ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология
ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ ӘДІСТЕРІ МЕН ҚҰРАЛДАРЫ
Сәйкестендіру тетіктері
2-бөлім
Симметриялық шифрлау алгоритмдері қолданылатын тетіктер

Информационная технология
МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ
Механизмы аутентификации
Часть 2
Механизмы с применением алгоритмов симметричного шифрования

ҚР СТ ИСО/МЭК 9798-2-2008

(ИСО/МЭК 9798-2:1999
«Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Сәйкестендіру тетіктері. 2-бөлік. «Симметриялық шифрлау алгоритмдері қолданылатын тетіктер», IDT)

Ресми басылым

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

Астана

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология

ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ ӘДІСТЕРІ МЕН ҚҰРАЛДАРЫ

Сәйкестендіру тетіктері
2-бөлім
Симметриялық шифрлау алгоритмдері қолданылатын тетіктер

ҚР СТ ИСО/МЭК 9798-2-2008
(ИСО/МЭК 9798-2:1999
«Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Сәйкестендіру тетіктері. 2-бөлік. «Симметриялық шифрлау алгоритмдері қолданылатын тетіктер», IDT)

Ресми басылым

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

Астана

Алғысөз

1 «Инфосистемы Джет» ЖАҚ **ӘЗІРЛЕДІ**

Қазақстан Республикасының Ақпараттандыру және байланыс агенттігі **ЕНГІЗДІ**

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

3 Осы стандарт Қазақстан Республикасының экономикалық қажеттіліктерін көрсететін қосымша талаптары мәтінде көлбеу қаріппен беріліп ИСО/МЭК 9798-2:1999 «Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Сәйкестендіру тетіктері. 2-бөлім. Симметриялық шифрлау алгоритмдері қолданылатын тетіктер» («Information technology. Security techniques. Entity authentication. Part 2. Mechanisms using symmetric encipherment algorithms»), IDT халықаралық стандартына сәйкес.

4 БІРІНШІ ТЕКСЕРУ МЕРЗІМІ 2013 жыл
ТЕКСЕРУ КЕЗЕҢДІЛІГІ 5 жыл

5 АЛҒАШ РЕТ ЕНГІЗІЛДІ

Мазмұны

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология
ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ ӘДІСТЕРІ МЕН ҚҰРАЛДАРЫ
Сәйкестендіру тетіктері
2-бөлім
Симметриялық шифрлау алгоритмдері қолданылатын тетіктер

Енгізілген күні 2008.07.01

1 Қолданылу саласы

Осы стандарт симметриялық алгоритмдерді қолданып шифрлаудың сәйкестендіру тетіктерін белгілейді. Осы тетіктердің төртеуі сенім білдірілген үшінші тарапты қатыстырмай екі мән арасындағы сәйкестендіруді қамтамасыз етеді: олардың екеуі – бір мәнді екіншісіне бір жақты сәйкестендіруге арналған тетіктер, басқа екеуі – екі мәнді өзара сәйкестендіруге арналған тетіктер. Қалған тетіктер ортақ құпия кілтті жасау үшін сенім білдірілген үшінші тараптың болуын көздейді және өзара немесе бір жақты сәйкестендіруді іске асырады.

Ақпараттың криптографиялық қорғаудың нақты құралдарын таңдау және қолдану Қазақстан Республикасының заңнамасымен регламенттеледі және осы стандарттың қарастыру заты болып табылмайды.

Осы стандартта көрсетілген тетіктер сол сәйкестендірілген ақпаратты кешігіп немесе бірнеше рет қабылдауды болдырмау үшін уақытқа байланысты параметрлерді, мысалы уақыт белгісін, жүйелі немесе кездейсоқ сандарды қолданады.

Егер сенім білдірілген үшінші тарап қатыстырылмаса және уақыт таңбасы немесе дәйекті сан пайдаланылса, онда бір жақты сәйкестендіру үшін бір өткелек қажет, ал өзара сәйкестендіру үшін екі өткелек қажет болады. Егер сенім білдірілген үшінші тарап тартылмаса және кездейсоқ сандарды қолдана отырып, шақыру мен жауап беру әдісі қолданылса, онда бір жақты сәйкестендіру үшін екі өткелек қажет, ал өзара сәйкестендіру үшін үш өткелек талап етіледі. Егер сенім білдірілген үшінші тарап тартылса, онда мәні мен сенім білдірілген үшінші тарап арасындағы кез келген қосымша байланыс ақпарат алмасу кезінде екі қосымша өткелекті талап етеді.

2 Нормативтік сілтемелер

Осы стандартта мынадай стандарттарға сілтемелер пайдаланылды:

ҚР СТ ИСО/МЭК 9798-1:2008 Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Сәйкестендіру. 1-бөлік. Жалпы

ережелер.

ҚР СТ ИСО/МЭК 11770-2:2008 Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Кілттерді басқару. 2-бөлік. Симметриялық әдістерді қолданатын тетіктер.

3 Терминдер мен анықтамалар

Осы стандартта *ҚР СТ ИСО/МЭК 9798-1* бойынша терминдер қолданылды.

4 Талаптар

Осы стандартта белгіленетін сәйкестендіру тетіктерінде сәйкестендіруге жататын мән – сәйкестендірудің құпия кілтін өзінің білетінін көрсету арқылы өзінің шынайылығын растайды. Мұны мән кейбір деректерді шифрлауға арналған өзінің құпия кілтін қолдану арқылы іске асырады. Шифрланған деректерді сәйкестендірудің жалпыға бірдей құпия кілтін пайдаланатын кез келген мәннің мағынасы ажыратылып оқылуы мүмкін.

Сәйкестендіру тетіктеріне мынадай талаптар қойылады. Егер осылардың қайсыбірі орындалмаса, онда сәйкестендіру процесі сенімсіз болуы мүмкін немесе оны жүзеге асыру мүмкін болмайды.

а) Верификаторды өзіне сәйкестендіретін талапкер осы верификаторға ортақ сәйкестендірудің құпия кілтін пайдалануы тиіс; мұндай жағдайда 5 бөлімнің тетіктері қолданылады немесе олардың әрқайсысы белгілі бір сенім білдірілген үшінші тараптың өздеріне тән құпия кілтін пайдалануы тиіс; мұндай жағдайда 6 бөлімнің тетіктері қолданылады. Мұндай кілттер сәйкестендіру тетіктерін кез келген нақты пайдалану басталғанға дейін тартылған тараптарға белгілі болуы тиіс. Бұған жәрдемі арқылы қол жеткізілетін әдіс осы стандарттың қолданылу саласынан тыс жатыр.

б) Егер сенім білдірілген үшінші тарап қатыстырылса, онда оған талапкер де, верификатор да сенім білдіруі тиіс.

в) талапкер мен верификатор немесе мән мен сенім білдірілген үшінші тарап бірлесіп пайдаланатын сәйкестендірудің құпия кілті осы екі тарапқа қана, ал ол екеуі сенім білдірген жағдайда басқа да мәндерге белгілі болуы тиіс.

Ескертпе – Шифрлаудың алгоритмі мен кілтті қолданудың мерзімі – кілтті оны қолданудың бүкіл мерзімі ішінде есептеп тану мүмкін болмайтындай таңдалуы тиіс. Бұдан басқа кілттің қолданыс мерзімі – белгілі ашық мәтіннің немесе іріктелген ашық мәтіннің негізінде шабуыл жасауды жүзеге асыру мүмкіндігін жоққа шығаратындай таңдалуы тиіс.

г) *eK-ні* шифрлаудың функциясына және *dK-ні* шифрлаудың тиісті функциясына қатысты – ықтимал *K* құпия кілтінің әрқайсысы үшін төмендегідей қасиеттер тән болуы тиіс: *eK(X)* жолдарына қолданылатын

кезде *dK-ні* ажыратып оқу процесі осы жолдарды алушыға жалған немесе өзгерген деректерді анықтауға мүмкіндік беруі тиіс яғни *K* құпия кілтінің иесі ғана *dK* –ні ажыратып оқу процесі жүзеге асқан кезде «қабылданатын» жолдардың өңін айналдырып оқуға қабілетті болуы тиіс.

Ескертпе – Іс жүзінде бұған бірнеше жолдармен қол жеткізілуі мүмкін. Төменде екі мысалы келтіріліп отыр:

1 Егер жеткілікті түрде басы артық ақпарат деректерде бар болса немесе оған толықтырылса, ал шифрлаудың алгоритмі мұқият түрде іріктелсе, онда тұтастыққа қойылатын талап қанағаттандырылуы мүмкін. Басы артық ақпаратты оқуға болатын деректер дұрысы ретінде қабылданғанға дейін алушы тексереді.

2 К кілті К' және К" сияқты екі кілтті қалыптастыру үшін пайдаланылады. К" кілті шифрлануы тиіс деректер хабарларын (Message Authentication Code - MAC) сәйкестендіру кодын есептеп шығару үшін пайдаланылады, ал К' кілті MAC-қа байланысты деректерді шифрлау үшін пайдаланылады. Алушы дұрысы ретінде оқуға болатын деректерді қабылдағанға дейін MAC мағынасының дұрыстығын тексереді.

