ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология
ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУДІҢ ӘДІСТЕРІ МЕН ҚҰРАЛДАРЫ
Сәйкестендіру тетіктері
3-бөлім
Цифрлық қолтаңба әдістерін қолдану тетіктері

Информационная технология
МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ
Механизмы аутентификации
Часть 3
Механизмы с применением методов цифровой подписи

ҚР СТ ИСО/МЭК 9798-3-2008

(ИСО/МЭК 9798-3:1999
«Ақпараттық технология. Қауіпсіздікті қамтамасыз етудің әдістері мен құралдары. Дәлме-дәлдік тетіктері.
3-бөлік. Цифрлық қолтаңба әдістерін қолдану тетіктері», IDT)

Ресми басылым

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

Астана

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология

ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУДІҢ ӘДІСТЕРІ МЕН ҚҰРАЛДАРЫ

Сәйкестендіру тетіктері
3-бөлім
Цифрлық қолтаңба әдістерін қолдану тетіктері

ҚР СТ ИСО/МЭК 9798-3-2008
(ИСО/МЭК 9798-3:1999
«Ақпараттық технология. Қауіпсіздікті қамтамасыз етудің әдістері мен құралдары. Дәлме-дәлдік тетіктері.
3-бөлік. Цифрлық қолтаңба әдістерін қолдану тетіктері», IDT)

Ресми басылым

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

Астана

Алғысөз

1 «Инфосистемы Джет» ЖАҚ **ӘЗІРЛЕДІ**

Қазақстан Республикасы Ақпараттандыру және байланыс агенттігі **ЕНГІЗДІ**

2 Қазақстан Республикасы Индустрия және сауда министрлігі 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 көлбеу қаріппен көрсетілген ИСО/МЭК 13888-2:1998 «Ақпараттық технология. Қауіпсіздікті қамтамасыз етудің әдістері мен құралдары. Сәйкестендіру тетіктері 3-бөлік. Цифрлық қолтаңба әдістерін қолдану тетіктері» («Information technology. Security techniques. Non-repudation. Part 2. Mechanisms using symmetric techniques»), IDT, халықаралық стандартына сәйкес болып табылады

4 БІРІНШІ ТЕКСЕРУ МЕРЗІМІ 2013 жыл
ТЕКСЕРУ КЕЗЕҢДІЛІГІ 5 жыл

5 АЛҒАШ РЕТ ЕНГІЗІЛДІ

Мазмұны

1 Қолданылу саласы 1
2 Нормативтік сілтемелер 1
3 Терминдер мен анықтамалар 2
4 Талаптар 2
5 Тетіктер 2
5.1 Бір жақты сәйкестендіру 4
5.2 Өзара сәйкестендіру 5
А қосымшасы. Мәтіндік алаңдарды қолдану 10

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология
ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ ӘДІСТЕРІ МЕН ҚҰРАЛДАРЫ
Сәйкестендіру тетіктері
3-Бөлім
Цифрлық қолтаңба әдістерін қолдану тетіктері

Енгізілген күні 2008.07.01

1 Қолданылу саласы

Осы стандарт асимметриялық әдістерге негізделген цифрлық қолтаңбаларды қолдана отырып, дәлме-дәлдік тетіктерін анықтайды. Екі тетік сәйкестендіруге бір мәнде қатысты болады (бір жақты сәйкестендіру), ал қалғандары екі мәннің өзара сәйкестендірілуі тетіктері болып табылады. Мәндердің шынайылығын тексеру үшін цифрлық қолтаңба пайдаланылады. Сондай-ақ сенім білдірілген үшінші жақ қатыстырылуы мүмкін.

Осы стандартта қолданылатын қауіпсіздік тетіктері криптографиялық әдістерді қолдануға негізделген. Ақпаратты криптографиялық қорғаудың нақты құралдарын таңдау және қолдану Қазақстан Республикасының заңнамасымен регламенттеледі және осы стандарттың қарастыру заты болып табылмайды.

Осы стандартта көрсетілген тетіктер уақытқа, мысалы, уақыт белгілері, сол сәйкестендіру ақпараттың біршама кешкі уақытта немесе бірнеше рет қабылдануы үшін жүйелі немесе кездейсоқ сандарға байланысты болатын параметрлер қолданылады.

Егер уақыт белгісі немесе жүйелі сан қолданылатын болса, онда бір жақты сәйкестендіру үшін бір өткін қажет болады, ал сол уақытта өзара сәйкестендіру үшін екі өткін қажет болады. Егер кездейсоқ сандарды пайдаланылатын шақыру мен жауап әдісі қолданылатын болса, онда бір жақты сәйкестендіру үшін екі және өзара сәйкестендіру үшін (пайдаланылатын тетікке қарай) үш немесе төрт өткін қажет болады.

2 Нормативтік сілтемелер

Осы стандартта мына стандартқа сілтеме пайдаланылды:

ҚР СТ ИСО/МЭК 9798-1:2006 Ақпараттық технология. Қауіпсіздікті қамтамасыз етудің әдістері мен құралдары. Сәйкестендіру тетіктері. 1- Бөлік. Жалпы ережелер.

Ресми басылым

3 Терминдер мен анықтамалар

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

4 Талаптар

Осы стандартта анықталатын сәйкестендіру тетіктерінде сәйкестендіруге жататын мән өзінің дұрыстығын қолтаңбаның құпия кілтін білуін көрсету арқылы дәлелдейді. Мән бұны кейбір деректерге қол қою үшін өзінің құпия кілтін қолдану арқылы іске асырады. Қолтаңба қолтаңбаны тексерудің ашық кілтін пайдаланатын кез келген мән тексере алады.

Сәйкестендіру тетіктеріне мына талаптар қойылады. Егер олардың қайсы бірі орындалмаса, онда сәйкестендіру процесі анықталмауы, немесе ол іске аспауы мүмкін.

а) верификатор үміткердің ашық кілтінің, яғни үміткер өзін жариялайтын объектінің күшін иеленуі тиіс.

б) қолтаңбаның жабық кілті тек үміткерге ғана белгілі болуы және тек өзі ғана пайдалануы тиіс.

Ескертпелер

1. Күші бар ашық кілтті алу жолдарының бірі сертификат[1] болып табылады (ҚР СТ ИСО/МЭК 9798-1 қосымшасын қараңыз). Сертификаттарды құру, бөлу және жою осы стандартты қолдану саласынан тыс болады. Осы мақсат үшін сенім білдірілген үшінші жақ болуы мүмкін. Күші бар ашық кілтті алудың басқа жолы – сенім білдірілген курьер.

2. Цифрлық қолтаңбаларының схемаларына сілтемелер ҚР СТ ИСО/МЭК 9798-1 (Г –қосымшасы) орналасқан.

