ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология
ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ ӘДІСТЕРІ ЖӘНЕ ҚҰРАЛДАРЫ
Сәйкестендіру тетіктері
1-бөлім
Жалпы ережелер

Информационная технология
МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ
Механизмы аутентификации
Часть 1
Общие положения

ҚР СТ ИСО/МЭК 9798-1-2008

ИСО/МЭК 9798-1:1997

«Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Сәйкестендіру тетіктері 1-бөлім Жалпы ережелер», IDT)

Ресми басылым

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

Астана

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология

ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ ӘДІСТЕРІ ЖӘНЕ ҚҰРАЛДАРЫ

Сәйкестендіру тетіктері
1-бөлім
Жалпы ережелер

ҚР СТ ИСО/МЭК 9798-1-2008
ИСО/МЭК 9798-1:1997
«Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Сәйкестендіру тетіктері 1-бөлім Жалпы ережелер», IDT)

Ресми басылым

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

Астана

Кіріспе

1 «Инфосистемы Джет» ЖАҚ **ӘЗІРЛЕДІ**

Қазақстан Республикасының Ақпараттандыру және байланыс агенттігі **ЕНГІЗДІ**

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

3 Осы стандарт Қазақстан Республикасы экономикасының қажеттіліктерін білдіретін қосымша талаптар көлбеу қаріппен белгіленіп ИСО/МЭК 9798-1:1997 «Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Сәйкестендіру тетіктері. 1-бөлім. Жалпы ережелер» («Information technology. Security techniques. Entity authentication. Part 1. General»), IDT, халықаралық стандартына сәйкес.

4 БІРІНШІ ТЕКСЕРУ МЕРЗІМІ 2013 жыл
ТЕКСЕРУ КЕЗЕҢДІЛІГІ 5 жыл

5 АЛҒАШ РЕТ ЕНГІЗІЛДІ

Мазмұны

Кіріспе

ҚР СТ ИСО/МЭК 9798-2008 «Ақпараттық технологиялар. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Сәйкестендіру тетіктері» жалпы атауымен мынадай бөліктерден тұрады:

- *1-бөлік. Жалпы ережелер;*
- *2-бөлік. Симметриялық санға бөлу алгоритмдері қолданылатын тетіктер.*
- *3-бөлік. Сандық қолтаңба әдістері қолданылатын тетіктер.*

ИСО/МЭК 9798-2008 халықаралық стандарты аталған бөліктерден басқа мыналарды қамтиды:

- *4-бөлік. Криптографиялық салыстырып тексеру қызметін пайдаланатын тетіктер.*
- *5-бөлік. Нөлдік мәнмен асимметриялық әдістерді пайдаланатын тетіктер.*

Халықаралық стандартқа олардың құрылуына қарай өзге бөліктері де қосыла алады.

Осы стандарт қосымшалары анықтамалық болып табылады.

ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ МЕМЛЕКЕТТІК СТАНДАРТЫ

Ақпараттық технология
ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ ӘДІСТЕРІ ЖӘНЕ ҚҰРАЛДАРЫ
Сәйкестендіру тетіктері
1-бөлім
Жалпы ережелер

Енгізілген күні 2008.07.01

1 Қолданылу саласы

Осы стандарт сәйкестендіру моделін анықтайды және мәндерді сәйкестендіру үшін қолданылатын қауіпсіздік тетіктеріне қойылатын жалпы талаптарды және шектеулерді белгілейді. Бұл тетіктер мәні осының өзін растау үшін қолданылады. Сәйкестендірілуге жататын мән қандай да бір құпия ақпаратты білуін көрсете отырып, өзінің түпнұсқалығын дәлелдейді. Тетіктер мәндер арасында ақпараттармен алмасу процестері ретінде, сондай-ақ қажет жағдайда, сенімді үшінші тараппен ақпарат алмасу процестері ретінде анықталады.

Сәйкестендіруші ақпараттар мәнін қоса алғанда, қауіпсіздік тетіктері толығырақ осы стандарттың келесі бөлімдерінде қарастырылған.

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.

ҚР СТ ИСО/МЭК 9798-2008 келесі бөлімдерінде қарастырылатын бірқатар тетіктер істен шықпауды (non-repudiation) қамтамасыз ететін сервистерді іске асыру барысында қолданылуы мүмкін. Бұлардың тетіктері *ИСО/МЭК 13888-2008* [2] стандартында анықталған. Мұндай сервистердің спецификациясы *ҚР СТ ИСО/МЭК 9798 – 2008* қолданылу саласынан тыс жатыр.