д) Осы стандартта келтірілген тетіктер уақыт таңбасы, дәйекті немесе кездейсоқ сандар сияқты уақытқа тәуелді өлшемдерді қолдануды талап етеді. Осы өлшемдердің ерекшелігі – атап айтқанда, сәйкестендірудің құпия кілтінің қолданыс мерзімі шегінде қолайсыз қайталануы осы тетіктердің қауіпсіздігін қамтамасыз ету үшін маңызды болып табылады. Қосымша ақпаратты ҚР СТ ИСО/МЭК 9798-1 Б қосымшасынан қараңыз.

5 Сенім білдірілген үшінші тарапты қолданбайтын тетіктер

Сенім білдірілген үшінші тарапты қолданбайтын сәйкестендірудің тетіктерінде *A* және *B* мәндері сәйкестендіру тетіктерін кез келген нақты пайдалану басталғанға дейін K_{AB} сәйкестендіруінің ортақ құпия кілтімен немесе бір бағыттағы K_{AB} және K_{BA} екі кілтімен бірлесіп иемденуі тиіс. Көрсетілген жағдайлардың соңғысында бір бағыттағы K_{AB} және K_{BA} кілттері тиісінше *A* мәнінің *B* мәнін және *B* мәнінің *A* мәнін сәйкестендіруі үшін қолданылады.

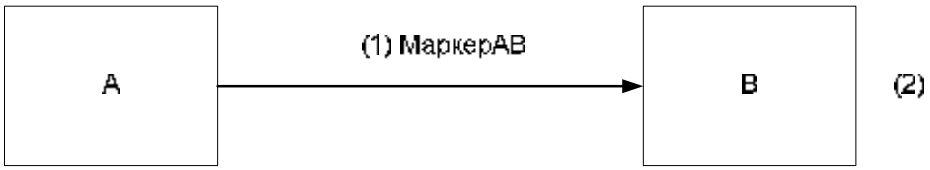
Бұдан әрі қаралатын мәтіндерде белгіленген барлық мәтіндік жиектер қосымшаларда пайдалану үшін қол жеткізімді, қосымшалар осы стандарттың қолданылу аясынан тыс жатады (жиектер бос болуы мүмкін). Мәтіндік жиектердің өзара байланысы және олардың мазмұны нақты қолдануға байланысты. Мәтіндік жиектерді қолдануға қатысты ақпаратты А қосымшасынан қараңыз.

5.1 Бір жақты сәйкестендіру

Бір жақты сәйкестендіру дегеніміз осы тетіктің көмегі арқылы екі мәннің біреуі ғана сәйкестендіріледі.

5.1.1 Бір өткелекті сәйкестендіру

Сәйкестендірудің осы тетігінде талапкер А процеске бастамашы болады және В верификаторымен сәйкестендіріледі. Бірегейлігі/ уақытылылығы уақыт таңбасын немесе дәйекті санды құрумен және тексерумен бақыланады. (ҚР СТ ИСО/МЭК 9798-1 стандартының Б қосымшасын қараңыз). Сәйкестендірудің тетігі 1-суретте көрсетілген.



1-сурет

Талапкер А – В верификаторына жолдаған маркер нысаны (*МаркерАВ*) төмендегідей сипатта жазылады :

$$МаркерАВ = Мәтін2 \| eK_{AB}\left(\begin{matrix} T_A \\ N_A \end{matrix} \| B \| Мәтін1\right), \qquad (1)$$

мұнда талапкер уақытқа тәуелді өлшем ретінде A не N_A дәйекті санын не T_A уақыт таңбасын пайдаланады. Таңдау талапкер мен верификатордың техникалық мүмкіндіктеріне, сондай-ақ ортаға байланысты. АВМаркеріне айырмашылықты В идентификаторын қосу міндетті болып табылмайды.

Ескертпе – В айырмашылықты идентификаторы В мәні болып бүркемеленгісі келетін А қиянат жасаушының мәнге арналған МаркерАВ-ны қайталап пайдаланбауын болдырмас үшін МаркераАВ-ға қосылған. Идентификатордың қосылуы мұндай қиянат орын алмайтын ортада іске қосылмауы үшін міндетті емес сипатта жасалған.

Егер бір бағыттағы кілт пайдаланылатын болса, В айырмашылықты идентификаторы да іске қосылмауы мүмкін.

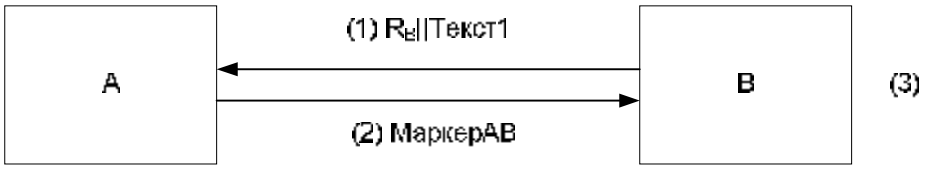
(1) А мәні *МаркерАВ-ны* жасайды және *В* мәніне жолдайды.

(2) *МаркерАВ-да* бар хабарды алғаннан кейін, *В* мәні шифрланған бөліктің мағынасын ашып, *МаркерАВ-ны* растайды (мағынасын ашу 4.d – тармағының талаптары сақталатындығын білдіреді), содан кейін, егер ол бар болса, В айырмашылықты идентификаторының дұрыстығын, сондай-ақ уақыт таңбасын және дәйекті санды тексереді.

5.1.2 Екі өткелекті сәйкестендіру

Сәйкестендірудің осы тетігінде талапкер А процеске бастамашы болатын В верификаторымен сәйкестендіріледі.

Бірегейлігі/уақытылылығы кездейсоқ R_B санын құрумен және тексерумен бақыланады (*ҚР СТ ИСО/МЭК 9798-1* стандартының Б қосымшасын қараңыз*)*. Сәйкестендіру тетігі 2 суретте көрсетілген.



2-сурет

Талапкер *А* – В верификаторына жолдаған маркердің нысаны *(МаркерАВ)* төмендегідей сипатта жазылады:

$$МаркерАВ = Мәтін\,3 \| eK_{AB}\left(R_B \| B \| Мәтін\,2\right) \qquad (2)$$

*МаркерАВ-ға а*йырмашылықты В идентификаторын қосу міндетті болып табылмайды.

1 Ескертпе – Белгілі ашық мәтіннің негізіндегі шабуылдың яғни криптоталдамашы шифрланған мәтіннің бір немесе бірнеше жолдары үшін ашық мәтінді толық білген жағдайда криптоталдамашының шабуылдау мүмкіндігін болдырмас үшін А мәні 2 мәтінге кездейсоқ RA санын қосады.

2 Ескертпе – В айырмашылықты идентификаторы шабуылға тойтарыс беруді (reflection attack) болдырмас үшін МаркерАВ-ға қосылған. Мұндай шабуылдар қиянат жасаушының А мәнін алмастыруға әрекеттеніп, В мәнінің RB шақыруына «тойтарыс беруімен» сипатталады. В айырмашылықты идентификатордың қосылуы мұндай қиянат орын алмайтын ортада іске қосылмауы үшін міндетті емес сипатта жасалған.

Егер бір бағыттағы кілт пайдаланылатын болса, В айырмашылықты идентификаторы да іске қосылмауы мүмкін.

(1) *В* мәні кездейсоқ R_B санын жасайды, сосын бұл санды А Мәніне жолдайды және қажет болған жағдайда *1* мәтіннің мәтіндік жиегіне жолдайды.

(2) *А* мәні *МаркерАВ-ны* жасайды және *В* мәніне жолдайды.

(3) *МаркерАВ-да* бар хабарды алғаннан кейін, *В* мәні шифрланған бөліктің мағынасын ашып, *МаркерАВ-ны* растайды (мағынасын ашу п.4.d талаптары сақталатындығын білдіреді), сосын, егер ол бар болса, В айырмашылықты идентификаторының дұрыстығын тексереді, сосын А Мәніне (1) қадаммен жолданған кездейсоқ R_B санының Маркер АВ – да бар кездейсоқ санмен келісетіндігін тексереді.

5.2 Өзара сәйкестендіру

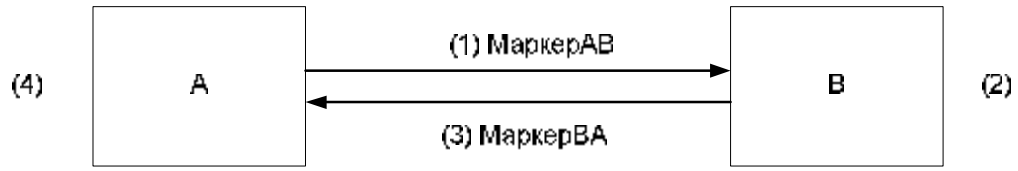
Өзара сәйкестендіру – байланысты қолдайтын екі мәннің тиісті тетіктің көмегі арқылы өзара сәйкестендірілуін білдіреді.

5.1.1 және 5.1.2-де сипатталған екі тетік өзара сәйкестендіруге қол жеткізу үшін тиісінше 5.2.1 және 5.2.2-ге бейімделген. Екі жағдайда да бұл тағы да екі қадамға әкелетін тағы бір өткелекті талап етеді.

Ескертпе – Өзара сәйкестендірілуге арналған үшінші тетік 5.1.2 –де белгіленген тетіктің екі нұсқасынан жасалуы мүмкін, бұл ретте сәйкестендірілудің бір процесіне А мәні, ал екіншісіне В мәні бастамашы болады.