5 Тетіктер

Осы бөлімде қарастырып отырған мәндердің сәйкестендіру тетіктері уақытқа қатысты, уақыт белгісі, жүйелі немесе кездейсоқ сандар сияқты параметрлерді пайдаланады (*ҚР СТ ИСО/МЭК 9798-1* Б қосымшасын және төменде көрсетілген 1 Ескертпесін қараңыз).

Осы стандартта маркерлер мына түрде болады:

$$Маркер = X_1 \| \cdots \| X_i \| sS_A(Y_1 \| \cdots \| Y_j) \qquad (1)$$

Осы стандартта «қол қойылған деректер» термині «$Y_1\|\ldots\|Y_j$» тізбегіне қатысты болады, ол қолтаңбалар сызбасы үшін кіріс мәліметтері ретінде пайдаланылады, ал «қол қойылмаған деректер» «$X_1\|\ldots\|X_j$» тізбегіне жатады.

Егер маркердің қол қойылған мәліметтеріндегі ақпарат қолтаңбадан қалпына келтірілетін болса, ол маркердің қол қойылмаған мәліметтерінде болмауы тиіс (мысалы, ИСО/МЭК 9796 стандартын қараңыз).

Егер маркердің қол қойылған мәліметтерінің мәтіндік өрісіндегі ақпарат қолтаңбадан қалпына келтірілмейтін болса, онда ол маркердің қол қойылмаған мәтіндік өрісінде болуы тиіс.

Егер маркердің қол қойылған мәліметтеріндегі ақпарат (мысалы, кездейсоқ сан) верификаторға белгілі болса, ол үміткер жіберген маркердің қол қойылмаған мәліметтерінде болмауы тиіс.

Бұдан әрі баяндалатын тетіктерде көрсетілген барлық мәтіндік өрістер осы стандарттың қолданылу саласынан тыс пайдалану үшін қол жетімді болады (олар бос болуы мүмкін). Олардың өзара әрекеті мен мазмұны нақты қолдануға байланысты. Мәтіндік өрістерді пайдалану жөніндегі ақпаратқа қатысты А қосымшаны қараңыз.

Ескертпелер

1. Басқа мән өзінің мақсаттарына түрленген бір мәнді мәліметтер блогына қол қою бірінші объекті арқылы өзі қол қоятын мәліметтер блогына өзінің дербес кездейсоқ санын енгізу арқылы жол берілмеуі мүмкін.

2. Сертификаттарды бөлу осы стандарттың қолданылу саласынан тыс орналасқандықтан, олардың барлық тетіктерге жіберілуі міндетті емес.

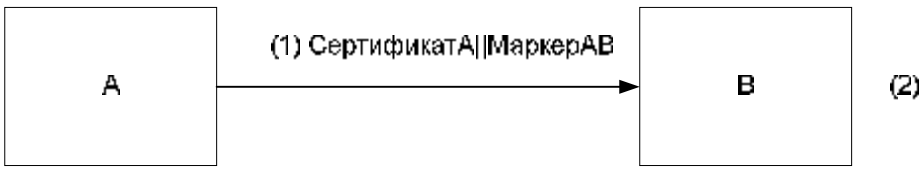
5.1 Бір жақты сәйкестендіру

Бір жақты сәйкестендіру мәндердің екеуінің біреуі ғана осы тетіктің көмегімен дәлме-дәл келеді.

5.1.1 Бір өткізгішті сәйкестендіру

Сәйкестендірудің осы тетігінде А үміткері процесті білдіреді және *B* верификаторымен дәлме-дәл келеді.

Бірегейлік/уақытылық уақыт белгісін немесе жүйелі санды құру және тексеру арқылы бақыланады (*ҚР СТ ИСО/МЭК 9798-1* стандартының Б қосымшасын қараңыз). Сәйкестендіру тетігі 1- суретте көрсетілген.



1 - сурет

A үміткерінің *B* верификаторына жіберген маркерінің (*МаркерAB*) *формасы* мынадай болады:

$$МаркерAB = \begin{matrix} T_A \\ N_A \end{matrix} \left\| B \right\| Mjтін\ 2 \left\| sS_A \left(\begin{matrix} T_A \\ N_A \end{matrix} \left\| B \right\| Mjтін\ 1 \right) \right. \qquad (2)$$

бұнда *A* үміткері уақытқа байланысты, немесе N_A жүйелі саны, немесе T_A уақыт белгісіне қатысты параметр ретінде пайдаланылады. Таңдау

үміткердің және верификатордың техникалық мүмкіндіктеріне, сондай-ақ ортаға байланысты болады.

B ерекшелігі бар сәйкестендіргішінің *ABМаркер*-іне енгізілуі міндетті емес.

Ескертпелер

1. В ерекше сәйкестендіргішінің МаркерАВ қол қойылған деректеріне енгізілуі МаркерАВ уәкілетті верификатордан басқа қандай да бір өзге мәннің пайдалануын болдырмау үшін қажет.

2. Жалпы жағдайда, мәтін 2 бұл процесте сәйкестендіруге келмейді.

3. Осы тетіктің қолданыстарының бірі кілттерді бөлу болуы мүмкін (ҚР СТ ИСО/МЭК 9798-1, А-қосымшасын қараңыз).

(1) *A* мәні *МаркерАВ* және, қажет болған жағдайда, өз сертификатын В мәніне жібереді.

(2) *МаркерАВ* бар хабарламаны алған соң *B* мәні мынадай қадамдарға барады:

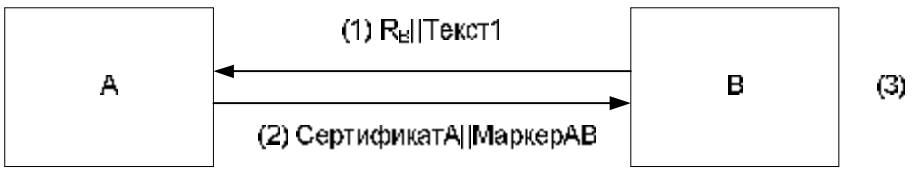
а) *B* мәні А мәнінің күші бар ашық кілтін иеленгендігін А мәнінің сертификатын тексере отырып, немесе басқа құралдардың көмегімен дәлелденеді;

б) *B* мәні осы маркердегі А мәнінің қолтаңбасын тексеру, уақыт белгісін немесе жүйелі сан мен *АВ Маркерінде* қол қойылған мәліметтеріндегі *(B)* сәйкестендіргіші өрісі мәнінің *B* мәнінің ерекше сәйкестендіргішінің мәнімен сәйкес келуін тексеру арқылы дәлелдейді.

5.1.2 Екі өткінді сәйкестендіру

Сәйкестендірудің осы тетігінде А үміткері процесті білдіретін В верификаторымен дәлме-дәл келеді.

