларда болмайды. Сандық сәйкестендіру белгі ассиметриялық алгоритм шарттау көмегімен құрылуы мүмкін, немесе мәліметті қарапайым шарттау, криптографиялық бақылау мағыналы мәліметтерді сандық қол қоюға қолданатын жеке кілт арқылы жүзеге асыруға болады. Сандық сәйкестендіру белгісі жататын мәліметтер шығу тегін сәйкестендіру үшін толығымен тәуелсіз немесе қатардағы тетіктер коммуникация құралдарымен бірге жүзеге асырылады.

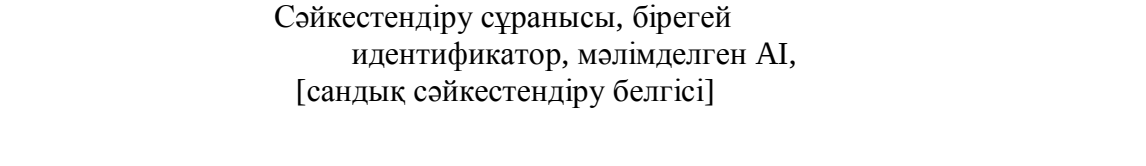
7.1.1 0 сынып (қорғалмаған)

0 сыныпта мәлімделген АІ мен бірегей нөмір бар және тек мәлімдеушіден верификаторға АІ айырбасының бөлігі ретінде беріледі. Бұған ең жақсы мысал парольді жіберу болып табылады. 0 сынып симметриялық сәйкестендіру мысалы болып табылады. Бұл тетіктер сыныбы сәйкестендіру ақпараты мен қайта жасау шабуылдарға осал болып табылады.

Туындау құралы 9 суретте көрсетілгендей кіру мәліметтерімен байланысты АІ айырбасын жасайды.

Тексеру құралы мәлімделген АІ бірегей номер алумен байланысты тексеру сәйкестендіру ақпараты мен пароль сәйкестігін тексереді.

0 сынып тетіктері объектілер сәйкестендірілуіне сонымен қатар мәліметтер шығу тегіне қатысты қолданылады.



9. сурет – 0 сынып тетігі (қорғалмаған)

7.1.2 1 сынып (ашылудан қорғалған)

Бұл тетік класы мәлімделген сәйкестендіру ақпараты ашылуынан сақтауды қамтамасыз етеді. 1 сынып тетігі нысандар мен мәліметтер шығу тегін сәйкестендіру мақсатында қолданған.

Бұл тетіктер түрлену қызметін қолданады, оның көмегімен мәлімделген АІ бірегей идентификатормен бірге түрленіп, онымен бірге ұсынылады. Шынайы мәлімделген сәйкестендіру ақпараты байланыс арнасы арқылы берілмейді. Төменде бірнеше мысалдар келтірілген:

– Бір жақты қызмет көмегімен түрленген парольді жіберу (мысалы, криптографиялық бақылау мағынасы немесе хэш-функциясы);

– Құпия кілт көмегімен шартталған сандық сәйкестендіру белгісін жіберу;

– Құпия кілт арқылы шартталған парольдерді жіберу;

– Жеке кілт арқылы шартталған сандық идентификациялық белгі;

Бұл түрдегі тетіктер сәйкестендіруге, мәліметтер шығу тегіне, сонымен қатар объектілерге қатысты қолданылады. Олар жасырын ауыстырып қою шабуылына төтеп бере алмайды, алайда мәлімделген АІ ашудан қорғанысын қамтамасыз етеді. Мысалы түрленген пароль айырбас хаттамасы деңгейінде қайталап берілуі мүмкін, бірақ жүйемен өзара әрекет деңгейінде қолданылатын парольдің мәтіні ашылмайды.

Туындау құралы мәлімделген АІ қолданады және қажет болса, 10 суретте көрсетілгендей криптографиялық түрлену мақсатында бірегей идентификаторлы және/немесе сандық идентификаторлық белгіні кіру ақпараты ретінде қолданылады.

Сәйкестендіру сұранысы, бірегей
идентификатор, Р(мәлімделген АІ, [сандық
идентификациялық белгі])

МӘЛІМДЕУШІ ВЕРИФИКАТОР

10 сурет – 1 сынып. Ашылудан қорғалған тетік

төменде түрлену қызметтерінің үш мысалы келтірілген (F):

а) бір жақты қызмет кезінде тексеру құралы мәлімделген АІ дың орнына тексеру АІ қатысты қолданады, содан кейін АІ айырбасының нәтижелерін салыстырады.

b) Симметриялық шарттау құралын қолданған кезде тексеру құралы алынған АІ айырбасы үшін тексеру АІ қолданады, содан кейін ашылған ақпарат дұрыстығын оның мәлімдеушінің бірегей идентификатор, дұрыс сандық идентификациялық белгі, пароль немесе тұрақты мағына секілді бірегей ерекшеліктер дұрыстығын тексереді.

с) Сандық қол қою құралы жағдайында алынған мәліметтерден сандық идентификациялық белгілерді есептеп шығарады және тексеру АІ алынған қолдың аталған идентификациялық белгіге қатысты күшке ие ма, жоқ па тексереді.

Одан басқа мәліметтердің шығу тегін сәйкестендірген кезде АІ айырбасы кезінде жаңадан құралған сандық идентификациялық белгімен салыстырылады, оларға сәйкестендіру талап етіледі.

Ескертпе – Егер принципиалдың бірегей идентификаторы мәлімделген сәйкестендіру ақпаратымен бірге қолданса, онда бұл жабуды жасауға кедергі жасайды. Уақыттың әр сәтінде барлық принципиалдарға шабуыл жасаудың орнына арнайы бір принципиалға қатысты бір шабуыл жасалады.

Түрлену қызметі құпиялығын қамтамасыз ету үшін ол кері функцияға ие болмауы керек. Егер кері функция орын алған болса, онда қарау есептеу шығындары тұрғысынан мәлімдеуші АІ қауіпсіздігін қамтамасыз ететін тарап үшін мүмкін емес болады (және сандық идентификациялық белгі)

7.1.3 2 сынып (ашылудан және түрлі верификаторлардың қайта жаңғыртудан қорғалған)

Бұл тетік сыныбы ақпаратты ашылудан және түрлі верификаторлар арқылы, бірақ сол бір верификатор арқылы қайта жаңғыртуды қамтамасыз етеді. Бұл тетік сыныбы 1 сыныппен ұқсас, бірегей сипаттамаға ие аталған верификатор түрлену қызметінің кіру мәліметтеріне қатыстылығынан басқа. Ол қосымша қорғанысты қамтамасыз етеді.

7.1.4 3 сынып (бір верификатордан ашылу және қайта жаңғыртудан қорғаныс)

Бұл тетік класы мәлімделген АІ ашылудан және оның сол верификатор арқылы қайта жаңғыртылуынан қорғауды қамтамасыз етеді . Бұл сыныпта сол верификатор қайта жаңғыртылуынан қорғауды қамтамасыз ету бірегей ақпаратпен бірге түрлену функцияларын қолданатын бірегей нөмірлер тетіктері арқылы қамтамасыз етіледі. Мәлімделген АІ және бірегей номер түрленеді және бірегей идентификатормен бірге беріледі.

Төменде бірегей нөмірлерге қатысты бірнеше мысалдар келтірілген:

a) Кездейсоқ және жасырын кездейсоқ нөмірлер. Бұндай сандар мәлімделген сәйкестендіру ақпаратын өмірлік циклінде кепілдендірілген түрде қайталанбайды. Кездейсоқ немесе жасырын кездейсоқ сандар неғұрлым үлкен ауқымда бір санның бұрын соңды қолданылған ықтималдығын төмендете алады.

b) Уақытша белгілер. Бірегей нөмірлер сенімді көзден алынған уақытша белгілер болып табылады және мәлімделген сәйкестендіру ақпаратының өмірі бойына бірегей болып қалыптасады. Ескі және бұрын қолданылған уақытша белгілер жойылады.

c) Есептеуіш. Бірегей нөмір дегеніміз сол мәлімденбеген АІ қолдану кезінде ұлғаятын есепші мағынасы.

d) Криптографиялық тізбек. Бірегей нөмір бұрынырақ мәлімдеуші мен верификатор арасында блоктар тіркесі көмегімен мәліметтерден шыққан мағынаны қамтиды.

Мәлімдеушіден тыс бұл нөмірдің бірегейлігі оның сол мәлімдеушіге бірегей болып табылатын мәліметтермен біріктіру арқылы қамтамасыз етілуі мүмкін (мысалы, оның бірегей идентификаторымен).

Сонымен қатар бұл технологияларды бірегей нөмірлер тағайындау мақсатында бірігіп қолдану да мүмкін.

Төменде түрлену қызметінің үш мысалы келтірілген (F):

a) Біржақты түрлену қызметі. Бірегей нөмір, мәлімделген АІ, бірегей идентификатор біржақты қызмет арқылы түрленеді. Сонымен қатар бірегей нөмір верификатор да осындай түрленуді орындау үшін беріледі.

b) *Асимметриялық алгоритм.* Басқарудың сыртқы параметрі жеке кілт болғанда, шақыру жеке кілт арқылы тіркеледі.

c) Симметриялық алгоритм. Сыртқы басқару параметрі құпия кілт болғанда шақыру шартталады немесе тексеру мағынасының көмегімен иесі белгісіз қол қойылады және сол құпия кілт ретінде қолданылады.

Бұл қосалқы класс мәліметтер шығу тегі мен объектілер сәйкестендірілуіне қолданылады.

Туындау құралы бірегей нөмірді жасайды. Содан кейін келесі кіріс ақпаратын қолдану арқылы шарттау жүзеге асырылады:

– Бірегей нөмір,

– Мәлімделген АІ,

– Бірегей идентификатор (міндетті емес),

– сандық идентификациялық белгі (егер мәліметтер шығу тегінің Сәйкестендірілуі жүзеге асырылса) және 11 суретте көрсетілгендей АІ айырбасының туындауы болады.

Сәйкестендіруге сұраныс, бірегей идентификатор,

_____

F (шақырулар, тексеру АІ,
[бірегей идентификатор])

шақыру, таңдалған мағыналар

МӘЛІМЕУШІ ВЕРИФИКАТОР

шақыру

11 сурет – 3 қосалқы клас. Бірегей нөмірлердің тетігі

Тексеру құралы АІ айырбасын тексеріп ашып, тексереді және 1 сыныпты сипаттау кезінде көрсетілгендері АІ арқылы айырбасты тексереді. Сонымен қатар алынған бірегей нөмірдің бұрын соңды қолданылмағанын тексеріледі. Егер нөмір бұрын алынған болса, онда оның қайта жаңғыртуы болғанын білдіреді. Мәліметтер шығу тегін сәйкестендіру кезінде бұған қоса сандық идентификациялық белгі АІ айырбасында алынған мәліметінен қайта жасалған сандық идентификациялық белгілерімен салыстырылады.

Ескертпе – Криптографиялық байланыс деген термин ИСО/МЭК Халықаралық стандартта алынған 10116 блоктар байланысы терминіне сәйкес келеді.

7.1.5 4 сынып (Сол немесе түрлі верификаторларға ашу және қайта құрудан қорғау)

7.1.5.1 4а қосалқы класс. Бірегей сандар тетігі

Бұл тетік сыныбы бірегей сипаттамаға ие аталған верификатор түрлену қызметінің кіру мәліметтеріне қатыстылығынан басқа 3 сыныппен ұқсас. Ол қосымша қорғанысты қамтамасыз етеді.

7.1.5.2 4б Қосалқы класы. Шақыру тетіктері

Шақыру тетігі қайта жаңғырту шабуылдарына қарсы әрекет етуге негізделген, яғни қайта жасалған АІ айырбасы арқылы сәйкестендіру жасау талпынысы сәтсіз болатындығын кепілдендіреді. Сәйкестендіруге сұраныс жауабына верификатор мәліметші шақыруын жасайды, ол шақыруда бірегей мағынасы бар элементтер бар. Мәліметші шақыру ақпаратын және қайсыбір қызметтер көмегімен мәліметші сәйкестендірулік ақпарат түрлендіреді.

Шақыру тетігі үш ақпарат өткізуді қамтиды:

– сәйкестендіруге сұраныс беру;

– шақыруды жүзеге асыру;

– мәлімделген АІ алынған мағынаны қамтитын жауапты жібері, арнайы қызметтер көмегімен бірегей идентификатормен, шақыру ақпаратымен біріктіру мүмкін (F).

Жалпы жағдайда бірегей идентификатор сәйкестендіру сұраныспен бірге немесе соңғы жауаппен жіберіледі.

Төменде шақыру тетігінде қолданылатын (F) түрлену қызметтерінің бірнеше мысалдары келтірілген:

а) *Біржақты түрлену қызметі*. Бірегей нөмір, мәлімделген АІ, бірегей идентификатор біржақты қызмет арқылы түрленеді.

б) *Асимметриялық алгоритм*. Басқарудың сыртқы параметрі жеке кілт болғанда, шақыру жеке кілт арқылы тіркеледі.

в) *Симметриялық алгоритм*. Сыртқы басқару параметрі құпия кілт болғанда шақыру шартталады немесе тексеру мағынасының көмегімен иесі белгісіз қол қойылады және сол құпия кілт ретінде қолданылады.

Шақыру тетігінің жасалған шақырудың сәйкестендіруге сұраныс жасалған кезде алынған идентификаторға тәуелді болу арнайы жағдайы болады. Бұл шақырудың арнайы тетігі деп аталады. Бұл жағдайда бірегей идентификатор сәйкестендіру сұранысы міндетті болып табылады. Қосымша ретінде түрлену қызметінің төртінші мысалын келтіреміз:

г) *Криптографияны қолданусыз*. Шақырушы объект белгілі жауапты талап еткен кезде сұрақ-жауап кестелерін қолдану;

Бұл қосалқы класс мәліметтер шығу тегі мен объектілер сәйкестендірілуіне қолдануға болады.

Тұндыру құралы сәйкестендіруге сұраныс жасайды (ол арнайы шақыру кезінде бірегей идентификатормен қолдануы қажет). Осы аталған сәйкестендіру сұранысты алғаннан кейін тексеру құралы АІ айырбасы түріндегі бірегей шақыруды жасап шығарады.

Содан кейін туындау құралы 12 суретте көрсетілгендей кіріс мәліметтерін түрлендіру көмегімен АІ айырбасын жасайды.

Біржақты түрлену қызметі жағдайында мәлімдеуші АІ орнына тексеру АІ қолданып, АІ айырбасымен салыстырады. Бұл аталған әрекеттерді орындау үшін верификаторға бірегей идентификатор мен тексеру құралы қолданатын мәліметтер қол жеткізерлік болулары қажет.

Басқа түрлену жағдайында тексеру құралы тексеруді қайталайды немесе кері немесе тексеру АІ қолдану арқылы мазмұнын тексереді.

Сәйкестендірулік сұраныс, [бірегей идентификатор]

шақыру

ӨТІНУШІ *л* ---------- ВЕРИФИКАТОР

[бірегей идентификатор]
Р(мәлімделген АІ, шақыру, [бірегей идентификатор], [сандық идентификациялық белгі])

12. сурет – 4б қосалқы класы. Шақыру тетігі.

7.1.5.3 4в. қосалқы класы. Арнайы шартталған шақырулар тетігі

Арнайы шартталған шақырулар тетігі сондай-ақ үш ақпарат өткізуін көздейді:

– сәйкестендіру мен бірегей идентификаторға сұраныс жіберу;

– шақыру мен тексеру АІ беру, бірегей идентификатормен және арнайы (F) функция арқылы түрленген идентификатормен бірігуі мүмкін;

– шақыру ақпаратынан тұратын жауапты жіберу.

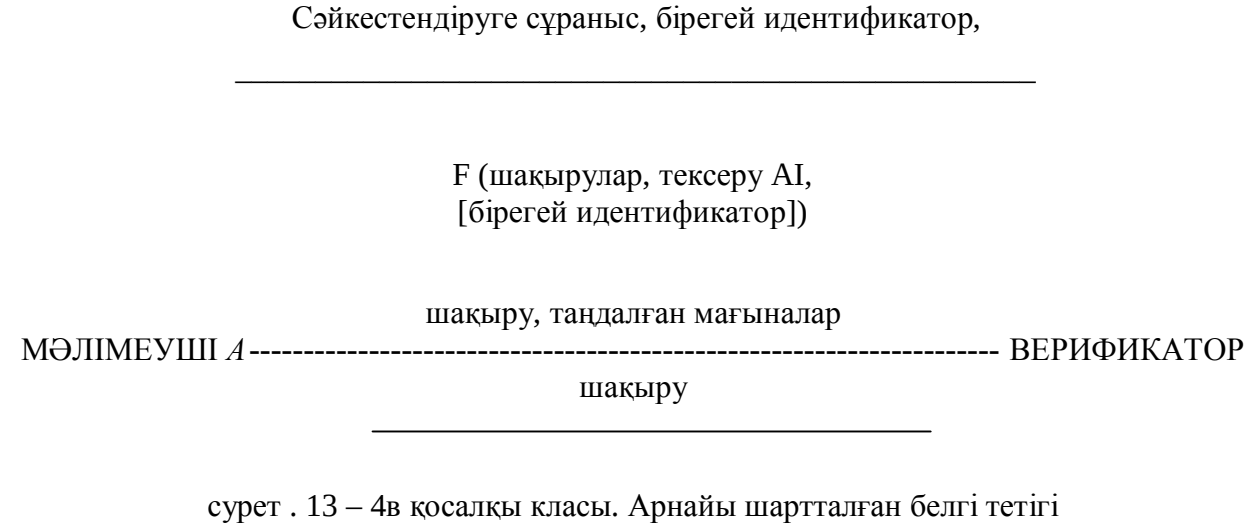
Төменде арнайы шарттау шақыруының екі тетігінің екі мысалы келтірілген:

а) *Асимметриялық алгоритм*. Басқарудың сыртқы параметрі жеке кілт болғанда, шақыру жеке кілт арқылы тіркеледі.

b) Симметриялық алгоритм. Сыртқы басқару параметрі құпия кілт болғанда шақыру шартталады немесе тексеру мағынасының көмегімен иесі белгісіз қол қойылады және сол құпия кілт ретінде қолданылады.

Бұл тетігі түрін тек объектілер сәйкестендірілуіне қолданамыз, мәліметтер шығу тегіне қатысты қолданылмайды.

Туындау құралы сәйкестендіру сұранысын жүзеге асырады. Сәйкестендіруге және бірегей идентификаторға сұранысты алған кезде тексеру құралы алдын ала болжай алмайтын шақыруды құрайды. Содан кейін ол 13 суретте көрсетілгендей АІ айырбасын құру мақсатында түрлену қызметтері көмегімен түрленеді.



сурет . 13 – 4в қосалқы класы. Арнайы шартталған белгі тетігі

Содан кейін туындау құралы тексеру АІ орнына АІ айырбасы ретінде қайтарылатын шақыруды алу мақсатында мәлімдеуші АІ-ды кері түрленуді жүзеге асырады. Атап өтетін жайт, шарттауды түрлендіру ғана осы сызбаға жарамды.

Соңғы сатыда тексеру құралы бұрын туындалған шақырумен салыстырады.

7.1.5.4 4г қосалқы класы. Есептелінген жауап тетіктері.

Бұл шақыру тетігінің қосалқы класы сондай-ақ үш ақпарат беруді көздейді:

– Таңдауға арналған мағыналар жиынтығы мен идентификациялық ақпаратпен бірге сәйкестендіруге сұраныс жіберу:

– Осындай мағынаны білдіретін шақыруды жасау верификатор арқылы таңдалып алынған;

– Бірегей нөмірден, шақырудан немесе жауапты есептеп шығаруға арналған мағыналардан, сонымен қатар қатысты функция көмегімен түрленген мәлімделген АІ-дан тұратын жауапты жіберу.

Бұған «нөлдік білім» бар технология мысал бола алады, верификатор бірнеше «тапсырмалардан» мәлімдеуші ашпастан шешуі қажет біреуін таңдайды. Бұл «қаскүнемнің» жасырын ауыстыру шабуылынан сақтайды, верификатор таңдап алатын ол барлық емес кей мағыналар үшін дұрыс жауапты есептеп шығара алады. Егер бір ғана ақпарат айырбасы орын алса, верификатор «қаскүнем» дұрыс жауабын білетін мағынаны таңдай алады. Ақпарат алмасудың санының өсуі бұндай шабуылдың сәтті болу ықтималын төмендетеді.

Туындау құралы ең алдымен 14 суретте көрсетілгендей АІ айырбасына енгізілетін бірегей нөмірді және мағыналар жиынтығын жасайды.

Сәйкестендіруге сұраныс, бірегей идентификатор,
бірегей нөмір, мағыналар жиынтығы

---------- ►

шақыру, таңдалған мағыналар
МӘЛІМЕУШІ <---------- ВЕРИФИКАТОР

F (шақырулар немесе таңдалып алынған мағыналар,
Мәлімделген AI,
[сандық идентификациялық белгі])

сурет . 14 – 4г қосалқы класс. Есептеліп шығарылған жауаптың жауабы

Тексеру құралы содан кейін жиынтық арасынан мағынаны таңдап алып, екінші ақпараттық айырбасты ұйымдастыру үшін шақырулар жасайды. Туындау қызметі шақыру немесе таңдалған мағыналар түрленуін мәлімденген AI қолдану арқылы жүзеге асырады.

Содан кейін соңғы сатыда тексеру құралы тексеруді қолдану арқылы кері түрленуді жүзеге асырады және алынған мағынаны тексереді.

7.2 Ақпаратты беруді бастау

7.1 тармақта ақпараттар айырбасы сәйкестендіруге сұраныс көмегімен басталады. Алайда сол қосалқы класс тетіктерінің объектілерін сәйкестендіру үшін верификатор шақыру мен сәйкестендіруді қолдану арқылы ақпарат алмасу бастамашысы болуы мүмкін. Бұл жағдайда ақпараттар алмасу саны түрлі болуы мүмкін. 7.5 тармақтағы №1 кестеде әр жағдайға жасалған ақпараттар алмасуының саны берілген.

7.3 Сәйкестендіру сертификаттары

Сәйкестендіру тетіктері тексерулік AI алу әдісі бойынша жіктеледі. Ол келесі әдістер бола алады:

оперативті мүмкін сәйкестендіру сертификаттары; автономды сәйкестендіру сертификаттар; алдын ала алынатын тексерулік AI, мысалы, қорғалған каналдар арқылы алынуы мүмкін.

Сәйкестендіру сертификаты 5.3. тармақта көрсетілген қағидалар көмегімен сәйкестендіруді қорғауды қамтамасыз етуге қолданылуы мүмкін г). Сәйкестендіру сертификаты сенім берілген үшінші жақтың осы бірегей идентификаторды арнайы тексерулік AI мен байланыстырғанын растайды.

7.4. Өзара сәйкестендіру

Өзіне тек бір жақты айырбасты қамтитын тетіктер қосалқы класы (яғни 1,2,3 және 4а қосалқы класстар) қандай тараптық ақпараттық айырбас болса да өзара сәйкестендіруге қолданылуы мүмкін.

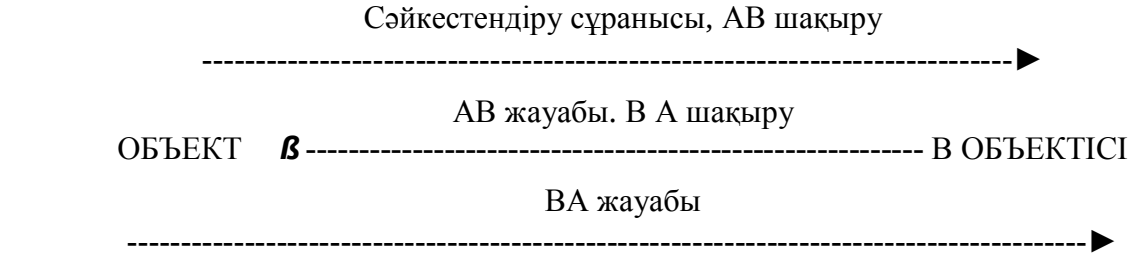
4б қосалқы классына тетіктің сол түрі екі жаққа да қолдануы мүмкін. Бірінші шақыру сәйкестендіру сұранысымен бірге, ал бірінші шақырудың өзгеруі екінші шақырумен (15 суретті қараңыз) жіберілуі мүмкін. Ол бір жақты сәйкестендірудегі айырбастар санын талап етеді.

Сондай–ақ 4с қосалқы класс бірінші шақыру бойынша өзгерістер сәйкестендіруге сұраныспен жіберіледі, ал екінші шақырылым өзгерісі біріншімен бірге жіберіледі.

4б қосалқы класс 4с қосалқы класс тетігімен бірге қолданылады. Екі сұранысы өзгерістік мәліметтерге қосылады. Көрсетілген және тексерулік АІ симметриялық мұқама жағдайында әр тарапта және өзгерістер бір рет қана өткізіледі.

Әр жақтағы ассиметриялық мұқама жағдайында екі өзгерістер жүзеге асырылады.

4 д қосалқы класс немесе үш немесе одан да көп мәліметтерді беру біржақты сәйкестендіруге қажетті. Өзара сәйкестендіру төрт және одан да көп мәліметтер айырбасы.



А ОБЪЕКТІСІ — сәйкестендіру бастамашысы

В ОБЪЕКТІСІ — жауапты

Ескертпе – Жауаптар мен бірегей мәліметтер идентификаторлар қосалқы класстарды сипаттау кезінде ескерулері қажет, сонымен қатар суретті қараңыз.

15 - сурет – Шақыру тетіктерін қолдануымен өзара сәйкестендіру.

7.5. Класс сипаттарының есебі

1 кестеде басты әртүрлі класстар мен қосалқы класстарды мінездеме мен дәлсіздіктер келтірілген. Класстар қасиеттер 6 тармақта көрсетілген.

Кесте 1 – Тетіктер сипаттамасы және дәлсіздігі

Қосалқы класс	0	1	2	3	4а	4б	4в	4г
Дәлсіздік								
Ашылуы	Иә	Жоқ	Жоқ	Жоқ	Жоқ	Жоқ	Жоқ	Жоқ
Түрлі верификаторларды шығару	Иә	Иә	Жоқ	Иә	Жоқ	Жоқ	Жоқ	Жоқ
Сол верификаторға шығару	Иә	Иә	Иә	Жоқ	Жоқ	Жоқ	Жоқ	Жоқ
Қосалқы класс	0	1	2	3	4а	4Ь	4с	4d
«қаскүнемнің» бастамасымен жасалған жасырын ауыстыруына шабуыл	Жоқ	Жоқ	Жоқ	Жоқ	Жоқ	Жоқ	Жоқ	Жоқ
«қаскүнемнің» жауабының жасырын ауыстырылуына	Иә	Жоқ	Жоқ	Жоқ	Жоқ	Жоқ	Жоқ	Жоқ
Қасиеттер								
симметриялық (сим)/ асимметриялық (асим)	сим	сим/ асим	сим/ асим	сим/ асим	сим/ асим	сим/ асим	сим/ асим	Асим
Шарт белгі қою (Иә)/(Жоқ)/	Жоқ	Иә/ Жоқ	Иә/ Жоқ	Иә/ Жоқ	Иә/ Жоқ	Иә/ Жоқ	Иә	Иә
Мәліметтерді беру саны								
Сәйкестендіруді мәлімдеуші бастайды	1	1	1	1	1	3	3	3
Сәйкестендіруді верификатор бастайды	2	2	2	2	2	2	4	4
Мәліметтердің шығуын Сәйкестендіру	Иә	Иә	Иә	Иә	Иә	Иә	Жоқ	Иә

7.6 Пішін көмегімен сұрыптау

Сәйкестендіру процессіне сенімді үшінші жақтар тартылуы мүмкін. Бұл жағдайда бастысы әр объекті мен сенім артқан үшінші тарап арасындағы сенімділік табиғатын анықтау қажет. Үшінші сенім атқан тарапты қолданудың ең қарапайым үлгісі сенім артқан жалғыз үшінші тарап үлгісі болып табылады. Басқа үлгілерде бірқатар сенім артқан үшінші тараптар қарастырылуы мүмкін, ол бір біріне сенім артады, ал жалпылай алған үлгілерде сенім артқан үшінші тараптар бір – бірлеріне сенім артпаулары мүмкін.

7.6.1 Сенім артқан үшінші тараптарды тарту кезіндегі модельдеу қағидалары

Кей жағдайларда верификатор егер бірнеше сенім артқан үшінші тұлғалардан кепілдік алған жағдайда принципиалдың ұқсастығына сенімді бола алады.

Егер сәйкестендіру процессіне үш немесе одан да көп сенім артқан үшінші тараптар тартылған болса, онда бір немесе одан да көп сенім артқан тараптардың бұрмалануынан сақтану мүмкін болады. Қауіпсіздік стратегиясының көпшілігінде көпшілік ережесі қолданылады. Бұдан былай тек жалғыз сенім артқан үшінші тарапты тарту ең қарапайым жағдайы қарастырылған.