2 Нормативтік сілтемелер

Осы стандартта мынадай стандарттарға сілтемелер пайдаланылды:

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

ҚР СТ ИСО/МЭК 10181-2-2008 Ақпараттық технология. Ашық жүйелердің өзара байланысы. Ашық жүйелерге арналған қауіпсіздік негіздері. 2-бөлік. Сәйкестендіру негіздері.

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

ҚР СТ ИСО/МЭК 13888-2:2008 Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері және құралдары. Істен шықпау. 2-бөлік. Симметриялық әдістерді қолданатын тетіктер.

ҚР СТ ИСО/МЭК 14888-2-2006 Ақпараттық технология. Ақпаратты қорғау әдістері. Қосымшалармен сандық қолдар. 2-бөлік. Түпнұсқалыққа негізделген тетіктер.

ИСО 7498-2: 2002 Ақпараттарды өңдеу жүйесі. Ашық жүйелердің өзара байланысы. Базалық эталондық үлгі. 2-бөлік. Қорғау архитектурасы.

3 Терминдер мен анықтамалар

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

3.1 Асимметриялық криптографиялық әдіс (asymmetric cryptographic technique): Екі өзара байланысты түрленулерді – ашық түрленуді (ашық кілтпен анықталатын) және жабық (құпиялы) түрленуді (жабық кілтпен анықталатын) қолданатын криптографиялық әдіс. Осы қос түрлену деректер блогының ашық түрленуін қолданумен есептеу арқылы осы деректер блогының жабық түрленуін алуға болатын қасиетке ие.

Ескертпе – Ассиметриялық криптографиялық әдістерге негізделген жүйе шифрлеу және қол қою құрастырылған жүйелері немесе кілттерді тарататын жүйе болуы мүмкін. Ассиметриялық криптографиялық әдістерде төрт қарапайым түрленулер қарастырылады: қол қою, шифрлеу жүйелері үшін қол қою және қол қоюды тексеру, шифрлеу жүйесі үшін шифрлеу және шифрді ашу. Қол қою және шифрді ашу түрленулерінің құпиялығы олардың қолданылатын мәндерімен сақталуы тиіс, бұл жағдайда осы қол қою және шифрді ашу түрленулері ашық болып табылады. Барлық төрт қарапайым функциялар екі түрленумен ғана іске асатын ассиметриялық криптожүйелер болады (мысалы, RSA): бір жабық түрлену мәліметке қол қою және шифрді ашу үшін, ал бір ашық түрлену қол қоюды тексеру және мәліметті шифрлеу үшін жеткілікті. Бірақ, осыған ұқсас мысал жалпы жағдай болып, ҚР СТ ИСО/МЭК 9798-2008 барлық төрт қарапайым түрленулер және тиісті кілттер әртүрлі болып саналады.

3.2 Асимметриялық шифрлеу жүйесі (asymmetric cryptographic system): Ашық түрлену шифрлеу үшін және жабық түрлену шифрді ашу үшін қолданылатын асимметриялық криптографиялық әдістерге негізделген жүйе.

3.3 Асимметриялық кілттер жұбы (asymmetric key pair): Жабық кілт жабық (құпиялы) түрленуді, ал ашық кілт ашық түрленуді анықтайтын өзара байланысты кілттер жұбы.

3.4 Асимметриялық қолтаңбалар жүйесі (asymmetric signature system): Қол қоюға жабық түрленуді, ал ашық түрленуді қолтаңбалардың түпнұсқалығын тексеру үшін қолданатын асимметриялық криптография әдістеріне негізделген жүйе.

3.5 Шақыру (challenge): Верификаторға жіберілетін жауапты қалыптастыру үшін үміткерге белгілі құпиялы ақпаратпен үміткермен қолданылатын верификатормен үміткерге жіберілген және өздігінен таңдап алынған деректер элементі.

3.6 Шифрленген мәтін (ciphertext): Өзінің ақпараттық мағлұматын қысқарту үшін шифрлеу алгоритмі бойынша шифрлі түрге түрленген деректер.

3.7 Криптографиялық бақылау қызметі (cryptographic check function): Кірісте құпия кілтті және өзіндік жолды ала отырып, шығыста криптографиялық бақылау мәнін есептейтін криптографиялық түрлену. Дұрыс бақылау мәнді құпия кілтті білмей анықтау мүмкін емес болуы керек.

3.8 Шифрді ашу (decipherment): Шифрді сәйкес түрлендіруге кері түрлендіру.

3.9 Ерекше сәйкестендіргіш (distinguishing identifier): Сәйкестендіруші мәнді бір жақты анықтайтын ақпарат.

3.10 Шифрлеу (encipherment): Шифрленген мәтін алу үшін, яғни деректерде жазылатын ақпараттарды қысқарту үшін криптографиялық алгоритммен деректерді түрлендіру.