5.2.1 Екі өткелекті сәйкестендіру

Сәйкестендірудің осы тетігіндегі бірегейлілік/уақытылылық уақыт таңбасын немесе дәйекті сандар құрумен және тексерумен бақыланады (*ҚР СТ ИСО/МЭК 9798-1* стандартының Б қосымшасын қараңыз*)*. Сәйкестендіру



3 сурет

тетігі 3 суретте көрсетілген.

А мәні В мәніне жолдаған маркер нысаны *(МаркерAB)* 5.1.1-де белгіленгеніне ұқсас.

$$МаркерAB = Мәтін\,2 \| eK_{AB}\left(\begin{matrix} T_A \\ N_A \end{matrix} \| B \| Мәтін\,1\right) \qquad (3)$$

В мәні *А* мәніне жолдаған маркер нысанының *(МаркерBA)* түрі мынадай:

$$МаркерBA = Мәтін\,4 \| eK_{AB}\left(\begin{matrix} T_B \\ N_B \end{matrix} \| A \| Мәтін\,2\right) \qquad (4)$$

В айырмашылықты идентификаторының *МаркерAB-ға* қосылуы және *А* айырмашылықты идентификаторының *МаркерAB-ға* қосылуы міндетті (тәуелсіз) болып табылмайды.

1 ескертпе – В айырмашылықты идентификаторы В мәні болып бүркемеленгісі келетін қиянат жасаушының А мәніне арналған МаркерAB-ны қайталап пайдаланбауын болдырмас үшін МаркераAB-ға қосылған. Тап осындай себептермен А идентификаторы МаркераAB-ға қосылған. Идентификаторлардың қосылуы мұндай қиянат орын алмайтын ортада бір немесе екі идентификатор іске қосылмауы үшін міндетті емес сипатта жасалған.

Егер бір бағыттағы кілттер пайдаланылатын болса, А және В айырмашылықты идентификаторлары да іске қосылмауы мүмкін (төменде қараңыз).

Қаралып отырған тетікте не уақыт таңбасын не дәйекті сандарды пайдалануды таңдау талапкер мен верификатордың мүмкіндігіне, сондай-ақ жұмыс істеу ортасына байланысты.

(1) және (2) қадамдар бір өткелекті аутентификациялауға арналған 5.1.1-де белгіленген қадамдарға ұқсас.

(3) *В* мәні *МаркерBA-ны* жасайды және *А* мәніне жолдайды.

(4) (3) қадамындағы хабар 5.1.1-дегі (2) қадамға ұқсас тәсілмен өңделеді.

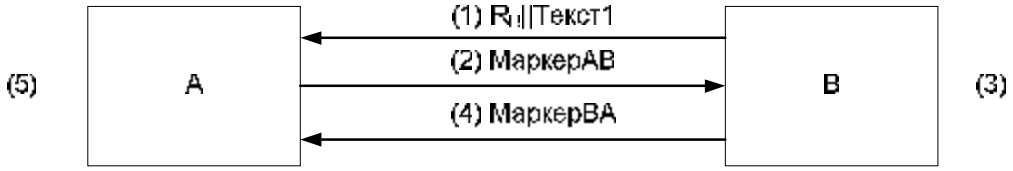
2 Ескертпе – Осы тетіктің екі хабары анық емес бір мезгілдікті қоспағанда, бір бірімен ештеңемен де байланыспаған. Қаралып отырған тетік 5.1.1. тетігін тәуелсіз

қолдануды екі рет пайдаланады. Бұл хабарларды бұдан былайғы байланыстыруға мәтін жиектерін тиісті пайдалану арқылы қол жеткізілуі мүмкін.

Егер бір бағыттағы кілттер пайдаланылатын болса, онда *МаркереВА-дағы* K_{AB} кілті K_{BA} кілтімен ауыстырылады және (4) қадамда тиісті кілт пайдаланылады.

5.2.2 Үш өткелекті сәйкестендіру

Сәйкестендірудің осы тетігінде бірегейлілік/уақытылылық кездейсоқ сандарды құрумен және тексерумен бақыланады (ҚР СТ ИСО/МЭК 9798-1 стандартының Б қосымшасын қараңыз). Сәйкестендірудің тетігі 4 суретте көрсетілген.



4-сурет

Маркерлердің мынадай нысандары бар:

$$МаркерАВ = Мәтін\ 3 \| eK_{AB}\left(R_A \| R_B \| B \| Мәтін\ 2\right),$$
$$МаркерВА = Мәтін\ 5 \| eK_{AB}\left(R_B \| R_A \| Мәтін\ 4\right) \qquad (5)$$

В айырмашылықты идентификаторын МаркерАВ-ға қосу міндетті болып табылмайды.

Ескертпе – В айырмашылықты идентификаторы шабуылға тойтарыс беруді (reflection attack) болдырмас үшін МаркерАВ-ға қосылған. Мұндай шабуылдар қиянат жасаушының А мәнін алмастыруға әрекеттеніп, В мәнінің RB шақыруына «тойтарыс беруімен» сипатталады. В айырмашылықты идентификатордың қосылуы мұндай қиянат орын алмайтын ортада іске қосылмауы үшін міндетті емес сипатта жасалған.

Егер бір бағыттағы кілт пайдаланылатын болса, В айырмашылықты идентификаторы іске қосылмауы мүмкін.

(1) *В* мәні кездейсоқ R_B санын жасайды, сосын бұл санды, қажет болған жағдайда, *А* мәнінің 1 Мәтінінің мәтіндік жиегіне жолдайды.

(2) *А* мәні кездейсоқ R_A санын жасайды, сондай-ақ *МаркерАВ-ны* жасайды және *В* мәніне жолдайды.

(3) *АВ Маркері* бар хабарды алғаннан кейін А мәні шифрланған бөліктің мағынасын ашып, *МаркерАВ-ны* растайды, (мағынасын ашу п.4.d талаптары сақталатындығын білдіреді), ал сосын (1) қадаммен В мәніне жолданған кездейсоқ R_B саны *МаркерАВ-да* бар кездейсоқ санмен келісілгендігін және (2) қадаммен В мәніне жолданған кездейсоқ R_A саны *МаркерАВ-да* бар кездейсоқ санмен келісілгендігін тексереді.

(4) *B* мәні *МаркерBA-ны* жасайды және А мәніне жолдайды.

(5) *AB Маркері* бар хабарды алғаннан кейін А мәні шифрланған бөліктің мағынасын ашып, *МаркерAB-ны* растайды, (мағынасын ашу 4.d-тармағының талаптары сақталатындығын білдіреді), ал содан кейін (1) қадаммен В мәніне жолданған кездейсоқ R_B саны *МаркерAB-да* бар кездейсоқ санмен келісілгендігін және (2) қадаммен В мәніне жолданған кездейсоқ R_A саны *МаркереAB-да* бар кездейсоқ санмен келісілгендігін тексереді.

Егер бір бағыттағы кілттер пайдаланылатын болса, онда *МаркереBA-дағы* K_{AB} кілті K_{BA} кілтімен ауыстырылады және (5) қадамда тиісті кілт пайдаланылатын болады.

6 Сенім білдірілген үшінші тарапты қолданатын тетіктер

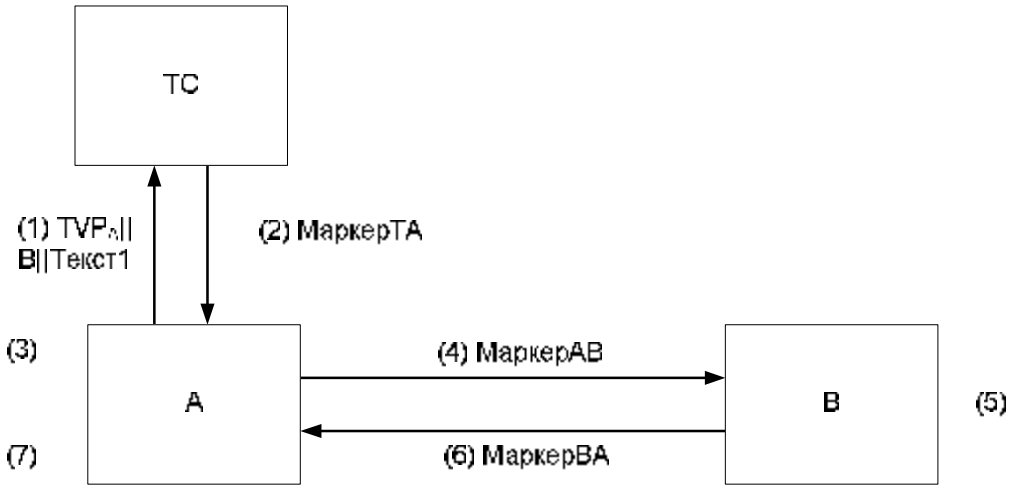
Сәйкестендіру процесі басталғанға дейін осы бөлімде қаралатын сәйкестендіру тетіктері екі мән үшін де ортақ болып табылатын құпия кілтті пайдаланбайды. Оның орнына мәндер сенім білдірілген үшінші тарапты пайдаланады (ТС айрықша идентификаторы бар), онымен А және В мәндерінің әрқайсысының тиісінше K_{AT} және *KBT* сияқты ортақ құпия кілттері болады. Әрбір тетікте мәндердің біреуі сенім білдірілген үшінші тараптан K_{AB} кілтін сұрайды. Одан әрі тиісінше 5.2.1 және 5.2.2-де сипатталған тетіктердің бейімделуі керек.