Мәлімдеуші, верификатор және жалғыз үшінші сенім артылған тарап араларындағы қарым қатынастар келесі ұғымдар бойынша моделденуі мүмкін:

– сатылар, олар 5.4. тармағында анықталғандай (атап айтқанда, таратылу, алу, верификацияларды беру сатылары);

– бастапқы ақпаратқа ие болу.

7.6.1.1 Сатылар үлгілері

Сатылар әртүрлі объектілермен келесі түрде сәйкестенеді:

– Тарату сатысында мәлімдеуші, верификатор және сенім артқан үшінші тараптар қатысады:

– Қабылдау сатысында мәлімдеуші және үшінші сенім артқан тарап немесе верификатор және үшінші сенім артқан тарап қатысады;

– тапсыру сатысында кез мәлімдеушіден, верификатордан және сенім артылған үшінші тараптан тұратын кез - келген сыңар;

– Верификациялау сатысында верификатор және сенім артылған үшінші тарап қатысады.

Қабылдау, тарату және верификациялау сатылары 8.1. тармақтағы көрсетілген тетіктерді қолдануға болады.

Тарату сатысы оперативті немесе автономды болады. Автономды түрде тарату сатысы әдетте Сәйкестендірулік айырбастан бұрын жүзеге асырылады. Бұл жағдайларда мәлімделген ИА дің әлі де дәл екендігіне кепілдік жоқ (яғни жойылмаған).

16 суретте көрсетілгендей сәйкестендірудің бірнеше сызбасын анықтауға болады. Ол суретте А объектісі мәлімдеуші, ал В – верификатор болып табылады. Бұл сурет тек түсіндіру үшін қолданылады және онда көрсетілген сызба міндетті түрде толық болып табылмайды.

А сызбасы бойынша А объектісі мәлімденген ИА-ды сенім артылған үшінші тараптан ол тараппен сәйкестендіру айырбас жасалғаннан кейін алады; В объектісі тексеруші ИА ды сенім артылған үшінші тараптан алады. Содан кейін В объектісі верификацияны локальды түрде жүзеге асырады.

В сызбасында А объектісі мәлімденген ИА ды сенім артылған үшінші тараптан сәйкестендіру айырбас жасалғаннан кейін алады, В объектісі ИА айырбасын көрсетеді, оны А объектінен алады, ол объект өз кезегінде үшінші тарапқа верификация үшін берілген.

С сызбасында А объектісі өзінің мәлімделген ИА сенім артылған үшінші тараптан сәйкестендірулік айырбастан кейін В объектісіне локальды верификация жасау үшін қажетті тексеруші ИА секілді алады.

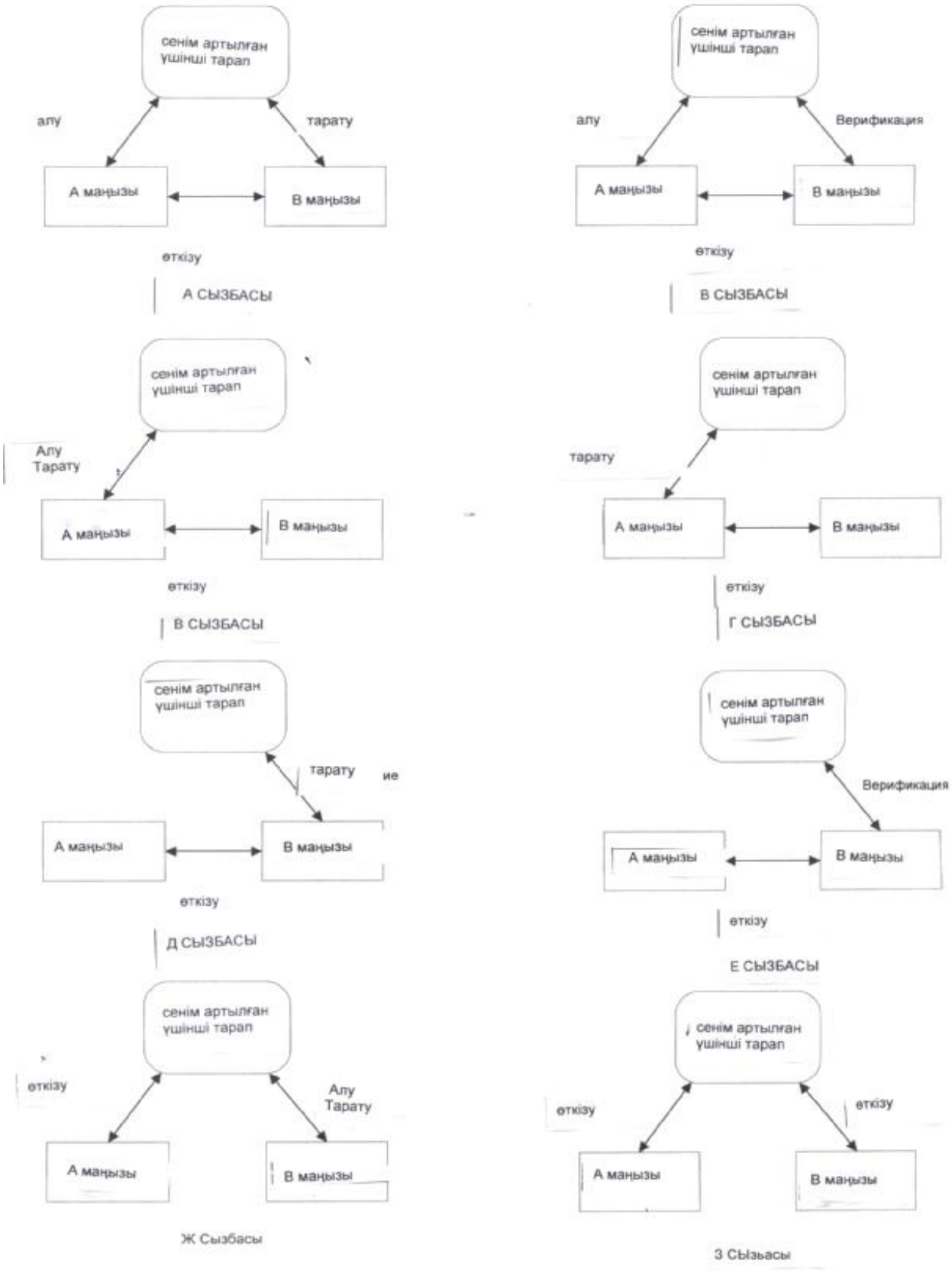
Г сызбасында А объектісі тексеруші В объектінен тексеруші Сәйкестендірулік ақпаратты локальды түрде верификациялау үшін алады, сонымен қатар локальды деңгейде ол ИА айырбасының орын алуына түрткі болады. Айырбас ИА және тексеруші ИА В объектісіне бірге беріледі.

Е сызбасында А объектісі локальды деңгейде өзінің AI айырбасын туындап, оны В объектісіне ұсынады, содан кейін В объектісі сенім артылған үшінші тараптан локальды деңгейде верификация өткізу үшін қажетті тексеруші ИА ды алады.

F сызбасында А объектісі локальды деңгейде ИА айырбасын туындап, оны В объектісіне ұсынады, содан кейін В объектісі А объектінен алынған ИА айырбасын верификациялау үшін сенім артылған үшінші тарапқа ұсынады.

Орнатылған сенімділік қатынасын білдіретін G сызбасында А объектісі локальды деңгейде ИА айырбасын туындап, оны сенім артылған үшінші тарапқа ұсынады, содан кейін сенім артылған тарап оны В объектісіне Сәйкестендірулік сертификат пен локальды деңгейде Сәйкестендіру жүргізуге қажетті тексеру ИА береді.

Орнатылған сенімді қатынастың басқа бір жағдайы болап табылатын Н сызбасында А объектісі локальды деңгейде өзінің ИА айырбасын туындап, оны сенім артылған үшінші тарапқа береді, содан кейін сенім артылған үшінші тарап оны В объектісіне А объектісінің ұқсастығын тексергендігін мақұлдау үшін жібереді.



16 сурет – Сәйкестендіру сызбасы

7.6.1.2 Бастапқы ақпарат негізінде үлгілеу

Мәлімдеуші (А объектісі) мен верификатор (В объектісі) ақпараттың Сәйкестендірулік айырбас болуынан бұрын бірқатар бастапқы ақпараттарды қолданулары қажет. Егер сәйкестендіру процессінде сенім артылған үшінші тарап қатысса, ол мәлімдеушінің верификатор қолданатын жалпы кілт пен құпия кілтті білмейтіндігін білдіреді. Төменде көрсетілгендей, бастапқы әртүрлі ақпараттарды қарастыруға болады.

7.6.1.2.1 Мәлімдеуші мен сенім артылған үшінші тараптың бірге қолданған бастапқы ақпараты

Мына жағдайлар қарастырылады:

а) Мәлімдеуші мен сенім артылған үшінші тарап бірігіп қолданатын құпия кілт мәлімдеуші мен сенім артылған үшінші тарапқа белгілі болады (құпия кілтпен бірге шартбелгі технологиясы) ;

б) Мәлімдеушінің жеке кілті мәлімдеушінің тек өзіне аян (А объектісі), мәлімдеушінің жалпы кілті сенім артылған үшінші тарапқа белгілі (асимметриялық технология);

в) Мәлімдеушінің жеке кілті мәлімдеуші мен сенім артылған үшінші тарапқа белгілі («нөлдік білімді» талап ететін кейбір технологиялар).

7.6.1.2.2 Верификатор мен сенім артылған үшінші тарап бірігіп қолданатын бастапқы ақпарат

Үш түрлі жағдай кездеседі:

а) Верификатор (В объектісі) мен сенім артылған үшінші тарап бірігіп қолданатын (құпия кілт технологиясы) құпия кілті верификаторға мен сенім артылған үшінші тарапқа белгілі;

б) Сенім артылған үшінші тараптың жалпы кілті верификаторға (В объектісі) аян (асимметриялық технологиялар және «нөлдік білімді» талап ететін технологиялар).

7.6.2 Сәйкестендіруге тартылған сенім артылған үшінші тараптар арасындағы қарым – қатынас.

7.6.2.1 Шұғыл түрде қол жеткізетін сенім артылған үшінші тараптар

Сәйкестендіру ақпаратының айырбасы үшін оперативті түрде қол жеткізерлік сенім артылған үшінші тараптар қажет болулары мүмкін. Бір қауіпсіздік доменінің оперативті түрде қол жеткізерлік сенім артылған үшінші тараптары доменде бұрынырақ тіркелген мәлімдеуші ИА және/немесе тексеруші ИА объектілеріне ие болулары мүмкін.

Осы қауіпсіздік доменінде түрлі принципиалдар бір атпен тіркелуі мүмкіндігінің жоқтығын кепілдендіретін хаттамалар немесе процедуралар болулары қажет.

Сенім артылған үшінші тараптардың үнемі қол жеткізерлік болуы аса маңызды, болмаса оперативті түрде сенім артылған үшінші тараптардың

қолдану арқылы орын алатын Сәйкестендіру айырбас қызмет көрсетуде бас тартудың себебі бола алады. Бірнеше сенім артылған үшінші тараптар арқылы Сәйкестендірулік ақпаратты еселеу қызмет көрсетуден бас тарту ықтималдылығын азайтады. Сонымен қатар сәйкестендіру ақпаратты көбейтуді қамтамасыз ететін хаттамалар қажет. Сенім артылған үшінші тараптардың арасында тексеру ИА айырбасы кезінде мәліметтердің тұтастығы мен қауіпсіздігі туралы қызметтер қажет.

Оған қосымша қауіпсіздік доменінің түрлі оперативтік сенім артылған үшінші тараптары жасаған тіркеу журналдарын айырбастау қажет болуы мүмкін.

7.6.2.2 Автономды сенім артылған үшінші тараптар

Автономды сенім артылған үшінші тараптарды автономды Сәйкестендірулік сертификат шығару қабілетіне байланысты көптеген жағдайларда сертификаттау органдарына жатқызады. Автономды Сәйкестендірулік сертификаттарға қосымша қорғаныс талап етілмейді, себебі олар өзін өзі қорғау қасиетіне ие. Автономды сәйкестендірулік сертификаттың қол жеткізерлігі маңызды фактор болып табылады, керісінше болған жағдайда автономды сәйкестендіру сертификаттарын қолдана отырып жасалған сәйкестендірулік айырбас қызмет көрсетуден бас тартуға әкеліп соғады. Аталған ақпаратты бірқатар түрлі репозиториялар көмегімен еселеу қызмет көрсетуден бас тарту ықтималдығын азайтады.

8 Қауіпсіздіктің басқа қызметтерімен/тетіктерімен өзара әрекет ету

8.1 Мүмкіндіктерді басқару

Қолданушыларға мүмкіндікті басқару туралы ақпаратты алуға рұқсат берместен бұрын олардың сәйкестендіруден өтуі қажет болуы мүмкін, ол өз кезегінде мүмкіндіктерді басқару стратегияларына сәйкес ресурстарға қол жеткізу мүмкіндігін береді. Сәйкестендіруге қатысты қызметі сәйкестендіру нәтижелерін мүмкіндіктерді басқару қызметіне беруі мүмкін, ол нәтижелерді мүмкіндіктерді басқару қызметі қолдануы мүмкін.

Сәйкестендіру ақпараты жоққа шығару қолданыстағы ресурстарға қол жеткізуді жоққа шығаруды талап етуі мүмкін.

8.2 Мәлімет тұтастығы

Сәйкестендірудің үзілместігін кепілдендіретін және мәліметтер шығу тегінің шынайылығын анықтау үшін сәйкестендіру мәліметтері тұтастығын бақылаумен бірге қолдануы мүмкін.

Кейбір сәйкестендіру тетіктері тура немесе жанама түрде шешуші материалдарды таратуға қолданылулары мүмкін, ол материалдарды тұтастық қызметі қолдануы мүмкін.

Шешуші материал жанама түрде анықталған кезде оны берілген мәліметтер ішінен жекелеп алу әдісі белгілі болуы керек немесе ол әдіс Сәйкестендірулік айырбас кезінде көрсетілуі қажет.

Ол материал тура анықталса, сәйкестендірулік айырбас кезінде кез келген бір бағытта қосымша мәліметтер жіберілуі қажет.

8.3. Мәліметтер құпиялығы

Кейбір Сәйкестендірулік тетіктер тура немесе жанама түрде шешуші материалдарды таратуға қолданылулары мүмкін, ол материалдарды қауіпсіздік қызметі қолдануы мүмкін.

Шешуші материал жанама түрде анықталған кезде оны берілген мәліметтер ішінен жекелеп алу әдісі белгілі болуы керек немесе ол әдіс сәйкестендірулік айырбас кезінде көрсетілуі қажет.

Ол материал тура анықталса, сәйкестендірулік айырбас кезінде кез келген бір бағытта қосымша мәліметтер жіберілуі қажет.

8.4 Бас тартпау

Кейбір сәйкестендіру тетіктері тура немесе жанама түрде шешуші материалдарды таратуға қолданылулары мүмкін, ол материалдарды авторлықты растау қызметі қолдануы мүмкін.

Шешуші материал жанама түрде анықталған кезде оны берілген мәліметтер ішінен жекелеп алу әдісі белгілі болуы керек немесе ол әдіс Сәйкестендірулік айырбас кезінде көрсетілуі қажет.

Ол материал тура анықталса, сәйкестендірулік айырбас кезінде кез келген бір бағытта қосымша мәліметтер жіберілуі қажет.

8.5 Аудит

Аудит үшін сәйкестендірумен байланысты мына ақпараттар қолданылуы мүмкін:

а) Сәйкестендіру нәтижелері (яғни ұқсастырылған кепілдендірілген объект);

б) Сәйкестендірулік ақпаратты жоққа шығаруға қатысты ақпарат;

в) Сәйкестендіру үздіксіздігін кепілдендіретін ақпарат;

г) Сәйкестендіру үрдісіне қатысты басқа да ақпарат.

А қосымшасы
(анықтамалық)

Қолданушы адамдарды сәйкестендіру

А.1 Жалпы ережелер

Ашық жүйе адамдар қызметін қолдаған кезде қолданушы адамдардың дұрыс сәйкестендірілуі ашық жүйе қауіпсіздігі үшін аса маңызды болуы мүмкін. Қолданушы адамдар мен компьютер жүйелерінің арасындағы диалог жүйеге заңсыз кіру мүмкіндігін ұлғайтуы мүмкін. Қолданушы адамдарды сәйкестендіру әдістері адамдарға қолайлы болулары қажет, және олар үнемді және қауіпсіз болулары қажет. Қолайсыз әдістер кей кезде адамдарды процедурадан бас тарту жолдарын іздестіруге итермелейді, ол заңсыз кіру мүмкіндігін арттыра түседі.

Қолданушы адамдарды сәйкестендіру қағидалары мына категорияларға бөлінетін сәйкестендіру қағидаларына негізделеді:

а) белгілі бір нәрсе;

б) қол да бар нәрсе;

в) қолданушы адамның жеке мінездемесі;

г) қолданушы – адам мен белгілі сенім артылған үшінші тарап ұқсастығын қабылдау;

д) контекст (сұраныс көзінің мекен жайы).

Жалпы жағдайда қолданушы адамды сәйкестендіру өзіне қолданушының сәйкестендірулік ақпаратпен бірге орнату сатысында өткізген куәліктерді салыстыруды қамтиды.

А.1.1 Белгілі бір нәрсе арқылы сәйкестендіру

Бұл категорияға өте жиі қолданылатын сәйкестендіру ақпараты – пароль болып табылады. Жүйеге қол жеткізерлік жағдайда қолданушы адам парольді енгізеді, ал сәйкестендіру жүйе болса қолданушы адамды тексеру мақсатында оны парольдер тізіміндегі қатысты жазбалармен салыстырады. Парольдер таптырмайтындай күрделі болулары қажет, парольдерді басқаруға арналған толық ойластырылған жүйе қажет. Керісінше болған жағдайда оны ынтасыз ашу қаупі бар.

А.1.2 Қолда бар арқылы сәйкестендіру

Бұл категорияға төмендегі секілді түрлі физикалық тасымалдауыштар жатады:

а) магниттік жолағы бар карточкалар;

б) интегральды микросызбалары бар карточкалар;

Магнитті жолағы бар карточканы қолданған жағдайда қолданушы – адам физикалық тасымалдаушы болып табылады, ал Сәйкестендірулік жүйе болса, Сәйкестендірулік ақпаратты физикалық тасымалдауыштан оқиды және оны сақталудағы аутентификациялық ақпаратпен салыстырады да, қолданушы адамды растайды.

Магнитті жолағы бар карточкалардың бір осалдығы оларды оңай көшіруге болатындығы, екіншісі – магнитті жолағы бар карточканы басқа адамның қолдану мүмкіндігінің барлығы.

Интегралды микросызбалары бар карточкаларды қолдану кезінде қолданушы адам физикалық тасымалдаушы болып табылады, ал сәйкестендіру жүйе болса, сәйкестендірулік ақпаратты физикалық тасымалдауыштан АІ айырбасын жүзеге асыру үшін оқиды және оны сақталудағы аутентификациялық ақпаратпен салыстырады да, қолданушы адамды растайды.

Интегралды микросызбалары бар карточкалардың артықшылықтары оларды оңай көшіру мүмкіндігінің болуы.

Интегралды микросызбалы карточканың оның ұстаушысын сәйкестендіру қабілетіне қарай екі вариант қарастырылады.

Егер интегралды микросызбалы карточка өзінің ұстаушысын сәйкестендіретін болса, онда екі сәйкестендіру сызбасы орын алады, онда қолданушы верификатор арқылы сәйкестендіріледі, ол транзитивтік жағынан қолданушының тікелей сәйкестендірумен тең.

Интегралды микросызбалы карточка өзінің ұстаушысын сәйкестендіру қабілеті жоқ болған жағдайда және объект ол тұлғаға қатысты емес болса, онда бұл сәйкестендіру әдісі сәтсіз болып аяқталады

А.1.3 Уақытқа тәуелді парольдер генераторы

Сәйкестендіру құралдарының бір түрі уақытқа тәуелді парольдер шығару қол жабдығы болып табылады. Айырбас кезінде қолданылатын сәйкестендіру ақпараты мына үйлесімділіктерді қолданады:

– Жабдықта сақталған құпия ақпарат ;

– Ағымдағы уақыт;

– PIN енгізуге арналған тетік көмегімен қолданушының жеке PIN- шартбелгісін енгізуі.

Осылайша орын алатын АІ айырбасы жабдықта көрсетіледі. Одан кейін ол шарттамаған түрде тексеру жүйесіне жіберіледі. Бұл жүйеге карточка арқылы синхронизация талап етіледі. Бұл сәйкестендіру тетігінің түрі осындай жабдық арқылы сәйкестендіру жасайтын тұлғадан мынаны талап етеді:

а) Қажетті жабдықты меңгеруді;

б) PIN-шартбелгісін білуді.

А.1.4 Қолданушы адамның жеке мінездемесі бойынша сәйкестендіру

Шартбелгілер өте сезімтал келеді, егер онымен белгіленген жолмен жұмыс жасамаса, түрлі материалдық жабдықтар ұрлануы мүмкін, сонымен қатар магнитті жолағы бар карточкалар санкцияланған жолдан тыс көшірілулері мүмкін. Қолданушы-адамдардың сәйкестендіру әдістерінің жоғарыда аталып өткен кемшіліктері жоқ класстар бар. Бұл әдістер адамдардың келесі жекеше қасиеттеріне негізделген:

– Жазудың жекеше ерекшеліктері;

– Саусақ іздері;

– Дауыс ерекшеліктері;

– Көз торларының ерекшеліктері;

Тетіктің көмегімен мәлімет енгізудің динамикалық ерекшеліктері. Қолданушы адамның жеке ерекшеліктерімен байланысты әдістер статистикалық және динамикалық болып екіге бөлінеді. Динамикалық әдістерді қолдану кезінде қысым, уақытша сипаттамалар, жазу жабдығының көшуі туралы ақпараттар сарапталады.

Тетікпен мәліметтерді енгізу ерекшеліктерін сараптау үздіксіз сәйкестендіруді қамтамасыз етеді.

Тіркеу сатысында Қолданушы адамның жекеше мінездемесі тіркеу жүйесіне енгізіледі. Қолданушы талап етілетін процедураны орындайды, мысалы, планшетте жазып оны саусағымен басады, арнайы сөздерді айтады. Сенімді ақпаратты алу үшін процедураны бірнеше мәрте қайталау қажет болуы мүмкін. Жүйе қолданушы адамның жекеше мінездемесін сараптап, оны қолданушы профиліне сақтайды.

Верификациялау/өткізу сатысында қолданушы-адам сәйкестендірудің қажетті процедурасын орындайды. Жүйе қолданушыдан сол қолданушы профилінде сақталған мәліметтерді салыстырады.

А.2 Қолданушы атынан әрекет ететін процесс

Кей жағдайда қолданушының өзі қатысуын болдырмау қажет болады. Осындай жағдайларда қолданушы жүйеде өз өкілдігіне ие болуы қажет, өмір уақытысы қолданушы қатысуына байланысты емес.

Өкілдік қолданушы секілді әрекет еткендіктен, қолданушы әрекеттері қолданушының қатысынсыз ұсынылуы мүмкін. Мысалы, қолданушы адам жүйеде тіркелуі мүмкін, содан кейін әрқайсысында тіркеу қажетінсіз түрлі компьютерлерді қолданады.

Тәуелсіз өмір уақыттары бар өкілдіктердің қолдауымен қатар, қосымша тетіктері бар өкілдіктерді қолдануына болады, олардың өмір уақыты қолданушының қатысуына байланысты.

Б қосымшасы
(анықтамалық)

OSI моделінде сәйкестендіру

(Бұл қосымша осы стандарттың біртұтас бөлшегі болып табылмайды)

Қауіпсіздік қызметтерінің анықтама моделі арасындағы өзара байланыс ИСО 7498-2 моделінде анықталады. Осы қосымша сәйкестендіруге қатысты ақпараттар жиынтығы болып табылады. Қауіпсіздік қызметінің екі түрі қарастырылады: тең объектілердің сәйкестендірілуі, ақпараттың шығу тегін сәйкестендіру.

Б.1 Тең құқылы объектілердің сәйкестендірілуі

Тең құқылы объектілердің сәйкестендірілуі қосуды орнату кезінде немесе бір немесе бірнеше объектілермен байланысты объектілер ұқсастығын растау мақсатында мәліметтерді беру сатысында қолданылуы мүмкін. Бұл қызметтер қосылуға бағытталған хаттамаларда және қосылуды орнатуды іске асыру хаттамаларда да қол жеткізерлік. Тең құқылы объектілер сәйкестендіру біржақты және екі жақты болуы мүмкін.

Б.2 Мәліметтердің шығу тегін сәйкестендіру

Мәліметтердің шығу тегін сәйкестендіру мәліметтер элементтерінің шығу тегін растауды қамтамасыз етеді. Қызметтер мәліметтер элементтерді еселеуден қорғауды қамтамасыз етеді.

Б.3 OSI моделінің түрлі деңгейлерінде сәйкестендіруді қолдану

Тең құқылы объектілердің сәйкестендірілуі және мәліметтердің шығу тегі OSI моделінің мына деңгейлеріне қатынасы бар: тораптық деңгей (3 деңгей); көліктік деңгей (4 деңгей); қолданбалы деңгей (7 деңгей).

Б.3.1 Тораптық деңгейде сәйкестендіруді қолдану

Тораптық деңгейде қолданылатын тең құқылы объектілердің сәйкестендірілуі тораптық объектілер ұқсастығын растауды қамтамасыз етеді. Бұл қызмет байланыс тораптарын, кіші тораптарды және ретрансляторларды сәйкестендіруге мұрсат береді.

Тораптық деңгейде қолданылатын мәліметтер шығу тегін сәйкестендіру мәліметтер элементінің ұқсастығын растау мүмкіндігін береді. Оның көзі болбыр торап, кіші торап, ретранслятор болулары мүмкін.

Тораптар деңгейінде қолданылатын тетіктер деңгей ішінде орналасқан.

Б.3.2 Көліктік деңгейде қолданылатын сәйкестендіру

Көліктік деңгейде қолданылатын тең құқылы объектілер сәйкестендірілуі көліктік объектілер ұқсастығын растау мүмкіндігін береді. Бұл қызмет аяқталған жүйелерді сәйкестендіруге мүмкіндік береді. Осы аяқталған жүйелермен қолпашталатын түрлі қосымшалар сәйкестендірілмеуі мүмкін.

Көліктік деңгейде қолданылатын мәліметтер шығу тегін сәйкестендіру мәліметтер шығу тегін растау мүмкіндігін береді. Мәліметтер көзі болып аяқталған жүйе табылады.

Көліктік деңгейде қолданылатын мәліметтер шығу тегі деңгей ішінде орналасқан.

Б.3.3 Сәйкестендіруді қолданбалы деңгейде қолдану

Қолданбалы деңгейде қолданылатын тең құқылы объектілер сәйкестендірілуі аяқталған жүйенің қосымша объектілерінің ұқсастығын растайды. Бұл қызмет қосымша объектілерінің немесе қосымша процесстерін сәйкестендіруге мүмкіндік береді. Осы аяқталған жүйемен қолданылатын қосымшаның немесе қосымша процесстері сәйкестендірілуі мүмкін.

Қолданбалы деңгейде мәліметтің шығу тегін сәйкестендіру мәліметтер көздерін растау мүмкіндігін береді. Мәліметтер көзі қосымша объектісі немесе қосымша процессі бола алады.

Қолданбалы деңгейде қолданылатын тетіктер қолданбалы деңгейде немесе мәліметтерді ұсыну деңгейінде орналасуы мүмкін. Қолданбалы деңгейде жүзеге асырылатын сәйкестендіру торабы және көлік деңгейлеріне ұсынатын сәйкестендіру қызметтері үшін қолданылады.

В қосымшасы
(анықтамалық)

Бірегей нөмірлер немесе шақырулар көмегімен қайта жаңғыртуға қарсы әрекет ету

В.1 Бірегей нөмірлер

Бірегей нөмірлерді мәлімдеушілер жасайды. Бір бірегей нөмірлер екі рет бір верификаторлармен қабылданбауы қажет. Бұған бірнеше тістер арқылы қол жеткізуге болады. Тиімді көрінетін кейбір технологиялар тәжрибеде пайдасыз болуы мүмкін. Бұндай технологияға қарапайым мысалы айырбас сәйкестендірілуі кезінде сәтті қолданылғанда алынған бірегей номерлерді бақылау болып табылады. Бұл сәтті сәйкестендіру сандарының көбейген кезде жады көлеміне талаптардың өсуіне әкеліп соғады. Бұндай әдіс құны/немесе өнімділігі жағынан тиімсіз болып табылады.

Верификатор жағынан жады көлеміне қойылатын талаптарды төмендетудің бір ғана жолы бірнеше уақыт кезеңі ішінде барлық сәтті қолданылған бірегей номерлерді тіркеу болып табылады.