3.11 Мәннің сәйкестендірілуі (entity authentication): Мән мағынаның жариялағанын растау.

3.12 Кірістірмелермен шабуыл (interleaving attack): Айналмалар арқылы шабуыл түрлері, ол арқылы сәйкестендіру процестерін жүзеге асыратын немесе бұрын жүзеге асырған ақпараттық алмасумен алынған ақпарат қолданылады.

3.13 Кілт (key): Криптографиялық түрлендіру процесін басқаратын белгілер кезектілігі (мысалы, шифрлеу, шифрді ашу, криптографиялық бақылау қызметімен есептеу, қолтаңбаларды құру немесе тексеру).

3.14 Өзара байланысты сәйкестендіру (mutual authentication): Қос мәнге бір бірінің түпнұсқалығына кепілдік берілетін сәйкестендіру мәндері.

3.15 Ашық мәтін (plaintext): Шифрленбеген ақпарат.

3.16 Шифрді ашудың жабық кілті (private decipherment key): Шифрді ашудың жабық түрленуін анықтайтын жабық кілт.

3.17 Жабық кілт (private key): Мәндердің асимметриялық кілт жұптарынан алынған кілт, ол осы мәнмен ғана қолданылуы тиіс.

Ескертпе – Асимметриялық қолтаңбалар жүйесі кезінде жабық кілт қол қоюдың түрленуін анықтайды. Асимметриялық шифрлеу жүйесі кезінде жабық кілт шифрді ашудағы түрленуді анықтайды.

3.18 Қолтаңбаның жабық кілті (private signature key): Қол қоюдың жабық түрленуін анықтайтын жабық кілт.

Ескертпе – Кейде қолтаңбаның жеке кілті ретінде қарастырылады.

3.19 Шифрлеудің ашық кілті (public encipherment key): Шифрлеудің ашық түрленуін анықтайтын ашық кілт.

3.20 Ашық кілт (public key): Жалпыға белгілі маңызды асимметриялық кілт жұптарынан алынған кілт.

Ескертпе – Асимметриялық қол қою жүйесі кезінде ашық кілт қол таңбаны тексерудің түрленуін анықтайды. Асимметриялық шифрлеу жүйесі кезінде бұл кілт шифрлеудің түрленуін анықтайды. «Жалпыға белгілі» кілт жалпыға қол жетерлік болуы міндетті емес. Кілт күні бұрын анықталған топ мүшелеріне ғана белгілі болуы мүмкін.

3.21 Ашық кілт сертификаты/сертификат (public key certificate/certificate): Куәландырылған орталықпен қол қойылған ашық кілт мәні туралы ақпарат, бұл жасанды түрінде қарастырылмайды. (сондай-ақ В қосымшасын қараңыз). Осы терминге балама Қазақстан Республикасы заңнамасында қолданылатын «тіркеу куәлігі» термині болып табылады.

3.22 Ашық кілт туралы ақпарат (public key information): Мәннің ерекше, сонымен қатар ең болмағанда, осы мән үшін бір ашық кілтті құрайтын жеке мәнге қатысты ақпарат. Ашық кілт туралы ақпарат куәландыратын орталық, мән және ашық кілттің қолдану мерзімі, тиісті жабық кілттің қолданылу мерзімі немесе қолданылатын криптографиялық алгоритмдердің идентификаторы сияқты ашық кілт туралы қосымша мәліметтерді қамтуы мүмкін (сондай ақ В қосымшасын қараңыз).

3.23 Түпнұсқалықты тексеретін ашық кілт (public verification key): Түпнұсқалықты тексерудің ашық түрленуін анықтайтын ашық кілт.

3.24 Кездейсоқ сан (random number): Мәні анықталмаған уақытқа байланысты параметр (сондай ақ, Б қосымшасын қараңыз).

3.25 Шағылысу шабуылы (reflection attack): Бұрын жіберілген мәліметті оның жіберушісіне кері қайтару жіберілімі қолданылатын айналым шабуылының түрлері.

3.26 Қайталау шабуылы (replay attack): Бұрын жіберілген мәліметтер қолданылатын айналым шабуылының түрлері.

3.27 Кезекті сан (sequence number): Белгілі уақыт аралығында қайталанбайтын мәні берілген кезектіліктен таңдап алынатын уақытқа байланысты параметр (сондай-ақ Б қосымшасын қараңыз).