Егер бір жақты сәйкестендіру ғана талап етілсе, төменде сипатталатыны сияқты әрбір тетікте кейбір өткелектер іске қосылмауы мүмкін.

Бұдан былайғы қаралатын тетіктерде белгіленген барлық мәтіндік жиектерді осы стандарттың қолданылу саласынан тысқары жатқан, қосымшаларда қолдануға болады. Мәтіндік жиектердің өзара байланысы және олардың мазмұны нақты қолдануға байланысты. Мәтіндік жиектерді пайдалануға қатысты ақпаратты А қосымшасынан қараңыз.

6.1 Алты өткізгішті сәйкестендіру

Сәйкестендірудің осы тетігінде бірегейлілік/уақытылылық уақытқа тәуелді өлшемдерді пайдаланумен бақыланады (ҚР СТ ИСО/МЭК 9798-1стандартының Б қосымшасын қараңыз). Сәйкестендіру тетігі 5-суретте көрсетілген.



5 сурет

ТС-тің сенім білдірілген үшінші тарапы А мәніне жолдаған маркердің (*МаркерТА*) нысаны төмендегідей сипатта жазылады:

$$МаркерТА = Mjtін\,4 \| eK_{AT}\left(TVP_A \| K_{AB} \| B \| Mjtін\,3\right) \| eK_{BT}\left(\begin{matrix} T_{TC} \\ N_{TC} \end{matrix} \| K_{AB} \| A \| Mjtін\,2\right) \quad (6)$$

А мәні В мәніне жолдаған маркердің (*МаркерАВ*) нысаны төмендегідей сипатта жазылады:

$$МаркерАВ = Mjtін\,6 \| eK_{BT}\left(\begin{matrix} T_{TC} \\ N_{TC} \end{matrix} \| K_{AB} \| A \| Mjtін\,2\right) \| eK_{AB}\left(\begin{matrix} T_A \\ N_A \end{matrix} \| B \| Mjtін\,5\right) \quad (7)$$

В мәні А мәніне жолдаған маркердің (*МаркерВА*) нысаны төмендегідей сипатта жазылады:

$$МаркерВА = Mjtін\,8 \| eK_{AB}\left(\begin{matrix} T_B \\ N_B \end{matrix} \| A \| Mjtін\,7\right) \quad (8)$$

Уақытқа не уақыт таңбасына не дәйекті сандарға тәуелді өлшемдер ретінде осы тетіктегі таңдау – процеске тартылған мәндердің мүмкіндігіне, сондай-ақ ортаға байланысты.

2 суреттегі (1)-(3) қадамдардағы TVP_A өлшем уақытысына тәуелді қолданылуы, төменде көрсетілгені сияқты, оның әдеттегі қолданылуынан біршама ерекшеленеді. Бұл А мәніне (2) жауап хабарды (1) хабар туралы сұрау салумен байланыстыруға мүмкіндік береді. Осы айтылған жағдайда уақытқа тәуелді өлшемнің маңызды ерекшелігі оның қайталанбауы болып табылады. Аталған ерекшелік алдын ала пайдаланылған ТАМаркерін қайталап пайдалану мүмкіндігін шектейді.

Ескертпе – Уақытқа тәуелді өлшем ретінде кездейсоқ сан пайдаланылуы мүмкін. Алайда осы стандартта пайдаланылатын белгілі тетіктердегі кездейсоқ сандардан ерекшелігі – сенім білдірілген үшінші тарап үшін TVPA-дың болжап болмайтындай қажеттілігі жоқ және есептеп табылған мәннің қайталанбауы талап етілмейді.

(1) *А* мәні уақытқа, TVP_A-ға тәуелді өлшем жасайды, сосын осы өлшемді ТС-тің сенім білдірілген үшінші тарапына, В айырмашылықты идентификаторына және қажеттілік болған жағдайда 1Мәтіннің мәтіндік жиегіне жолдайды.

(2) ТС-тің сенім білдірілген үшінші тарапы МаркерТА-ны жасайды және А мәніне жолдайды.

(3) *МаркерТА-сы* бар хабарды алғаннан кейін *А* мәні K_{AT} кілтімен шифрланған деректердің мағынасын ашып, (мағынасын ашу п.4.d талаптарының сақталатындығын білдіреді) *МаркерТА-ны* растайды, сосын айырмашылықты *В* идентификаторының дұрыстығын тексереді, сондай-ақ (1) қадаммен сенім білдірілген үшінші тарапқа жолданған ТС-тің уақытқа тәуелді өлшемі *МаркереТА-да бар* уақытқа тәуелді өлшеммен келісілгендігін тексереді. Бұдан басқа А мәні сәйкестендірудің K_{AB} құпия кілтін алады, сосын *МаркерАВ-ны* құру үшін *МаркерТА-дан* төмендегі ақпаратты алады:

$$eK_{BT}\left(\begin{matrix}T_{TC}\\N_{TC}\end{matrix}\left\|K_{AB}\right\|A\right\|Mjmih\,2\Big) \qquad (9)$$

(4) *А* мәні *МаркерАВ-ны* жасайды және *В* мәніне жолдайды.

(5) *МаркерАВ-да* бар хабарды алғаннан кейін *В* мәні шифрланған бөліктің мағынасын ашып (мағынасын ашу п.4.d талаптарының сақталатындығын білдіреді) *МаркерАВ-ны* растайды, сосын айырмашылықты *А* және *В* идентификаторларының дұрыстығын, сондай-ақ уақыт таңбасын немесе дәйекті санды тексереді. Бұдан басқа *В* мәні сәйкестендірудің K_{AB} құпия кілтін алады.

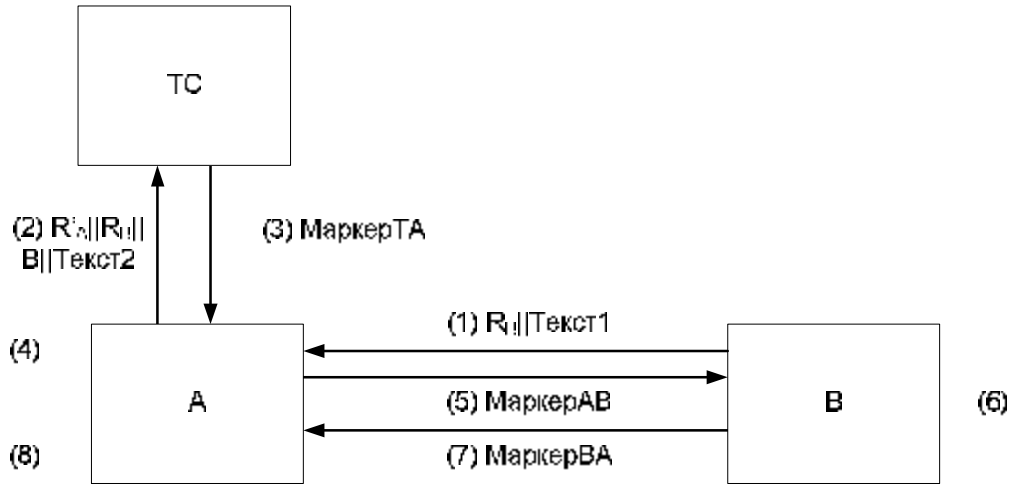
(6) *В* мәні *МаркерВА-ны* жасайды және *А* мәніне жолдайды.

(7) *МаркерВА-да* бар хабарды алғаннан кейін *А* мәні шифрланған бөліктің мағынасын ашып (мағынасын ашу п.4.d талаптарының сақталатындығын білдіреді) *МаркерВА-ны* растайды, сосын айырмашылықты *А* идентификаторының дұрыстығын, сондай-ақ уақыт таңбасын немесе дәйекті санды тексереді.

Егер В мәні А мәнін бір жақты аутентификациялауы талап етілсе (6) и (7) қадамдары іске қосылмауы мүмкін.

6.2 Бес өткізгішті сәйкестендіру

Өзара сәйкестендірудің осы тетігінде бірегейлілік/уақытылылық уақытқа кездейсоқ сандарды пайдаланумен бақыланады (ҚР СТ ИСО/МЭК 9798-1стандартының Б қосымшасын қараңыз). Осы тетік ҚР СТ ИСО/МЭК 9798-2 кілтін жасауға арналған 9 тетікке балама. Сәйкестендіру тетігі 6-суретте көрсетілген.



6 сурет

Сенім білдірілген үшінші тарап жолдаған *ТС* маркерінің *(МаркерТА)* нысаны мынадай түрде жазылады:

$$МаркерТА = Мұтін\ 5 \| eK_{AT}\left(R'_A \| K_{AB} \| B \| Мұтін\ 4\right) \| eK_{BT}\left(R_B \| K_{AB} \| A \| Мұтін\ 3\right) \qquad (10)$$

А мәні В мәніне жолдаған маркердің *(МаркерАВ)* нысаны келесі түрде жазылады :

$$МаркерАВ = Мұтін\ 7 \| eK_{BT}\left(R_B \| K_{AB} \| A \| Мұтін\ 3\right) \| eK_{AB}\left(R_A \| R_B \| Мұтін\ 6\right) \qquad (11)$$

В мәні А мәніне жолдаған маркердің *(МаркерАВ)* нысаны келесі түрде жазылады:

$$МаркерВА = Мұтін\ 9 \| eK_{AB}\left(R_B \| R_A \| Мұтін\ 8\right) \qquad (12)$$

(1) *В* мәні кездейсоқ R_B санын жасайды, сосын осы санды қажет болған жағдайда А мәнінің 1Мәтінің мәтіндік жиегіне жолдайды.