Бұл бірегей номерлердің бөлігі ретінде уақытша белгіні қолдану қажеттілігіне әкеліп соғады, сондықтан тек «жақындағы» бірегей номерлер ғана верификатор жадысында сақталады. Тәжрибеде бірнеше минут көлемі жеткілікті болып табылады. Ол бір жағынан жады көлеміне талапты шектейді, ал тағы бір жағынан принципиал мен верификаторлар түрлі уақытша сілтемелер синхронизациямен байланысты қиыншылықтарды жояды,

Қызмет көрсетуден бас тартуды болдырмау мақсатында, екі түрлі принципиалдардан туындаған бірегей нөмірлер арасындағы конфликті болдырмау қажет. Ол үшін бірегей номерлер диапазоны мейлінше үлкен болуы қажет. Бірегей номерлер диапазоны уақыт бірлігінде (мысалы, бір секунд ішінде) жүзеге асырылатын Сәйкестендірулердің максималды сандарымен байланысты, ол әр верификатор үшін есепке алынуы қажет, ол арқылы Сәйкестендіруге талпыныс жасалады. Егер принципиал қолданатын уақытша сілтеме ондай сандар диапазонын қамтамасыз етпесе, бірегей номер диапазонын кеңейту үшін онда уақытша белгіге кездейсоқ сан қосылады.

В.2 Шақырулар

Шақыруларды верификаторлар жасайды. Бір ғана түрлі шақыру екі мәрте бір верификатормен жасалмауы қажет. Оған тек бірнеше жолмен жасалады.

Теориялық жағынан тиімді көрінетін кейбір технологиялар тәжрибеде пайдасыз болуы мүмкін. Бұндай технологияға шыққан барлық шақыруларды тіркеу болып табылады. Бұл сәтті сәйкестендіру сандарының көбейген кезде жады көлеміне талаптардың өсуіне әкеліп соғады. Бұндай әдіс құны/немесе өнімділігі жағынан тиімсіз болып табылады.

Верификатор жағынан жады көлеміне қойылатын талаптарды төмендетудің бірнеше жолдары бар.

– шақыруларда кезекті мағыналарды беру және тек соңғы мағынаны сақтау.

– шақыруларда кездейсоқ сандарды көрсету, бұл «бір ғана шақыруды бір верификатор екі рет жасауға болмайды» деген ережені бұзса да, бұндай оқиғаның ықтималдығын үлкен диапазон ішінен кездейсоқ сандарды қолдануда керекті деңгейге дейін төмендетуге болады.;

– шақыруда уақыт белгілерін жасау;

– уақытша белгіледің сәйкестігі мен кездейсоқ сандарды қолдану.

Г қосымшасы
(анықтамалық)

Сәйкестендіруге жасалатын шабуылдардың кейбір түрлерінен қорғану

Г.1 Тың тыңдау – жаңғырту шабуылдары

Жаңғыртудың екі вариантын қарастыру қажет. Оған айырбас кезінде қолданылатын қандайда бір сәйкестендіру ақпаратты жаңғырту жатады:

– Бір верификаторға;

– Басқа верификаторға.

Соңғы жағдай принципиалдың верификациялық ақпараты бірқатар верификаторларға аян болады. Жаңғырту шабуылы жасырын ауыстырудың жеке жағдайы болады.

Жаңғыртудың екі жағдайында да шақырудың көмегімен қарсы тұруға болады. Шақыруды верификаторлар тудырады. Бір ғана шақыру бір верификаторға екі рет берілмеуі қажет. Оған екі жолмен жетуге болады (В Қосымшасын қараңыз).

Г.2 Сол верификаторға қайта жаңғырту

Сол бір верификаторға қайта жаңғыртуға бірегей номерлер немесе шақырулар арқылы әсер етуге болады.

Бірегей номерді мәлімдеуші жасайды. Бір бірегей номер ешқашан верификатормен екі рет қабылданбайды. Оған бірнеше жолдармен қол жеткізуге болады (В қосымшасын қараңыз).

Г.3 Басқа верификаторға қайта жасау

Басқа верификаторға қайта жасауға шақыруларды қолдану арқылы қарсы тұруға болады. Басқа жағынан АІ айырбасы кезінде осы верификаторға таңсық кез келген параметрлермен қарсы тұруға болады. Ол верификатордың аты, оның тораптық мекен жайы, жалпы жағдайда, верификаторға қатысты бір ғана тексеру АІ қолданатын бірегей атрибут болып табылатын қолдануға болады.

Г.4 Жолда ұстау- жасырын айырбас шабуылдары.

Г.4.1 Тікелей шабуылдар

Шабуылдардың бір түрі (тікелей шабуыл) «қаскүнем» Сәйкестендіру бастамашысы болып табылады деп болжайды. Бұндай шабуыл тек мәлімдеуші мен верификатор «қаскүнем» арқылы Сәйкестендірулік ақпаратпен алмасады, оны білместен, яғни «қаскүнем» мәлімдеуші алдында белгілі верификатор ал, верификатор алдында мәлімдеуші болғансып алдайды.

Мысалы, С «қаскүнем» В верификаторы алдында А мәлімдеуші болғансыса, С әсерін А мен В-дан бастайды. С А ға В мын деп хабарлайды, А В ға қатысты Сәйкестендіруді сұрайды, сонымен қатар В ға А мын деп айтып өзін сәйкестендіруді сұрайды.

Сәйкестендіру барысында А В ға қатысты мәліметші ретінде әрекет етеді, (шындығында В рөлінде С ойнайды) сондықтан С В ға қатысты сәйкестендіру мақсатында қолданатын ақпаратты алады. В верификатор рөлін орындайды сондай ақ С ақпаратын береді, оны соңғысы верификатор ролін ойнауға қажет етеді. Сәйкестендіруден кейін «қаскүнем» С В алдында сәйкестендірілген А секілді көрінеді.

Аталған шабуыл түріне қарсы тұру әдістері түрлі верификаторларға арналған қайта жасаудан сақталады:

а) сәйкестендіруді бастаған объект үнемі мәлімдеуші болады;

б) айырбас кезінде қолданылатын және оны мәлімдеуші берген сәйкестендіру сұранысының бастамашысы немесе сәйкестендіру шақыруына жауапты ретіндегі рөліне байланысты болады. Бұл айырмашылық верификаторға жоғарыда қарастырылған шабуыл түрін анықтауға мүмкіндік береді. Бұл Г қосымшасында толығырақ көрсетілген.

Г.4.2 Оппортунистік шабуылдар

Шабуылдардың бір түрінде «қатысушы» сәйкестендірулік айырбасқа сәйкестендіру ақпаратын алып, сонымен қатар өзіне мәлімдеуші ролін ала отырып қатысады.

Аталған шабуыл түріне қарсы әрекет қосымша қызметті қолдану (мәліметтер тұтастығы немесе қауіпсіздік) болып табылады. ИА айырбасы қандай да бір ақпаратпен толықтырылады, сәйкестендіру процессінің заңды қатысушылары болып табылатын верификатор мен мәлімдеушіге кілт алуға мүмкіндік беретін ақпаратты береді. Алынған кілт криптографияға негізделген тұтастықты қамтамасыз ету немесе қауіпсіздікті қамтамасыз ету тетіктерінде қолданылады.

Аталған шабуылға қарсы әрекет етудің басқа жолы мәліметтерді беру торабының ішінде қамтуды жүзеге асыру мүмкін болмаған жағдайда, яғни мәліметтер арналған жерге өзгерместен жеткізілген жағдайда қолданылады. Бұл жағдайда шабуылға қарсы әрекет ету үшін тораптық адресін туындау қызметі қосымша ақпарат есебінде қолдануы мүмкін. Онда ИА айырбас тораптық адреске байланысты болады.

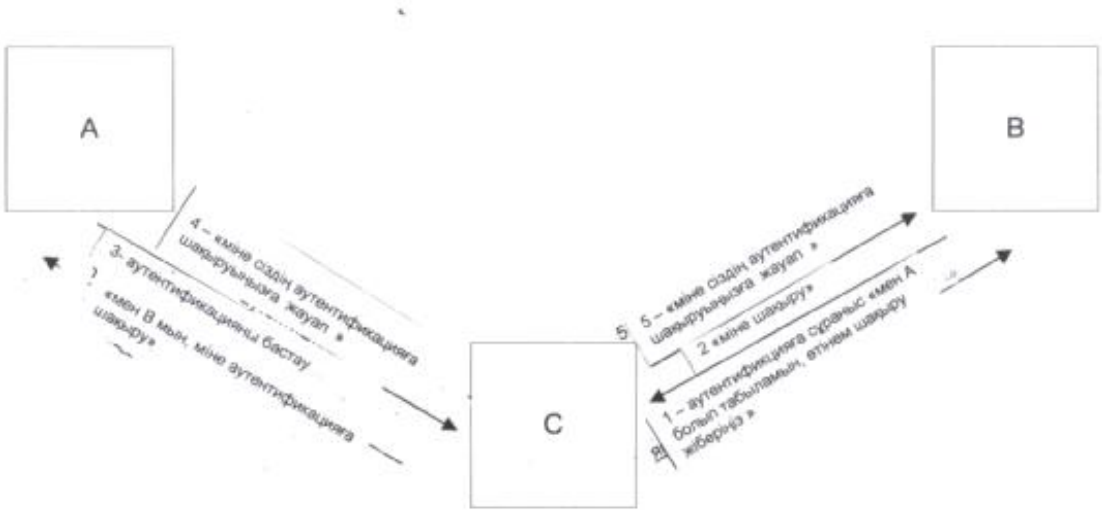
Г 5 «қаскүнемдер» шабуылынан қорғанудың шектелген формасы

Г.4 бөлімінде қарастырылған шабуылдың екінші түрі шақыруларды немесе бірегей номерлерді қолданған кезде мүмкін болады. Қорғаныс дегеніміз мәлімдеушінің сәйкестендіруге шақыру немесе сәйкестендіру сұранысы соңынан жауабы бар ма жоқ па анықтау белгісін қолдануды көздейді. Белгі (мысалы, бірліктерге орнату кезінде), сәйкестендіру соңынан жауаптың барын немесе (нөлге орнату кезінде), аутентификацияға сұранысқа жауаптың болғанын көрсетіп тұрады. Белгі мағынасы жауапты шығарғанда қолданылатындықтан мәлімдеушінің жауабы оның мағынасына байланысты екенін білдіреді. Бұдан әрі біз қарастырылған белгіні шақыру/сұраныс белгілері деп санаймыз.

Г.6 Шақыруды қолданатын хаттама

Шақыруларды қолданғанда С А болып алдайды да В-ға сәйкестендірулік сұраныс жібереді (бірінші айырбас). В С шақыруын жасайды (екінші айырбас). С А сәйкестендірілуіне шақыру жібереді алынғанын В ға береді (үшінші айырбас). А С дан алған шақыруды қолдана отырып, өзінің жауабын есептеп шығарады шақыру /сұраныс белгісін соңғысы «шақыру» күйінде жасайды. С В ға А дан алған жауабын береді. В жауапты тексереді. Ең басында Сәйкестендірулік сұраныс С дан алынғандықтан В шақыру/сұраныс белгісі «сұраныс» күйінде орнатылған. Алған жауапта шақыру/сұраныс «шақыру» күйінде орнатылғандықтан сәйкестендіруге жасалған сұраныс қайтарылады (D.1 суретін қараңыз).

Егер В сұраныстарды да сәйкестендіруге шақыруларды да қолдап отырса, В ға сақтанудың қосымша шараларын қолдану қажет. В осы шақыру қай мәлімдеушіге берілгені туралы ақпаратты сақтау қажет, сондықтан В оны сәйкестендіруге шақыруды берген кезде басқа мәлімдеушімен қолдана алмайды. (үшінші айырбас).

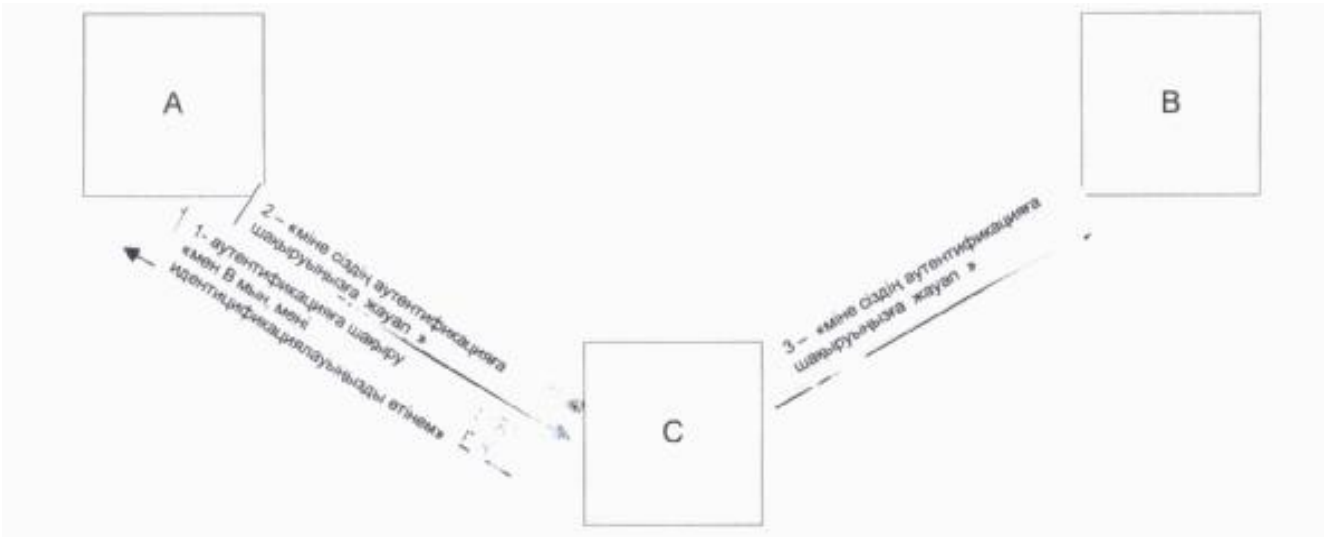


Г.1 сурет– шақыруларды қолдану кезінде «қаскүнем» шабуылдарына қарсы әрекет ету

Ескертпе – тікелей шабуылдарға а) немесе б), әдістері арқылы қарсы тұру, Г.4.1 бөліміндегі көрсетілгендей, оппортунистік шабуылдарға осалдық сақталады.

Г.7 Бірегей номерлерді қолданатын хаттама

Бірегей номерлерді қолдануда С В болып алдайды да А Сәйкестендіруге шақыру жасайды (бірінші айырбас). А бірегей номерді қолдану арқылы өз жауабын есептеп шығарады шақыру/сұраныс белгісі «шақыру» сәтінде құралады (екінші жауап). С В-ға А-дан алған жауабын жібереді (үшінші айырбас). В жауапты тексереді. Ол «шақыру» кезінде қалыптасқан шақыру/сұраныс белгіге ие. Бірақ В еш сәйкестендіруге шақырулар жасамады ол сәйкестендірулік ақпаратты жоққа шығарады (Г.2 суретін қараңыз).



Г.2. суреті – Бірегей нөмірлерді қолдану кезінде «қаскүнемдер» шабуылынан қорғану

Д Қосымшасы
(анықтамалық)

Сәйкестендіру тетіктерінің кейбір тән мысалдары

Осы қосымшада Сәйкестендіру тетіктердің екі мысалы келтірілген.

Д.1 Бірегей нөмірлерді оперативті түрде қол жеткізерлік сәйкестендіру сертификаттармен бірге қолданудың тура мысалы

Бұл мысал 8.1. тармақта сипатталғандай 3 Сыныпқа бірегей нөмірлер тетігін қолдануды суреттейді. Бұл мысалда оперативті түрде қол жеткізерлік сәйкестендіру сертификаттар, бірегей идентификатор, қорғаныс әдісі, қорғаныс параметрі, сәйкестендіру сертификаттарына енгізілген әрекет уақыты қолданылады. Бұл мысалда қолданылатын әдіс бір ғана ақпаратты айырбасты қажет етеді және бір ғана сәйкестендіру сертификаты бір реттен көп қолдануына болады.

Қорғаныс әдісі сертификатқа тіркелген қорғаныс параметрі мен сәйкестендіру сертификатын заңсыз қолдануды қорғайтын басқарудың сыртқы параметрі арасындағы қатынасты анықтайды. Басқарудың сыртқы параметрі қорғаныс параметрінен біржақты түрленудің көмегімен сыртқы қорғаныстан алынуы мүмкін, ол мынау:

– Сыртқы басқару параметрі тексеру мағынасына ие, ал қорғаныс параметрі тексерулік мағынаға біржақты қызметті қолдану нәтижесі болып табылады;

– Басқарудың сыртқы параметрі жеке кілт болып табылады, ал қорғаныс параметрі оған сәйкес жалпы кілт болып табылады.

Тексеру мағынасы сыртқы басқару параметрі ретінде қолданған жағдайда, ол верификаторға сәйкестендіру сертификатын иеленудің растау ретінде жіберіледі. Беру кезінде кілт қорғанған болу қажет, яғни мәлімдеуші арқылы сыртқы құпия кілт көмегімен шартталады, сыртқы құпия кілт өз кезегінде мәліметтер беру каналымен байланысты немесе мәліметтер беру каналының қабылдау ұшымен байланысты болады.

Жеке меншіктік құқықтық қорғау мен көшіруден қорғау шақыру мен түрлену функциясы арқылы жүзеге асады. Сыртқы басқару параметрінің түріне байланысты түрленудің үш түрлі функциясы қолданылады (F):

а) *Біржақты функция:* Сыртқы басқару параметрі тексеру мағынасына ие болғанда шақыру мен тексеру мағынасы Г-да біржақты қызмет арқылы түрленеді. Нәтиже мен шақыру верификаторға ұқсас түрленуіне мұрсат беріп барып өтеді.

b) Асимметриялық алгоритм. Басқарудың сыртқы параметрі жеке кілт болғанда, шақыру жеке кілт арқылы тіркеледі.

c) Симметриялық алгоритм. Сыртқы басқару параметрі құпия кілт болғанда шақыру шартталады немесе тексеру мағынасының көмегімен иесі белгісіз қол қойылады және сол құпия кілт ретінде қолданылады.

Бұл мысал сәйкестендірулік шығу тегі бар мәліметтерге де объектілерге де қатысты қолданылады. Мәліметтер шығу тегін сәйкестендірілген жағдайда немесе мәліметтердің сандық идентификациялық белгісі F функциясы арқылы түрленеді.

Оперативті түрде қол жеткізерлік қызметі Сәйкестендірулік сертификатты алуға сұраныс қызметі және сыртқы басқару параметрі қолданылады. Содан кейін түртікі болу қызметі бірегей нөмірді шығарып, келесі кіру мәліметтерін қолдана отырып, түрленуді жүзеге асырады:

– бірегей нөмір:

– сыртқы басқарушы параметр;;

– бірегей идентификатор (міндетті емес параметр);

– сандық идентификациялық белгі (мәліметтердің шығу тегін сәйкестендірілген кезде).

Бұдан басқа, егер басқарушы мағына тексерулік мағына немесе құпия басқару кілті болған кезде, түрткі қызметі ол мағынаны шартталған күйінде жібереді, ол шартбелгіні тек верификатор ғана таба алады және 14 суретте көрсетілгендей ИА айырбасын құрады.

Қызмет айырбас кезінде қолданылған сәйкестендірілген ақпараттың сәйкестендіру сертификатындағы қорғаныс мағынасы көмегімен оның растығын тексереді. Сонымен қатар, тексеру мағынасын немесе құпия басқару кілтін қолдану кезінде тексеру қызметі шартталған тексеру мағынасы мен басқарудың құпия кілтін ашады және оның қорғаныс мағынасына сәйкестігін тексереді. Қызмет сонымен қатар бірегей нөмірдің сәтті Сәйкестендіру жағдайында бұрын қолданылмағанын тексереді.

Сәйкестендіру сұранысы (бірегей сан), AUC
(айырым идентификаторы, [қорғаныс әдісі],
қорғаныс маңызы),[C (басқару
мағыналары)] F (басқарушы мағына,
сұраныс, [айырым идентификаторы],
(сандық таңба)

МӘЛІМДЕУШІ_____ВЕРИФИКАТОР

Д.1 суреті – Оперативті түрде қол жеткізерлік Сәйкестендірулік сертификатты қолданған кездегі бірегей нөмірлер тетігі

Ескертпе

1 ALC(...) жақшаларда көрсетілген параметрлерді қамтитын сәйкестендіру сертификатын белгілеу үшін қолданылады;

2 C(...) қауіпсіздік сервисін белгілеу мақсатында қолданылады; бұл тек тексеру мағынасында басқару параметрін қолдану мағынасында пайдаланады.

Д.2 Шақыру тетігі және оперативті түрде қол жеткізерлік сәйкестендіру сертификаты

Бұл тетік 5.3. тармақта көрсетілген қағидаларды және 8.1.5.2. (Е 2 суретті қараңыз) тармақта сипатталған шақыру тетігін сәйкестендірілуін растау кезінде сәйкестендіру сертификаты қолданады. Сәйкестендіру сертификаты сенім артылған үшінші жақтың сертификат иесін бірегей идентификатор көмегімен сәйкестендіргенін растауды қамтамасыз етеді. Тетік растау құралдарын қамтамасыз етеді, сондықтан осы бірегей идентификатордың сәйкестендіру сертификатының иесі мәлімдеуші болып табылады.

Бұл мысал оперативті түрде қол жеткізерлік сәйкестендіру сертификаттарды, бірегей идентификаторды, қорғау әдісін, сәйкестендіру сертификатына тіркелген қорғау параметрлері мен әрекет уақытын қолданады. Бұл мысал бойынша сәйкестендіру сертификатты бірнеше рет қолдануға болады.

Қорғаныс әдісі сертификатқа тіркелген қорғаныс параметрі мен сәйкестендіру сертификатын заңсыз қолданудан қорғайтын басқарудың сыртқы параметрі арасындағы қатынасты анықтайды. Басқарудың сыртқы параметрі қорғаныс параметрінен біржақты түрленудің көмегімен сыртқы қорғаныстан алынуы мүмкін, ол мынау:

Сыртқы басқару параметрі тексеру мағынасына ие, ал қорғаныс параметрі тексерулік мағынаға біржақты қызметті қолдану нәтижесі болып табылады;

Басқарудың сыртқы параметрі жеке кілт болып табылады, ал қорғаныс параметрі оған сәйкес жалпы кілт болып табылады.

Тексеру мағынасы сыртқы басқару параметрі ретінде қолданған жағдайда, ол верификаторға сәйкестендіру сертификатын иеленудің растау ретінде жіберіледі. Беру кезінде кілт қорғанған болу қажет, яғни мәлімдеуші арқылы сыртқы құпия кілт көмегімен шартталады, сыртқы құпия кілт өз кезегінде мәліметтер беру каналымен байланысты немесе мәліметтер беру арнасының қабылдау ұшымен байланысты болады.

Жеке меншіктік құқықтық қорғау мен көшіруден қорғау шақыру мен түрлену функциясы арқылы жүзеге асады. Сыртқы басқару параметрінің түріне байланысты түрленудің үш түрлі функциясы қолданылады (F):

а) *Біржақты қызмет:* Сыртқы басқару параметрі тексеру мағынасына ие болғанда шақыру мен тексеру мағынасында біржақты қызмет арқылы түрленеді.

Нәтиже мен шақыру верификаторға ұқсас түрленуіне мұрсат беріп барып өтеді.

b) Асимметриялық алгоритм. Басқарудың сыртқы параметрі жеке кілт болғанда, шақыру жеке кілт арқылы тіркеледі.

c) Симметриялық алгоритм. Сыртқы басқару параметрі құпия кілт болғанда шақыру шартталады немесе тексеру мағынасының көмегімен иесі белгісіз қол қойылады және сол құпия кілт ретінде қолданылады.

Бұл мысал сәйкестендірулік шығу тегі бар мәліметтерге де объектілерге де қатысты қолданылады. Мәліметтер шығу тегін сәйкестендірілген жағдайда немесе мәліметтердің сандық баламалық белгісі F қызметі арқылы түрленеді.

Сұраныс қызметі сәйкестендіру сертификатын алуға және сыртқы басқару параметріне қолданылады. Түрткі болу қызметі сәйкестендіру сұранысын құрады. Сәйкестендіру сұранысын алған кезде тексеру қызметі сәйкестендіретін ақпарат түрінде айырбас кезінде қолданылатын шақыру жасайды. Содан кейін түрткі қызметі келесі кіру мәліметтерін қолдана отырып, түрленуді жүзеге асырады.

– шақыру;

– сыртқы басқарушы параметр;

– бірегей идентификатор (міндетті емес параметр);

– сандық идентификациялық белгі (мәліметтердің шығу тегін сәйкестендірілген кезде).

Егер басқарушы мағына тексерулік мағына немесе құпия басқару кілті болған кезде, түрткі қызметі ол мағынаны шартталған күйінде жібереді, ол шартбелгіні тек верификатор ғана таба алады және 16 суретте көрсетілгендей ИА айырбасын құрады. Тексеру қызметі ИА айырбасының шынайылығын Сәйкестендірулік сертификаттағы қорғаныс параметрі арқылы қарастырады. Сонымен қатар тексеру мағынасын немесе құпиялық басқару кілтін қолданған кезде тексеру қызметі шартталған тексеру қызметін немесе құпия басқару кілтін ашады да, оны қорғаныс мағынасына сәйкестігін тексереді. Сонымен қатар шақырудың жіберілген шақырумен сәйкестігі тексеріледі.

Сәйкестендіруге тапсырыс, сұраныс

МӘЛІМДЕУШІ_____ВЕРИФИКАТОР

_____

AUC (айырым идентификаторы, [қорғаныс әдісі], қорғаныс маңызы),[C (басқару мағыналары)] F (басқарушы мағына, сұраныс, [айырым идентификаторы], (сандық таңба)

Ескертпе

AUC (...) белгісі дөңгелек жақша ішінде көрсетілген параметрлерді қамтитын Сәйкестендірулік сертификат үшін қолданылады.

C (...) белгісі қауіпсіздік қызметінің әрекеттерін орындайтын қосымша үшін қолданылады. Бұл тек басқарушы параметр тексерулік маңызға ие болған жағдайда ғана қолданылады.

Д.2 сурет – Сәйкестендіру сертификатын қолдану кезінде шақыру тетігі

ӘОЖ 681.324:006.354 **МСЖ 35.100**

Түйінді сөздер: мәліметтерді өңдеу, ақпараттық айырбас, тораптардың өзара әсері, ашық жүйелердің өзара әсері, коммуникациялық процедуралар, ақпаратты қорғау, қауіпсіздік технологиясы, шолу.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология

ВЗАИМОДЕЙСТВИЕ ОТКРЫТЫХ СИСТЕМ

Основы безопасности для открытых систем
Часть 2
Основы аутентификации

СТ РК ИСО/МЭК 10181-2-2008
(ИСО/МЭК 10181-2:1996 «Информационная технология. Взаимодействие открытых систем. Основы безопасности для открытых систем: Основы аутентификации», IDT)

Издание официальное

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

Астана

Предисловие

1 ПОДГОТОВЛЕН ЗАО «Инфосистемы Джет».

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 10181-2:1996 «Информационная технология. Взаимодействие открытых систем. Основы безопасности для открытых систем: Основы аутентификации» («Information technology. Open Systems Interconnection. Security frameworks for open systems: Authentication 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

СТ РК ИСО/МЭК 10181-2008 под общим заголовком "Информационная технология. Взаимодействие открытых систем. Основы безопасности для открытых систем" состоит из следующих частей:

– Часть 1. Обзор

– Часть 2. Основы аутентификации

– Часть 3. Основы управления доступом

– Часть 4. Основы неотказуемости от авторства

– Часть 5. Основы конфиденциальности

– Часть 6. Основы целостности

– Часть 7. Основы учета событий безопасности и оперативного оповещения.

Приложения настоящего стандарта являются справочными.

Ко многим приложениям предъявляются требования обеспечения безопасности с целью противостояния угрозам, сопутствующим передаче информации. Некоторые наиболее известные угрозы безопасности, а также сервисы и механизмы безопасности, которые могут быть использованы для защиты от угроз, описаны в ГОСТ ИСО 7498-2-2002.

Настоящий стандарт определяет общие основы для предоставления сервисов аутентификации.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология ВЗАИМОДЕЙСТВИЕ ОТКРЫТЫХ СИСТЕМ. ОСНОВЫ БЕЗОПАСНОСТИ ДЛЯ ОТКРЫТЫХ СИСТЕМ Часть 2 Основы аутентификации

Дата введения 2008.07.01

1 Область применения

Настоящий стандарт устанавливает Основы безопасности, предназначенные для решения задачи применения сервисов безопасности в среде открытых систем. Под термином «Открытые системы» понимаются такие области, как базы данных, распределенные приложения, открытая распределенная обработка и взаимодействие открытых систем.

Основные положения безопасности оперируют как с элементами данных, так и с последовательностями действий (но не элементами протоколов), используемыми для получения специфических сервисов безопасности. Эти сервисы безопасности могут применяться как к взаимодействующим сущностям систем, так и к обмену данными между системами, а также к данным, которыми управляют системы.

Настоящий стандарт устанавливает:

- основные понятия аутентификации;
- возможные классы механизмов аутентификации;
- сервисы для этих классов механизмов аутентификации;
- функциональные требования к протоколам для поддержки этих классов механизмов аутентификации;
- общие требования к управлению аутентификацией.