Бірегейлік/уақытылық RB кездейсоқ санын құру мен тексеру арқылы бақыланады (СТ РК ИСО/МЭК 9798-1 стандартының Б қосымшасын қараңыз). Сәйкестендіру тетігі 2-суретте көрсетілген.



2-сурет

A үміткерінің *B* верификаторына жіберген (*МаркерАВ*) маркерінің формасы мынадай болады:

$$МаркерАВ = R_A \| R_B \| B \| Мәтін\ 3 \| sS_A\left(R_A \| R_B \| B \| Мәтін\ 2\right) \qquad (3)$$

В ерекшелігі бар сәйкестендіргішінің *АВМаркер*іне енгізілуі міндетті емес. Бұл сәйкестендірудің осы тетігі пайдаланылатын ортаға байланысты.

Ескертпелер

1. В міндетті емес верификаторының МаркерАВ қол қойылған деректеріне енгізілуі маркерді тек қана уәкілетті верификатордың емес, сондай-ақ басқалардың да пайдалануын болдырмауға көмектеседі (мысалы, «ортадағы қаскүнемнің» шабуылы кезінде).

2. RA кездейсоқ санының МаркерАВ қол қойылған деректеріне енгізілуі В мәнінің сәйкестендіру тетігінің жұмысы басталардан бұрын таңдалып алынған деректерде В мәнінің А мәнінің қолтаңбасын алуды болдырмайды. Бұл мысалы, А мәнінің бір және тек сол кілтті сәйкестендіру үшін емес, басқа да мақсаттарға пайдаланған жағдайда қажет болуы мүмкін.

(1) *В* мәні R_B кездейсоқ санын және, қажет болған жағдайда, *А* мәнінің 1 *Мәтін* мәтіндік өрісіне жібереді.

(2) *А* мәні *МаркерАВ* және, қажет болған жағдайда, өз сертификатын *В* мәніне жібереді.

(3) *МаркерАВ* хабарламаны алған соң, *В* мәні мынадай қадамдар жасайды:

а) *В* мәні А мәнінің күші бар ашық кілтін иеленгендігін А мәнінің сертификатын тексере отырып, немесе басқа құралдардың көмегімен дәлелденеді;

б) *В* мәні бұл маркерде бар *А* мәнінің қолын тексеру арқылы, *АВ Маркерінде* бар кездейсоқ мәнмен келісуі тиіс қадамда (1) *А* мәніне жіберілген RB–ның кездейсоқ санын тексеру арқылы және егер мұндай бар болса *В* мәнінің ерекше сәйкестендіргішінің мәнімен *АВ Маркерінде* қол қойылған мәліметтеріндегі *(В)* сәйкестендіргіші өрісі мәнінің сәйкес келуін тексеру арқылы *АВ Маркерін* растайды.

5.2 Өзара сәйкестендіру

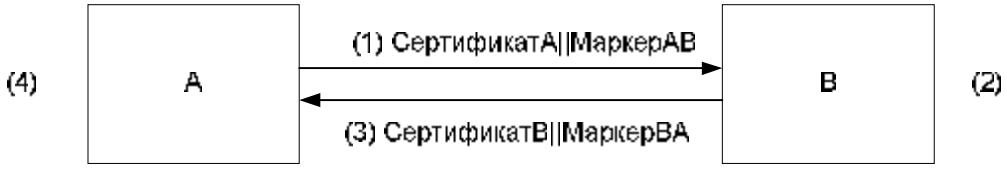
Өзара сәйкестендіру екі бір-бірін қолдайтын байланыстағы мәндердің бір бірімен тиісті тетіктер арқылы сәйкес келетіндігін білдіреді.

5.1.1- және 5.1.2-тармақтарында суреттелген екі тетік 5.2.1 және 5.2.2-тармақта тиісінше өзара сәйкестендіруді іске асыру үшін бейімделеді. Бұл тағы да екі қосымша хабарламаға әкелетін бір қосымша хабарламаны беру арқылы жүзеге асады.

5.2.3-тармақта қарастырылған тетік төрт хабарламаны пайдаланады, алайда олар барлығы жүйелі түрде жіберілуі міндетті емес. Сонымен, сәйкестендіру процесі тездетілуі мүмкін.

5.2.1 Екі өткінді сәйкестендіру

Сәйкестендірудің осы тетігінде бірегейлік/уақытылық уақыт белгісі немесе жүйелі сандарды жасау мен тексеру арқылы бақыланады (*ҚР СТ ИСО/МЭК 9798-1* стандартының Б қосымшасын қараңыз). Сәйкестендіру тетігі 3-суретте көрсетілген.



3- сурет

А мәнінің В мәніне жіберген (*МаркерАВ)* маркерінің формасы 5.1.1. анықталғанға сәйкес келеді.

$$МаркерАВ = \begin{matrix} T_A \\ N_A \end{matrix} \left\| B \right\| Mjтін\ 2 \left\| sS_A \left(\begin{matrix} T_A \\ N_A \end{matrix} \left\| B \right\| Mjтін\ 1 \right) \right. \qquad (4)$$

А мәнінің В мәніне жіберген (*МаркерВА)* маркерінің нысаны мына түрде болады:

$$МаркерАВ = \begin{matrix} T_B \\ N_B \end{matrix} \left\| A \right\| Mjтін\ 4 \left\| sS_B \left(\begin{matrix} T_B \\ N_B \end{matrix} \left\| A \right\| Mjтін\ 3 \right) \right. \qquad (5)$$

Осы тетіктегі уақыт белгісін немесе жүйелі сандарды пайдалануды таңдау үміткердің және верификатордың техникалық мүмкіндіктеріне, сондай-ақ ортаға байланысты.

Ескертпелер

1. А және В сәйкестендіргіштерінің тиісінше МаркерАВ және МаркерВА қол қойылған деректеріне енгізу көрсетілген маркерлерді уәкілетті верификаторлардан басқа тағы да басқалардың пайдалануын болдырмау үшін қажетті болып табылады.

(1)-(2) қадамдар бір өткін сәйкестендіру үшін 5.1.1. анықталған, қадамдарға сәйкес келеді.

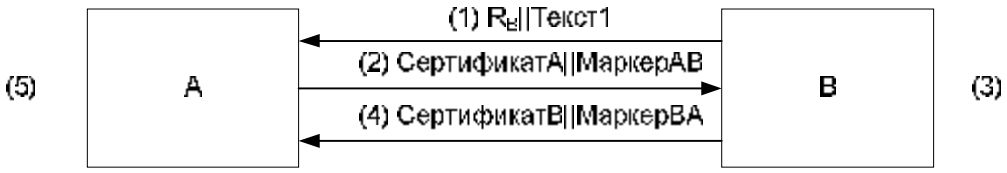
(3) *В* мәні *МаркерВА* және, қажет болған жағдайда, өз сертификатын *А* мәніне жібереді.