(2) *А* мәні кездейсоқ R'_A санын жасайды және жолдайды, сондай-ақ кездейсоқ R_B санын айырмашылықты *В* идентификаторына және қажет болған жағдайда *ТС-тің* сенім білдірілген үшінші тарапының 2Мәтінінің мәтіндік жиегіне жолдайды.

(3) *ТС-тің* сенім білдірілген үшінші тарапы *МаркерТА-ны* жасайды *А* мәніне жолдайды.

(4) *МаркерТА-сы* бар хабарды алғаннан кейін *А* мәні K_{AT} кілтімен шифрланған деректердің мағынасын ашып, (мағынасын ашу п.4.d талаптарының сақталатындығын білдіреді) *МаркерТА-ны* растайды, сосын айырмашылықты *В* идентификаторының дұрыстығын тексереді, сондай-ақ (2) қадаммен ТС-тің сенім білдірілген үшінші тарапына жолданған кездейсоқ R'_A саны *МаркерТА-да бар* кездейсоқ санмен келісілгендігін тексереді. Бұдан басқа А мәні сәйкестендірудің K_{AB} құпия кілтін алады, сосын *МаркерАВ-ны* құру үшін *МаркерТА-дан* төмендегі ақпаратты алады:

$$eK_{BT}\left(R_B \| K_{AB} \| A \| Mjmih\,3\right) \qquad (13)$$

(5) *A* мәні кездейсоқ екінші R_A санын жасайды, сондай-ақ *МаркерАВ-ны* жасап *В* мәніне жолдайды.

(6) *МаркерВА-да* бар хабарды алғаннан кейін *В* мәні K_{AT} кілтімен шифрланған бөліктің мағынасын ашып, (мағынасын ашу п.4.d талаптарының сақталатындығын білдіреді) *МаркерАВ-ны* растайды, сосын айырмашылықты *А* идентификаторының дұрыстығын тексереді, сондай-ақ (1) қадаммен А мәніне жолданған кездейсоқ R_B саны *МаркерАВ-да бар* екі көшірмесімен келісілгендігін тексереді. Бұдан басқа В мәні аутентификациялаудың K_{AB} құпия кілтін алады.

(7) *В* мәні *МаркерВА-ны жасайды және А* мәніне жолдайды.

(8) *МаркерВА-да* бар хабарды алғаннан кейін *А* мәні шифрланған бөліктің мағынасын ашып, (мағынасын ашу п.4.d талаптарының сақталатындығын білдіреді) *МаркерВА-ны* растайды, сосын В мәнінен (1) қадаммен алынған кездейсоқ R_B саны *МаркерАВ-да бар* кездейсоқ санмен келісілгендігін және (5) қадаммен В мәніне жолданған кездейсоқ R_A санының МаркерВА-да бар кездейсоқ санмен келісілгендігін тексереді. Бұдан басқа В мәні аутентификациялаудың K_{AB} құпия кілтін алады.

Егер В мәні А мәнін бір жақты сәйкестендірілуі талап етілсе, (7) және (8) қадамдар іске қосылмауы мүмкін.

А қосымшасы
(анықтамалық)
Мәтіндік өрістерді қолдану

Осы стандарттың 5 және 6 бөлімдерінде келтірілген маркерлерде мәтіндік өрістер бар. Сәйкестендірудің нақты өту тетігіндегі түрлі мәтіндік жиектер арасында нақты қолдану және өзара байланыс нақты қолданудан тәуелді болады.

Егер маркерлерде (жеткілікті түрде) басы артық ақпарат болмаса, шифрланатын мәтіндік жиектер қосымша ақпаратты қамтамасыз ету үшін пайдаланылуы мүмкін.

Құпиялылықты немесе деректер көзін сәйкестендіруді талап ететін кез келген ақпарат маркердің шифрланған бөлігіне орналастырылуы тиіс.

ӘОЖ 681.324:006.354 **МСЖ 35.040**

Түйінді сөздер: деректерді өңдеу, ақпараттық алмасу, ақпаратты қорғау, қорғаудың әдістері мен құралдары, сәйкестендіру, маркер, шифрлау, алгоритмдер.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Механизмы аутентификации
Часть 2
Механизмы с применением алгоритмов симметричного шифрования

СТ РК ИСО/МЭК 9798-2-2008

(ИСО/МЭК 9798-2:1999
«Информационная технология. Методы и средства обеспечения безопасности. Механизмы аутентификации.
Часть 2. Механизмы с применением алгоритмов симметричного шифрования», 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 9798-2:1999 «Информационная технология. Методы и средства обеспечения безопасности. Механизмы аутентификации. Часть 2. Механизмы с применением алгоритмов симметричного шифрования» («Information technology. Security techniques. Entity authentication. Part 2. Mechanisms using symmetric encipherment algorithms»), 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

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ МЕХАНИЗМЫ АУТЕНТИФИКАЦИИ Часть 2 Механизмы с применением алгоритмов симметричного шифрования

Дата введения 2008.07.01

1 Область применения

Настоящий стандарт устанавливает механизмы аутентификации с применением симметричных алгоритмов шифрования. Четыре из этих механизмов обеспечивают аутентификацию между двумя сущностями без вовлечения доверенной третьей стороны: два из них – это механизмы для односторонней аутентификации одной сущности другой, два других – это механизмы для взаимной аутентификации двух сущностей. Остальные механизмы предполагают наличие доверенной третьей стороны для создания общего секретного ключа и реализуют взаимную или одностороннюю аутентификацию.

Выбор и применение конкретных средств криптографической защиты информации регламентируется законодательством Республики Казахстан и не является предметом рассмотрения настоящего стандарта.

Механизмы, указанные в настоящем стандарте, используют параметры, зависящие от времени, например, метки времени, последовательные или случайные числа для предотвращения принятия той же самой аутентификационной информации в более позднее время или неоднократно.

Если доверенная третья сторона не привлечена и используется метка времени или последовательное число, то необходим один проход для односторонней аутентификации, в то время как для взаимной аутентификации необходимы два прохода. Если доверенная третья сторона не привлечена и используется метод вызова и ответа с применением случайных чисел, то необходимы два прохода для односторонней аутентификации, в то время как для взаимной аутентификации требуется три прохода. Если доверенная третья сторона привлечена, то любая дополнительная связь между сущностью и доверенной третьей стороной требует двух дополнительных проходов при обмене информацией.

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. Аутентификация. Часть 1. Общие положения.

СТ РК ИСО/МЭК 11770-2-2008 Информационные технологии. Методы и средства обеспечения безопасности. Управление ключами. Часть 2. Механизмы, использующие симметричные методы.

3 Термины и определения

В настоящем стандарте применены термины по СТ РК ИСО/ МЭК 9798-1.

4 Требования

В механизмах аутентификации, определяемых в настоящем стандарте, сущность, которая подлежит аутентификации, подтверждает свою подлинность демонстрацией своих знаний секретного ключа аутентификации. Сущность реализует это путем применения своего секретного ключа для шифрования некоторых данных. Зашифрованные данные могут быть расшифрованы любой сущностью, использующей имеющийся у нее секретный ключ аутентификации.

К механизмам аутентификации предъявляются следующие требования. Если какое-либо из них не выполнено, то процесс аутентификации может быть недостоверным или может быть неосуществим.

а) Претендент, аутентифицирующий себя верификатору, должен использовать общий с этим верификатором секретный ключ аутентификации; в этом случае применяются механизмы раздела 5, или каждый из них должен использовать свой секретный ключ аутентификации с одной и той же доверенной третьей стороной; в этом случае применяются механизмы раздела 6. Такие ключи должны быть известны вовлеченным сторонам до начала любого конкретного использования механизма аутентификации. Метод, с помощью которого это достигается, находится вне области действия настоящего стандарта.

б) Если вовлечена доверенная третья сторона, то ей должны доверять и претендент, и верификатор.

в) Секретный ключ аутентификации, используемый совместно претендентом и верификатором или сущностью и доверенной третьей стороной, должен быть известен только этим двум сторонам, а, возможно, и другим сущностям, которым они оба доверяют.

Примечание. Алгоритм шифрования и срок действия ключа должны быть выбраны так, чтобы было вычислительно неосуществимо узнать ключ в течение его срока действия. Кроме того, срок действия ключа должен быть выбран так, чтобы

предотвратить возможность осуществления атак на основе известного открытого текста или выбранного открытого текста.

г) Для каждого возможного секретного ключа *K* функция шифрования *eK* и соответствующая функция расшифрования *dK* должны обладать следующим свойством: процесс дешифрования *dK*, когда он применим к строке *eK(X)*, должен давать возможность получателю этой строки обнаруживать сфальсифицированные или измененные данные, т.е. только владелец секретного ключа *K* должен быть способен генерировать строки, которые будут "приняты", когда осуществится процесс расшифрования *dK*.