Настоящий стандарт может быть применен в различных типах стандартов, включая:

1) стандарты, в которых фигурирует понятие аутентификации;

2) стандарты, предоставляющие сервис аутентификации;

3) стандарты, использующие сервис аутентификации;

4) стандарты, специфицирующие средства и методы предоставления аутентификации в архитектуре открытых систем;

5) стандарты, специфицирующие механизмы аутентификации. [Следует заметить, что случаи 2), 3) и 4) могут включать в себя аутентификацию, но иметь иную основную цель.]

Эти стандарты могут применять настоящий стандарт следующим образом:

– стандарты типов 1), 2), 3), 4) и 5) могут использовать терминологию настоящего стандарта;

– стандарты типов 2), 3), 4) и 5) могут использовать сервисы, определенные в разделе 7 настоящего стандарта;

– стандарты типа 5) могут базироваться на механизмах, определенных в разделе 8 настоящего стандарта.

Как и другие сервисы безопасности, аутентификация может предоставляться только в контексте определенной политики безопасности для конкретного приложения. Определение политики безопасности находится вне рамок настоящего стандарта.

Рамки настоящего стандарта не охватывают спецификацию деталей протокольных обменов, которые необходимо выполнить для осуществления аутентификации.

Настоящий стандарт не специфицирует конкретные механизмы для поддержки сервисов аутентификации. В других стандартах (таких, как *СТ РК ИСО/МЭК 9798-2008*) конкретные методы аутентификации проработаны более детально. Кроме того, примеры подобных методов фигурируют в других стандартах (таких, как ИСО/МЭК 9594-8) для освещения специфических требований аутентификации.

Некоторые процедуры, описанные в настоящем стандарте, обеспечивают безопасность путем использования криптографических методов. Настоящий стандарт не зависит от использования конкретных криптографических или иных алгоритмов, хотя некоторые классы механизмов аутентификации могут зависеть от свойств конкретного алгоритма, например, от свойств асимметричности. *Выбор и применение конкретных средств криптографической защиты информации регламентируется законодательством Республики Казахстан и не является предметом рассмотрения настоящего стандарта.*

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

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

СТ РК ИСО/МЭК 9798-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Механизмы аутентификации. Часть 2. Механизмы с применением алгоритмов симметричного шифрования.

СТ РК ИСО/МЭК 9798-3-2008 Информационная технология. Методы и средства обеспечения безопасности. Механизмы аутентификации. Часть 3. Механизмы с применением методов цифровой подписи.

СТ РК ИСО/МЭК 10116-2008 Информационная технология. Методы и средства обеспечения безопасности. Режимы работы n-битовых блочных шифров.

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

ГОСТ ИСО 7498-2:2002 Информационная технология. Взаимосвязь открытых систем. Базовая эталонная модель. Часть 2. Архитектура защиты информации.

ИСО/МЭК 8348-2002 Информационные технологии. Взаимодействие открытых систем. Определение сетевой службы.

ИСО/МЭК 8824-2002 (в 4 частях) Информационная технология. Абстрактная система обозначения синтаксиса версии один (ASN.1).

ИСО/МЭК 9545-1994 Информационные технологии. Взаимодействие открытых систем. Структура прикладного уровня.

ИСО/МЭК 9594-8-2001 Информационные технологии. Взаимодействие открытых систем. Справочник. Шифрование открытым ключом и качественные сертификатные структуры

ИСО/МЭК 9979-1991 Криптографические методы. Процедуры регистрации криптографических алгоритмов.

3 Термины, определения

В настоящем стандарте применены термины по *СТ РК ИСО/МЭК 10116-2008*, *СТ РК ИСО/МЭК 10181-1-2008*, ГОСТ ИСО 7498-2, а также следующие термины с соответствующими определениями:

3.1 Автономный аутентификационный сертификат (off-line authentication certificate) - аутентификационный сертификат, привязывающий отличительный идентификатор к верификационной ИА, который может быть доступен всем сущностям.

3.2 Асимметричный метод аутентификации (asymmetric authentication method) - метод аутентификации, в котором не вся информация аутентификации разделяется обеими сущностями.

3.3 Аутентификационный обмен (authentication exchange) - последовательность одной или более передач обменной информации аутентификации (ИА) с целью выполнения аутентификации.

3.4 Аутентификационный сертификат (authentication certificate) - сертификат безопасности, заверенный уполномоченным по аутентификации,

который может использоваться для подтверждения подлинности некоторой сущности.

3.5 Аутентификация (authentication) - предоставление гарантии заявленной подлинности некоторой сущности.

3.6 Аутентифицированная сущность (authenticated identity) - отличительный идентификатор принципала (объекта аутентификации), удостоверенный в процессе аутентификации.

3.7 Верификатор (verifier) - сущность, которая либо сама, либо представляет сущность, подтверждающую подлинность. Верификатор обладает функциональностью, необходимой для осуществления информационного обмена данными в процессе аутентификации.

3.8 Верификационная информация аутентификации (верификационная ИА) (verification authentication information, verification AI) - информация, используемая верификатором для верификации сущности, заявленной в обменной ИА.

3.9 Запрос (challenge) - параметр, переменный по времени, генерируемый верификатором.

3.10 Заявитель (claimant) - сущность, являющаяся или представляющая принципала для целей аутентификации. Заявитель включает функции, необходимые для участия в аутентификационных обменах от имени принципала.

3.11 Заявляемая информация аутентификации (заявляемая ИА) (claim authentication information, claim ИА) - информация, используемая заявителем для генерации обменной ИА, необходимой для аутентификации принципала.

3.12 Инициатор аутентификации (authentication initiator) - сущность, начинающая аутентификационный обмен.

3.13 Информация аутентификации (ИА) (authentication information) - информация, используемая для целей аутентификации.

3.14 Обменная аутентификационная информация (обменная ИА) (exchange authentication information, exchange ИА) - информация, которой обмениваются заявитель и верификатор в процессе аутентификации принципала.

3.15 Оперативный аутентификационный сертификат (on-line authentication certificate) - аутентификационный сертификат, предназначенный для использования в аутентификационном обмене, получаемый непосредственно заявителем от уполномоченного, удостоверяющего его.

3.16 Отличительный идентификатор (distinguishing identifier) - данные, однозначно идентифицирующие сущность в процессе аутентификации. Настоящий стандарт требует, чтобы подобный идентификатор был уникальным, по крайней мере, в пределах домена безопасности.

3.17 Параметр, переменный по времени (time variant parameter) - элемент данных, используемый сущностью для верификации того, что сообщение не является результатом воспроизведения.

3.18 Принципал (объект аутентификации) (principal) – сущность, подлинность которой может быть подтверждена.

3.19 Симметричный метод аутентификации (symmetric authentication method) - метод аутентификации, в котором обе сущности разделяют общую информацию аутентификации.

3.20 Уникальный номер (unique number) - параметр, переменный по времени, сгенерированный заявителем.

4 Общие сведения об аутентификации

4.1 Основные понятия аутентификации

Аутентификация обеспечивает доверие к заявленной сущности. Аутентификация имеет смысл только в контексте взаимосвязи между принципалом и верификатором. Имеется два важных случая: принципал представлен заявителем, имеющим особую коммуникационную взаимосвязь с верификатором (аутентификация сущности) и принципал является источником элемента данных, доступного верификатору (аутентификация источника данных).

Настоящий стандарт различает эти две формы аутентификации. Аутентификация сущности обеспечивает подтверждение подлинности принципала (объекта аутентификации) в контексте коммуникационной взаимосвязи. Аутентифицированная сущность принципала удостоверяется, только если этот сервис включен. Удостоверение неразрывности аутентификации может быть получено так, как это описано в 4.2.7. Примером служит одноранговая аутентификация ВОС, определенная в ГОСТ ИСО 7498-2.

Аутентификация источника данных обеспечивает подтверждение подлинности принципала, ответственного за конкретный блок данных.

Примечание.

1. При использовании аутентификации источника данных необходимо также иметь адекватное доверие к тому, что данные не были модифицированы. Этого можно достичь путем использования сервиса целостности, например:

а) использованием среды, в которой данные не могут быть изменены;

б) верификацией того, что полученные данные соответствуют цифровому отпечатку отправленных данных;

в) использованием механизма цифровой подписи;

г) использованием симметричного криптографического алгоритма.

2. Термин **коммуникационная взаимосвязь,** использованный в определении аутентификации сущности, допускает широкую интерпретацию и может относиться,

например, к ВОС-соединению, межпроцессным коммуникациям или взаимодействию между пользователем и терминалом.

4.1.1 Идентификация и аутентификация

Принципал — это сущность, подлинность которой может быть установлена (аутентифицирована). Принципал имеет один или несколько отличительных идентификаторов, ассоциированных с ним. Сервисы аутентификации могут быть использованы сущностями для верификации принципалов. Верифицированная таким образом подлинность принципала называется аутентифицированной сущностью.

Примерами принципалов, которые могут быть идентифицированы и затем аутентифицированы, являются:

- пользователи-люди;
- процессы;
- реальные открытые системы;
- сущности уровней ВОС;
- предприятия.

Требуется, чтобы отличительные идентификаторы были уникальны в пределах домена безопасности. Отличительные идентификаторы отличают принципала от других в том же домене одним из двух способов:

- при низком уровне детализации — посредством принадлежности к группе сущностей, считающихся эквивалентными для целей аутентификации (в этом случае вся группа рассматривается как один принципал и имеет один отличительный идентификатор);
- при самом высоком уровне детализации — идентифицируя одну и только одну сущность.

Когда имеет место аутентификация между различными доменами безопасности, отличительного идентификатора может быть недостаточно для однозначной идентификации сущности, так как уполномоченные по различным доменам безопасности могут использовать одинаковые отличительные идентификаторы. В этом случае отличительные идентификаторы должны использоваться совместно с идентификатором домена безопасности, чтобы предоставить уникальный идентификатор сущности.

Примерами типичных отличительных идентификаторов являются:

- имена каталогов (ИСО/МЭК 9594-8);
- сетевые адреса (ИСО/МЭК 8348);
- имена прикладных процессов и сущностей прикладного уровня (ИСО/МЭК 9545);
- идентификаторы объектов (ИСО/МЭК 8824);
- имена людей (уникальные в контексте домена);

– номера паспортов или номера социального страхования.

4.1.2 Сущности аутентификации

Термин «заявитель» используется для описания сущности, которая является или представляет принципала для целей аутентификации. Заявитель включает функции, необходимые для участия в аутентификационных обменах от имени принципала.

Термин «верификатор» используется для описания сущности, которая либо сама является, либо представляет сущность, подтверждающую подлинность. Верификатор обладает функциональностью, необходимой для осуществления информационного обмена данными в процессе аутентификации.

Сущность, вовлеченная во взаимную аутентификацию (см. 4.2.4), будет принимать на себя роли как заявителя, так и верификатора.

Термин «доверенная третья сторона» используется для описания уполномоченного по безопасности или его агента, пользующегося доверием других сущностей применительно к действиям, связанным с безопасностью. В контексте настоящего стандарта доверенная третья сторона пользуется доверием заявителя и/или верификатора для целей аутентификации.

Примечание. Заявитель или верификатор могут быть детализированы в виде нескольких функциональных компонентов, возможно, располагающихся в разных открытых системах.

4.1.3 Информация аутентификации

Типами информации аутентификации являются:

– обменная информация аутентификации (обменная ИА);

– заявляемая информация аутентификации (заявляемая ИФ);

– верификационная информация аутентификации (верификационная ИА).

Термин «аутентификационный обмен» используется для описания последовательности из одной или нескольких передач обменной ИА с целью выполнения аутентификации.

Рисунок 1 иллюстрирует взаимосвязи между заявителем, верификатором и доверенной третьей стороной, а также три перечисленных типа информации аутентификации.

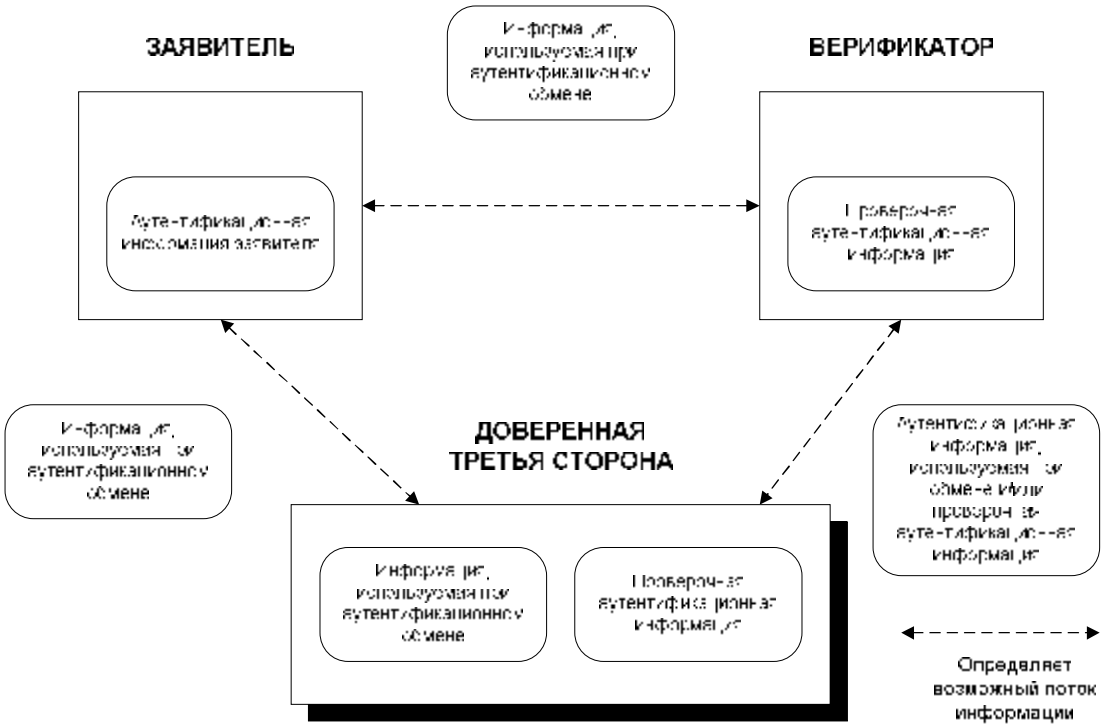


Рисунок 1. Иллюстрация взаимосвязей между заявителем, верификатором и доверенной третьей стороной, а также типов информации аутентификации

Примечание.

1. В некоторых сценариях доверенная третья сторона может отсутствовать.

2. Верификационная ИА может относиться как к принципалу, так и к доверенной третьей стороне (см. 4.5).

В некоторых случаях, чтобы сгенерировать обменную ИА, заявитель может нуждаться во взаимодействии с доверенной третьей стороной. Аналогично, чтобы верифицировать обменную ИА, верификатор может нуждаться во взаимодействии с доверенной третьей стороной. В этих случаях доверенная третья сторона может хранить верификационную ИА, относящуюся к принципалу.

Возможно также, что доверенная третья сторона используется при передаче обменной ИА.

Сущности могут также нуждаться в хранении информации аутентификации, используемой при аутентификации доверенной третьей стороны.

Примеры трех типов информации аутентификации даны в 5.1.

Примечание. Поскольку термин «удостоверения» (credentials) не всегда согласованно используется в других стандартах, в настоящих Основах безопасности этот термин не используется. Термин «удостоверения», определенный в ГОСТ ИСО 7498-2, может служить примером обменной ИА.

4.2 Аспекты сервиса аутентификации

4.2.1 Угрозы аутентификации

Целью аутентификации является подтверждение подлинности принципала. Механизмы выполнения аутентификации обычно должны исключить угрозы маскарада и воспроизведения.

Под маскарадом понимается попытка сущности выдать себя за другую сущность, то есть притвориться другой сущностью, связанной с верификатором особым образом (например, через источник данных или коммуникационные взаимосвязи). Эти типы угроз включают воспроизведение, перенаправление или компрометацию заявляемой ИА.

Угроза маскарада возникает в контексте действий (например, порождение данных или коммуникационная взаимосвязь), инициированных либо заявителем, либо верификатором. Защита действий от угрозы маскарада требует использования сервиса целостности для связывания элементов данных с аутентификационным обменом. Для противодействия угрозам, относящимся к маскараду, аутентификация должна использоваться совместно с некоторой формой сервиса целостности, связывающего аутентифицированную сущность с действием.

Воспроизведение означает повторное использование обменной ИА для получения несанкционированного эффекта. Воспроизведение обычно используется в комбинации с другими атаками, такими как модификация данных. Не все механизмы аутентификации в равной степени устойчивы к воспроизведению. Воспроизведение может быть угрозой для других сервисов безопасности. Аутентификация может использоваться для противодействия воспроизведению, так как она предлагает средства, чтобы установить источник обменной информации.

4.2.2 Продвижение аутентификации

В некоторых обстоятельствах у принципала могут иметься требования неявных действий в системе. В таких случаях должно быть создано его представление в системе. Более того, до создания представления принципала в системе принципал должен быть аутентифицирован.

Когда представление действует от имени принципала, оно будет аутентифицировано вместо последнего. Поскольку представление действует так, как если бы оно было принципалом, действия принципала в системе могут проводиться, не требуя его непосредственного вовлечения, см. пример в приложении А.

Когда принципалом является пользователь-человек, могут использоваться механизмы, ограничивающие время жизни представления периодом, в течение которого пользователь физически присутствует в определенном месте.

Заявитель, действуя от имени принципала, может обращаться к другой системе, которая после аутентификации создает собственное представление принципала. Создание этого представления называется продвижением аутентификации.

На возможность подобного продвижения аутентификации может влиять политика безопасности.

4.2.3 Односторонняя и взаимная аутентификация

Аутентификация может быть односторонней или взаимной.

Односторонняя аутентификация подтверждает подлинность только одного принципала. Взаимная аутентификация подтверждает подлинность обоих принципалов.

Аутентификация сущностей может быть как взаимной, так и односторонней. По самой своей природе аутентификация источника данных всегда односторонняя.

4.2.4 Инициация аутентификационного обмена

Аутентификационный обмен может быть инициирован заявителем или верификатором. Сущность, запускающая аутентификационный обмен, называется инициатором аутентификации.

4.2.5 Отзыв информации аутентификации

Отзывом информации аутентификации называется долгосрочное придание верификационной ИА статуса недействительной. В некоторых ситуациях отзыва информации аутентификации может требовать политика безопасности. Решение об отзыве информации аутентификации может быть обусловлено выявленными нарушениями безопасности, изменением политики безопасности или иными причинами. Отзыв информации аутентификации может повлечь или не повлечь отзыв существующего доступа или иметь другие производные эффекты.

Кроме того, могут быть предприняты следующие действия, относящиеся к управлению:

а) запись события в регистрационный журнал;

б) локальное оповещение о событии;

в) удаленное оповещение о событии;

г) разрыв коммуникационной взаимосвязи.

Конкретное действие, предпринимаемое для каждого события, зависит от действующей политики безопасности и других факторов, связанных со статусом коммуникационной взаимосвязи, например, произошло ли изменение, когда принципал был зарегистрированным и активным.

4.2.6 Удостоверение неразрывности аутентификации

Аутентификация сущности подтверждает ее подлинность только в определенный момент времени. Одним из способов получения удостоверения неразрывности аутентификации является связывание сервиса аутентификации с сервисом целостности данных.

Говорят, что сервисы аутентификации и целостности связаны, когда принципал сначала аутентифицируется, используя сервис аутентификации, после чего данные, посылаемые от имени принципала, связываются вместе с обменной ИА, используя сервис целостности. Тем самым обеспечивается, что последующая информация не может быть изменена никакой иной сущностью и, следовательно, обязана исходить от первоначально аутентифицированного принципала. Важно, чтобы сервис целостности предоставлялся по всему маршруту, проходимому информацией от принципала к верификатору. Например, маскарад возможен, если часть информации может быть порождена принципалами, отличными от аутентифицированного.

Другим способом вновь удостовериться, что та же удаленная сущность все еще присутствует, является осуществление время от времени дальнейших аутентификационных обменов. Однако это не предотвращает вторжений в промежутках, то есть не удостоверяет неразрывность аутентификации. Например, возможна следующая атака: нарушитель, получив вызов на проведение дополнительной аутентификации, позволяет законной стороне выполнить аутентификационные действия, а по их завершении вновь принимается за дело.

Если механизму целостности требуется ключ, то этот ключ может быть получен из параметров, заданных во время аутентификационного обмена. Тем самым устанавливается, что ключ ассоциирован с аутентифицированным принципалом, а его использование в механизме целостности будет обслуживать взаимосвязь обоих сервисов, предоставляемых описанным выше образом.

Способ получения ключа для сервиса целостности может быть специфицирован как часть параметров, специфицирующих, какие методы и алгоритмы следует использовать для всего аутентификационного обмена.

Примечание. При использовании других сервисов безопасности также возможно получение сервисной информации (например, ключа конфиденциальности) из параметров, специфицированных во время аутентификационного обмена.

4.2.7 Распределение аутентификационных компонентов между несколькими доменами

Домены безопасности могут вступать во взаимосвязи, такие, что заявитель из одного домена может аутентифицироваться верификатором из

другого домена. Возможно вовлечение нескольких доменов безопасности, включая:

– домен безопасности, в котором располагается инициатор;

– домен безопасности, в котором располагается верификатор;

– домены безопасности, в которых располагаются доверенные третьи стороны.

Не все перечисленные выше домены должны быть различными.

Чтобы аутентификация между различными доменами безопасности стала возможной, необходимо установить политику безопасного взаимодействия.

4.3 Источники, используемые в аутентификации

В общем случае выбор конкретного метода аутентификации зависит от цепочки предположений или ожиданий, относящихся к одному или нескольким источникам.

Используемые источники включают в себя:

а) нечто, что знают, например пароль;

б) нечто, чем обладают, например магнитная или интеллектуальная карта;

в) некоторые неизменные характеристики, например биометрические идентификаторы;

г) принятие того, что третейская сущность (доверенная третья сторона) произвела аутентификацию;

д) контекст, например адрес принципала.

Необходимо отметить, что у всех перечисленных источников имеются присущие им слабости. Например, аутентификация чего-то обладаемого зачастую есть аутентификация обладаемого объекта, а не его держателя. В некоторых случаях слабости могут быть преодолены путем комбинирования нескольких источников. Например, при использовании интеллектуальных карт (нечто, чем обладают) слабость может быть преодолена добавлением персонального идентификационного кода (нечто, что знают), чтобы аутентифицировать пользователя по отношению к карте. Более того, источник д) наиболее слаб и практически всегда используется совместно с другими источниками.

В источнике г) имеются два типа рекурсии:

– чтобы быть идентифицированной, третейская сущность сама может требовать аутентификации;

– аутентификация, осуществляемая третейской сущностью, может использовать четвертую сторону и т.д.

Анализ реальных методов аутентификации, включающих перечисленные источники, выявит вовлеченные сущности, используемые источники и аутентифицируемых принципалов.

4.4 Этапы аутентификации

При аутентификации могут встречаться следующие этапы:

- этап инсталляции;
- этап изменения информации аутентификации;
- этап распространения;
- этап сбора;
- этап передачи;
- этап верификации;
- этап блокирования;
- этап разблокирования;
- этап деинсталляции.

Описываемые здесь этапы не обязательно разделены во времени, то есть они могут перекрываться.

Для данной схемы аутентификации требуются не все перечисленные этапы. Кроме того, в некоторых случаях последовательность этапов может отличаться от последовательности, подразумеваемой нижеследующим описанием.

4.4.1 Этап инсталляции

На этапе установки определяются заявляемая и верифицируемая ИА.

4.4.2 Этап изменения информации аутентификации

На этапе изменения информации аутентификации принципал или администратор вызывают изменение заявляемой и верифицируемой ИА (например, изменяется пароль).

4.4.3 Этап распространения

На этапе распространения верификационная ИА доводится до сущности (например, заявителя или верификатора) для использования при верификации обменной ИА. Например, при применении автономных подходов сущности могут получать аутентификационные сертификаты, списки отзыва сертификатов и списки отзыва уполномоченных. Этап распространения может встречаться до, в течение или после этапа передачи.

4.4.4 Этап сбора

На этапе сбора заявитель или верификатор могут получать информацию, требуемую для генерации конкретной обменной ИА для проводимой аутентификации. Различные процедуры могут собирать обменную ИА путем взаимодействия с доверенной третьей стороной или путем обмена сообщениями между аутентифицируемыми сущностями.

Например, при использовании оперативного центра распределения ключей, заявитель или верификатор могут получать некоторую

информацию, например, аутентификационный сертификат (см. 5.1.3) из центра распределения ключей, чтобы сделать возможной аутентификацию с другой сущностью.

4.4.5 Этап передачи

На этапе передачи обменная ИА передается между заявителем и верификатором.

4.4.6 Этап верификации

На этапе верификации обменная ИА сравнивается с верификационной. На этом этапе сущность, не способная самостоятельно верифицировать обменную ИА, может обратиться к доверенной третьей стороне, которая выполнит верификацию обменной ИА. В этом случае доверенная третья сторона вернет положительный или отрицательный ответ.

4.4.7 Этап блокирования

На этапе блокирования устанавливается состояние, посредством которого принципал, ранее обладавший возможностью быть аутентифицированным, временно лишается этой возможности.

4.4.8 Этап разблокирования

На этапе разблокирования прекращается действие состояния, установленного на этапе блокирования.

4.4.9 Этап деинсталляции

На этапе деинсталляции принципал удаляется из состава принципалов.

4.5 Привлечение доверенной третьей стороны

Механизмы аутентификации можно охарактеризовать числом вовлеченных доверенных третьих сторон.

4.5.1 Аутентификация без привлечения доверенной третьей стороны

В простейшей ситуации ни заявитель, ни верификатор при генерации и верификации обменной ИА не поддерживаются какой-либо иной сущностью. В этом случае верификационная ИА принципала должна быть уже установлена у верификатора.

Хотя для большинства сущностей число возможных партнеров по коммуникациям невелико, подобный подход имеет ограниченную применимость в крупномасштабной коммуникационной среде. В худшем случае каждый верификатор должен обладать верификационной ИА для всех принципалов домена безопасности, а общий объем требуемой информации растет как квадрат числа вовлеченных сущностей (см. рисунок 2).

Рисунок 2. Аутентификация без доверенной третьей стороны

4.5.2 Аутентификация с привлечением доверенной третьей стороны

Верификационная ИА может быть получена путем взаимодействия с доверенными третьими сторонами с обеспечением целостности этой информации. Необходимо также поддерживать конфиденциальность заявляемой ИА доверенной третьей стороны, а также верификационной ИА, если заявляемая ИА может быть выведена из нее.

К аутентификации может быть привлечена одна доверенная третья сторона или цепочка доверенных третьих сторон, что отражено в источнике г) в 4.3. Введение дополнительных доверенных третьих сторон делает возможной аутентификацию для больших совокупностей сущностей, каждая из доверенных третьих сторон поддерживает информацию только об ограниченном числе сущностей (но не обо всех сущностях). Таким образом, с ростом числа вовлеченных сущностей общий объем информации может расти линейно.

Взаимосвязи многих сущностей могут быть охарактеризованы в соответствии с коммуникационными требованиями (числом активных связей между сущностями), а также в соответствии со степенью имеющегося управленческого контроля, например, задержкой, неизбежной при отзыве информации аутентификации.

4.5.2.1 Встроенная аутентификация.

В случае встроенной аутентификации доверенная третья сторона (посредник) непосредственно вмешивается в аутентификационный обмен между заявителем и верификатором. Принципал аутентифицируется посредником, который затем подтверждает его подлинность в последующем встроенном аутентификационном обмене.

При встроенной аутентификации (см. рисунок 3) требуется, чтобы верификатор доверял посреднику в том, что тот должным образом аутентифицировал принципала, и чтобы верификатор подтвердил подлинность посредника посредством аутентификации.

Отзыв возможности аутентифицировать может контролироваться с точностью до следующей попытки аутентификации. Если информация

аутентификация заявителя отозвана, посредник может немедленно изменить статус заявителя и отвергать все последующие попытки аутентификации.

Иногда возможно расширение, так что может быть получен гарант, включающий цепочку доверенных посредников. В зависимости от проводимой в жизнь политики безопасности, либо верификатор, либо последняя ДТС в цепочке несет ответственность за определение годности цепочки посредников.

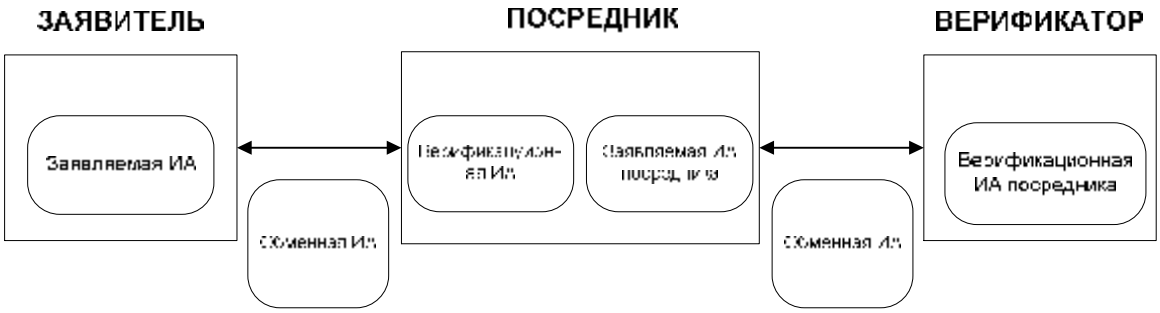


Рисунок 3. Встроенная аутентификация

4.5.2.2 Оперативная аутентификация.