(4) (3) қадамдағы хабарлама 5.1.1. (2) қадамы үшін ұқсас тәсілмен өңделеді.

2. Бұл тетіктің екі хабарламасы бір-бірімен айқын емес уақытылықтан басқа ешнәрсемен байланыспайды. Қарастырылып отырған тетік 5.1.1. тетігін тәуелсіз қолдануды екі рет пайдаланады. Бұл хабарламалардың одан әрі байланысуына мәтіндік өрістердің тиісінше пайдалану арқылы қол жеткізіледі.

5.2.2 Үш өткінді сәйкестендіру

Сәйкестендірудің осы тетігінде бірегейлік/уақтылық кездейсоқ сандарды қалыптастыру мен тексеру арқылы бақыланады (*СТ РК ИСО/МЭК 9798-1* стандартының Б қосымшасын қара). Сәйкестендіру тетігі 4-суретте көрсетілген.



4-сурет

Маркерлер мына нысанда болады:

$$МаркерAB = R_A \| R_B \| B \| Мәтін\ 3 \| sS_A\left(R_A \| R_B \| B \| Мәтін\ 2\right),$$
$$МаркерBA = R_B \| R_A \| A \| Мәтін\ 5 \| sS_B\left(R_B \| R_A \| A \| Мәтін\ 4\right) \qquad (6)$$

B параметрінің *МаркерAB*-іне және *A* параметрінің *МаркерBA*-іне енгізілуі міндетті емес. Бұл сәйкестендіру тетігі пайдаланылатын ортаға байланысты.

Ескертпе – RA кездейсоқ санының МаркерAB қол қойылған деректеріне енгізілуі B мәнінің сәйкестендіру тетігінің жұмысы басталардан бұрын таңдалып алынған деректерде B мәнінің A мәнінің қолтаңбасын алуды болдырмайды. Бұл мысалы, A мәнінің бір және тек сол кілтті сәйкестендіру үшін емес, басқа да мақсаттарға пайдаланған жағдайда қажет болуы мүмкін. RB кездейсоқ санының МаркерAB-іне енгізілуі, A мәнін бұл санды бірінші хабарламада жіберілген мәнге сәйкестігін тексеруді орындауға итермелейтін қауіпсіздік жағынан қажет болса да, бірақ B мәні үшін сол қорғауды қамтамасыз ете алмайды, себебі RB саны A мәніне RA саны таңдалып алынғанға дейін белгілі болатын. Егер қорғаудың осы типі талап етілсе, онда B мәні R'B қосымша кездейсоқ санын МаркерAB үшін мәтіндік өрістердің Мәтін4 және Мәтін5 енгізуі мүмкін.

(1) *B* мәні R_B кездейсоқ санын және, қажет болған жағдайда, 1 *Мәтін* мәтіндік өрісін *A* мәніне жібереді.

(2) *A* мәні *МаркерAB* және, қажет болған жағдайда, өз сертификатын *B* мәніне жібереді.

(3) *МаркерAB* тұратын хабарламаны алған соң, *B* мәні мына әрекеттерді орындайды:

а) *B* мәні *A* мәнінің күші бар ашық кілтін иеленгендігін *A* мәнінің сертификатын тексере отырып, немесе басқа құралдардың көмегімен дәлелденеді;

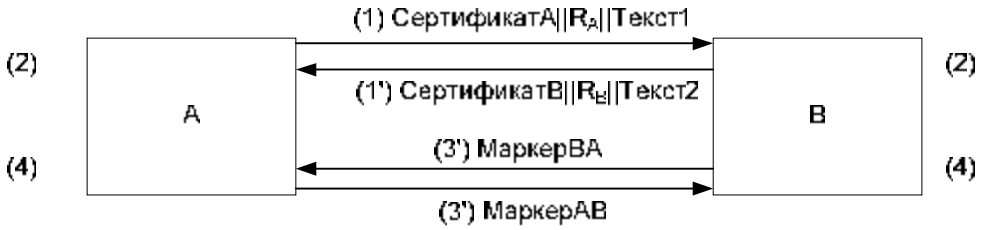
б) *B* мәні *МаркерAB*, осы маркердегі *A* мәнінің қолтаңбасы арқылы, A мәнінің (1) қадамында жіберген *МаркерAB*-індегі кездейсоқ санмен келісілуі тиіс R_B санын тексеру арқылы және *МаркерAB* қол қойылған (*B*) сәйкестендіргіші өрісінің мәнінің, егер бұндай болса, *B* мәнінің ерекше сәйкестендіргішінің мәнімен салыстыру арқылы дәлелдейді.

(5) *B* мәні *МаркерBA* және, қажет болған жағдайда, өз сертификатын *A* мәніне жібереді.

(6) МаркерВА-ындағы хабарламаны алған соң, А мәні осылайша (3) қадамдарының (i) және (ii) іс-әрекеттерін орындайды. Бұдан басқа, *А* мәні *МаркераВА* қол қойылған деректеріндегі R_B кездейсоқ санының мәні және (1) қадамында алынған R_B кездейсоқ санының мәні сәйкес келуін тексереді.

5.2.3 Екі өткінді параллель сәйкестендіру

Бұл тетікте сәйкестендіру параллель орындалады. Бірегейлік/уақытылық кездейсоқ сандардың қалыптасуы мен тексерілуі арқылы бақыланады (*СТ РК ИСО/МЭК 9798-1* стандартының Б қосымшасын қара). Сәйкестендіру тетігі 5-суретте көрсетілген.



5-сурет

Маркерлер нысаны 5.1.2.-де пайдаланылатын нысанға ұқсас.

$$МаркерАВ = R_A \| R_B \| B \| Мәтін\ 4 \| sS_A\left(R_A \| R_B \| B \| Мәтін\ 3\right),$$
$$МаркерВА = R_B \| R_A \| A \| Мәтін\ 6 \| sS_B\left(R_B \| R_A \| A \| Мәтін\ 5\right). \qquad (7)$$

В параметрінің *МаркерАВ*-іне және *А* параметрінің *МаркерВА*-іне енгізілуі міндетті емес. Бұл сәйкестендіру тетігі пайдаланылатын ортаға байланысты.