3.28 Симметриялық криптографиялық әдіс (symmetric cryptographic technique): Жіберуші тарапынан түрлендіру сияқты, мәліметті алушы тарапынан түрлендіру ретінде бір құпия кілтті қолданатын криптографиялық әдіс. Құпия кілтті білмей жіберуші тарапынан немесе мәліметті алушы тарапынан түрлендіруді ашу мүмкін емес.

3.29 Симметриялық шифрлеу алгоритмі (symmetric encipherment algorithm): Жіберуші тарапынан түрлендіруге сияқты, мәліметті алушы тарапынан түрлендіруге де бір құпиялы кілт қолдануға негізделген шифрлеу алгоритмі.

3.30 Уақыт таңбасы (time stamp): Уақытты жалпы санауда уақыт сәтін белгілейтін уақытқа байланысты параметр (сондай-ақ Б қосымшасын қараңыз).

3.31 Уақытқа байланысты параметр (time variant parameter): Мәліметтің қайта жіберілмегендігін тексеруге қолданылатын деректер элементі; ол кездейсоқ санды, кезекті санды, сондай-ақ уақыт белгісін анықтауға қолданылады (сондай-ақ Б қосымшасын қараңыз).

3.32 Маркер (token): Криптографиялық әдіс көмегімен түрленген ақпаратты қамтитын байланысты нақты сеансына қатысы бар деректер өрісін құрайтын мәлімет.

3.33 Бір тараптық сәйкестендіру (unilateral authentication): Түпнұсқалық кепілдігі басқа мәнге ұсынылатын және кері құбылыс орындалмайтын мән сәйкестендірілуі.

4 Белгілеулер

Осы стандарт мәтінінде мынадай таңбалар мен белгілер қолданылады:

A	*A* мәнін ерекшелейтін сәйкестендіргіш.
B	*B* мәнін ерекшелейтін сәйкестендіргіш.
TP	Сенімді үшінші тарапты ерекшелейтін сәйкестендіргіш.
K_{XY}	*X* және *Y* мәндеріне белгілі құпиялы кілт; симметриялық криптографиялық әдістерде ғана қолданылады.
P_X	*X* мәнімен байланысты түпнұсқаны тексеретін ашық кілт, асимметриялық криптографиялық әдістерде қолданылады.
S_X	*X* мәнімен байланысты түпнұсқаны тексеретін жабық кілт, асимметриялық криптографиялық әдістерде қолдан.
N_X	*X* мәнімен ұсынылған кезекті сан.
R_X	*X* мәнімен ұсынылған кездейсоқ сан.
T_X	*X* мәнімен ұсынылған уақыт белгісі.
T_X N_X	*X* мәнімен ұсынылған уақытқа байланысты параметр және T_X уақыт белгісі немесе N_X кезекті сан болып табылады
$Y\|\|Z$	Белгілі тәртіппен *Y* және Z деректер элементінің кезекті қосылу нәтижесі.
$eK(Z)$	*K* кілтін қолданатын симметриялық шифрлеу алгоритмімен Z деректерді шифрлеу нәтижесі .
$dK(Z)$	*K* кілтін қолданатын симметриялық шифрлеу алгоритмімен Z деректердің шифрлерін ашу нәтижесі

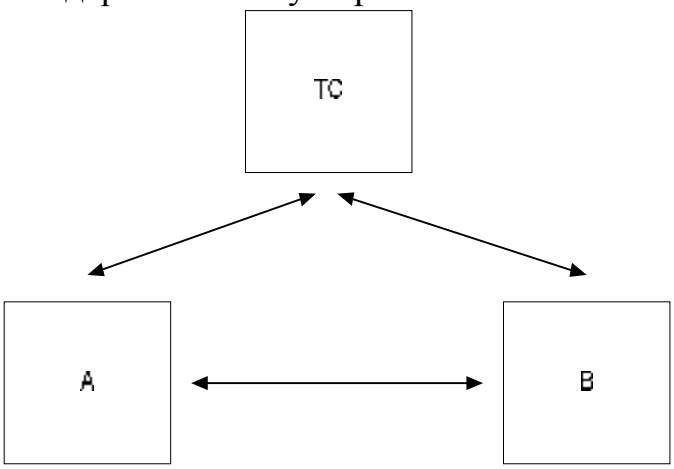
$f_K(Z)$	Кіріс параметрлерін *K* құпиялы кілт және Z деректерінің өзіндік жолы ретінде қолданатын *f* криптографиялық бақылау қызметін қолдану нәтижесі болып табылатын криптографиялық бақылау мәні.
CertX	*X* мәнінің сенімді үшінші тараппен берілген сертификат.
TokenXY	*X* мәнінен *Y* мәніне жіберілген маркер.
TVP	Уақытқа байланысты параметр.
$sS_X(Z)$	S_X қолтаңбаның жабық кілтін қолдану арқылы Z деректеріне қол қоюдың жабық түрленуін қолдану көмегімен алынатын қолтаңба .