Примечание. На практике это может быть достигнуто несколькими путями. Ниже представлено два примера.

1. Если достаточная избыточность присутствует в данных или добавлена к ним, а алгоритм шифрования выбирается тщательно, то требование к целостности может быть удовлетворено. Избыточность проверяется получателем на корректность до того, как расшифрованные данные могут быть приняты в качестве правильных.

2 Ключ *K* используется для формирования пары ключей *K'* и *K''*. Ключ *K*" затем используется для вычисления кода аутентификации сообщений (Message Authentication Code - MAC) данных, которые должны быть зашифрованы, в то время, как ключ *K'* используется для шифрования данных, связанных с MAC. Получатель проверяет корректность значения MAC до принятия расшифрованных данных в качестве правильных.

д) Механизмы, представленные в настоящем стандарте, требуют применения параметров, зависящих от времени, таких, как метки времени, последовательные или случайные числа. Свойства этих параметров, в частности, крайне нежелательная повторяемость в пределах срока действия секретного ключа аутентификации, являются важными для обеспечения безопасности этих механизмов. Дополнительную информацию см. в Приложении Б стандарта *СТ РК ИСО/МЭК 9798-1-2008*.

5 Механизмы, не использующие доверенную третью сторону

В механизмах аутентификации, не использующих доверенную третью сторону, сущности *A* и *B* должны совместно владеть общим секретным ключом аутентификации K_{AB} или двумя однонаправленными ключами K_{AB} и K_{BA} до начала любого конкретного применения механизмов аутентификации. В последнем из указанных случаев однонаправленные ключи K_{AB} и K_{BA} применяются соответственно для аутентификации сущности *A* сущностью *B* и сущности *B* сущностью *A*.

Все текстовые поля, определенные в рассматриваемых далее механизмах, доступны для применения в приложениях, которые находятся вне сферы применения настоящего стандарта (поля могут быть пустыми). Взаимосвязь текстовых полей и их содержание зависят от конкретного применения. Информацию относительно применения текстовых полей см. в приложении А.

5.1 Односторонняя аутентификация

Односторонняя аутентификация подразумевает, что только одна из двух сущностей аутентифицируется при помощи этого механизма.

5.1.1 Однопроходная аутентификация

В этом механизме аутентификации претендент А инициирует процесс и аутентифицируется верификатором *B*. Уникальность/своевременность контролируется созданием и проверкой метки времени или последовательного числа (см. приложение Б стандарта *СТ РК ИСО/МЭК 9798-1-2008).* Механизм аутентификации представлен на рисунке 1.

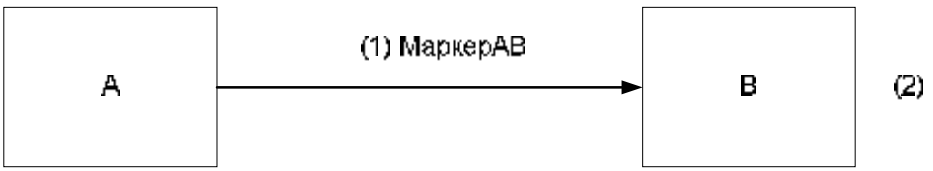


Рисунок 1

Форма маркера (*МаркерAB*), посланного претендентом А верификатору В выглядит следующим образом:

$$МаркерAB = Текст2 \| eK_{AB}\begin{pmatrix} T_A \\ N_A \end{pmatrix} \| B \| Текст1 \qquad (1)$$

где претендент *A* использует либо последовательное число N_A, либо метку времени T_A в качестве параметра, зависящего от времени. Выбор зависит от технических возможностей претендента и верификатора, а также от среды.

Включение отличительного идентификатора *B* в *МаркерAB* является необязательным.

Примечание. Отличительный идентификатор *B* включен в *МаркерAB* для предотвращения повторного использования *МаркераAB* для сущности А злоумышленником, маскирующимся под сущность В. Включение идентификатора сделано необязательным для того, чтобы в среде, где такие нарушения не могут иметь место, он мог быть опущен.

Отличительный идентификатор *B* также может быть опущен, если используется однонаправленный ключ.

(1) Сущность А создает и посылает *МаркерAB* сущности *B*.

(2) После получения сообщения, содержащего *МаркерAB*, сущность *B* подтверждает *МаркерAB*, расшифровывая зашифрованную часть (где расшифрование подразумевает, что требования пункта 4.г соблюдаются), а затем, проверяя правильность отличительного идентификатора *B*, если он имеется, а также метку времени или последовательное число.

5.1.2 Двухпроходная аутентификация

В этом механизме аутентификации претендент *A* аутентифицируется верификатором *B*, который инициирует процесс.

Уникальность/своевременность контролируется созданием и проверкой случайного числа R_B (см. приложение Б стандарта *СТ РК ИСО/МЭК 9798-1-2008)*. Механизм аутентификации представлен на рисунке 2.

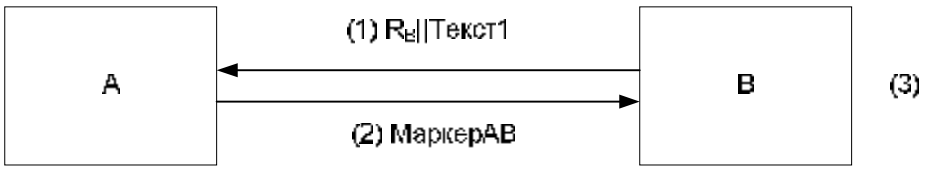


Рисунок 2

Форма маркера *(МаркерAB)*, посланного претендентом *A* верификатору B, выглядит следующим образом:

$$МаркерAB = Текст3 \| eK_{AB}\left(R_B \| B \| Текст2\right) \qquad (2)$$

Включение отличительного идентификатора *B* в *МаркерAB* является необязательным.

Примечание.

1. Для того, чтобы предотвратить возможность атаки на основе известного открытого текста, т.е. криптоаналитической атаки, когда криптоаналитик знает полный открытый текст для одной или нескольких строк зашифрованного текста, сущность *A* может включить случайное число R_A в *Текст2*.

2. Отличительный идентификатор *B* включен в *МаркерAB* для предотвращения так называемых атак отражением (reflection attack). Подобные атаки характеризуется тем, что злоумышленник «отражает» вызов R_B сущности *B*, пытаясь подменить сущность *A*. Включение отличительного идентификатора *B* сделано необязательным, чтобы в среде, где такие нарушения не могут иметь место, он мог быть опущен.

Отличительный идентификатор *B* также может быть опущен, если используется однонаправленный ключ.

(1) Сущность *B* создает случайное число R_B, затем посылает сущности A это число и, при необходимости, текстовое поле *Текст1*.

(2) Сущность *A* создает и посылает *МаркерAB* сущности *B*.

(3) После получения сообщения, содержащего *МаркерAB*, сущность *B* подтверждает *МаркерAB*, расшифровывая зашифрованную часть (где расшифрование подразумевает, что требования пункта 4.г соблюдаются), а затем проверяет правильность отличительного идентификатора *B*, если он имеется, и проверяет, чтобы случайное число R_B, посланное сущности *A* на шаге (1), согласовывалось со случайным числом, содержащимся в *МаркереAB*.

5.2 Взаимная аутентификация

Взаимная аутентификация подразумевает, что две поддерживающих связь сущности аутентифицируются между собой при помощи соответствующего механизма.

Два механизма, описанные в 5.1.1 и 5.1.2, приспособлены в 5.2.1 и 5.2.2 соответственно для достижения взаимной аутентификации. В обоих случаях это требует еще одного прохода, приводящего к еще двум шагам.

Примечание. Третий механизм для взаимной аутентификации может быть создан из двух вариантов механизма, определенного в 5.1.2, при этом один процесс аутентификации инициируется сущностью *A*, а второй – сущностью *B*.

5.2.1 Двухпроходная аутентификация

В этом механизме аутентификации уникальность/своевременность контролируется созданием и проверкой меток времени или последовательных чисел (см. приложение Б стандарта *СТ РК ИСО/МЭК 9798-1-2008*). Механизм аутентификации представлен на рисунке 3.

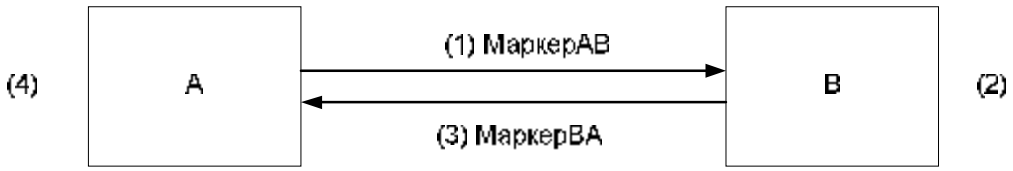


Рисунок 3

Форма маркера *(МаркерAB)*, посланного сущностью *A* сущности *B*, идентична той, которая определена в 5.1.1.

$$МаркерAB = Текст2 \| eK_{AB}\begin{pmatrix} T_A \\ N_A \end{pmatrix} \| B \| Текст1 \qquad (3)$$

Форма маркера *(МаркерBA)*, посланного сущностью *B* сущности *A*, имеет вид:

$$МаркерBA = Текст4 \| eK_{AB}\begin{pmatrix} T_B \\ N_B \end{pmatrix} \| A \| Текст2 \qquad (4)$$

Включение отличительного идентификатора *B* в *МаркерAB* и включение отличительного идентификатора *A* в *МаркерBA* являются (независимо) необязательными.