Ескертпе – RA кездейсоқ санының МаркерАВ қол қойылған деректеріне енгізілуі В мәнінің сәйкестендіру тетігінің жұмысы басталардан бұрын таңдалып алынған деректерде В мәнінің А мәнінің қолтаңбасын алуды болдырмайды. Бұл мысалы, А мәнінің бір және тек сол кілтті сәйкестендіру үшін емес, басқа да мақсаттарға сәйкестендіруге қосымша ретінде пайдаланған жағдайда қажет болуы мүмкін. Осы себептерге байланысты МаркерАВ-інде RB кездейсоқ саны қатысып отырады. (1) және (1') қадамдарында жіберілген хабарламаларды алудың салыстырмалы уақытына қарай тараптардың бірі басқа тараптың кездейсоқ санын оның кездейсоқ санын таңдау кезінде білуі мүмкін. Егер бұл қалаусыз болса, онда екі тарап та RA және RB қосымша кездейсоқ сандарын МаркерАВ үшін мәтіндік өрістердің Мәтін3 және Мәтін4 және МаркерВА үшін мәтіндік өрістердің Мәтін5 және Мәтін6 енгізуі мүмкін.

(1) *А* мәні R_A кездейсоқ санын және, қажет болған жағдайда, өз сертификаты мен мәтіндік өріс *Мәтін*1 *В* мәніне жібереді.

(1')*В* мәні R_B кездейсоқ санын және, қажет болған жағдайда, өз сертификаты мен мәтіндік өрісін *Мәтін*2 *А* мәніне жібереді.

(2) *A* және *B* мәндері басқа мәннің күші бар ашық кілтін иеленгендігі немесе тиісті сертификатты тексере отырып, немесе қандай да бір басқа құралдардың көмегімен расталады.

(3) *A* мәні *МаркерAB*-ін *B* мәніне жібереді.

(3') *B* мәні *МаркерBA*-ін *A* мәніне жібереді.

(4) *A* және *B* мына іс-әрекеттерді орындайды:

Мәндердің әрқайсысы алынған маркерлерді алынған маркердегі қолтаңбаны тексеру арқылы, сондай-ақ басқа мәннің алдын-ала жіберген кездейсоқ санының және алынған маркердегі қол қойылған деректердегі кездейсоқ санның сәйкестігін тексеру арқылы бекітіледі.

2. 5.2.3 тетігіне балама – 5.1.2 тетігінің симметриялық қолданылуы. 5.2.3 тетігінің бірінші хабарламаларына сертификаттарды енгізу сәйкестендіру процесін тездете алатын оларды ертерек тексеруді көздейді.

А қосымшасы

(анықтамалық)

Мәтіндік алаңдарды қолдану

Осы стандарттың 5-бөлімінде келтірілген маркерлер мәтіндік өрістен тұрады. Сәйкестендірудің тапсырылған өткіні кезінде әр түрлі мәтіндік өрістер арасындағы нақты қолдану және өзара тәуелділік нақты қолдануға байланысты. Бұдан әрі бірнеше мысал қарастырылады; сонымен бірге *СТ РК ИСО/МЭК 9798-1,* А-қосымшасын қараңыз.

Егер қолтаңба сызбасы хабарламаны қалпына келтірмей-ақ қолданылатын болса және қол қойылған мәтіндік өріс бос болмаса, онда верификатор қолтаңбаны растағанша мәтінді иеленуі тиіс. Осы қосымшада «қол қойылған мәтіндік өрістер» термині қол қойылған мәліметтердегі мәтіндік өрістерге жатады, ал «қол қойылмаған мәтіндік өрістер» термині қол қойылмаған мәліметтердегі мәтіндік өрістерге жатады.

Мысалы, цифрлық қолтаңба сызбасы хабарламаны қалпына келтірмей-ақ қолданылатын болса, мәліметтердің шығу тегінің сәйкестендірілуін талап ететін кез келген ақпарат қол қойылған мәтіндік өріске және (бөлік ретінде) маркердегі қол қойылмаған мәтіндік өріске орналасуы керек.

Егер маркерлер (жеткілікті) артықшылықты иеленбейді, қол қойылған мәтіндік өрістер қосымша артықшылықты қамтамасыз ету үшін пайдаланыла алады.

Қол қойылған мәтіндік өрістер маркердің сәйкестендіру үшін ғана күші бар екендігін көрсету үшін қолданылуы мүмкін. Егер пайдаланушылардың бірі «туа біткен» мәнді екінші мәннің қолтаңбасы үшін жаман оймен таңдап алу мүмкіндігі туындайтын болса, онда екінші мән кездейсоқ санды мәтіндік өріске шығаруы мүмкін.

Егер алгоритм өзі байланысатын верификаторлардың барлығы үшін бір және тек сол кілтті қандай да бір үміткердің пайдалануына негізделген шабуылдарды іске асыру мүмкіндігі бар жерде қолданылатын болса, және ондай шабуылдар қауіп төндіреді деп есептелсе, онда уәкілетті верификаторлардың шынайылығы қол қойылған мәтіндік өріске және, қажет болған жағдайда, қол қойылмаған мәтіндік өріске енгізілуі тиіс.

Қол қойылмаған мәтіндік өрістер үміткер ұсынуды талап ететін сенімді ақпаратты верификаторға ұсыну үшін пайдаланыла алады. Егер ашық кілттерді бөлу үшін сертификаттан өзге құралдар пайдаланылса, онда бұндай ақпарат верификатордың үміткердің дәлме-дәлдігі үшін қандай ашық кілтті пайдалану қажет екендігін анықтауы үшін қажет болуы мүмкін.

ӘОЖ 681.324:006.354 **МКС 35.040**

Түйінді сөздер: деректерді өңдеу, ақпараттық алмасу, деректер беру, ақпаратты қорғау, қорғау әдістері, кодтау (түрлендіру), сәйкестендіру, хабарламалардың сәйкестендіру кодтары, алгоритмдер.

Ескертулер үшін

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Механизмы аутентификации
Часть 3
Механизмы с применением методов цифровой подписи

СТ РК ИСО/МЭК 9798-3-2008

(ИСО/МЭК 9798-3:1998 «Информационная технология. Методы и средства обеспечения безопасности. Механизмы аутентификации. Часть 3. Механизмы с применением методов цифровой подписи», 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 9798-3:1998 «Информационная технология. Методы и средства обеспечения безопасности. Механизмы аутентификации. Часть 3. Механизмы с применением методов цифровой подписи» («Information technology. Security techniques. Entity authentication. Part 2. Mechanisms using digital signature techniques»), 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

1 Область применения 1
2 Нормативные ссылки 1
3 Термины и определения 2
4 Требования 2
5 Механизмы 2
5.1 Односторонняя аутентификация 3
5.2 Взаимная аутентификация 5
Приложение А. Применение текстовых полей 10

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ МЕХАНИЗМЫ АУТЕНТИФИКАЦИИ Часть 3 Механизмы с применением методов цифровой подписи

Дата введения 2008.07.01

1 Область применения

Настоящий стандарт определяет механизмы аутентификации с применением цифровых подписей, основанных на асимметричных методах. Два механизма относятся к аутентификации одной сущности (односторонняя аутентификация), а остальные являются механизмами для взаимной аутентификации двух сущностей. Для проверки подлинности сущностей используется цифровая подпись. Также может быть привлечена доверенная третья сторона.