5. Сәйкестендіру моделі

Мәндерді сәйкестендіру тетіктеріне арналған жалпы модель 1-суретте көрсетілген. Барлық мәндердің және сәйкестендірудің әрбір нақты механизмінде ақпаратпен алмасу тараптарының қатысуы міндетті емес.

ҚР СТ ИСО/МЭК 9798-2008 стандартының басқа бөлімдерінде толығырақ мазмұндалған сәйкестендіру тетіктері үшін бір тараптық сәйкестендіру кезінде *A* мәні үміткер, ал *B* мәні верификатор ретінде қарастырылады. Өзара сәйкестендіру кезінде А және В мәндері үміткер және верификатор қызметтерін орындайды.

Сәйкестендіру мақсаттары үшін мәндер маркер деп аталатын стандартталған мәліметтерді басқарады және алмасады. Бір тараптық сәйкестендіру барысында ең болмағанда, бір маркермен және өзара сәйкестендіру кезінде екі маркермен алмасу талап етіледі. Егер сәйкестендіру процесінің деректерімен алмасуды инициалдау үшін қоңырау шалынатын болса, онда қосымша жол талап етілуі мүмкін. Сондай-ақ, сәйкестендіруші алмасу процесіне сенімді үшінші тарап тартылған болса, тағы да қосымша жолдар талап етілуі мүмкін.



1-сурет. Сәйкестендіру моделі

1- суретте мегзермен мүмкін ақпараттық ағыстар көрсетілген. А және В мәндері бір бірімен өзара немесе ТС сенімді үшінші тараппен тікелей өзара әрекет етуі, А немесе сәйкесінше В арқылы сенімді үшінші тараппен өзара әрекет етуі немесе сенімді үшінші тараппен ұсынылған кейбір ақпаратты қолдануы мүмкін.

Сәйкестендіру механизмдері толығырақ *ҚР СТ ИСО/МЭК 9798* стандарттың келесі бөлімдерінде қарастырылған.

6. Жалпы талаптар және шектеулер

Бір мән басқаны сәйкестендіру үшін олардың екеуі де криптографиялық әдістер мен параметрлердің жалпы жинағын қолдануы тиіс.

Кілт қолданыста болатын уақытқа байланысты кілт қолданған сайын барлық параметрлердің мәндері (яғни, уақыт белгісі, кезекті және кездейсоқ сандар) ең болмағанда, жоғары ықтималдықпен қайталанбауы керек.

Сәйкестендіру тетіктерін қолдану процесінде *А* және *В* мәндеріне олардың әрқайсысына жеке-жеке бір бірі туралы мәліметтер белгілі болатындығы болжанады. Бұған осы мән алмасатын ақпаратқа идентификаторды қосу арқылы немесе тетікті қолдану контекстінен қол жеткізуге болады.

Мәндердің түпнұсқалығы деректерді сәйкестендірумен алмасу кезінде белгіленуі мүмкін. Кешірек жіберілген деректердің түпнұсқалығына кепілдік беру үшін сәйкестендірумен алмасу процесі ақпараттық қауіпсіздікті қамтамасыз ету құралдарының жиынтығымен қолданылуы тиіс (мысалы, бақылау құралдарының жиынтығымен).

А қосымшасы
(анықтамалық)

МӘТІН ЖОЛДАРЫН ПАЙДАЛАНУ

ҚР СТ ИСО/МЭК 9798-2008 стандартының келесі бөлімдерінде қарастырылатын маркерлер мәтіндік өрістерді қамтиды. Сәйкестендіру механизмінің нақты жолындағы түрлі мәтіндік өрістердің нақты қолданылуы және олардың арасындағы өзара байланыс қосымшаға байланысты болады.

Мәтіндік өрістер уақытқа байланысты қосымша параметрлерді қамтуы мүмкін. Мысалы, егер маркерде кезекті сан қолданылатын болса, маркердің мәтіндік өрісінде уақыт белгісі болуы мүмкін. Егер мәлімет алушы мәліметтегі кез келген уақыт белгісі белгілі аралық шегінде болса, бұл мәжбүрлі іркілістерді анықтауға мүмкіндік береді (Б қосымшасын қараңыз).

Бірнеше қолданыстағы кілттер болған жағдайда кілт идентификаторы ашық мәтіндегі мәтіндік өріске енгізілуі мүмкін. Егер сәйкестендіру процесінде бірнеше сенімді үшінші тараптар қатысатын болса, онда мәтіндік өрістер сенімді үшінші тараптың ерекше идентификаторын сұрауға қосуға қолданылуы мүмкін.