В случае оперативной аутентификации одна или несколько доверенных третьих сторон активно участвуют во всех аутентификационных обменах (см. рисунок 4). Однако, в отличие от встроенной аутентификации, при оперативной аутентификации доверенные третьи стороны не располагаются непосредственно на маршруте аутентификационного обмена между заявителем и верификатором. Оперативные доверенные третьи стороны могут запрашиваться заявителем для генерации обменной ИА и помогать верификатору при верификации обменной ИА. Оперативная доверенная третья сторона может генерировать оперативные аутентификационные сертификаты (см. 5.1.3).

Оперативная аутентификация требует, чтобы между верификатором и доверенной третьей стороной, способной проверить достоверность заявляемой ИА принципала, имелась цепочка доверенных третьих сторон, вовлеченных в генерацию обменной ИА. В простейшем случае единственная доверенная третья сторона должна взаимодействовать непосредственно с заявителем или верификатором. Однако, возможно расширение до цепочки доверенных третьих сторон, прямо или косвенно взаимодействующих с заявителем или верификатором.

Отзыв возможности аутентифицировать может контролироваться с точностью до следующей попытки аутентификации.

Примерами оперативных доверенных третьих сторон являются оперативные серверы аутентификации или центры распределения ключей.

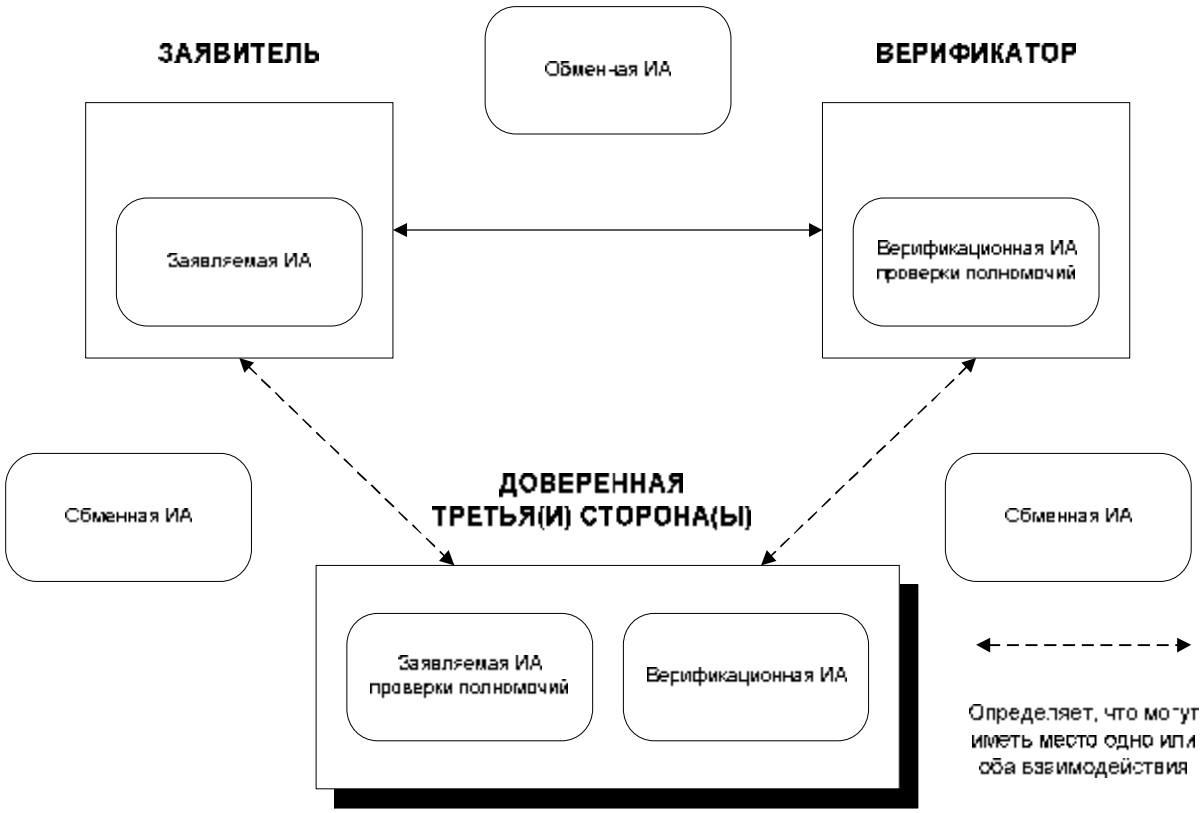


Рисунок 4. Оперативная аутентификация

Примечание. Истинная обменная ИА, появляющаяся между тремя показанными на рисунке различными сущностями, не одна и та же.

4.5.2.3 Автономная аутентификация.

Автономная аутентификация характеризуется необходимостью использовать сертифицированные списки отозванных сертификатов, сертификатные списки отозванных сертификатов, сертификатные задержки или другие опосредованные методы отзыва верификационной ИА.

В случае автономной аутентификации одна или несколько доверенных третьих сторон поддерживают аутентификацию без вовлечения в каждый акт аутентификации (см. рисунок 5). Автономная доверенная третья сторона заблаговременно генерирует и распространяет автономные аутентификационные сертификаты, которые верификатор впоследствии может использовать для проверки достоверности аутентификационного обмена. Таким образом, аутентификационный обмен происходит автономно, без вмешательства уполномоченного.

Поскольку доверенным третьим сторонам нет необходимости непосредственно взаимодействовать с заявителем или верификатором в процессе аутентификации, этот подход может быть более эффективным по числу требуемых взаимодействий.

Отзыв должен полагаться на дополнительные меры, такие как истечение срока годности и обновление сертификатов, а также сертифицированные списки отозванных сертификатов.

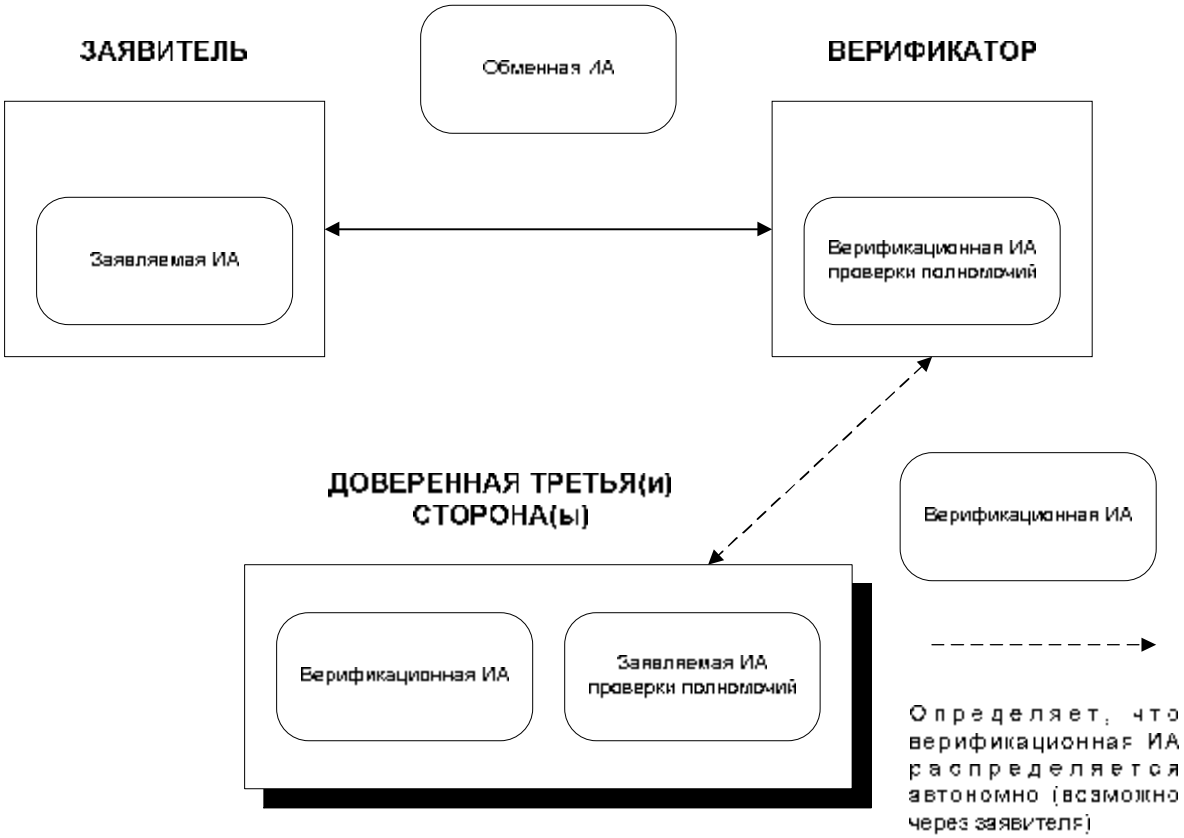


Рисунок 5. Автономная аутентификация

Примерами автономных доверенных третьих сторон являются удостоверяющие центры, выпускающие автономные аутентификационные сертификаты (см. 6.1.3).

4.5.3 Доверие заявителя верификатору

Механизмы, требующие доверия к верификатору, неадекватны, если нельзя доверять всем возможным верификаторам. Это связано с тем, что если подлинность верификатора не аутентифицирована, его благонадежность неизвестна. Например, при простом использовании паролей для аутентификации необходимо верить, что верификатор не сохранил и не использовал пароль повторно.

4.6 Типы принципалов

Принципалы могут быть категорированы разными способами, такими как:

а) те, кто обладает пассивными характеристиками (например, отпечатки пальцев, характеристики радужной оболочки глаза);

б) те, кто обладает способностью обмена и обработки информации;

в) те, кто обладает способностью хранения информации;

г) те, кто расположен в однозначно определенном, фиксированном месте.

Принципалы могут попадать более, чем в одну категорию [например, люди попадают в категории а), б) и в)]. В каждом случае применяется свой метод аутентификации:

а) измерение пассивных характеристик;

б) сложные вычисления типа запрос-ответ;

в) запоминание секрета (например, пароля);

г) определение местоположения.

4.7 Аутентификация пользователей-людей

В акте аутентификации может быть необходимо аутентифицировать конечного пользователя-человека, а не процесс, действующий от его имени.

Методы аутентификации пользователей-людей должны быть приемлемыми для людей, экономически целесообразными и безопасными. Неприемлемые методы могут подтолкнуть пользователей на поиск путей обхода этих процедур, что увеличивает потенциал вторжений.

Подходы к аутентификации людей основаны на источниках, описанных в 4.3. Процедуры аутентификации пользователей-людей основаны на этапах, описанных в 4.4.

В приложении А представлена дополнительная информация по аутентификации пользователей-людей, а также процессов, действующих от их имени.

4.8 Типы атак на аутентификацию

Рассматриваются три формы атак:

- **атаки воспроизведением**, в которых обменная ИА читается, а позднее воспроизводится;
- **атаки перенаправлением**, инициированные нарушителем;
- **атаки перенаправлением**, в которых нарушитель отвечает.

В атаках перенаправлением обменная ИА перехватывается и затем немедленно переадресуется.

4.8.1 Атаки воспроизведением

Следует рассмотреть два случая воспроизведения. Это воспроизведение некоторой обменной ИА:

- тому же верификатору;
- другому верификатору.

Последний случай возможен, когда (одна и та же) верификационная ИА принципала известна нескольким верификаторам. Успешное воспроизведение является частным случаем маскарада.

Противодействовать обоим случаям воспроизведения можно с помощью запросов. Запросы генерируются верификатором. Один и тот же запрос никогда не должен выдаваться дважды одним и тем же верификатором. Этого можно достичь несколькими способами (см. приложение В).

4.8.1.1 Воспроизведение одному и тому же верификатору.

Противодействовать воспроизведению одному и тому же верификатору можно, используя уникальные номера или запросы.

Уникальные номера генерируются заявителем. Один и тот же уникальный номер никогда не должен приниматься дважды одним и тем же верификатором. Этого можно достичь несколькими способами (см. приложение В).

4.8.1.2 Воспроизведение другому верификатору.

Воспроизведению другому верификатору можно противодействовать с помощью запросов. Кроме того, этому можно противодействовать, используя при вычислении обменной ИА любую характеристику, уникальную для верификатора. Такой характеристикой может быть имя верификатора, его сетевой адрес или, в общем случае, любой атрибут, уникальный по отношению к верификаторам, разделяющим одну и ту же верификационную информацию аутентификации.

4.8.2 Атаки перенаправлением

4.8.2.1 Атаки перенаправлением, инициированные нарушителем.

В этом типе атаки нарушитель вовлечен как инициатор аутентификации. Эта атака возможна, только если и заявитель, и верификатор могут инициировать аутентификацию. В этой атаке заявитель и верификатор обмениваются информацией аутентификации через нарушителя, не зная об этом, то есть нарушитель выдает себя за определенного верификатора перед заявителем и за того же заявителя перед этим верификатором.

Предположим, например, что нарушитель С хочет выдать себя перед верификатором В за заявителя А. С начинает взаимодействие и с А, и с В. С сообщает А, что он есть В, предлагает А аутентифицироваться у В, а также сообщает В, что он есть А и что он хочет аутентифицироваться (см. рисунок 6).

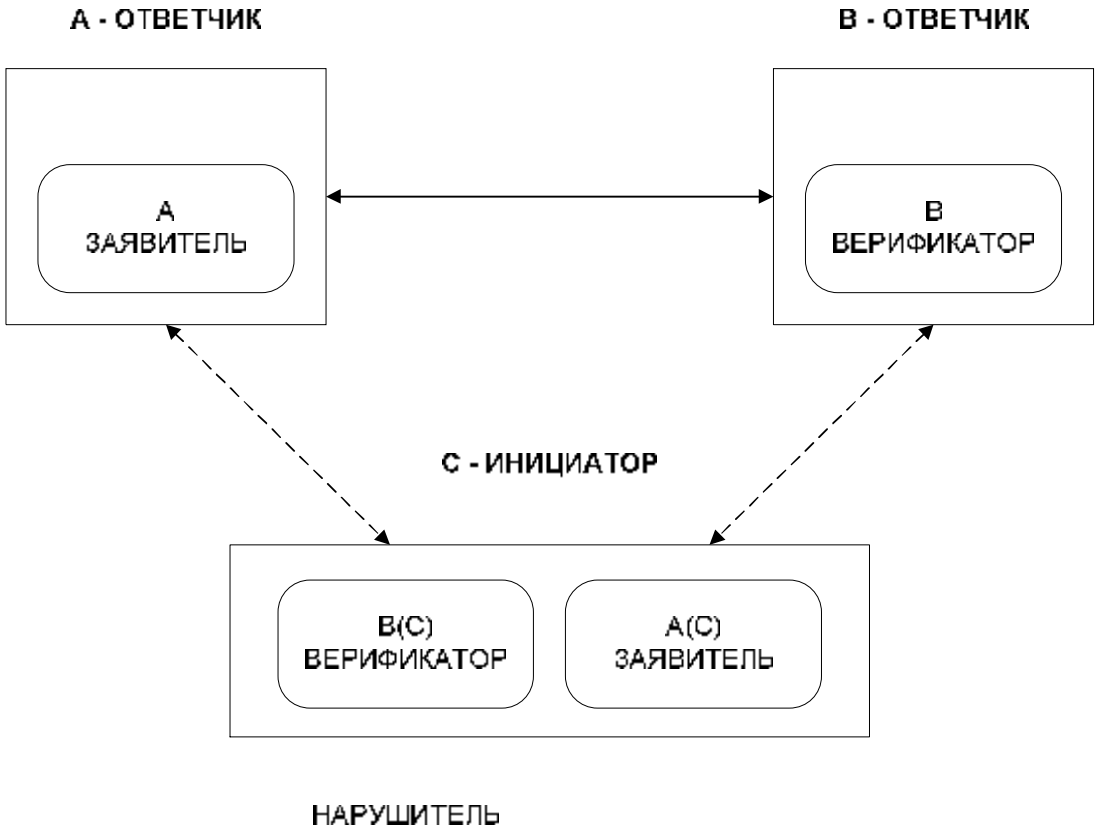


Рисунок 6. Атака перенаправлением, инициированная нарушителем

В процессе аутентификации А действует как заявитель по отношению к В (в действительности по отношению к С, действующему под видом В) и потому предоставляет информацию, которую С может использовать для аутентификации у В. В действует как верификатор и также предоставляет информацию, которая нужна С, чтобы играть роль верификатора. После аутентификации нарушитель С будет выглядеть для В как аутентифицированный А.

Противодействовать такому типу атаки можно, если:

а) сущность, начинающая взаимодействие, либо всегда заявитель, либо всегда верификатор (это может быть невозможным, если используется взаимная аутентификация);

б) обменная ИА, предоставляемая заявителем, различается в зависимости от его роли инициатора заказа аутентификации или отвечающего на приглашение к аутентификации. Это различие позволяет верификатору выявить описанный перехват. Дальнейшие детали см. в приложении Г.

4.8.2.2 Атаки перенаправлением, в которых нарушитель отвечает.

В этом типе атаки нарушитель располагается в середине аутентификационного обмена, перехватывает информацию аутентификации

и переадресует ее, принимая на себя роль инициатора (см. рисунок 7). Этот тип атаки может строиться либо в расчете на благоприятное стечение обстоятельств, и в этом случае нарушитель ожидает, когда его ошибочно примут за отвечающего, либо систематически, и в этом случае нарушитель афиширует себя как отвечающего (например, в центральной таблице размещения ресурсов).

Обычный способ противодействия данному типу атаки требует использования дополняющих сервисов (целостности или конфиденциальности) для последующих обменов данными. Обменная ИА комбинируется с некоторой другой информацией, которая дает заявителю и верификатору возможность при условии, что они являются законными сторонами, произвести ключ. Затем произведенный ключ может быть использован, как ключ для криптографических механизмов целостности или конфиденциальности.

Другой способ противодействия этому типу атаки уместен, когда коммуникационная сеть не подвержена внутренним перехватам, то есть она всегда доставляет данные неизмененными по правильному адресу. В такой ситуации этой атаке можно противодействовать, встраивая сетевой адрес в обменную ИА (например, подписывая сетевой адрес).

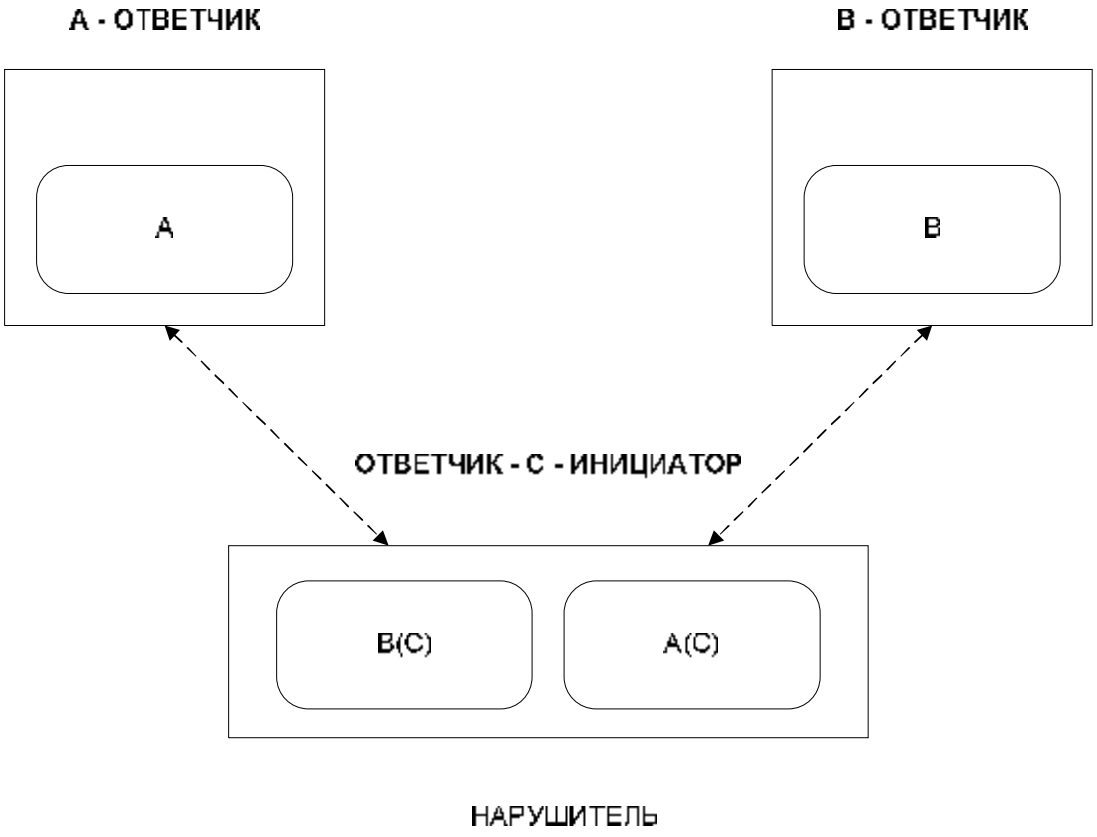


Рисунок 7. Атаки перенаправлением, в которых нарушитель отвечает

Примечание.

1. Даже если атакам, инициированным нарушителем, противодействуют, используя методы a) или b) из 4.8.2.1, метод аутентификации все же будет уязвимым для атаки с отвечающим нарушителем.

2. Запись X(Y) означает, что X выдает себя за Y.

5 Информация и средства аутентификации

5.1 Информация аутентификации

5.1.1 Заявляемая информация аутентификации

Заявляемая ИА — это информация, используемая для генерации обменной ИА, необходимой для аутентификации принципала.

Примерами заявляемой ИА являются:

а) **Пароль.**

б) **Секретный ключ.** Он предназначен для использования с механизмами аутентификации, использующими симметричные алгоритмы.

в) **Закрытый ключ.** Он предназначен для использования с механизмами аутентификации, использующими асимметричные алгоритмы.

5.1.2 Верификационная информация аутентификации

Верификационная ИА — это информация, используемая для верификации сущности, заявленной посредством обменной ИА.

Примерами верификационной ИА являются:

а) **Пароль,** связанный с подлинностью принципала.

б) **Секретный ключ**, связанный с подлинностью принципала или уполномоченного. Он предназначен для использования с механизмами аутентификации, использующими симметричные алгоритмы.

в) **Открытый ключ,** связанный с подлинностью принципала или уполномоченного. Он предназначен для использования с механизмами аутентификации, использующими асимметричные алгоритмы.

Верификационная ИА может быть предоставлена в форме аутентификационной таблицы и/или автономного аутентификационного сертификата (см. 5.1.4.2).

Аутентификационная таблица является набором записей, непосредственно доступным верификатору. Маршрут, используемый для доступа к таблице, получает защиту целостности и, дополнительно для симметричных механизмов, защиту конфиденциальности.

Примерами элементов, которые могут содержаться в записи аутентификационной таблицы, являются:

– подлинность принципала;

– верификационная ИА, например пароль, секретный ключ или открытый ключ;

- срок годности этой записи;
- политика безопасности, применимая к этой записи;
- уполномоченный, ответственный за эту запись.

5.1.3 Обменная информация аутентификации

Обменная ИА — это информация, которой обмениваются заявитель и верификатор в процессе аутентификации принципала. Примерами обменной информации аутентификации являются:

- заявленный отличительный идентификатор;
- пароль;
- запрос;
- ответ на запрос;
- уникальный номер;
- отличительный идентификатор верификатора;
- результат функции преобразования, примененной к или использующей заявляемую ИА и другие данные (например, временной штамп, случайное число, счетчик, запрос, подлинность верификатора, цифровой отпечаток, подлинность заявителя); примерами функций преобразования являются односторонняя функция, функция асимметричного зашифрования и функция симметричного зашифрования;
- оперативный сертификат;
- автономный сертификат.

Часть или вся обменная ИА, передаваемая за одну пересылку, может быть представлена в форме маркера безопасности.

5.1.4 Аутентификационные сертификаты

Обычной формой аутентификационной информации является аутентификационный сертификат. Аутентификационный сертификат является особым типом сертификата безопасности, удостоверенного доверенным уполномоченным, который может быть использован для аутентификации.

Различными типами аутентификационных сертификатов являются:

- оперативные аутентификационные сертификаты;
- автономные аутентификационные сертификаты;
- аутентификационные сертификаты отзыва;
- списки отзыва аутентификационных сертификатов.

Автономные сертификаты (см. 5.1.4.2) применимы, прежде всего, к относящейся к открытым ключам верификационной ИА. Автономный сертификат может быть отозван посредством использования либо сертификата отзыва, либо списка отзыва сертификатов.

Примерами элементов, которые могут содержаться в любом аутентификационном сертификате, являются:

– идентификация метода и/или ключа, использованного для генерации криптографического контрольного значения;

– Идентификационные данные уполномоченного по аутентификации и агента, выпустившего аутентификационный сертификат (если уполномоченный представлен несколькими агентами, данные агента позволяют точно установить, какой из агентских ключей был использован);

– время создания аутентификационного сертификата (время создания может быть использовано для целей аудита, а также в тех случаях, когда срок годности аутентификационного сертификата не представлен; по истечении периода времени, зависящего от политики безопасности, слишком старые аутентификационные сертификаты могут отвергаться);

– срок годности (ни до, ни после) аутентификационного сертификата (этот срок может учитываться, если это допускается политикой безопасности получателя, в противном случае время прекращения действия сертификата будет выведено из времени создания в соответствии с политикой безопасности получателя);

– политика безопасности, применимая к аутентификационному сертификату;

– ссылочный номер сертификата, являющийся уникальным для этого аутентификационного сертификата по отношению ко всем аутентификационным сертификатам одного и того же агента уполномоченного;

– тип сертификата;

– идентификационные данные или атрибуты верификатора, для которого предназначен аутентификационный сертификат (сущности могут проверять это значение, если оно присутствует, и отвергать некорректные значения. Идентификационными данными/атрибутами могут быть, например, имена пользователей-людей, идентификаторы прикладных процессов и/или физических машин).

Дополнительные элементы для различных типов аутентификационных сертификатов идентифицированы в следующих подразделах.

В стандартах приложений могут быть определены профили, специфицирующие, какие элементы являются обязательными, а какие — необязательными.

5.1.4.1 Оперативнные аутентификационные сертификаты.

Оперативный аутентификационный сертификат создается доверенной третьей стороной по непосредственному запросу заявителя. Оперативный аутентификационный сертификат обычно передается верификатору, как часть обменной ИА.

Примерами дополнительных элементов, которые могут содержаться в оперативном аутентификационном сертификате, являются:

– отличительный идентификатор принципала;

– цифровой отпечаток данных, если используется аутентификация источника данных;

– симметричный ключ, присвоенный принципалу для аутентификации, вместе с идентификацией алгоритма, который следует использовать совместно с этим ключом; необходимо поддерживать конфиденциальность этой информации;

– метод аутентификации, использованный для получения этого аутентификационного сертификата;

– метод(ы) аутентификации, совместно с которым(и) этот аутентификационный сертификат может быть использован;

– идентификация метода, который должен быть использован для защиты аутентификационного сертификата при передаче, а также любые ассоциированные параметры, необходимые для обеспечения такой защиты (примерами подобных защитных параметров являются запрос, уникальный номер или ключ защиты).

5.1.4.2 Автономные аутентификационные сертификаты.

Автономный аутентификационный сертификат связывает сущность с криптографическим ключом. Он создается уполномоченным, без необходимости непосредственного взаимодействия заявителя или верификатора с этим уполномоченным. Автономные аутентификационные сертификаты обычно применяются с аутентификационными механизмами, использующими асимметричные алгоритмы. Автономный аутентификационный сертификат может передаваться верификатору, как часть обменной ИА.

Примерами дополнительных элементов, которые могут содержаться в автономном аутентификационном сертификате, являются:

– отличительный идентификатор принципала;

– открытый ключ, присвоенный принципалу уполномоченным по аутентификации, вместе с идентификацией алгоритма, который следует использовать совместно с этим открытым ключом.

Автономный аутентификационный сертификат может быть отозван до окончания срока годности посредством использования сертификата отзыва или списков отзыва сертификатов.

5.1.4.3 Сертификаты отзыва.

Сертификат отзыва — это сертификат безопасности, выпущенный уполномоченным по безопасности, чтобы указать, что конкретный автономный аутентификационный сертификат отозван. Эта информация сохраняется, и к ней обращаются всякий раз при представлении

сертификата, чтобы определить, является ли представленный аутентификационный сертификат по-прежнему годным.

Примерами дополнительных элементов, которые могут содержаться в сертификате отзыва, являются:

– идентификационные данные принципала, группы принципалов или уполномоченного;

– дата и время, когда автономный аутентификационный сертификат был отозван;

– ссылочный номер отозванного сертификата.