Примечание. Отличительный идентификатор *B* включен в *МаркерAB* для предотвращения повторного использования *МаркераAB* для сущности *A* злоумышленником, маскирующимся под сущность *B*. По аналогичным причинам идентификатор *A* включен в *МаркерBA*. Включение идентификаторов сделано необязательным для того, чтобы в средах, где такие нарушения не могут иметь место, один или оба идентификатора могли быть опущены.

Отличительные идентификаторы *A* и *B* могут также быть опущены, если используются однонаправленные ключи (см. ниже).

Выбор использования в рассматриваемом механизме либо меток времени, либо последовательных чисел зависит от возможностей претендента и верификатора, а также от среды функционирования.

Шаги (1) и (2) идентичны шагам, определенным в 5.1.1, для однопроходной аутентификации.

(3) Сущность *B* создает и посылает *МаркерBA* сущности *A*.

(4) Сообщение на шаге (3) обрабатывается способом, аналогичным для шага (2) в 5.1.1.

Примечание. Два сообщения этого механизма не связаны друг с другом ничем, кроме как неявной одновременностью. Рассматриваемый механизм дважды использует независимое применение механизма 5.1.1. Дальнейшее связывание этих сообщений может быть достигнуто соответствующим использованием текстовых полей.

Если используются однонаправленные ключи, то ключ K_{AB} в *МаркереBA* заменяется ключом K_{BA} и соответствующий ключ используется на шаге (4).

5.2.2 Трехпроходная аутентификация

В этом механизме аутентификации уникальность/своевременность контролируется созданием и проверкой случайных чисел (см. приложение Б стандарта *СТ РК ИСО/МЭК 9798-1-2008*). Механизм аутентификации представлен на рисунке 4.

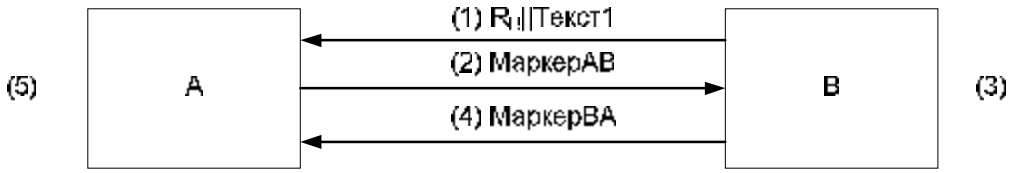


Рисунок 4

Маркеры имеют следующую форму:

$$МаркерAB = Текст3 \| eK_{AB}\left(R_A \| R_B \| B \| Текст2\right),$$
$$МаркерBA = Текст5 \| eK_{AB}\left(R_B \| R_A \| Текст4\right). \qquad (5)$$

Включение отличительного идентификатора B в *МаркерAB* является необязательным.

Примечание. Отличительный идентификатор *B* включен в *МаркерAB* для предотвращения так называемых атак отражением (reflection attack). Подобные атаки характеризуются тем, что злоумышленник «отражает» вызов R_B сущности *B*, пытаясь подменить сущность *A*. Включение отличительного идентификатора *B* сделано необязательным, с тем, чтобы в среде, где такие нарушения не могут иметь место, он мог быть опущен.

Отличительный идентификатор *B* также может быть опущен, если используется однонаправленный ключ.

(1) Сущность *B* создает случайное число R_B, затем посылает это число и, при необходимости, текстовое поле *Текст1* сущности *A*.

(2) Сущность *A* создает случайное число R_A, а также создает и посылает *МаркерAB* сущности *B*.

(3) После получения сообщения, содержащего *МаркерAB*, сущность *B* подтверждает *МаркерAB*, расшифровывая зашифрованную часть (где расшифрование подразумевает, что требования пункта 4.г соблюдаются), а затем проверяет правильность отличительного идентификатора *B*, если он имеется, и проверяет, чтобы случайное число R_B, посланное сущности *A* на шаге (1), согласовывалось со случайным числом, содержащимся в *МаркереAB*.

(4) Сущность *B* создает и посылает *МаркерBA* сущности *A*.

(5) После получения сообщения, содержащего *МаркерBA*, сущность *A* подтверждает *МаркерBA*, расшифровывая зашифрованную часть (где расшифрование подразумевает, что требования пункта 4.г соблюдаются), а затем проверяет, чтобы случайное число R_B, посланное сущности *B* на шаге (1), согласовывалось со случайным числом, содержащимся в *МаркереBA*, и случайное число R_A, посланное сущности *B* на шаге (2), согласовывалось со случайным числом, содержащимся в *МаркереBA*.

Если используются однонаправленные ключи, то ключ K_{AB} в *МаркереBA* заменяется ключом K_{BA} и соответствующий ключ используется на шаге (5).

6 Механизмы, использующие доверенную третью сторону

Рассматриваемые в данном разделе механизмы аутентификации до начала процесса аутентификации не используют секретный ключ, который является общим для двух сущностей. Вместо этого, сущности используют доверенную третью сторону (с отличительным идентификатором ТС), с которой каждая из сущностей *A* и *B* имеет общий секретный ключ, K_{AT} и *KBT* соответственно. В каждом механизме одна из сущностей запрашивает ключ K_{AB} от доверенной третьей стороны. Далее следует адаптация механизмов, описанных соответственно в 5.2.1 и 5.2.2.

Как описано ниже, некоторые проходы могут быть опущены в каждом механизме, если требуется только односторонняя аутентификация.

Все текстовые поля, определенные в рассматриваемых далее механизмах, доступны для применения в приложениях, которые находятся вне сферы применения настоящего стандарта (поля могут быть пустыми). Взаимосвязь текстовых полей и их содержание зависят от конкретного применения. Информацию относительно применения текстовых полей см. в приложении А.

6.1 Четырехпроходная аутентификация

В этом механизме аутентификации уникальность/своевременность контролируется использованием параметров, зависящих от времени (см. приложение Б стандарта *СТ РК ИСО/МЭК 9798-1-2008*). Данный механизм эквивалентен механизму 8 для создания ключа *СТ РК ИСО/МЭК 11770-2-2008*. Механизм аутентификации представлен на рисунке 5.

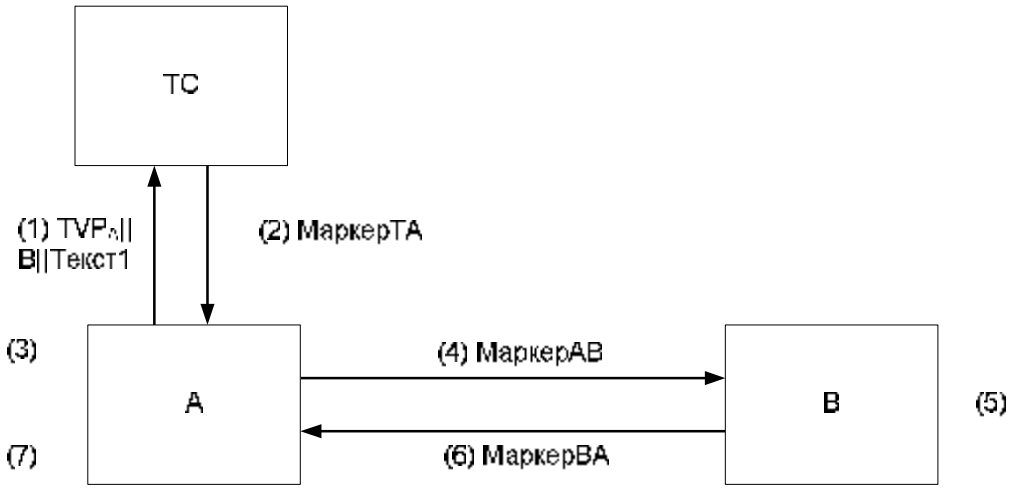


Рисунок 5

Форма маркера (*МаркерТА*), посланного доверенной третьей стороной *ТС* сущности *А* выглядит следующим образом:

$$МаркерТА = Текст4 \| eK_{AT}\left(TVP_A \| K_{AB} \| B \| Текст3\right) \| eK_{BT}\left(\begin{matrix} T_{TC} \\ N_{TC} \end{matrix} \| K_{AB} \| A \| Текст2\right) \qquad (6)$$

Форма маркера *(МаркерАВ)*, посланного сущностью *А* сущности *В*, выглядит следующим образом:

$$МаркерАВ = Текст6 \| eK_{BT}\left(\begin{matrix} T_{TC} \\ N_{TC} \end{matrix} \| K_{AB} \| A \| Текст2\right) \| eK_{AB}\left(\begin{matrix} T_A \\ N_A \end{matrix} \| B \| Текст5\right) \qquad (7)$$

Форма маркера (*МаркерВА*), посланного сущностью *В* сущности *А*, выглядит следующим образом:

$$МаркерВА = Текст8 \| eK_{AB}\left(\begin{matrix} T_B \\ N_B \end{matrix} \| A \| Текст7\right) \qquad (8)$$

Выбор в данном механизме в качестве параметров, зависящих от времени, либо меток времени, либо последовательных чисел зависит от возможностей вовлеченных в процесс сущностей, а также от среды.