Механизмы безопасности, используемые в настоящем стандарте, базируются на применении криптографических методов. 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 используется метка времени или последовательное число, то необходим один проход для односторонней аутентификации, в то время как для взаимной аутентификации требуется два прохода. Если применяется метод вызова и ответа, использующий случайные числа, то необходимы два прохода для односторонней аутентификации и три или четыре прохода (в зависимости от используемого механизма) для взаимной аутентификации.

2 Нормативные ссылки

В настоящем стандарте использована ссылка на следующий стандарт:

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

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 подтверждает свою подлинность демонстрацией своих знаний секретного ключа подписи. Сущность реализует это путем применения своего закрытого ключа для создания цифровой подписи некоторых данных. Подпись может быть проверена любой сущностью, использующей отрытый ключ проверки подписи.

К механизмам аутентификации предъявляются следующие требования:

а) верификатор должен иметь силу открытым ключом претендента, т.е. сущности, которой себя объявляет претендент;

б) закрытый ключ подписи должен быть известен только претенденту и использоваться только им.

Если какое-либо из них не выполнено, то процесс аутентификации может быть недостоверным, или не может быть осуществим.

Примечание.

1. Одним из путей получения имеющего силу открытого ключа является сертификат[1] (см. Приложение В *СТ РК ИСО/МЭК 9798-1-2008).* Создание, распределение и аннулирование сертификатов находятся вне области применения настоящего стандарта. Для этой цели может существовать доверенная третья сторона. Другой путь получения имеющего силу открытого ключа – доверенный курьер.

2. Ссылка на схемы цифровых подписей содержится в *СТ РК ИСО/МЭК 9798-1-2008* (Приложение Г).

5 Механизмы

Рассматриваемые в данном разделе механизмы аутентификации сущностей используют параметры, зависящие от времени, такие, как метки времени, последовательные или случайные числа (см. Приложение Б *СТ РК ИСО/МЭК 9798-1-2008* и приведенное ниже Примечание 1).

В настоящем стандарте маркеры имеют следующий вид:

$$Маркер = X_1 \| \cdots \| X_i \| sS_A(Y_1 \| \cdots \| Y_j) \qquad (1)$$

В настоящем стандарте термин «подписанные данные» относится к последовательности «$Y_1\|\ldots\|Y_j$», которая используется в качестве входных

[1] Эквивалентным этому термину является термин «регистрационное свидетельство», применяемый в законодательстве Республики Казахстан.

данных для схемы подписи, а термин «неподписанные данные» относится к последовательности «$X_1||\ldots||X_j$».

Если информация, содержащаяся в подписанных данных маркера, может быть восстановлена из подписи, она должна отсутствовать в неподписанных данных маркера (см. например, стандарт ИСО/МЭК 9796).

Если информация, содержащаяся в текстовом поле подписанных данных маркера, не может быть восстановлена из подписи, то она должна содержаться в неподписанном текстовом поле маркера.

Если информация в подписанных данных маркера (например, случайное число) уже известна верификатору, она должна отсутствовать в неподписанных данных маркера, посланного претендентом.

Все текстовые поля, указанные в изложенных далее механизмах, доступны для использования вне области применения настоящего стандарта (они могут быть пустыми). Их взаимосвязь и содержание зависят от конкретного применения. См. Приложение А относительно информации по использованию текстовых полей.

Примечание.

1 Подписывание одной сущностью блока данных, которым манипулировала другая сущность в неких своих целях, может быть предотвращено первым объектом путем включения его собственного случайного числа в блок данных, который он подписывает.

2 Поскольку распределение сертификатов находится вне области применения настоящего стандарта, их посылка не обязательна во всех механизмах.

5.1 Односторонняя аутентификация

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

5.1.1 Однопроходная аутентификация

В данном механизме аутентификации претендент А инициирует процесс и аутентифицируется верификатором *В*.

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.

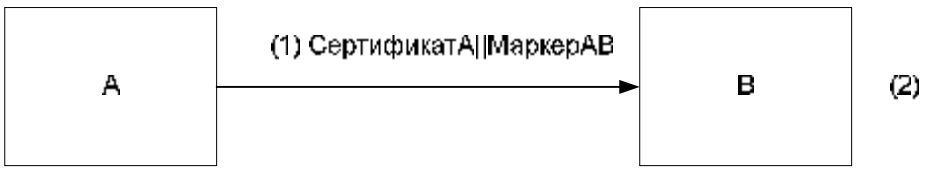


Рисунок 1

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

$$МаркерAB = \begin{matrix} T_A \\ N_A \end{matrix} \left\| B \| Текст2 \| sS_A \left(\begin{matrix} T_A \\ N_A \end{matrix} \left\| B \| Текст1 \right. \right) \right. \qquad (2)$$

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

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

Примечание.

1. Включение отличительного идентификатора B в подписанные данные МаркераAB необходимо для предотвращения использования МаркераAB какой-либо другой сущностью, кроме уполномоченного верификатора.

2. В общем случае текст2 не аутентифицируется в этом процессе.

3. Одним из применений данного механизма может быть распределение ключей (см. Приложение А *СТ РК ИСО/МЭК 9798-1-2008*).

(1) Сущность *A* посылает *МаркерAB* и, при необходимости, свой сертификат сущности *B*.

(2) После получения сообщения, содержащего *МаркерAB*, сущность *B* выполняет следующие шаги:

а) сущность *B* убеждается, что владеет имеющим силу открытым ключом сущности *A* либо проверяя сертификат сущности *A*, либо с помощью каких-либо других средств;

б) сущность *B* подтверждает *МаркерAB* через проверку подписи сущности *A*, содержащейся в этом маркере, через проверку метки времени или последовательного числа и через проверку совпадения значения поля идентификатора *(B)* в подписанных данных *МаркераAB* со значением отличительного идентификатора сущности *B*.

5.1.2 Двухпроходная аутентификация

В данном 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.

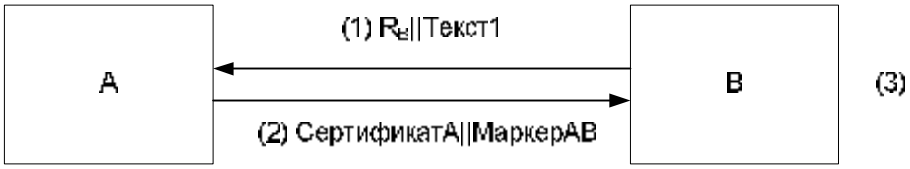


Рисунок 2

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

$$МаркерАВ = R_A \| R_B \| B \| Текст3 \| sS_A\left(R_A \| R_B \| B \| Текст2\right) \qquad (3)$$

Включение отличительного идентификатора *В* в *МаркерАВ* является необязательным. Это зависит от среды, в которой используется данный механизм аутентификации.