5.1.4.4 Списки отозванных сертификатов.

Список отозванных сертификатов — это удостоверенный список всех аутентификационных сертификатов, отозванных данным уполномоченным по безопасности, вместе с датой и временем выпуска этого списка. Эта информация сохраняется, и к ней обращаются всякий раз при представлении сертификата, чтобы определить, является ли представленный аутентификационный сертификат по-прежнему годным.

Список отозванных сертификатов может включать в себя следующее:

– сертификаты отзыва;

– ссылочные идентификаторы сертификатов отзыва;

– отозванные аутентификационные сертификаты;

– ссылочные идентификаторы отозванных аутентификационных сертификатов;

– дату выпуска списка;

– дату выпуска следующего списка.

5.1.4.5 Цепочки сертификатов.

Аутентификационные сертификаты всегда защищаются, чтобы обеспечить аутентификацию источника данных доверенной третьей стороной. Если верификатор не располагает верификационной ИА для проверки источника сертификата, может быть использована цепочка сертификатов. Сертификат, порожденный другим уполномоченным, удостоверяет верификационную ИА, используемую для подтверждения достоверности источника первого сертификата.

Цепочка сертификатов может быть использована рекурсивно, каждый раз удостоверяя верификационную ИА используемую для подтверждения достоверности источника предыдущего сертификата. Цепочка предоставляет **сертификационный маршрут** уполномоченных от верификатора до заявителя. Верификатор должен сам решить, можно ли доверять каждому сертификату в цепочке, основываясь на информации, которой он обладает или может получить от доверенной третьей стороны.

5.2 Средства

В этом разделе представлена общая модель аутентификации в терминах универсальных средств.

5.2.1 Информация о состоянии аутентификации

Информация о состоянии аутентификации представляет состояние аутентификации, сохраняемое между вызовами аутентификационных сервисов. Информация о состоянии аутентификации может включать:

– сеансовые криптографические ключи;

– порядковые номера сообщений.

Информация о состоянии аутентификации нуждается в безопасном хранении. Эта информация сохраняется поставщиками сервисов.

5.2.2 Сервисы, относящиеся к управлению

Средства аутентификации, относящиеся к управлению, могут включать в себя распространение описательной информации, паролей или ключей (используя управление ключами) сущностям, которым требуется выполнять аутентификацию. Может включаться также использование протокола между взаимодействующими сущностями и другими сущностями, предоставляющими аутентификационные сервисы. Управление аутентификацией может также включать в себя отзыв информации аутентификации.

5.2.2.1 Инсталлировать.

Средство «Инсталлировать» устанавливает заявляемую ИА и верификационную ИА. Это средство может быть далее детализировано в терминах средств «Зарегистрировать», «Утвердить», «Подтвердить».

5.2.2.1.1 Зарегистрировать.

Средство «Зарегистрировать» вызывает запись уполномоченным по безопасности некоторой верификационной информации аутентификации, ассоциированной с принципалом. Эта информация включает отличительный идентификатор, предоставляемый либо принципалом, либо уполномоченным по безопасности. Это средство вызывается принципалом, другой сущностью или уполномоченным по безопасности. (Записывающий уполномоченный по безопасности может потребовать от принципала предоставления свидетельств доверия в поддержку достоверности регистрации.) В этот момент времени принципал является кандидатом на вхождение в домен безопасности, но еще не признан членом домена безопасности. В этот момент времени обмен какой-либо аутентификационной информацией невозможен.

5.2.2.1.2 Утвердить.

Средство «Утвердить», выполняемое от имени уполномоченного по домену безопасности, вводит принципала в домен безопасности.

Проверка достоверности верификационной ИА, ассоциированной с принципалом, может включать в себя взаимодействие между уполномоченным по безопасности и другой сущностью, которое не обязательно осуществляется с использованием ВОС-коммуникаций. Средство «Утвердить» вызывает связывание отличительного идентификатора с верификационной ИА.

5.2.2.1.3 Подтвердить.

Средство «Подтвердить» вызывается вслед за средством «Утвердить». Оно возвращает определенную информацию принципалу или другим сущностям. Простейшей формой возвращаемой информации является подтверждение или отклонение инсталляции. Другими формами являются:

- автономный аутентификационный сертификат;
- принятый отличительный идентификатор;
- заявляемая ИА.

После подтверждения принципал может быть аутентифицирован.

5.2.2.2 Изменить ИА.

Средство «Изменить ИА» вызывается от имени принципала или администратора, чтобы произвести изменение информации аутентификации.

5.2.2.3 Распространить.

Средство «Распространить» позволяет любой сущности получить достаточную верификационную ИА, чтобы на ее основе верифицировать обменную ИА.

5.2.2.4 Блокировать.

Средство «Блокировать», вызываемое от имени уполномоченного по безопасности, производит установку состояния, при котором принципал временно не может быть аутентифицирован.

5.2.2.5 Разблокировать.

Средство «Разблокировать», вызываемое от имени уполномоченного по безопасности, прекращает действие состояния, установленного сервисом «Блокировать».

5.2.2.6 Деинсталлировать.

Средство «Деинсталлировать» вызывает удаление принципала из совокупности аутентифицируемых принципалов. Это средство может быть далее детализировано в терминах средств «Сделать недействительной», «Уведомить» и «Отменить регистрацию».

5.2.2.6.1 Сделать недействительной.

Средство «Сделать недействительной» является действием, производимым уполномоченным по безопасности, которое состоит в отзыве верификационной ИА и/или изменении информации о состоянии, ассоциированной с принципалом. Средство «Сделать недействительной» препятствует аутентификации принципала.

5.2.2.6.2 Уведомить.

Средство «Уведомить» может быть вызвано уполномоченным по безопасности после средства «Сделать недействительной». Оно возвращает принципалу уведомление о недействительности его ИА и, возможно, информацию о том, как восстановить регистрацию.

5.2.2.6.3 Отменить регистрацию.

Средство «Отменить регистрацию» вызывает изъятие принципала из домена безопасности. Это соответствует удалению идентификационных данных принципала и ассоциированной верификационной ИА. Это средство вызывается уполномоченным по безопасности.

5.2.3 Средства, относящиеся к эксплуатации

5.2.3.1 Собрать.

Средство «Собрать» позволяет заявителю или верификатору получить информацию, требуемую для генерации определенной обменной ИА для акта аутентификации. Это может потребовать взаимодействия с доверенной третьей стороной (например, сервером аутентификации). Возможными входными данными являются:

- тип аутентификационного обмена;
- отличительный идентификатор принципала;
- идентификационные данные верификатора;
- тип заявляемой ИА (например, пароль, ключ);
- заявляемая ИА (например, значение пароля);
- тип обменной ИА;
- годность (начало/конец срока годности).

Возможными выходными данными являются:

- статус (успех или неудача);
- информация, требуемая для генерации обменной ИА;
- годность (начало/конец срока годности).

5.2.3.2 Сгенерировать.

Средство «Сгенерировать» вызывается заявителем, чтобы сгенерировать обменную ИА и/или обработать полученную обменную ИА.

Возможными входными данными являются:

- тип аутентификационного обмена;
- отличительный идентификатор принципала;
- информация, требуемая для генерации обменной ИА, как выход средства «Собрать»;
- ссылка на сохраненную информацию о состоянии аутентификации;
- обменная ИА, полученная от верификатора;
- тип обменной ИА;
- идентификационные данные верификатора;

– заявляемая ИА.

Возможными выходными данными являются:

– статус (успех или неудача);

– ссылка на сохраненную информацию о состоянии аутентификации;

– обменная ИА для передачи верификатору.

Тип аутентификационного обмена может быть задан в качестве входных данных при первом вызове средства «Сгенерировать» в аутентификационном обмене, когда заявитель является инициатором аутентификации. При том же вызове в качестве выходных данных возвращается ссылка на сохраненную информацию о состоянии аутентификации. В последующих вызовах средства «Сгенерировать» для того же аутентификационного обмена эти входные и выходные данные не обязаны присутствовать, но ссылка на сохраненную информацию о состоянии аутентификации может быть предоставлена в качестве входных данных.

Информация о состоянии аутентификации сохраняется средством для дальнейшего использования при аутентификации, пока не будет возвращен успех или неудача.

Если возвращен результат «требуются дальнейшие передачи», заявителю придется вызвать средство «Сгенерировать» вслед за получением обменной ИА от другой сущности. От заявителя может потребоваться многократное выполнение подобных операций (то есть вызовов средства «Сгенерировать» с предыдущей информацией о состоянии аутентификации и полученной обменной ИА), пока не будут индицированы успех или неудача. Таким образом, это средство согласует множество схем, включая n-сторонние запросно-ответные обмены, равно как и обмены, требуемые некоторыми схемами с нулевым знанием.

5.2.3.3 Верифицировать.

Верификатор вызывает средство «Верифицировать» для верификации полученной от заявителя обменной ИА и/или для генерации обменной ИА для передачи заявителю.

Возможными входными данными являются:

– тип аутентификационного обмена;

– информация, требуемая для генерации обменной ИА, как выход средства «Собрать»;

– ссылка на сохраненную информацию о состоянии аутентификации;

– обменная, полученная от заявителя;

– верификационная ИА.

Возможными выходными данными являются:

– статус (успех, требуются дальнейшие передачи, неудача);

– ссылка на сохраненную информацию о состоянии аутентификации;

– обменная ИА для передачи заявителю (если статус — «требуются дальнейшие передачи»);

– отличительный идентификатор принципала (если статус — «успех»);

– годность (начало/конец срока годности);

– индикатор взаимной аутентификации.

Тип аутентификационного обмена может быть задан в качестве входных данных при первом вызове средства «Верифицировать» в аутентификационном обмене, когда верификатор является инициатором аутентификации. При том же вызове в качестве выходных данных возвращается ссылка на сохраненную информацию о состоянии аутентификации. В последующих вызовах средства «Верифицировать» для того же аутентификационного обмена эти входные и выходные данные не обязаны присутствовать, но ссылка на сохраненную информацию о состоянии аутентификации может быть предоставлена в качестве входных данных.

Информация о состоянии аутентификации сохраняется средством для дальнейшего использования при аутентификации, пока не будет возвращен успех или неудача.

Если возвращен статус «успех», возвращаются также аутентифицированные данные принципала.

5.2.3.4 Сгенерировать и верифицировать.

В случае взаимной аутентификации средства «Сгенерировать» и «Верифицировать» могут быть объединены в единое средство. Возможные входные и выходные данные являются объединением входных и выходных данных этих двух средств.

Примечание. Средства «Сгенерировать» и «Верифицировать» не передают никаких данных. Передача данных зависит от среды, в которой используется аутентификация. Это находится вне области действия настоящего стандарта.

5.2.3.5 Пример информационных потоков.

На рисунке 8 приведен пример информационных потоков, ассоциированных с вызовом средств «Собрать», «Сгенерировать» и «Верифицировать» и используемых для моделирования обеспечения аутентификации (например, для прикладных процессов).

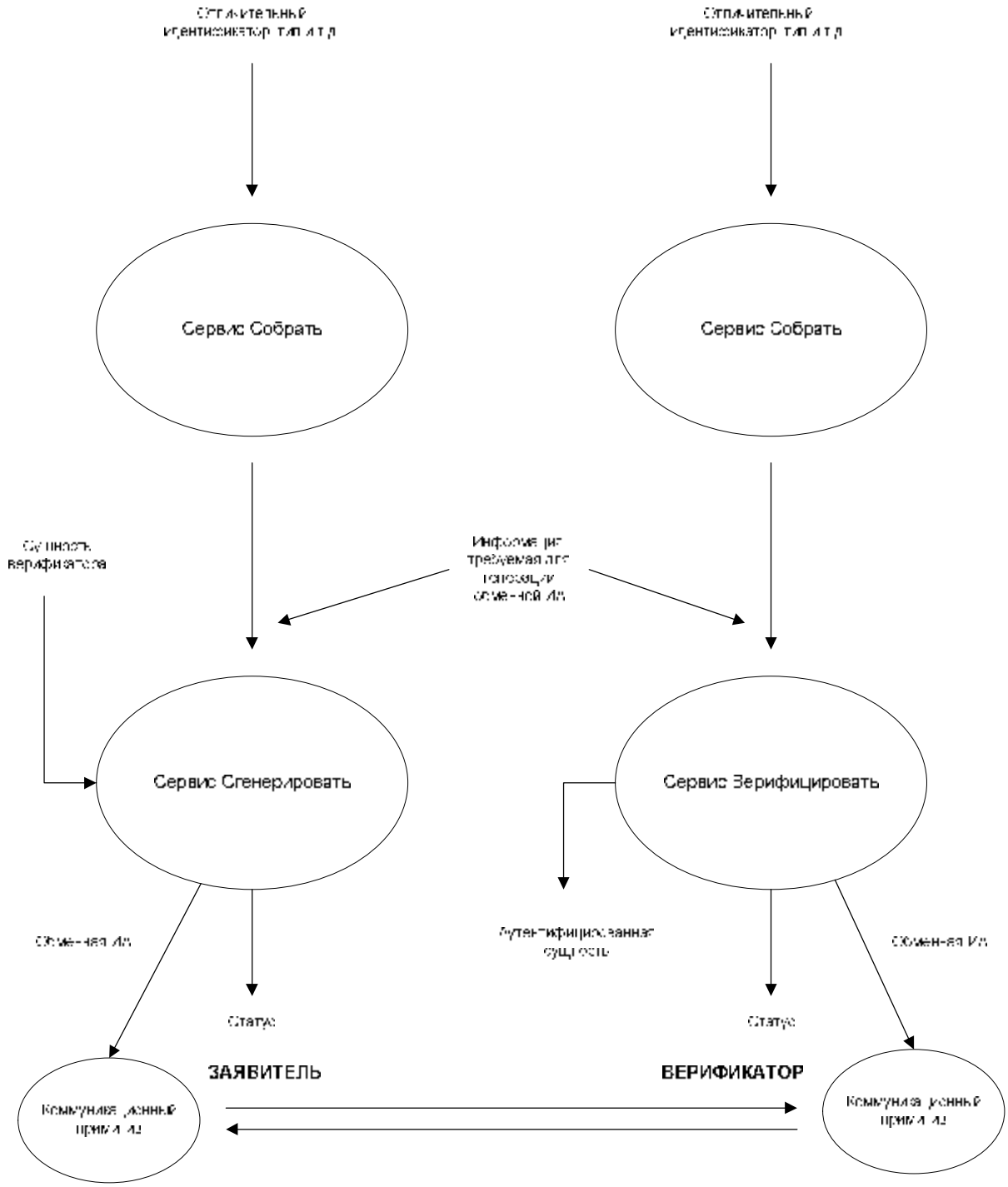


Рисунок 8. Пример информационных потоков в сервисах, относящихся к эксплуатации

Примечание. В этом примере сервис «Собрать» показан как вызываемый и заявителем, и верификатором. На практике он обычно будет вызываться только одной из этих сущностей или не вызывается вообще. Несмотря на наличие информационных потоков между «Сгенерировать» и «Верифицировать», ни один из этих сервисов не предполагает вызов коммуникационных примитивов.

6 Характеристики механизмов аутентификации

Механизмы аутентификации в рамках области действия настоящего стандарта могут базироваться на источниках а), г) и д) пункта 4.3. Источник г) включает в себя использование доверенной третьей стороны, как описано в 4.5.2, но эти механизмы в конечном счете будут полагаться на источники а) или д). Или же, в открытых системах, аутентификация удаленных принципалов зачастую базируется на источнике а), в котором используются секреты в форме ключа или пароля.

6.1 Симметрия/асимметрия

Аутентификация удаленного принципала зачастую базируется на секретах, принимающих форму пароля или ключа. Аутентификация включает в себя демонстрацию знания этого секрета. Методы подобной демонстрации подразделяются на две обширные категории:

– **симметричную**, в которой обе сущности разделяют общую информацию аутентификации;

– **асимметричную**, в которой не вся информация аутентификации разделяется обеими сущностями.

Примерами симметричных методов аутентификации являются:

– пароль;

– запрос, зашифрованный с использованием технологии симметричных ключей.

Примерами асимметричных методов аутентификации являются:

– технологии асимметричных ключей;

– технологии, в которых обладание информацией может быть верифицировано без раскрытия какой-либо части этой информации.

6.2 Использование криптографических/некриптографических технологий

Механизмы аутентификации, базирующиеся на чем-либо известном (см. 4.3), могут быть далее охарактеризованы использованием криптографических алгоритмов для защиты информации аутентификации. Симметричные, асимметричные или гибридные криптографические технологии могут быть использованы для обеспечения защиты целостности и, в некоторых случаях, конфиденциальности информации аутентификации.

Некриптографические технологии включают использование паролей или таблиц запрос-и-ответ. Примеры криптографических технологий включают использование зашифрования для защиты паролей при передаче.

6.3 Типы аутентификации

В аутентификацию сущности вовлечены две сущности. При односторонней аутентификации одна сущность действует как заявитель, а другая — как верификатор. Для взаимной аутентификации каждая сущность действует одновременно как заявитель и верификатор. Взаимной аутентификации можно достичь, используя одни и те же или различные механизмы аутентификации в каждом направлении.

6.3.1 Одностороння аутентификация

Односторонней аутентификации можно достичь, используя какой-либо из следующих способов:

– однократную передачу информации аутентификации, например, когда используются уникальные номера;

– три передачи информации аутентификации, когда используются запросы;

– более чем три передачи информации аутентификации. Этот случай применим к некоторым специфическим механизмам, использующим технологии с нулевым знанием.

В перечисленных выше случаях предполагается, что заявитель является инициатором аутентификации. Если инициатором аутентификации является верификатор, то число передач оказывается другим; подробнее см. 7.2.

6.3.2 Взаимная аутентификация

Взаимная аутентификация не обязательно влечет удвоение числа передач, не влечет она и использование одного и того же механизма аутентификации в обоих направлениях.

Для механизмов аутентификации, использующих три передачи информации аутентификации для односторонней аутентификации, взаимная аутентификация не требует какого-либо последующего обмена; заказ запроса может быть объединен с посылкой другого запроса, используемого верификатором (действующим тогда как заявитель) для аутентификации заявителя (действующего тогда в роли верификатора).

6.3.3 Подтверждение аутентификации

В некоторых случаях полезно подтверждение того факта, что аутентификация сущности принята или отклонена. Это подтверждение может быть заверено или быть просто ответом «да» или «нет» без какого-либо заверения. Подтверждение потребует дополнительной передачи.

7 Механизмы аутентификации

7.1 Классификация по уязвимостям

Механизмы аутентификации сами по себе могут быть уязвимы для атак, что ограничивает их эффективность (см. 4.8).

В этом подразделе механизмы аутентификации, которые могут применяться для поддержки аутентификации на этапе передачи, классифицируются в соответствии с угрозами, по отношению к которым они устойчивы. Все описанные механизмы базируются на источнике аутентификации «нечто, что знают» [см. подпункт а) пункта 4.3].

Все описанные механизмы применимы к аутентификации сущностей, а некоторые — и к аутентификации источника данных, например, цифровой отпечаток данных в аутентификационном обмене.

Определены следующие классы механизмов аутентификации:

– Класс 0. Не защищен.

– Класс 1. Защищен от раскрытия.

– Класс 2. Защищен от раскрытия и воспроизведения другим верификаторам.

– Класс 3. Защищен от раскрытия и воспроизведения тому же верификатору.

– Класс 4. Защищен от раскрытия и воспроизведения тому же или другим верификаторам.

Примечание. В классах 1-4 «защищен от раскрытия» означает защищенность от раскрытия заявляемой ИА.

При необходимости могут быть определены дополнительные классы. Для некоторых классов механизмов идентифицированы подклассы. Набор подклассов не обязательно является исчерпывающим.

Обменная ИА для каждого класса механизмов показана на диаграммах.

Если, как часть средства «Сгенерировать», используется функция зашифрования, то заявляемая ИА, возможно, вместе с другой информацией, используется для формирования ключа. Если, как часть средства «Верифицировать», используется функция расшифрования, то верификационная ИА, возможно, вместе с другой информацией, полученной в аутентификационном обмене, используется для формирования ключа.

Нижеследующие аутентификационные обмены описаны с точки зрения заявителя и всегда инициируются заявителем. По поводу обменов, инициированных верификатором, см. 7.2. Описанные обмены применимы к односторонней аутентификации. По поводу обменов, применимых к взаимной аутентификации, см. 7.4. В некоторых случаях необходимо подтверждение того факта, что аутентификация была успешной или неудачной. Для этого может понадобиться дополнительная передача данных.

Это не описано в данном разделе. Средства, фигурирующие в данном разделе, определены в 5.2.

На нижеследующих диаграммах обозначение в виде пары квадратных скобок [] указывает необязательный компонент передаваемой информации, включаемый только при некоторых условиях.

Необязательный компонент [цифровой отпечаток] присутствует в случае аутентификации источника данных и отсутствует в других случаях. Цифровой отпечаток может быть получен, например, с использованием асимметричного алгоритма зашифрования, либо просто путем зашифрования данных, либо путем предоставления криптографического контрольного значения этих данных, используя закрытый ключ подписывающего. Для аутентификации источника данных, передача данных, к которым относится цифровой отпечаток, может осуществляться полностью независимо от или может разделять использование коммуникационных средств, используемых нижеследующими механизмами.

7.1.1 Класс 0 (Не защищен)

В Классе 0 заявляемая ИА просто посылается вместе с отличительным идентификатором как часть обменной ИА от-заявителя-к-верификатору. Простым примером является посылка пароля. Класс 0 представляет собой случай симметричной аутентификации. Этот класс механизмов уязвим для атак раскрытия информации аутентификации и воспроизведения.

Средство «Сгенерировать» вырабатывает обменную ИА, как показано на рисунке 9, непосредственно из своих входных данных.

Средство «Верифицировать» верифицирует, что полученная заявляемая ИА (например, пароль), соответствует верификационной ИА, ассоциированной с полученным отличительным идентификатором.

Механизмы Класса 0 применимы для аутентификации как источника данных, так и сущностей.

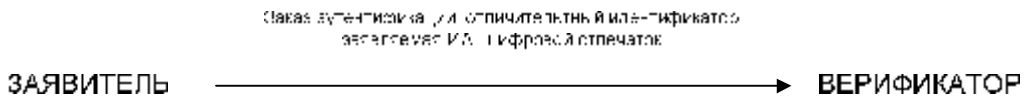


Рисунок 9. Механизм Класса 0 (Не защищен)

7.1.2 Класс 1 (Защищен от раскрытия)

Этот класс механизмов обеспечивает защиту от раскрытия заявляемой ИА. Механизмы Класса 1 применимы для аутентификации как источника данных, так и сущностей.

В этих механизмах применяется функция преобразования, в которой заявляемая ИА возможно, скомбинированная с отличительным

идентификатором, преобразуется этой функцией и передается вместе с отличительным идентификатором. Реальная заявляемая ИА не передается по коммуникационным каналам. Примеры включают:

– пересылку пароля, преобразованного односторонней функцией (например, криптографического контрольного значения или хэш-функции);

– пересылку цифрового отпечатка, зашифрованного секретным ключом;

– пересылку пароля, зашифрованного ключом конфиденциальности;

– пересылку цифрового отпечатка, подписанного с использованием закрытого ключа.

Механизмы этого типа применимы к аутентификации как источника данных, так и сущностей. Они уязвимы для атак воспроизведением, но обеспечивают защиту от раскрытия заявляемой ИА. Например, преобразованный пароль может быть воспроизведен на уровне протокольного обмена, но открытый текст пароля, используемый на уровне системного интерфейса, не раскрывается.

Средство «Сгенерировать» использует заявляемую ИА и, если требуется, отличительный идентификатор и/или цифровой отпечаток как входные данные для криптографического преобразования, чтобы сгенерировать обменную ИА, как показано на рисунке 10.

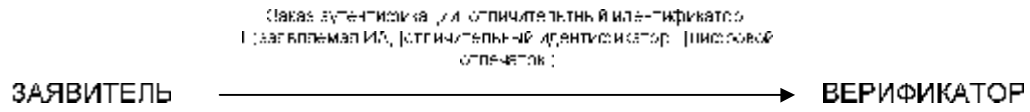


Рисунок 10. Класс 1. Механизм, защищенный от раскрытия

Три примера функции преобразования (F) состоят в следующем:

а) В случае односторонней функции средство «Верифицировать» повторяет одностороннюю функцию, используя верификационную ИА вместо заявляемой ИА, а сопоставляет это с обменной ИА.

б) В случае использования симметричного зашифрования средство «Верифицировать» использует верификационную ИА для расшифрования полученной обменной ИА и затем верифицирует корректность расшифрования, проверяя, что оно содержит отличительные признаки, такие как отличительный идентификатор заявителя, корректный цифровой отпечаток, пароль или постоянное значение.

в) В случае цифровой подписи средство «Верифицировать» перевычисляет цифровой отпечаток по полученным данным и использует верификационную ИА, чтобы проверить, что полученная подпись является достоверной подписью для этого отпечатка.

Кроме того, при аутентификации источника данных цифровой отпечаток из обменной ИА сопоставляется с перегенерированным цифровым отпечатком данных, требующих аутентификации.

Примечание. Если отличительный идентификатор принципала комбинируется с заявляемой ИА, это затрудняет проведение переборных атак. В каждый момент времени может быть проведена атака только на конкретного принципала вместо атаки сразу на всех принципалов.

Для обеспечения конфиденциальности функция преобразования не должна иметь обратной или, если таковая имеется, то обращение должно быть вычислительно неприемлемым для сторон, от которых заявляемую ИА (и цифровой отпечаток) следует скрывать.

7.1.3 Класс 2 (Защищен от раскрытия и воспроизведения другим верификаторам)

Этот класс механизмов обеспечивает защиту от раскрытия заявляемой ИА и воспроизведения другим верификаторам, но не от воспроизведения тому же верификатору. Этот класс механизмов идентичен Классу 1, за исключением того, что элемент данных, содержащий характеристику, уникальную для намеченного верификатора, включается в качестве входных данных функции преобразования. Это обеспечивает дополнительную защиту.

7.1.4 Класс 3 (Защищен от раскрытия и воспроизведения тому же верификатору)

Этот класс механизмов обеспечивает защиту от раскрытия заявляемой ИА и от воспроизведения тому же верификатору.

Для защиты от воспроизведения одному верификатору **механизмы уникальных чисел** в этом классе используют функции преобразования в сочетании с уникальной информацией. Заявляемая ИА и уникальное число преобразуются и передаются вместе с отличительным идентификатором.

Примерами источников уникальных чисел являются:

а) **Случайные или псевдослучайные числа**. Такие числа не повторяются намеренно в пределах времени жизни заявляемой ИА. Случайные или псевдослучайные числа из достаточно большого диапазона могут уменьшить риск (вероятность) того, что то же число уже было использовано.

б) **Временные штампы**. Уникальное число — это временной штамп, полученный из доверенного источника, являющийся уникальным в пределах времени жизни заявляемой ИА. Старые или ранее использованные временные штампы будут отвергнуты.

в) **Счетчик**. Уникальное число — это значение счетчика, который непрерывно увеличивается, пока используется одна и та же заявляемая ИА.

г) **Криптографическое зацепление**. Уникальное число — это значение, выведенное посредством зацепления блоков из содержимого предыдущих обменов данными между заявителем и верификатором.

Уникальность этого числа вне рамок заявителя может быть обеспечена путем его конкатенации с данными, уникальными для заявителя (такими как его собственный отличительный идентификатор).

Для выработки уникальных чисел можно также использовать комбинации перечисленных технологий.

Тремя примерами функции преобразования (F) являются:

а) **Односторонняя функция**. Уникальное число, заявляемая ИА и, возможно, отличительный идентификатор преобразуются односторонней функцией. Уникальное число также передается, так что верификатор может выполнить то же преобразование.

б) **Асимметричный алгоритм**. Когда заявляемая ИА является закрытым ключом, уникальное число подписывается этим закрытым ключом.

в) **Симметричный алгоритм**. Когда заявляемая ИА является секретным ключом, уникальное число зашифровывается этим секретным ключом.

Этот подкласс применим для аутентификации как источника данных, так и сущностей.

Средство «Сгенерировать» генерирует уникальное число. Затем осуществляется зашифрование с использованием следующих входных данных:

- уникальное число;
- заявляемая ИА;
- отличительный идентификатор (не обязательно);
- цифровой отпечаток (если аутентифицируется источник данных)

и вырабатывается обменная ИА, как показано на рисунке 11.

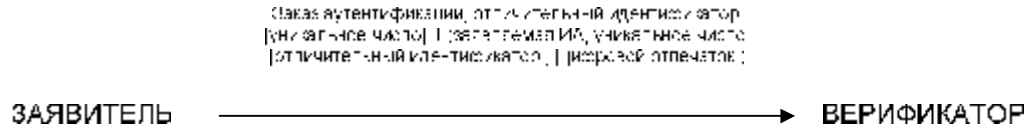


Рисунок 11. Подкласс 3. Механизм уникальных чисел

Средство «Верифицировать» расшифровывает и проверяет достоверность обменной ИА, используя верификационную ИА, как описано в Классе 1. Оно также проверяет, что полученное уникальное число не было получено ранее. Если число было получено ранее, это показывает, что имеет место воспроизведение. Кроме того, при аутентификации источника данных

цифровой отпечаток в обменной ИА сопоставляется с перегенерированным цифровым отпечатком полученных данных.