Применение зависящего от времени параметра TVP_A на шагах (1)-(3) рисунка 5, как показано ниже, несколько отличается от его обычного применения. Это позволяет сущности *A* связывать ответное сообщение (2) с запросом о сообщении (1). В данном случае важным свойством параметра, зависящего от времени, является его неповторяемость. Указанное свойство ограничивает возможное повторное использование предварительно использованного *МаркераТА*.

Примечание. В качестве параметра, зависящего от времени, может использоваться случайное число. Однако, в отличие от случайных чисел, используемых в определенных механизмах настоящего стандарта, нет необходимости в том, чтобы TVP_A было непредсказуемым для доверенной третьей стороны, и не требуется неповторяемость вычисленного значения.

(1) Сущность *A* создает параметр, зависящий от времени, TVP_A, затем посылает доверенной третьей стороне *TC* этот параметр, отличительный идентификатор *B* и, при необходимости, текстовое поле *Текст1*.

(2) Доверенная третья сторона *TC* создает и посылает сущности *A* *МаркерТА*.

(3) После получения сообщения, содержащего *МаркерТА*, сущность *A* подтверждает *МаркерТА*, расшифровывая данные, которые были зашифрованы ключом K_{AT} (где расшифрование подразумевает, что требования пункта 4.г соблюдаются), а затем проверяет правильность отличительного идентификатора *B*, а также проверяет, чтобы зависящий от времени параметр, отправленный доверенной третьей стороне *TC* на шаге (1), согласовывался с зависящем от времени параметром, содержащимся в *МаркереТА*. Кроме того, сущность *A* извлекает секретный ключ аутентификации K_{AB}, а затем для создания *МаркераАВ* извлекает из *МаркераТА*

$$eK_{BT}\begin{pmatrix} T_{TC} \\ N_{TC} \end{pmatrix} \| K_{AB} \| A \| Текст2 \qquad (9)$$

(4) Сущность *A* создает и посылает *МаркерАВ* сущности *B*.

(5) После получения сообщения, содержащего *МаркерАВ*, сущность *B* подтверждает *МаркерАВ*, расшифровывая зашифрованную часть (где расшифрование подразумевает, что требования пункта 4.г соблюдаются), а затем проверяет правильность отличительных идентификаторов *A* и *B*, а также метки(ок) времени или последовательного(ых) числа(ел). Кроме того, сущность *B* извлекает секретный ключ аутентификации K_{AB}.

(6) Сущность *B* создает и посылает *МаркерВА* сущности *A*.

(7) После получения сообщения, содержащего *МаркерВА*, сущность *A* подтверждает *МаркерВА*, расшифровывая зашифрованную часть (где расшифрование подразумевает, что требования пункта 4.г соблю-

даются), а затем, проверяет правильность отличительного идентификатора *A*, а также метки времени или последовательного числа.

Шаги (6) и (7) могут быть опущены, если требуется только односторонняя аутентификация сущности *A* сущностью *B*.

6.2 Пятипроходная аутентификация

В этом механизме взаимной аутентификации уникальность/своевременность контролируется использованием случайных чисел (см. приложение Б стандарта *СТ РК ИСО/МЭК 9798-1-2008*). Данный механизм эквивалентен механизму 9 для создания ключа *СТ РК ИСО/МЭК 11770-2-2008*. Механизм аутентификации представлен на рисунке 6.

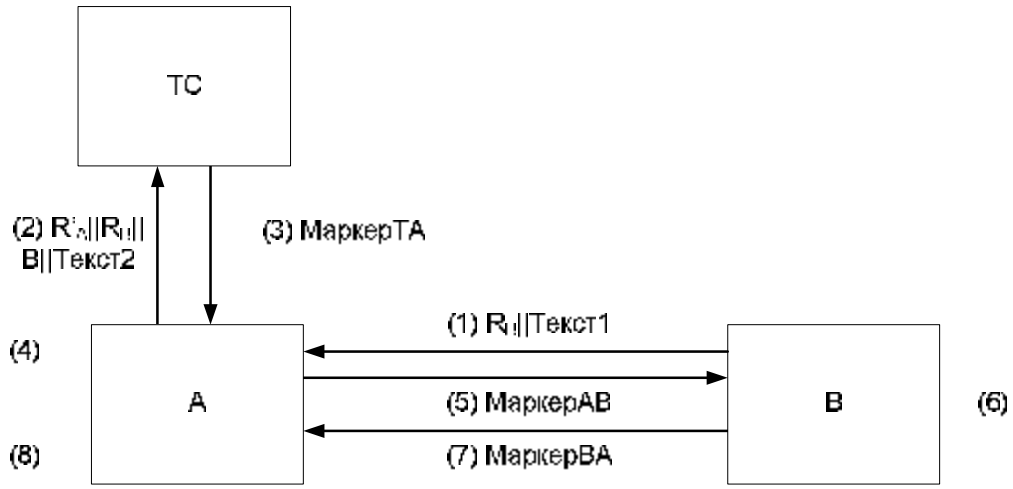


Рисунок 6

Форма маркера *(МаркерTA)*, посланного доверенной третьей стороной *TC* сущности *A* выглядит следующим образом:

$$МаркерTA = Текст5 \| eK_{AT}\left(R'_A \| K_{AB} \| B \| Текст4\right) \| eK_{BT}\left(R_B \| K_{AB} \| A \| Текст3\right) \qquad (10)$$

Форма маркера *(МаркерAB)*, посланного сущностью *A* сущности *B*, выглядит следующим образом:

$$МаркерAB = Текст7 \| eK_{BT}\left(R_B \| K_{AB} \| A \| Текст3\right) \| eK_{AB}\left(R_A \| R_B \| Текст6\right) \qquad (11)$$

Форма маркера (*МаркерBA*), посланного сущностью *B* сущности *A*, выглядит следующим образом:

$$МаркерBA = Текст9 \| eK_{AB}\left(R_B \| R_A \| Текст8\right) \qquad (12)$$

(1) Сущность *B* создает случайное число R_B, затем посылает это число и, при необходимости, текстовое поле *Текст1* сущности *A*.

(2) Сущность *A* создает и посылает случайное число R'_A, а также посылает случайное число R_B, отличительный идентификатор *B* и, при необходимости, текстовое поле *Текст2* доверенной третьей стороне *TC*.

(3) Доверенная третья сторона *TC* создает и посылает *МаркерTA* сущности *A*.

(4) После получения сообщения, содержащего *МаркерTA*, сущность *A* подтверждает *МаркерTA*, расшифровывая данные, которые были зашифрованы ключом $К_{AT}$ (где расшифрование подразумевает, что требования п.4.г соблюдаются), а затем проверяет правильность отличительного идентификатора *B*, а также проверяет, чтобы случайное число R'_A, отправленное доверенной третьей стороне *TC* на шаге (2), согласовывалось со случайным числом, содержащимся в *МаркереTA*. Кроме того, сущность *A* извлекает секретный ключ аутентификации K_{AB}, а затем для создания *МаркераAB* извлекает из *МаркераTA*

$$eK_{BT}\left(R_B \| K_{AB} \| A \| Текст3\right) \qquad (13)$$

(5) Сущность *A* создает второе случайное число $R_{A,}$ а также создает и посылает *МаркерAB* сущности *B*.

(6) После получения сообщения, содержащего *МаркерAB*, сущность *B* подтверждает *МаркерAB*, расшифровывая зашифрованную часть (где расшифрование подразумевает, что требования пункта 4.г соблюдаются), а затем проверяет правильность отличительного идентификатора *A*, а также проверяет, чтобы случайное число R_B, посланное сущности *A* на шаге (1), согласовывалось с обеими копиями, содержащимися в *МаркереAB*. Кроме того, сущность *B* извлекает секретный ключ аутентификации K_{AB}.

(7) Сущность *B* создает и посылает *МаркерBA* сущности *A*.

(8) После получения сообщения, содержащего *МаркерBA*, сущность *A* подтверждает *МаркерBA*, расшифровывая зашифрованную часть (где расшифрование подразумевает, что требования пункта 4.г соблюдаются), а затем проверяет, чтобы полученное на шаге(1) от сущности *B* случайное число R_B, согласовывалось со случайным числом, содержащимся в *МаркереAB*, и чтобы случайное число $R_{A,}$ посланное сущности *B* на шаге (5), согласовывалось со случайным числом, содержащимся в *МаркереBA*.

Шаги (7) и (8) могут быть опущены, если требуется только односторонняя аутентификация сущности *A* сущностью *B*.

Приложение А
(справочное)
Применение текстовых полей

Маркеры, приведенные в разделах 5 и 6 настоящего стандарта, содержат текстовые поля. Фактическое применение и взаимозависимость между различными текстовыми полями в конкретном проходе механизма аутентификации зависит от конкретного применения.

Если маркеры не содержат (достаточной) избыточности, шифруемые текстовые поля могут использоваться, чтобы обеспечить дополнительную избыточность.

Любая информация, требующая конфиденциальности или аутентификации источника данных, должна быть помещена в зашифрованную часть маркера.

УДК 681.324:006.354 **МКС 35.040**

Ключевые слова: обработка данных, информационный обмен, защита информации, методы и средства защиты, аутентификация, маркер, шифрование, алгоритмы.

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