Примечание.

1. Включение необязательного идентификатора В в подписанные данные МаркераАВ поможет предотвратить использование маркера кем-либо еще, не только уполномоченным верификатором (например, при атаке «злоумышленника в середине).

2. Включение случайного числа RA в подписанные данные МаркераАВ предотвратит получение сущностью В подписи сущности А на данных, выбранных сущностью В до начала работы механизма аутентификации. Это может потребоваться, например, в случае, когда один и тот же ключ используется сущностью А для других целей, а не для аутентификации.

(1) Сущность *В* посылает случайное число R_B, и, при необходимости, текстовое поле *Текст*1 сущности *А*.

(2) Сущность *А* посылает *МаркерАВ* и, при необходимости, свой сертификат сущности *В*.

(3) После получения сообщения, содержащего *МаркерАВ*, сущность *В* следующие шаги:

а) сущность *В* убеждается, что владеет имеющим силу открытым ключом сущности *А* либо проверяя сертификат сущности *А*, либо с помощью каких-либо других средств;

б) сущность *В* подтверждает *МаркерАВ* через проверку подписи сущности *А*, содержащейся в этом маркере, через проверку случайного числа R_B, посланного сущности *А* на шаге (1), которое должно согласовываться со случайным числом, содержащимся в *МаркереАВ*, и через проверку совпадения значения поля идентификатора *(В)* в подписанных данных *МаркераАВ*, если таковое имеется, со значением отличительного идентификатора сущности *В*.

5.2 Взаимная аутентификация

Взаимная аутентификация подразумевает, что две поддерживающие связь сущности аутентифицируются одна другой 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 реализации взаимной аутентификации. Это реализовано передачей одного дополнительного сообщения, приводящего к еще двум дополнительным шагам.

Механизм, рассмотренный в 5.2.3, использует четыре сообщения, которые, однако, не обязательно должны посылаться все последовательно. Таким образом, процесс аутентификации может быть ускорен.

5.2.1 Двухпроходная аутентификация

В данном 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.

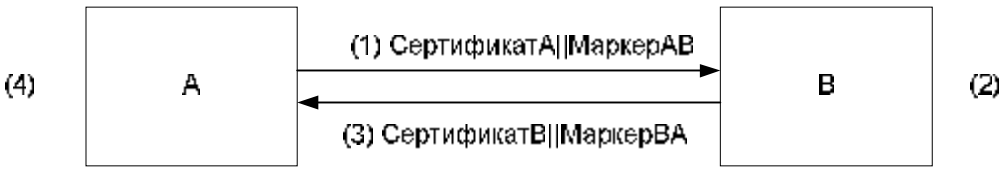


Рисунок 3

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

$$МаркерAB = \begin{matrix} T_A \\ N_A \end{matrix} \left\| B \right\| Текст2 \left\| sS_A \left(\begin{matrix} T_A \\ N_A \end{matrix} \left\| B \right\| Текст1 \right) \right. \qquad (4)$$

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

$$МаркерAB = \begin{matrix} T_B \\ N_B \end{matrix} \left\| A \right\| Текст4 \left\| sS_B \left(\begin{matrix} T_B \\ N_B \end{matrix} \left\| A \right\| Текст3 \right) \right. \qquad (5)$$

Выбор использования меток времени или последовательных чисел в данном механизме зависит от технических возможностей претендента и верификатора, а также от среды.

Примечание.

1 Включение идентификаторов A и B в подписанные данные МаркераAB и МаркераBA соответственно является необходимым для предотвращения использования указанных маркеров кем-либо еще, кроме уполномоченного верификатора.

(1)-(2) шаги идентичны шагам, определенным в 5.1.1, для однопроходной аутентификации.

(3) Сущность *B* посылает *МаркерBA* и, при необходимости, свой сертификат сущности *A*.

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

2 Два сообщения этого механизма не связаны друг с другом ничем, кроме как неявной своевременностью. Рассматриваемый механизм дважды использует независимое

применение механизма 5.1.1. Дальнейшее связывание этих сообщений может быть достигнуто соответствующим использования текстовых полей.

5.2.2 Трехпроходная аутентификация

В данном 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.

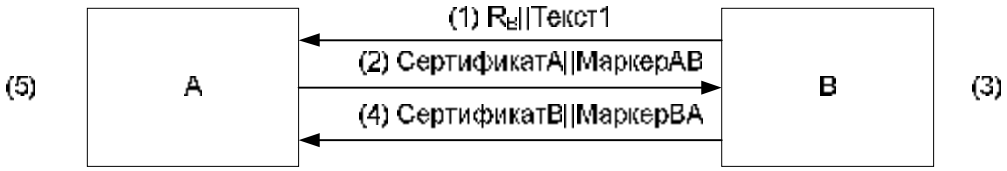


Рисунок 4

Маркеры имеют следующую форму:

$$МаркерAB = R_A \| R_B \| B \| Текст3 \| sS_A\left(R_A \| R_B \| B \| Текст2\right),$$
$$МаркерBA = R_B \| R_A \| A \| Текст5 \| sS_B\left(R_B \| R_A \| A \| Текст4\right) \qquad (6)$$

Включение параметра B в *МаркерAB* и параметра A в *МаркерBA* является необязательным. Это зависит от среды, в которой используется механизм аутентификации.

Примечание. Включение случайного числа RA в подписанные данные МаркераAB предотвратит получение сущностью B подписи сущности A на данных, выбранных сущностью B до начала работы механизма аутентификации. Это может потребоваться, например, в случае, когда один и тот же ключ используется сущностью A для других целей, а не для аутентификации. Включение случайного числа RB в МаркерAB, хотя и необходимо по соображениям безопасности, которые заставляют сущность A выполнить проверку этого числа на соответствие значению, посланному в первом сообщении, однако не может обеспечить ту же защиту для сущности B, поскольку число RB известно сущности A до того, как выбрано число RA. Если требуется данный тип защиты, то сущность B может ввести дополнительное случайное R'B в Текст 4 и Текст 5 текстовых полей для МаркераAB.

(1) Сущность B посылает случайное число R_B и, при необходимости, текстовое поле *Текст* 1 сущности A.

(2) Сущность A посылает *МаркерAB* и, при необходимости, свой сертификат сущности B.