Примечание. Использование здесь термина «криптографическое зацепление» соответствует определению «зацепления блоков» в *СТ РК ИСО/МЭК 10116-2008*.

7.1.5 Класс 4 (Защищен от раскрытия и воспроизведения тому же или другим верификаторам)

7.1.5.1 Подкласс 4а. Механизмы уникальных чисел.

Данный подкласс механизмов идентичен Классу 3 за исключением того, что элемент данных, содержащий характеристику, уникальную для намеченного верификатора, включен в обмен в качестве входных данных функции преобразования. Это обеспечивает дополнительную защиту.

7.1.5.2 Подкласс 4б. Механизмы запросов.

Назначение механизма запросов — противодействие атакам воспроизведением, то есть обеспечение того, что любая попытка аутентификации посредством воспроизведения обменной ИА не принесет успеха. В ответ на заказ аутентификации верификатор выдает заявителю запрос в форме элемента данных с уникальным значением. Заявитель преобразует запросную информацию и заявляемую ИА с помощью некоторой функции и возвращает результат этого преобразования верификатору.

Таким образом, механизмы запросов включают в себя трехстороннюю передачу информации:

- посылку заказа аутентификации;
- выдачу запроса;
- посылку ответа, содержащего значение, полученное из заявляемой ИА, возможно, скомбинированное с отличительным идентификатором, и запросную информацию, преобразованные некоторой подходящей функцией (F).

В общем случае отличительный идентификатор может быть послан либо вместе с заказом аутентификации, либо с заключительным ответом.

Примерами функций преобразования (F), используемых в механизмах запросов, являются:

а) **Односторонняя функция**. Запрос и заявляемая ИА преобразуются односторонней функцией.

б) **Асимметричный алгоритм**. Когда заявляемая ИА является закрытым ключом, запрос подписывается этим закрытым ключом.

в) **Симметричный алгоритм**. Когда заявляемая ИА является секретным ключом, запрос зашифровывается этим секретным ключом.

Как особый случай механизма запросов, сгенерированный запрос может зависеть от сущности, полученной в заказе аутентификации. Это называется механизмом выделенных запросов. В таком случае отличительный

идентификатор является обязательным при заказе аутентификации. Кроме того, четвертой возможной функцией преобразования является:

г) **Некриптографическая.** Один из примеров — использовать таблицу пар запрос-ответ, когда запрашивающая сущность заказывает конкретный ответ. Другой пример — биометрическая схема, такая как система голосового повтора.

Этот подкласс применим для аутентификации как источника данных, так и сущностей.

Средство «Сгенерировать» вырабатывает заказ аутентификации (который в случае выделенного запроса должен сопровождаться отличительным идентификатором). После получения этого заказа аутентификации средство «Верифицировать» генерирует в качестве обменной ИА уникальный запрос.

Затем средство «Сгенерировать» вырабатывает обменную ИА как преобразование входных данных, как показано на рисунке 12.

В случае односторонней функции средство «Верифицировать» повторяет преобразование, используя верификационную ИА вместо заявляемой ИА, и сравнивает результат с полученной обменной ИА. Чтобы повторить эту функцию, верификатор должен располагать отличительным идентификатором и данными, к которым применяется сервис. В случае других преобразований средство «Верифицировать» либо повторяет преобразование, либо выполняет обратную функцию и проверяет содержимое, используя верификационную ИА.

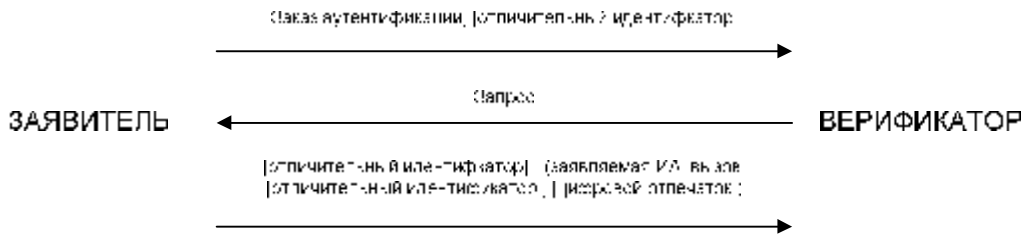


Рисунок 12. Подкласс 4б. Механизм запросов

7.1.5.3 Подкласс 4в. Механизм выделенных зашифрованных запросов

Механизмы выделенных зашифрованных запросов также включают в себя трехстороннюю передачу информации:

– посылку заказа аутентификации и отличительного идентификатора;

– выдачу запроса и верификационной ИА, возможно, скомбинированных с отличительным идентификатором и преобразованных некоторой подходящей функцией (F);

– посылку ответа, состоящего из запросной информации.

Двумя примерами механизмов выделенных зашифрованных запросов являются:

а) **Асимметричный алгоритм**. Когда заявляемая ИА является закрытым ключом, запрос зашифровывается соответствующим открытым ключом.

б) **Симметричный алгоритм**. Когда заявляемая ИА является секретным ключом, запрос зашифровывается этим секретным ключом. Запрос зашифровывается запрашивающей сущностью.

Этот тип механизмов применим для аутентификации сущностей, но не для аутентификации источника данных.

Средство «Сгенерировать» вырабатывает заказ аутентификации. Получив заказ аутентификации и отличительный идентификатор, средство Верифицировать генерирует непредсказуемый запрос. Затем он подвергается воздействию функции преобразования, чтобы выработать обменную ИА, как показано на рисунке 13.

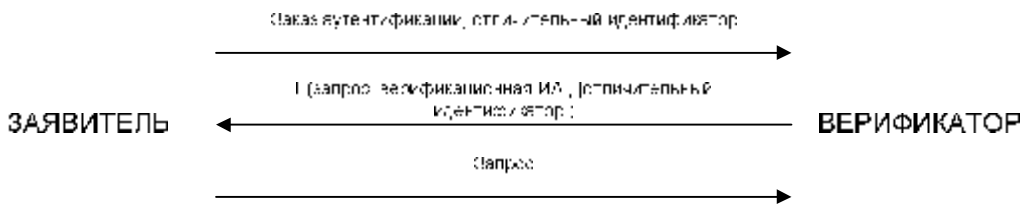


Рисунок 13. Подкласс 4в. Механизм выделенных зашифрованных запросов

Затем средство «Сгенерировать» выполняет обратное преобразование, используя заявляемую ИА вместо верификационной ИА для получения запроса, который возвращается для использования в качестве обменной ИА. В этой схеме уместны только преобразования зашифрования.

Наконец, средство «Верифицировать» сравнивает запрос с тем, что было сгенерировано ранее.

7.1.5.4 Подкласс 4г. Механизмы вычисляемых ответов

Этот подкласс механизмов также включает в себя трехстороннюю передачу информации:

– посылку заказа аутентификации с набором выбираемых значений и идентифицирующей информацией;

– выдачу запроса, который указывает, какие значения были выбраны верификатором;

– посылку ответа, состоящего из уникального числа, запроса или значений, выбранных для вычисления ответа, и заявляемой ИА, преобразованных некоторой подходящей функцией.

Одним из примеров является технология с нулевым знанием, в которой верификатор выбирает одну из несколько «задач», которую(ые) заявитель должен решить, не раскрывая, как именно.

Обмены могут быть повторены, чтобы обеспечить более высокий уровень доверия сущности. Это защищает от маскарадных атак нарушителя, который способен вычислить правильный ответ для некоторых, но не всех значений, которые может выбрать верификатор. Если обмен только один, верификатор может случайно выбрать значение, для которого нарушитель знает правильный ответ. Увеличение числа обменов уменьшает вероятность успеха подобной атаки.

Средство «Сгенерировать» сначала генерирует уникальное число и набор значений, а затем помещает их в обменную ИА, как показано на рисунке 14.

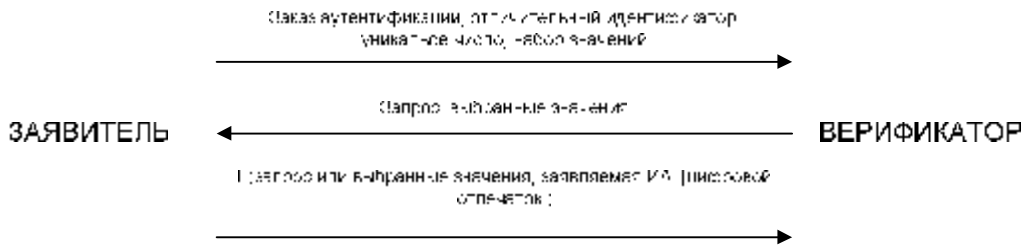


Рисунок 14. Подкласс 4г. Механизм вычисляемых ответов

Затем средство «Верифицировать» выбирает значения из этого набора и генерирует запрос для формирования второй обменной ИА.

Средство «Сгенерировать» выполняет преобразование запроса или выбранных значений, используя заявляемую ИА.

Затем средство «Верифицировать», наконец, выполняет обратное преобразование, используя верификационную ИА, и сравнивает полученные значения.

7.2 Инициация передачи

В 8.1 описаны обмены, инициированные заявителем посредством **заказа аутентификации**. Однако для аутентификации сущностей те же подклассы механизмов могут вовлекать верификатора в инициацию обмена, используя **приглашение к аутентификации**. В этом случае число передач будет иным. В таблице 1 пункта 7.5 приведено число передач для каждого из этих случаев.

7.3 Использование аутентификационных сертификатов

Механизмы аутентификации могут быть классифицированы в терминах средств, используемых для сбора верификационной ИА. Возможные средства включают:

- оперативные аутентификационные сертификаты;
- автономные аутентификационные сертификаты;

– верификационная ИА, предоставленная заранее, например, с использованием защищенных каналов.

Аутентификационный сертификат может быть использован для предоставления доказательства аутентификации, используя источник, описанный в подпункте г) пункта 4.3. Аутентификационный сертификат предоставляет доказательство того, что доверенная третья сторона ассоциировала данный отличительный идентификатор с конкретной верификационной ИА.

7.4 Взаимная аутентификация

Для подклассов механизмов, включающих в себя односторонний обмен (то есть подклассов 1, 2, 3 и 4а), обмен той же формы может быть использован в любом направлении для взаимной аутентификации.

Для подкласса 4б один и тот же тип механизмов может быть использован в обоих направлениях. Первый запрос может быть послан вместе с заказом аутентификации, а преобразование первого запроса — вместе со вторым запросом (см. рисунок 15). Это требует того же числа обменов, что и для односторонней аутентификации.

Аналогично, для подкласса 4в преобразование первого запроса может быть послано вместе с заказом аутентификации, а преобразование второго запроса — вместе с первым запросом.

Подкласс 4б может использоваться совместно с механизмами подкласса 4в. Оба запроса размещаются в преобразованных данных. В случае симметричного зашифрования заявляемая и верификационная ИА на обеих сторонах одна и та же и преобразование выполняется только один раз. В случае асимметричного зашифрования эти два преобразования выполняются на обеих сторонах.

Для подкласса 4г для односторонней аутентификации необходимы три или более передачи. Взаимная аутентификация требует четырех или более передач.

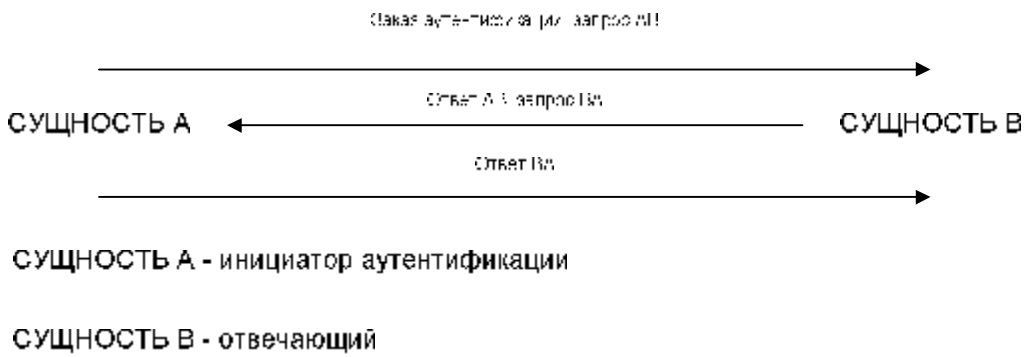


Рисунок 15. Взаимная аутентификация с использованием механизмов запросов

Примечание. По поводу деталей ответов и передачи отличительных идентификаторов см. описания подклассов и рисунки.

7.5 Сводка характеристик классов

В таблице 1 сведены уязвимости и характеристики различных классов и подклассов. Характеристики описаны в 6.

Таблица 1. Уязвимости и характеристики механизмов

Подкласс	0	1	2	3	4а	4б	4в	4г
Уязвимость								
Раскрытие	Да	Нет	Нет	Нет	Нет	Нет	Нет	Нет
Воспроизведение другим верификаторам	Да	Да	Нет	Да	Нет	Нет	Нет	Нет
Воспроизведение тому же верификатору	Да	Да	Да	Нет	Нет	Нет	Нет	Нет
Атака перенаправлением, инициированная нарушителем	Нет	Нет	Нет	Нет	Нет	Нет	Нет	Нет
Атака перенаправлением, в которой нарушитель отвечает	Да	Нет	Нет	Нет	Нет	Нет	Нет	Нет
Характеристики								
Симметрия (сим.)/ ассимметрия (ассим.)	сим	сим/ асим	сим/ асим	сим/ асим	сим/ асим	сим/ асим	сим/ асим	асим
Криптографический (Да)/ Некриптографический (Нет)/	Нет	Да/ Нет	Да/ Нет	Да/ Нет	Да/ Нет	Да/ Нет	Да	Да
Число передач								
Инициатор заявитель	1	1	1	1	1	3	3	3
Инициатор верификатор	2	2	2	2	2	2	4	4
Поддержка аутентификации источника данных	Да	Да	Да	Да	Да	Да	Нет	Да

7.6 Классификация по конфигурации

Когда сущности желают аутентифицироваться, они могут нуждаться в привлечении одной или нескольких доверенных третьих сторон. Следует определить природу доверия между каждой сущностью и некоторой доверенной третьей стороной. Простейшая модель, включающая в себя доверенные третьи стороны, содержит единственную доверенную третью сторону. В других моделях может рассматриваться множество доверенных третьих сторон, доверяющих друг другу, в то время как более общая модель

включает в себя множество доверенных третьих сторон, которые не доверяют друг другу.

7.6.1 Принципы моделирования при привлечении доверенных третьих сторон

В некоторых случаях верификатор может удостовериться в подлинности принципала, только если он получает подтверждение подлинности этой сущности от многочисленных доверенных третьих сторон.

Когда привлекаются три и более доверенных третьих сторон, можно защититься от искажения одной или нескольких доверенных третьих сторон. При некоторых политиках безопасности может применяться правило большинства.

Ниже рассматривается только простейший случай привлечения единственной доверенной третьей стороны.

Взаимосвязи между заявителем, верификатором и единственной доверенной третьей стороной могут моделироваться в терминах:

– этапов, как определено в 4.4 (в частности, этапов распространения, сбора, передачи и верификации);

– начального знания информации.

7.6.1.1 Модель этапов

Этапы связаны с различными сущностями следующим образом:

– этап распространения применим к взаимодействию между заявителем, верификатором и доверенной третьей стороной;

– этап сбора применим к взаимодействию между заявителем и доверенной третьей стороной или верификатором и доверенной третьей стороной;

– этап передачи применим к взаимодействию между любой парой, образованной заявителем, верификатором и доверенной третьей стороной;

– этап верификации применим к взаимодействию между верификатором и доверенной третьей стороной.

Этапы сбора, передачи и верификации могут использовать механизмы аутентификации из классов, определенных в 7.1.

Этап распространения может быть оперативным или автономным. Автономное распространение обычно осуществляется до аутентификационного обмена. В этих случаях нет гарантии, что заявляемая ИА все еще достоверна (то есть не отозвана).

Можно идентифицировать несколько различных схем аутентификации, как показано на рисунке 16. На этом рисунке сущность А соответствует заявителю, а сущность В — верификатору. Этот рисунок служит только иллюстративным целям и не обязательно является исчерпывающим.

В схеме А сущность А получает заявляемую ИА от доверенной третьей стороны после аутентификационного обмена с доверенной третьей стороной,

а сущность В получает верификационную ИА от доверенной третьей стороны. Сущность В производит верификацию локально.

В схеме Б сущность А получает заявляемую ИА от доверенной третьей стороны поле аутентификационного обмена с доверенной третьей стороной, а сущность В представляет обменную ИА, полученную от сущности А, доверенной третьей стороне для верификации.

В схеме В сущность А получает свою заявляемую ИА от доверенной третьей стороны после аутентификационного обмена с доверенной третьей стороной, равно как и верификационную ИА, необходимую сущности В, чтобы произвести верификацию локально.

В схеме Г сущность А получает верификационную ИА, необходимую сущности В, чтобы произвести верификацию локально, и локально генерирует обменную ИА. Обменная ИА и верификационная ИА совместно представляются сущности В.

В схеме Д сущность А локально генерирует свою обменную ИА и представляет ее сущности В, затем сущность В получает от доверенной третьей стороны верификационную ИА, необходимую, чтобы произвести верификацию локально.

В схеме Е сущность А локально генерирует свою обменную ИА и представляет ее сущности В, затем сущность В представляет обменную ИА, полученную от сущности А, доверенной третьей стороне для верификации.

В схеме Ж, которая представляет собой встроенное отношение доверия, сущность А локально генерирует свою обменную ИА и представляет ее доверенной третьей стороне, затем доверенная третья сторона посылает сущности В аутентификационный сертификат вместе с верификационной ИА, необходимой, чтобы произвести верификацию локально.

В схеме З, которая является другим случаем встроенного отношения доверия, сущность А локально генерирует свою обменную ИА и представляет ее доверенной третьей стороне, затем доверенная третья сторона посылает сущности В уведомление о том, что подлинность сущности А была верифицирована.

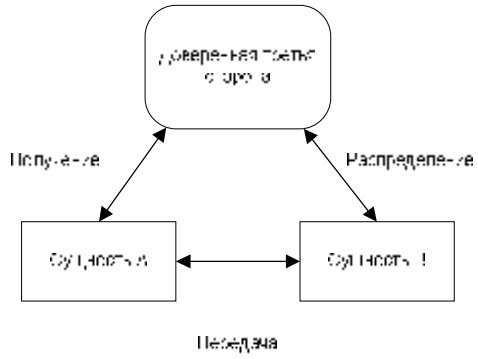


Схема А

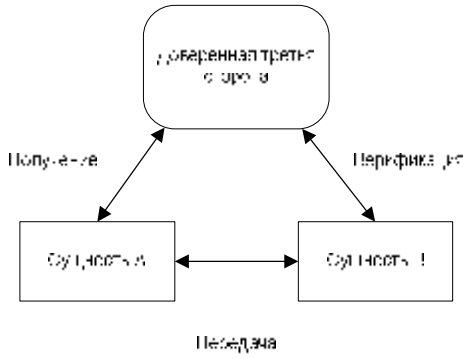


Схема Б

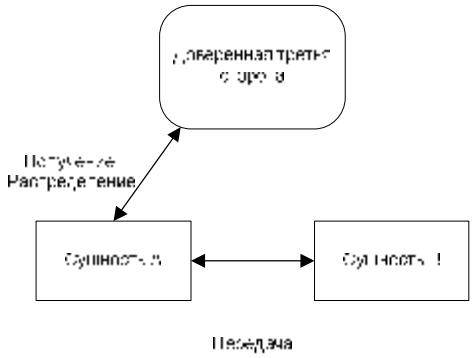


Схема В

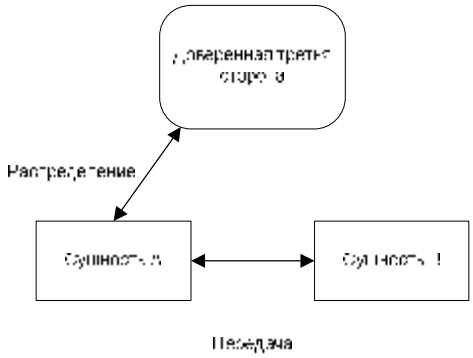


Схема Г

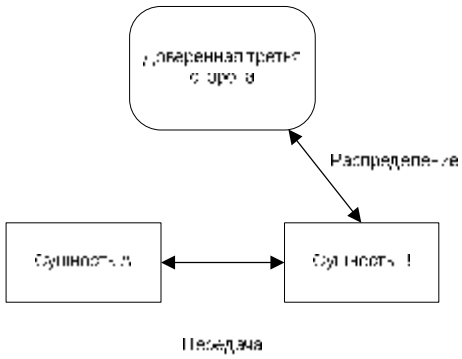


Схема Д

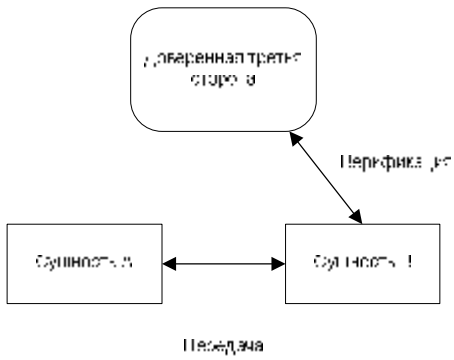


Схема Е

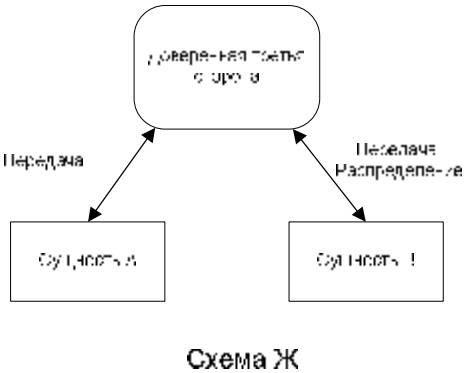


Схема Ж

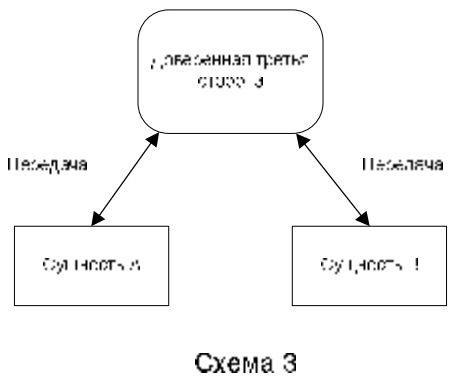


Схема З

Рисунок 16. Схемы аутентификации

7.6.1.2 Моделирование с использованием начального знания информации.

Заявитель (сущность А) и верификатор (сущность В) должны использовать некоторую начальную информацию, прежде чем может произойти аутентификационный обмен. Если привлечена доверенная третья сторона, это означает, что заявитель не знает непосредственно открытый ключ или секретный ключ, пригодный для использования верификатором. Можно рассматривать различные виды начального знания, как описано ниже.

7.6.1.2.1 Начальная информация, разделяемая между заявителем и доверенной третьей стороной

Различными случаями являются:

а) секретный ключ, разделяемый между заявителем и доверенной третьей стороной, известный заявителю и доверенной третьей стороне (технологии с секретным ключом);

б) закрытый ключ заявителя, известный только заявителю (сущность А);

в) открытый ключ заявителя, известный доверенной третьей стороне (асимметричные технологии);

г) закрытый ключ заявителя, известный заявителю и доверенной третьей стороне (некоторые технологии с нулевым знанием).

7.6.1.2.2 Начальная информация, разделяемая между верификатором и доверенной третьей стороной

Различными случаями являются:

а) секретный ключ, разделяемый между верификатором (сущность В) и доверенной третьей стороной, известный верификатору и доверенной третьей стороне (технологии с секретным ключом);

б) открытый ключ доверенной третьей стороны, известный верификатору (сущность В) (асимметричные технологии и технологии с нулевым знанием).

7.6.2 Взаимосвязи между доверенными третьими сторонами, вовлеченными в аутентификацию

7.6.2.1 Оперативные доверенные третьи стороны.

Оперативные доверенные третьи стороны могут быть необходимы, чтобы мог произойти аутентификационный обмен. Оперативные доверенные третьи стороны того же домена безопасности могут быть держателями заявляемой ИА и/или верификационной ИА сущностей, которые были ранее зарегистрированы в домене.

Требуются протоколы и/или процедуры, обеспечивающие, что в данном домене безопасности различные принципалы не могут быть зарегистрированы под одним именем.

Важным моментом является доступность оперативных доверенных третьих сторон, иначе аутентификационные обмены с использованием

оперативных доверенных третьих сторон могут оказаться подверженными отказу в обслуживании. Репликация информации аутентификации в ряде различных доверенных третьих сторон может уменьшить эту проблему. Для репликации информации аутентификации также требуются протоколы. Когда необходим обмен верификационной ИА, необходимы сервис целостности и, в некоторых случаях, сервис конфиденциальности между доверенными третьими сторонами аутентификации. Когда необходим обмен заявляемой ИА, необходимы сервис целостности и сервис конфиденциальности между доверенными третьими сторонами.

Кроме того, может оказаться необходимым принять во внимание обмен регистрационными журналами, поддерживаемыми различными оперативными доверенными третьими стороны домена безопасности. Для посылки и получения регистрационных журналов требуются протоколы.

7.6.2.2 Автономные доверенные третьи стороны

Автономные доверенные третьи стороны часто называют **удостоверяющими центрами**, так как они могут выпускать автономные аутентификационные сертификаты. Для автономных аутентификационных сертификатов не требуется особая защита, так как они являются самозащищенными. Важным моментом является доступность автономных доверенных третьих сторон, иначе аутентификационные обмены с использованием автономных доверенных третьих сторон могут оказаться подверженными отказу в обслуживании. Репликация этой информации в ряде различных хранилищ (например, Каталогов) может уменьшить эту проблему.

8 Взаимодействие с другими сервисами/механизмами безопасности

8.1 Управление доступом

Пользователи могут нуждаться в аутентификации, прежде чем им будет позволено получить информацию управления доступом, которая разрешит доступ к ресурсам, подчиненным политике управления доступом. Соответственно, сервис аутентификации может передать результаты аутентификации сервису управления доступом для использования сервисом управления доступом.

Отзыв информации аутентификации может повлечь отзыв существующего доступа.

8.2 Целостность данных

Аутентификация может использоваться совместно с целостностью данных, чтобы обеспечить удостоверение неразрывности аутентификации и обосновать подтверждение источника данных.

Некоторые механизмы аутентификации могут быть использованы для распространения, прямого или косвенного, ключевого материала, который может использоваться для сервиса целостности. Когда этот ключевой материал определен неявно, способ его вывода из переданных данных должен быть известен или специфицирован во время аутентификационного обмена. Когда ключевой материал определен явно, дополнительные данные должны быть переданы в одном из направлений во время аутентификационного обмена.

8.3 Конфиденциальность данных

Некоторые механизмы аутентификации могут быть использованы для распространения, прямого или косвенного, ключевого материала, который может использоваться для сервиса конфиденциальности. Когда этот ключевой материал определен неявно, способ его вывода из переданных данных должен быть известен или специфицирован во время аутентификационного обмена. Когда ключевой материал определен явно, дополнительные данные должны быть переданы в одном из направлений во время аутентификационного обмена.

8.4 Неотказуемость

Некоторые механизмы аутентификации могут быть использованы для распространения, прямого или косвенного, ключевого материала, который может использоваться для сервиса неотказуемости. Когда этот ключевой материал определен неявно, способ его вывода из переданных данных должен быть известен или специфицирован во время аутентификационного обмена. Когда ключевой материал определен явно, дополнительные данные должны быть переданы в одном из направлений во время аутентификационного обмена.

8.5 Аудит

Информация, относящаяся к аутентификации, которая может быть использована для аудита, может включать:

а) результаты аутентификации (то есть удостоверенную идентификацию);

б) информацию, относящуюся к отзыву информации аутентификации;

в) информацию по удостоверению неразрывности аутентификации;

г) другую информацию, относящуюся к процессу аутентификации.

Приложение А
(справочное)
Аутентификация пользователей людей

А.1 Общие положения

Корректная аутентификация пользователей-людей может быть необходимой для безопасности открытых систем, когда открытая система поддерживает деятельность людей. Диалог между пользователями-людьми и компьютерными системами может увеличить возможность вторжения путем маскарада. Методы аутентификации пользователей-людей должны быть приемлемыми для них, равно как экономичными и безопасными. Неудобные методы иногда толкают людей на поиск путей обхода процедур, так что потенциал вторжения возрастает.

Аутентификация пользователей-людей основывается на источниках аутентификации из одной или нескольких нижеследующих категорий:

а) нечто, что знают;

б) нечто, чем обладают;

в) характеристики отдельного пользователя-человека;

г) принятие того, что идентифицированная доверенная третья сторона установила подлинность пользователя-человека;

д) контекст (например, исходный адрес заказа).

В общем случае процесс аутентификации пользователя-человека включает в себя сопоставление удостоверений, представленных пользователем, с информацией аутентификации, полученной на этапе инсталляции.