Мәтіндік өрістер кілттердің таратылуына қолданылуы мүмкін (ИСО/МЭК 11770-2 және [1] қараңыз).

ҚР СТ ИСО/МЭК 9798 стандартының келесі бөлімдерінде мазмұндалған кез келген тетіктердің бірі кез келген пайдаланушыға сәйкестендіру процесін механизмнің жұмысы алдында қосымша мәліметті қолдану арқылы іске қосуға мүмкіндік беретін қосымшада құрастырылған болса, бұл қауіпсіздікті бұзуы мүмкін. Бұзушы заңсыз алынған маркерді бірнеше рет қолдана алатын бұзушылықтарға жол бермес үшін сәйкестендірумен талап етілетін мәндерді анықтау мақсатында мәтіндік өрістерді қолдана алады (*ҚР СТ ИСО/МЭК 10181-2* стандартын қараңыз).

Бұл аталмыш мысалдармен ғана шектелмейді.

Б қосымшасы
(анықтамалық)
УАҚЫТҚА БАЙЛАНЫСТЫ ПАРАМЕТРЛЕР

Уақытқа байланысты параметрлер бірегейлікті\уақыттылықты тексеруге қолданылады. Олар бұрын жіберілген мәліметтердің қайталанып жіберілуін анықтауға мүмкіндік береді. Ол үшін сәйкестендіру ақпараты бір процестен келесі процеске өзгеруі тиіс.

Уақытқа байланысты параметрлердің кейбір түрлері «мәжбүрлі іркілістердің» (қаскүнемдердің коммуникациялық ортасына қосылған іркілістердің) анықталуына мүмкіндік береді. Бір жолды пайдаланатын тетіктерде мәжбүрлі іркілістер басқа құралдармен (мысалы, жеке мәліметтер арасындағы уақыт бойынша қосымша ең жоғары аралықтарды шектеуге қолданылатын «тайм аут санауыштары») анықталуы мүмкін.

ҚР СТ ИСО/МЭК 9798 стандарттың келесі бөлімдерінде уақытқа байланысты параметрлердің уақыт белгісі, кезекті сан және кездейсоқ сан деп бөлінетін үш түрі қолданылады. Нақты іске асыру талаптары уақытқа байланысты сол немесе өзге параметрлерді әртүрлі қосымшаларда басымдылық функциясын жүктеуі мүмкін. Кейбір жағдайларда уақытқа байланысты бір параметрді ғана қолданған мақсатты болуы мүмкін (мысалы, уақыт белгісін және кезекті сандар). Параметрлерді таңдауға қатысты бөлшектер *ҚР СТ ИСО/МЭК 9798* стандартының осы бөлімін қолдану саласынан тыс.

Б.1 Уақыт белгісі

Уақыт белгісін қолданатын тетіктер үміткер мен верификаторды логикалық байланыстыратын уақытты санаудың жалпы жүйесіне сүйенеді. Ұсынылатын уақыт жүйесі – үйлестірілген дүниежүзілік уақыт (UTC). Верификатор қабылдау терезесі ретінде белгіленген өлшемнің кейбір уақыт шектері қолданылады. Верификатор тексерілетін алынған маркердегі уақыт белгісі мен маркерді алу барысында верификатормен саналған уақыт арасындағы айырмашылықты есептеп, уақыттылықты тексереді. Егер уақыт айырмашылығы бос уақыт шегінде болса, онда мәлімет қабылданады. Бірегейлік ағымдық бос уақыт шегінде барлық мәліметтерді тіркеумен және осы бос уақыт ішінде қайталанған және кезекті ұқсас мәліметтерді қайтарумен тексерілуі мүмкін.

Ақпараттармен алмасатын мәндер сағатын синхрондауға кепілдік беру үшін белгілі механизмдер қолданылуы тиіс. Сондай-ақ, сағаттарды синхрондау дәлдігі қайта жіберу арқылы алмасу ықтималдығын мүмкіндігінше төмен жасау үшін жеткілікті жоғары болу керек. Сонымен қатар уақыт белгісін тексерумен және әсіресе, екі мәннің жүйелік сағаттармен ақпараттық алмасу процесіне қатысуымен байланысты барлық ақпараттың бұзылудан сенімді қорғалғандығына кепілдік қамтамасыз етілуі тиіс.

Уақыт белгісін қолданатын тетіктер мәжбүрлі іркілістерді анықтауға мүмкіндік береді.