(3) После получения сообщения, содержащего *МаркерAB*, сущность B выполняет следующие действия:

а) сущность B убеждается, что владеет имеющим силу открытым ключом сущности *A*, либо проверяя сертификат сущности *A*, либо с помощью каких-либо других средств;

б) сущность *B* подтверждает *МаркерAB* через проверку подписи сущности *A*, содержащейся в этом маркере, через проверку случайного числа R_B, посланного сущности *A* на шаге (1), которое должно согласовываться со случайным числом, содержащимся в *МаркереAB*, и через проверку совпадения значения поля идентификатора *B* в подписанных данных *МаркераAB*, если таковое имеется, со значением отличительного идентификатора сущности *B*.

(4) Сущность *B* посылает *МаркерBA* и, при необходимости, свой сертификат сущности *A*.

(5) После получения сообщения, содержащего *МаркерBA*, сущность *A* аналогичным образом выполняет действия (i) и (ii) шага 3. Кроме того, сущность *A* проверяет, чтобы значения случайного числа R_B, содержащегося в подписанных данных *МаркераBA*, и случайного числа R_B, полученного на шаге (1), совпадали.

5.2.3 Двухпроходная параллельная аутентификация

В данном механизме аутентификация выполняется параллельно. Уникальность/своевременность контролируется созданием и проверкой случайных чисел (см. Приложение Б стандарта *СТ РК ИСО/МЭК 9798-1-2008*). Механизм аутентификации представлен на рисунке 5.

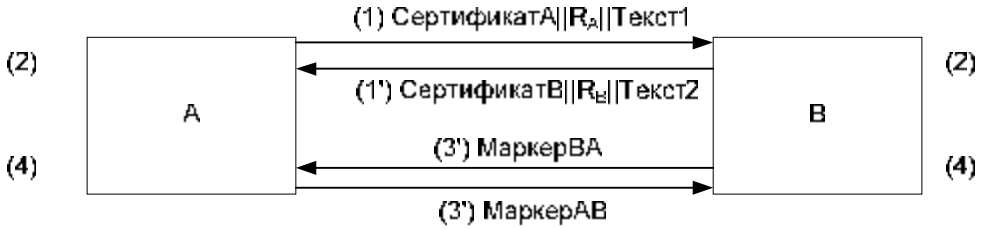


Рисунок 5

Форма маркеров аналогична той, что используется в 5.1.2.

$$МаркерAB = R_A \| R_B \| B \| Текст4 \| sS_A\left(R_A \| R_B \| B \| Текст3\right),$$
$$МаркерBA = R_B \| R_A \| A \| Текст6 \| sS_B\left(R_B \| R_A \| A \| Текст5\right). \qquad (7)$$

Включение параметра *B* в *МаркерAB* и параметра *A* в *МаркерBA* является необязательным. Это зависит от среды, в которой используется механизм аутентификации.

Примечание.

1. Включение случайного числа RA в подписанные данные МаркераАВ предотвратит получение сущностью В подписи сущности А на данных, выбранных сущностью В до начала работы механизма аутентификации. Это может потребоваться, например, в случае, когда один и тот же ключ используется сущностью А для других целей в дополнение к аутентификации. По тем же причинам в МаркереАВ присутствует случайное число RB. В зависимости от относительного времени получения сообщений, посланных в шагах (1) и (1'), одна из сторон может знать случайное число другой стороны при её выборе случайного числа. Если это нежелательно, то обе стороны могут ввести дополнительное случайное число RA и RB в Текст 3 и Текст 4 текстовых полей для МаркераАВ и в Текст 5 и Текст 6 текстовых полей для МаркераВА.

(1) Сущность A посылает случайное число R_A и, при необходимости, свой сертификат и текстовое поле *Текст* 1 сущности *B*.

(1') Сущность *B* посылает случайное число R_B и, при необходимости, свой сертификат и текстовое поле *Текст*2 сущности *A*.

(2) Сущности *A* и *B* убеждаются, что владеют имеющим силу открытым ключом другой сущности либо проверяя соответствующий сертификат, либо с помощью каких-либо других средств.

(3) Сущность *A* посылает *МаркерAB* сущности *B*.

(3') Сущность *B* посылает *МаркерBA* сущности *A*.

(4) Сущности *A* и *B* выполняют следующие действия.

1. Каждая из сущностей подтверждает полученный маркер через проверку подписи, содержащейся в полученном маркере, а также через проверку соответствия случайного числа, предварительно посланного другой сущности, и случайного числа, содержащегося в подписанных данных полученного маркера.

2. Альтернатива механизму 5.2.3 – симметричное применение механизма 5.1.2. Включение сертификатов в первых сообщениях механизма 5.2.3 предусматривает более раннюю их проверку, что может ускорить процесс аутентификации.

Приложение А
(справочное)
Применение текстовых полей

Маркеры, приведенные в разделах 5 настоящего стандарта, содержат текстовые поля. Фактическое применение и взаимозависимость между различными текстовыми полями при заданном проходе механизма аутентификации зависит от конкретного применения. Далее рассматриваются несколько примеров; см. также Приложение А *СТ РК ИСО/МЭК 9798-1-2008*.

Если используется схема подписи без восстановления сообщения и подписанное текстовое поле не является пустым, то верификатор должен владеть текстом до подтверждения подписи. В данном приложении термин «подписанные текстовые поля» относится к текстовым полям в подписанных данных, а термин «неподписанные текстовые поля» относится к текстовым полям в неподписанных данных.

Например, если используется схема цифровой подписи без восстановления сообщения, то любая информация, требующая аутентификации происхождения данных, должна быть помещена в подписанное текстовое поле и (как часть) в неподписанное текстовое поле в маркере.

Если маркеры не имеют (достаточной) избыточности, подписанные текстовые поля могут использоваться для обеспечения дополнительной избыточности.

Подписанные текстовые поля могут использоваться для указания того, что маркер имеет силу только для аутентификации. Если существует вероятность, что один из пользователей может выбрать «вырожденное» значение со злым умыслом для подписи второй сущностью, то эта вторая сущность может ввести случайное число в текстовое поле.

Если алгоритм используется там, где есть возможность осуществления атак, основанных на использовании каким-либо претендентом одного и того же ключа для всех верификаторов, с которыми он связывается, и если такие атаки считаются угрозами, то подлинность уполномоченного верификатора должна быть включена в подписанное текстовое поле и, при необходимости, в неподписанное текстовое поле.

Неподписанные текстовые поля могут также использоваться для предоставления верификатору информации, содержащей (неаутентифицированную) подлинность, которую требует предоставить претендент. Если используются иные, чем сертификаты, средства для распределения открытых ключей, то такая информация может требоваться для определения верификатором, каким открытым ключом нужно пользоваться для аутентификации претендента.

УДК 681.324:006.354 **МКС 35.040**

Ключевые слова: обработка данных, информационный обмен, передача данных, защита информации, методы защиты, кодирование (преобразование), аутентификация, коды аутентификации сообщений, алгоритмы.

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