А.1.1 Аутентификация посредством того, что знают

В этой категории наиболее широко используемой информацией аутентификации являются пароли. При доступе к системе пользователь-человек представляет пароль, и аутентифицирующая система сравнивает его с соответствующим значением в списке паролей, чтобы удостоверить подлинность пользователя-человека. Пароли должно быть трудно угадать, их следует тщательно администрировать. В противном случае они потенциально подвержены ненамеренному раскрытию.

А.1.2 Аутентификация посредством того, чем обладают

В эту категорию попадают различные физические носители, такие как:

а) карточки с магнитной полосой;

б) карточки с интегральными микросхемами.

В случае карточек с магнитной полосой пользователь-человек представляет физический носитель, а аутентификационная система считывает аутентификационную информацию с физического носителя, чтобы сравнить ее с хранимой аутентификационной информацией и подтвердить идентичность пользователя-человека.

Одной из уязвимых сторон карточек с магнитной полосой является то, что их легко копировать, другой — возможность использования карты с магнитной полосой другим пользователем.

При использовании карточек с интегральными микросхемами пользователь-человек представляет физический носитель, а аутентификационная система использует аутентификационную информацию, хранимую на физическом носителе для порождения ИА обмена, чтобы подтвердить идентичность пользователя-человека. Достоинством карточек с интегральными микросхемами является то, что они не могут быть легко скопированы.

Могут быть рассмотрены два варианта в зависимости от того, может ли карточка с интегральной микросхемой аутентифицировать ее держателя.

Когда карточка с интегральной микросхемой способна аутентифицировать держателя карточки, то имеет место двойная аутентификационная схема, где пользователь аутентифицируется верификатором, это по транзитивности эквивалентно непосредственной аутентификации пользователя.

Когда карточка с интегральной микросхемой не способна аутентифицировать держателя карточки и объект принадлежит не той сущности, то данный подход к аутентификации терпит неудачу.

А.1.3 Генератор паролей, зависящих от времени

Одним из типов аутентификационных средств является ручное устройство, генерирующее пароли, зависящие от времени. Аутентификационная информация, используемая при обмене, использует сочетание:

–секретной информации, хранящейся в устройстве;

–текущего времени;

–личного PIN-кода, вводимого пользователем с помощью клавишной панели для ввода PIN.

Порождаемая таким образом ИА обмена отображается устройством. Затем она пересылается пользователем в незашифрованном виде проверяющей системе. Этой системе может потребоваться синхронизация с карточкой. Этот вид аутентификационного механизма требует от личности, пытающейся осуществить аутентификацию с помощью такого устройства:

а) обладания надлежащим устройством;

б) знания PIN-кода.

А.1.4 Аутентификация по индивидуальным характеристикам пользователя-человека

Пароли чувствительны к раскрытию, если не обращаться с ними надлежащим образом, различные материальные устройства могут быть украдены, а карточки с магнитной полосой, кроме того, несанкционированно скопированы. Имеется класс методов аутентификации пользователей-людей, у которых отсутствуют перечисленные выше недостатки. Эти методы основаны на индивидуальных признаках людей, таких как:

–индивидуальные особенности почерка;

–отпечатки пальцев;

–особенности голоса;

–особенности сетчатки глаза;

–динамические особенности ввода данных с клавиатуры.

Методы, связанные с индивидуальными особенностями пользователя-человека, подразделяются на статические и динамические. При использовании динамических методов анализируются давление, временные характеристики, информация о перемещении пишущего устройства.

Анализ динамических особенностей ввода с клавиатуры обеспечивает непрерывную аутентификацию.

На этапе регистрации индивидуальные характеристики пользователя-человека заносятся в систему регистрации. Пользователь выполняет требуемую процедуру, например, пишет на планшете, прижимает к нему палец, произносит определенные слова. Может потребоваться многократное повторение процедуры для получения надежной информации. Система анализирует индивидуальные характеристики действий пользователя-человека и сохраняет их в профиле пользователя.

На этапе передачи/верификации пользователь-человек выполняет требуемую процедуру аутентификации. Система проверки сравнивает данные, полученные от пользователя, с хранимыми в профиле данного пользователя.

А.2 Процесс, действующий от имени пользователя

При некоторых обстоятельствах может оказаться необходимым избежать личного присутствия пользователя. В таких случаях пользователь должен иметь представительство в системе, время жизни которого не зависит от присутствия пользователя.

Поскольку представительство действует так, как будто оно является пользователем, действия пользователя могут быть продолжены, не требуя непосредственного участия пользователя. Например, пользователь-человек может зарегистрироваться в системе, а затем использовать различные компьютеры без необходимости регистрации на каждом из них.

Наряду с поддержкой представительств с независимыми временами жизни, могут использоваться представительства с дополнительными механизмами, время жизни которых зависит от присутствия пользователя.

Приложение Б
(справочное)
Аутентификация в модели OSI

Взаимосвязь служб безопасности со справочной моделью определена в стандарте ГОСТ ИСО 7498-2. Данное Приложение является сводкой информации, относящейся к аутентификации. Рассматриваются две службы безопасности: аутентификация равноправных объектов; аутентификация происхождения информации.

Б.1 Аутентификация равноправных объектов

Аутентификация равноправных объектов может быть использована при установлении соединения или на этапе передачи данных для подтверждения идентичности объектов, соединенных с одним или несколькими объектами. Эти службы доступны как в протоколах, ориентированных на соединение, так и протоколах, функционирующих без установления соединения. Возможна как односторонняя, так и взаимная аутентификация равноправных объектов.

Б.2 Аутентификация происхождения данных

Аутентификация происхождения данных обеспечивает подтверждение источника элемента данных. Службы не обеспечивают защиты от дублирования элементов данных.

Б.3 Использование аутентификации на различных уровнях модели OSI

Аутентификация равноправных объектов и происхождения данных имеет отношение только к следующим уровням модели OSI: сетевой уровень (уровень 3); транспортный уровень (уровень 4); прикладной уровень (уровень 7).

Б.3.1 Использование аутентификации на сетевом уровне

Аутентификация равноправных объектов, используемая на сетевом уровне, позволяет подтвердить идентичность сетевых объектов. Эта служба позволяет аутентифицировать узлы сетей, подсети или ретрансляторы.

Аутентификация происхождения данных, используемая на сетевом уровне, позволяет подтвердить идентичность источника элемента данных. Источником может быть узел сети, подсети или ретранслятор.

Механизмы, используемые на сетевом уровне, расположены внутри уровня.

Б.3.2 Использование аутентификации на транспортном уровне

Аутентификация равноправных объектов, используемая на транспортном уровне, позволяет подтвердить идентичность транспортных объектов. Эта служба позволяет аутентифицировать оконечные системы. Различные приложения, поддерживаемые данной оконечной системой, не могут быть аутентифицированы.

Аутентификация происхождения данных, используемая на транспортном уровне, позволяет подтвердить идентичность источника данных. Источником данных является оконечная система.

Механизмы, используемые на транспортном уровне, расположены внутри уровня.

Б.3.3 Использование аутентификации на прикладном уровне

Аутентификация равноправных объектов, используемая на прикладном уровне, позволяет подтвердить идентичность объектов-приложений оконечной системы. Эта служба позволяет аутентифицировать объекты приложений или процессы приложений. Могут быть аутентифицированы различные объекты приложений или процессы приложений, поддерживаемые данной оконечной системой.

Аутентификация происхождения данных, используемая на прикладном уровне, позволяет подтвердить идентичность источника данных. Источником данных может быть объект приложения или процесс приложения.

Механизмы, используемые на прикладном уровне, могут быть расположены на прикладном уровне или уровне представления данных. Аутентификация, осуществляемая на прикладном уровне, может быть использована для аутентификации служб, предоставляемых сетевым и транспортным уровнями.

Приложение В
(справочное)
Противодействие воспроизведению с помощью уникальных номеров или вызовов

В.1 Уникальные номера

Уникальные номера порождаются заявителем. Один и тот же уникальный номер не может быть принят дважды одним и тем же верификатором. Этого можно достичь несколькими способами. Некоторые технологии, кажущиеся теоретически эффективными, могут оказаться бесполезными на практике. Простым примером такой технологии является отслеживание всех полученных уникальных чисел, успешно использованных во время аутентификационного обмена. Это приводит к увеличению требований к объему памяти при увеличении числа удачных аутентификаций. Такой подход может оказаться неприемлемым по причине стоимости и/или производительности.

Одним из путей снизить требования к объему памяти, требуемой на стороне верификатора, является регистрация всех успешно использованных уникальных номеров только в течение некоторого периода времени. Это приводит к необходимости использования временной метки как части уникального номера, так что только «недавние» уникальные номера сохраняются в памяти верификатора. На практике достаточной является величина периода времени в несколько минут. Это с одной стороны ограничивает как требования к объему памяти, а с другой снимает затруднения, связанные с синхронизацией различных временных ссылок, используемых принципалом и верификатором.

Для того чтобы предотвратить отказ от обслуживания, целесообразно предотвращать непреднамеренные конфликты между уникальными номерами, порожденными двумя различными принципалами. Для этого диапазон уникальных чисел должен быть достаточно большим. Диапазон уникальных чисел связан с максимальным числом аутентификаций, осуществляемых за единицу времени (например, за секунду), что должно быть учтено для каждого верификатора, с помощью которого делается попытка аутентификации. Если временная ссылка, используемая принципалом, не обеспечивает такого диапазона чисел, то к временной метке может быть добавлено случайное число для расширения диапазона уникальных чисел.

В.2 Вызовы

Вызовы порождаются верификатором. Один и тот же вызов никогда не должен быть выдан дважды одним и тем же верификатором. Достичь этого можно несколькими путями.

Некоторые технологии, кажущиеся теоретически эффективными, могут оказаться бесполезными на практике. Простым примером такой технологии является регистрация всех выданных вызовов. Это приводит к увеличению требований к объему памяти при увеличении числа удачных аутентификаций, осуществленных с помощью этих вызовов. Такой подход может оказаться неприемлемым по причине стоимости и/или производительности.

Существует несколько путей снизить требования к объему памяти на стороне верификатора:

–выдача последовательных значений в вызовах и сохранение только последнего значения;

–выдача случайных чисел в вызовах; хотя это нарушает правило, что «один и тот же вызов никогда не должен быть выдан дважды одним и тем же верификатором», вероятность такого события можно снизить до приемлемого уровня при использовании случайных чисел из достаточно большого диапазона;

–использование временных меток в вызове;

–использование сочетания временной метки и случайного числа.

Приложение Г
(справочное)
Защита от некоторых видов атак на аутентификацию

Г.1 Атаки прослушивания-воспроизведения

Необходимо рассмотреть два варианта воспроизведения. К ним относятся воспроизведение некоторой аутентификационной информации, используемой при обмене:

−одному и тому же верификатору;

−другому верификатору.

Последний случай возможен тогда, когда верификационная информация принципала известна нескольким верификаторам. Атака-воспроизведение является частным случаем атаки подмены.

Обоим вариантам воспроизведения можно противостоять с помощью вызовов. Вызовы порождаются верификатором. Один и тот же вызов никогда не должен быть выдан дважды одним и тем же верификатором. Этого можно достичь двумя путями (см. Приложение В).

Г.2 Воспроизведение тому же верификатору

Воспроизведению тому же верификатору можно противодействовать с помощью уникальных номеров или вызовов.

Уникальные номера порождаются заявителем. Один и тот же уникальный номер никогда не должен быть принят дважды одним и тем же верификатором. Этого можно достичь несколькими способами (см. Приложение В).

Г.3 Воспроизведение другому верификатору

Воспроизведению другому верификатору можно противодействовать, используя вызовы. С другой стороны ему можно противодействовать, используя при порождении ИА обмена любые параметры, уникальные для данного верификатора. Это может быть имя верификатора, его сетевой адрес или, в общем случае, любой атрибут, уникальный по отношению к верификаторам, совместно использующим одну и ту же проверочную ИА.

Г.4 Атаки перехвата-подмены

Г.4.1 Прямые атаки

Один из типов атак (прямая атака) предполагает, что «злоумышленник» является инициатором аутентификации. Такая атака возможна только, если и заявитель, и верификатор могут инициировать аутентификацию. Во время такой атаки заявитель и верификатор обмениваются аутентификационной информацией через «злоумышленника», не зная об этом, то есть «злоумышленник» притворяется определенным верификатором перед заявителем и заявителем перед верификатором.

Например, предположим, что «злоумышленник» С притворяется перед верификатором В, что является заявителем А. С начинает взаимодействие с А и В. С сообщает А, что он является В, прося А аутентифицироваться по отношению В, а также сообщает В, что он А и что он хочет аутентифицировать себя.

Во время процесса аутентификации А действует как заявитель по отношению В (на самом деле С выступает в роли В) и поэтому выдает информацию, которую С может использовать для аутентификации по отношению к В. В выступает в роли верификатора и также выдает информацию С, в которой последний нуждается для того, чтобы играть роль верификатора. После аутентификации «злоумышленник» С будет выглядеть перед В как аутентифицированный А.

Возможные способы противодействия данному типу атаки требуют защиты от воспроизведения для различных верификаторов:

а) объект, начинающий аутентификацию, всегда является заявителем;

б) аутентификационная информация, используемая при обмене и выдаваемая заявителем, различается в зависимости от роли инициатора аутентификационного запроса или ответчика на приглашение к аутентификации. Это различие позволяет верификатору обнаружить рассмотренный выше тип атаки. Более подробно это рассмотрено в Приложении Г.

Г.4.2 Оппортунистические атаки

В одном из типов атак «злоумышленник» участвует в аутентификационном обмене, перехватывая и передавая аутентификационную информацию, а также беря на себя роль заявителя.

Обычным методом противодействия данному типу атаки является использование дополнительной службы (целостности данных или безопасности). ИА обмена дополняется некоторой информацией, дающей возможность заявителю и верификатору, являющимися законными участниками процесса аутентификации, получать ключ. Полученный ключ может быть использован в механизмах обеспечения целостности, основанных на криптографии, или в механизмах обеспечения безопасности.

Другой способ противодействия данному типу атаки применим в тех случаях, когда перехват не может быть осуществлен внутри сети передачи данных, то есть когда данные всегда доставляются неизмененными надлежащему адресату. В этой ситуации для противодействия атаке сетевой адрес может быть использован службой порождения в качестве дополнительной информации. Тогда ИА обмена будет зависеть от сетевого адреса.

Г.5 Ограниченная форма защиты от атак «злоумышленников»

Второй тип атак, рассмотренных в Г.4, возможен либо при использовании вызовов, либо уникальных чисел. Защита предусматривает использование заявителем признака, определяющего, следует ли ответ за приглашением к аутентификации или запросом на аутентификацию. Признак может указывать (например, при установке его в единицу), что ответ последовал за приглашением к аутентификации или (при установке признака в ноль), что ответ последовал на запрос на аутентификацию. Так как значения признака используются при вычислении ответа, это означает, что ответ заявителя зависит от его значения. В дальнейшем рассмотренный признак будет называться признаком приглашения/запроса.

Г.6 Протокол, использующий вызовы

При использовании вызовов С притворяется, что является А, и посылает аутентификационный запрос В (первый обмен). В выдает вызов С (второй обмен). С посылает приглашение на аутентификацию А и передает полученный от В вызов А (третий обмен). А вычисляет собственный ответ, используя как вызов, полученный от С, так и признак приглашения/запроса, устанавливая последний в состояние «приглашение». С передает В ответ, полученный от А. В проверяет ответ. Так как аутентификационный запрос первоначально получен от С, В ожидает, что признак приглашения/запроса установлен в состояние «запрос». Так как в полученном ответе признак приглашения/запроса установлен в «приглашение», то запрос на аутентификацию отвергается (см. рисунок Г.1).

Если В поддерживает как запросы, так и приглашения на аутентификацию, В необходимо принять дополнительные меры предосторожности. В должен сохранять информацию о том, какому заявителю выдан данный вызов, так что В не сможет

использовать его с другим заявителем при передаче приглашения на аутентификацию (третий обмен).

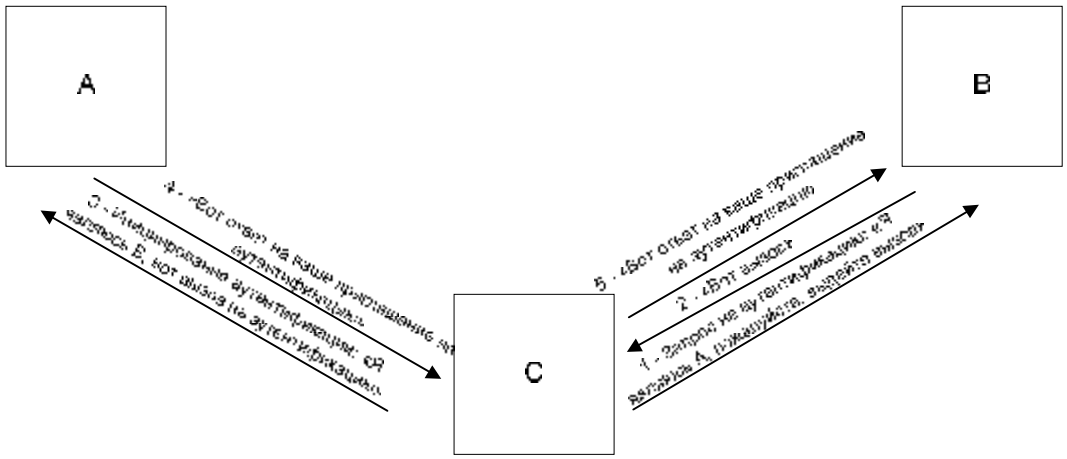


Рисунок Г.1. Противодействие атакам «злоумышленника» при использовании вызовов

Примечание. При противодействии прямым атакам с помощью способов а) или б), как это объяснено в Г.4.1, сохраняется уязвимость к оппортунистическим атакам.

Г.7 Протокол, использующий уникальные номера

При использовании уникальных номеров С притворяется, что является В и посылает А приглашение на аутентификацию (первый обмен). А вычисляет свой ответ, используя уникальный номер, признак приглашение/запрос устанавливается в состояние «приглашение» (второй ответ). С передает В ответ, полученный от А (третий обмен). В проверяет ответ. Он содержит признак приглашение/запрос, установленный в состояние «приглашение», но В не выдавал никакого приглашения на аутентификацию, так что он отвергает аутентификационную информацию (см. рисунок Г.2).

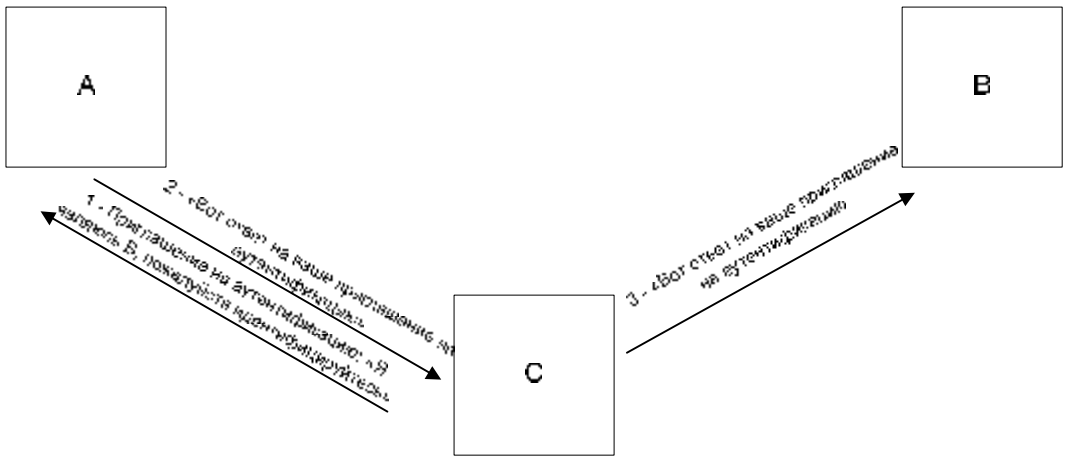


Рисунок Г.2. Защита от атак «злоумышленника» при использовании уникальных номеров

Приложение Д
(справочное)
Некоторые характерные примеры аутентификационных механизмов

В этом приложении приведены два примера аутентификационных механизмов.

Д.1 Конкретный пример использования уникальных номеров в сочетании с оперативно доступным аутентификационным сертификатом

Этот пример иллюстрирует использование механизма уникальных номеров для Класса 3, как это было описано в 7.1. В этом примере используются оперативно доступные сертификаты, уникальный идентификатор, метод защиты, параметр зашиты, время действия, которые включены в аутентификационный сертификат. Метод, используемый в данном примере, нуждается в единственном информационном обмене и позволяет использовать один и тот же аутентификационный сертификат более одного раза.

Метод защиты определяет отношение между параметром защиты, хранимым в сертификате, и внешним управляющим параметром, защищающим аутентификационной сертификат от несанкционированного использования. Внешний управляющий параметр может быть связан с параметром защиты с помощью однонаправленного отношения, такого как:

– внешний управляющий параметр представляет собой проверочное значение, а параметр защиты представляет собой результат применения однонаправленной функции к проверочному значению;

– внешний управляющий параметр является личным ключом, а параметр защиты — соответствующий ему общий ключ.

При использовании проверочного значения в качестве внешнего управляющего параметра, он посылается верификатору в качестве подтверждения обладания аутентификационным сертификатом. Во время передачи проверочное значение должно быть защищено, то есть передано заявителем верификатору в зашифрованном с помощью внешнего секретного ключа, связанного с каналом передачи данных, либо с приемным концом канала передачи данных.

Защита права собственности и защита от воспроизведения достигается использованием уникальных номеров и функции преобразования. В зависимости от вида внешнего управляющего параметра могут быть использованы три вида функций преобразования (F):

а) **Односторонняя функция**. Когда внешний управляющий параметр является проверочным значением, тогда уникальный номер и проверочное значение преобразуются с помощью односторонней функции. Результат и уникальный номер передаются так, чтобы верификатор смог сделать аналогичное преобразование.

б) **Асимметричный алгоритм**. Когда внешний управляющий параметр является личным ключом, уникальный номер подписывается с помощью личного ключа.

в) **Симметричный алгоритм**. Когда внешний управляющий параметр является секретным ключом, уникальный номер шифруется или снабжается безличной подписью с помощью проверочного значения, используемого в качестве секретного ключа.

Этот пример применим как для аутентификации происхождения данных, так и объектов. При аутентификации происхождения данных либо сами данные, либо их цифровая идентификационная метка могут быть также преобразованы с помощью функции F.

Для получения оперативно доступного аутентификационного сертификата используется служба запроса и внешний управляющий параметр. Служба порождения затем генерирует уникальный номер и выполняет преобразование, используя следующую входную информацию:

–уникальный номер;

–внешний управляющий параметр;

–уникальный идентификатор (необязательный параметр);

–цифровая идентификационная метка (при аутентификации происхождения данных).

В дополнение, когда внешний управляющий параметр является проверочным значением или секретным управляющим ключом, служба порождения посылает значение, зашифрованное так, что только верификатор, которому оно предназначено, может дешифровать его и породить ИА обмена, как показано на рисунке 14.

Служба проверяет аутентификационную информацию, используемую при обмене, на достоверность с помощью значения защиты в аутентификационном сертификате (см. рисунок Д.1). В дополнение, при использовании проверочного значения или секретного управляющего ключа, служба проверки дешифрует зашифрованное проверочное значение и секретный ключ управления, а также проверяет соответствие его значению защиты. Служба также проверяет, что уникальный номер не использовался ранее при успешной аутентификации.

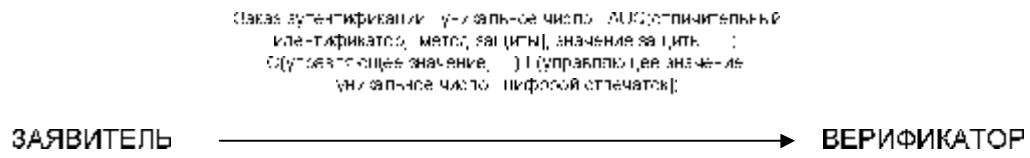


Рисунок Д.1 – Механизм уникальных номеров при использовании оперативно доступного аутентификационного сертификата

Примечания

1 ALC(...) используется для обозначения аутентификационного сертификата, включающего себя, указанные в скобках параметры;

2 C(...) используется для обозначения применения сервиса безопасности. Это применимо только в случае использования параметра управления в качестве проверочного значения.

Д.2 Механизм вызова и оперативно доступный аутентификационный сертификат

Этот механизм использует аутентификационный сертификат для подтверждения аутентификации при использовании принципов, рассмотренных в 4.3 и механизма вызова, описанного в 7.1.5.2 (см. рисунок Д.2). Аутентификационный сертификат обеспечивает подтверждение того, что доверенная третья сторона аутентифицировала держателя сертификата с помощью особого уникального идентификатора. Механизм обеспечивает средства подтверждения, что держателем аутентификационного сертификата для данного уникального идентификатора является заявитель.

Этот пример использует оперативно доступные аутентификационные сертификаты, уникальный идентификатор, метод защиты, параметр защиты и время действия, включенные в аутентификационный сертификат. Этот пример позволяет использовать аутентификационный сертификат многократно.

Метод защиты определяет отношение между параметром защиты, содержащемся в сертификате, и внешним параметром управления, используемом для защиты аутентификационного сертификата от несанкционированного использования. Внешний параметр управления может быть получен из параметра защиты с помощью одностороннего преобразования, такого как:

–внешний управляющий параметр является проверочным значением, а параметр защиты является результатом применения односторонней функции к проверочному значению;

–внешний параметр управления является личным ключом, а параметр защиты является соответствующим ему общим ключом.

Когда проверочное значение используется в качестве внешнего управляющего параметра, он посылается верификатору как подтверждение владения аутентификационным сертификатом. При передаче ключ должен быть защищен, то есть зашифрован заявителем с помощью внешнего секретного ключа, связанного с каналом передачи данных или с приемным концом канала передачи данных.

Защита права собственности и защита от воспроизведения достигается использованием вызова и функции преобразования. В зависимости от вида внешнего параметра управления могут быть использованы три вида функций преобразования (F):

а) **Односторонняя функция**. Когда внешний управляющий параметр является проверочным значением, тогда вызов и проверочное значение преобразуются с помощью односторонней функции. Результат и вызов передаются так, чтобы верификатор смог сделать аналогичное преобразование.

б) **Асимметричный алгоритм**. Когда внешний параметр управления является личным ключом, вызов подписывается с помощью личного ключа.

в) **Симметричный алгоритм**. Когда внешний управляющий параметр является секретным ключом, вызов шифруется или снабжается безличной подписью с помощью проверочного значения, используемого в качестве секретного ключа.

Этот пример применим как для аутентификации происхождения данных, так и объектов. При аутентификации происхождения данных данные или цифровая идентификационная метка данных могут быть преобразованы с помощью функции F.

Служба запроса используется для получения аутентификационного сертификата и внешнего управляющего параметра. Служба порождения создает аутентификационный запрос. При получении аутентификационного запроса служба проверки порождает вызов в виде аутентификационной информации, используемой при обмене. Служба порождения затем проводит преобразование, используя следующие входные данные:

– вызов;

– внешний управляющий параметр;

– уникальный идентификатор (необязательный параметр);

– цифровая идентификационная метка (при аутентификации происхождения данных).

Когда управляющий параметр представляет собой проверочное значение или секретный управляющий ключ, служба порождения пересылает это значение, зашифрованное так, что только предназначенный для этого верификатор может расшифровать его и создать ИА обмена, как показано на рисунке 16. Служба проверки проверяет ИА обмена на подлинность с помощью параметра защиты в аутентификационном сертификате. Кроме того, при использовании проверочного значения или секретного управляющего ключа служба проверки расшифровывает зашифрованное проверочное значение или секретный управляющий ключ и проверяет его

на соответствие значению защиты. Также осуществляется проверка соответствия вызова тому, которому был отправлен.

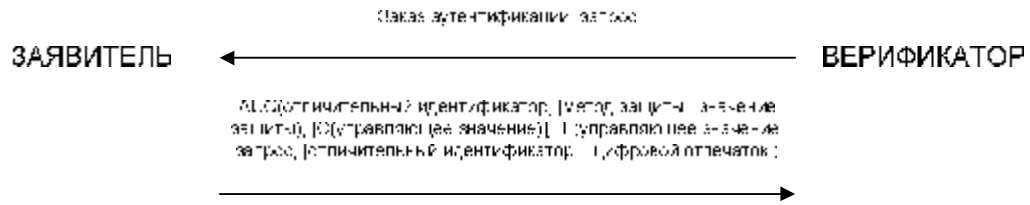


Рисунок Д.2. Механизм вызова при использовании аутентификационного сертификата

Примечание.

1. Обозначение AUC (...) используется для аутентификационного сертификата, включающего в себя параметры, заключенные в круглые скобки.

2. Обозначение C (...) используется для приложения, выполняющего функции службы безопасности. Это применимо только в том случае, когда управляющий параметр является проверочным значением.

УДК 681.324:006.354 **МКС 35.040**

Ключевые слова: обработка данных, информационный обмен, взаимодействие сетей, взаимодействие открытых систем, коммуникационные процедуры, защита информации, технологии безопасности, обзор.

Для заметок

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