Б.2 Кезекті сандар

Бірегейлік кезекті сандарды қолдану арқылы тексерілуі мүмкін, себебі олар верификаторға мәліметтердің қайта жіберілуіне мүмкіндік береді. Үміткер және верификатор күні бұрын ерекше түрде мәліметтерді нөмірлеу саясаты туралы шарттасады. Жалпы идея нақты нөмірленген мәлімет кездейсоқ уақыт аралығында ғана (немесе белгіленген уақыт ішінде) қабылдануы мүмкін. Верификатор алған әрбір мәліметпен берілген нөмір келісілген нөмірлеу саясатына сәйкесімділікке тексеріледі. Егер онымен ілесетін кезекті саны келісілген саясатқа сәйкес келмесе, мәлімет кейінге қалдырылады.

Кезекті сандарды қолдану қосымша тізімді құрастыруды талап етуі мүмкін. Үміткер қолданылған кезекті сандарды және\немесе кезекті қолдануға мүмкін болатын кезекті сандарды құрайтын жазбаларды қамтамасыз етуі тиіс. Үміткер байланысуға болатын барлық әлеуетті верификатор үшін жазбаларды жүргізуі тиіс. Сәйкесінше верификатор барлық әлеуетті үміткерлерге сәйкес келетін жазбаларды қамтамасыз етуі тиіс. Сонымен қатар қалыпты кезектілікті бұзатын жағдайдағы (жүйенің істен шығуы сияқты жағдайдағы) кезекті санды қалпына келтіретін және\немесе түсіретін ерекше процедураларды талап етуі мүмкін.

Кезекті сандарды қолдану верификатор мәжбүрлі іркілістерді анықтауға қабілетті болатын үміткермен кепілдік берілмейді. Егер мәлімет жіберуші мәлімет жіберу мен күтілетін жауапты алу арасындағы уақыт аралығын өлшейтін және іркіліс белгіленген уақыт аралығынан көп болған жағдайда одан бас тартатын болса, екі немесе бірнеше мәліметтерді қолданатын тетіктер үшін мәжбүрлі іркілістер анықталуы мүмкін.

Б.3 Кездейсоқ сандар

ҚР СТ ИСО/МЭК 9798 стандарттың кезекті бөлімдерінде көрсетілген тетіктерде қолданылатын кездейсоқ сандар қайталау немесе ендірмелер көмегімен шабуылдарды тоқтатады. Сондықтан *ҚР СТ ИСО/МЭК 9798* стандартында қолданылатын барлық кездейсоқ сандар оларды бір кілтпен қолдану барысында қайталау ықтималдығы және үшінші тараппен белгіленген мәнді болжау ықтималдығы төмен болу үшін жеткілікті үлкен ауқымнан таңдап алыну керек. *ҚР СТ ИСО/МЭК 9798* стандартының контекстінде "кездейсоқ сандар" термині осы талаптарды қанағаттандыратын жалған кездейсоқ сандарды қамтиды.

Қайталау немесе ендірмелер көмегімен шабуылдарды болдырмау үшін верификатор үміткерге жіберілетін кездейсоқ санды жібереді, ал үміткер алынған кездейсоқ санды қайтарылатын маркердің қорғалатын бөліміне қосу арқылы жауап береді. (Әдетте осы процедура қоңырауға жауап беру болып саналады.) Осы процедура нақты кездейсоқ санды құрайтын екі мәліметті қосады. Егер осы бір кездейсоқ сан верификатормен қайта қолданылатын болса, сәйкестендіру кезінде түпнұсқаны жазатын үшінші тарап жазылған маркерді верификаторға жібереді және өзінің түпнұсқалығын үміткер ретінде жалған растай алады. Мұндай бұзушылықтарды алдын алу үшін кездейсоқ сандар жоғары деңгейде қайталанбау керек.

Верификатор мәжбүрлі тоқтатуды анықтай алатын қабілетіне Үміткермен қолданылатын кездейсоқ сандар кепілдік бермейді.

В қосымшасы
(анықтамалық)
СЕРТИФИКАТТАР

ҚР СТ ИСО/МЭК 9798 стандартының келесі бөлімдерінде ашық кілт сертификаттары (сертификаттар) ашық кілттердің түпнұсқалығына кепілдік беру үшін қолданылуы мүмкін. Бұл жағдайда сертификат мәннің ерекше сәйкестендіргішін және ашық кілтті құрайтын мәннің кілті туралы жалпыға мүмкін ақпаратты қамтиды. Сертификат сертификаттау орталығы, мәні және ашық кілттің қолданылу мерзімі, онымен байланысты жабық кілттің қолданылу мерзімі немесе алгоритмдер тетігінде қолданылған идентификатор сияқты ашық кілт туралы мазмұндалған кілт жайында жалпыға жарияланатын ақпаратқа енгізілген басқа да мәліметтерді қамтуы мүмкін. Сенімді үшінші тараппен қол қойылған кілт туралы жалпыға жарияланатын ақпаратты қамтиды.

Сертификатты тексеру сенімді үшінші тараптың қолтаңбасын растауды және егер сертификаттың қолданылуымен, мысалы, оны жоюмен немесе қолдану мерзімімен байланысты басқа шарттарды тексеруді қарастырады.

Сертификаттар ашық кілттердің түпнұсқалығына кепілдік беретін дара амал болып табылады. Мәннің басқа құралдарды қолдану кезінде басқа мәндердің жалпыға мүмкін кілттерін алуына мүмкіндік болу үшін *ҚР СТ ИСО/МЭК 9798* стандартының келесі бөлімдерінде мазмұндалған барлық тетіктерде сертификаттарды қолдану міндетті емес. Ашық кілттердің түпнұсқалығына кепілдік беретін басқа әдістер ИСО/МЭК 14888-2 стандартында анықталған сұлбаларға ұқсас қолтаңбалардың түпнұсқалығын тексеруге негізделген сұлбаларды қолданады.

Қосымша
(анықтамалық)

Библиография

[1] ИСО/МЭК 11770-3-1999 *Ақпараттық технология. Қорғау әдістері. Кілттерді басқару. 3 бөлім. Асимметриялық әдістерді қолданатын тетіктер*
[2] ИСО/МЭК *Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері мен құралдары. Бас тартпаушылық*

ӘОЖ 681.324:006.354 **МСЖ 35.040**

Түйінді сөздер: деректерді өңдеу, ақпараттық алмасу, ақпараттарды қорғау, қорғау әдістері және құралдары, сәйкестендіру, мәліметтерді сәйкестендіруші кодтары, модельдер.

Ескертулер үшін

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология

МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ

Механизмы аутентификации
Часть 1
Общие положения

СТ РК ИСО/МЭК 9798-1-2008
(ИСО/МЭК 9798-1:1997
«Информационная технология. Методы и средства обеспечения безопасности. Механизмы аутентификации
Часть 1
Общие положения, 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 9798-1:1997 «Информационная технология. Методы и средства обеспечения безопасности. Механизмы аутентификации. Часть 1. Общие положения» («Information technology. Security techniques. Entity authentication. Part 1. General»), IDT, с дополнительными требованиями, отражающими потребности экономики Республики Казахстан, которые выделены курсивом.

4 СРОК ПЕРВОЙ ПРОВЕРКИ 2013 год
ПЕРИОДИЧНОСТЬ ПРОВЕРКИ 5 лет

5 ВВЕДЕН ВПЕРВЫЕ

Содержание

Введение

СТ РК ИСО/МЭК 9798-2008 под общим названием *"Информационные технологии. Методы и средства обеспечения безопасности. Механизмы аутентификации"* состоит из следующих частей:

– *Часть 1. Общие положения.*

– *Часть 2. Механизмы с применением алгоритмов симметричного шифрования.*

– *Часть 3. Механизмы с применением методов цифровой подписи.*

Международный стандарт ИСО/МЭК 9798-2008 кроме названных частей включает следующие:

– *Часть 4. Механизмы, использующие криптографическую проверочную функцию.*

– *Часть 5. Механизмы с использованием асимметричных методов с нулевым знанием.*

В международный стандарт могут войти и другие части по мере их создания.

Приложения настоящего стандарта справочные.

ГОСУДАРСТВЕННЫЙ СТАНДАРТ РЕСПУБЛИКИ КАЗАХСТАН

Информационная технология
МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ
МЕХАНИЗМЫ АУТЕНТИФИКАЦИИ
Часть 1
Общие положения

Дата введения 2008.07.01

1 Область применения

Настоящий стандарт устанавливает модель аутентификации и общие требования и ограничения к механизмам безопасности, используемым для аутентификации сущностей. Эти механизмы используются для подтверждения того, что сущность является именно той, за которую себя выдает. Сущность, подлежащая аутентификации, доказывает свою подлинность, демонстрируя знание какой-либо секретной информации. Механизмы определяются как процессы обмена информацией между сущностями, а также, при необходимости, как процессы обмена информацией с доверенной третьей стороной.

Подробно механизмы безопасности, включая содержимое аутентификационной информации, рассмотрены в последующих частях настоящего стандарта.

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.

Ряд механизмов, устанавливаемых в последующих частях *СТ РК ИСО/МЭК 9798-2008* может быть использован при реализации сервисов обеспечения неотказуемости (non-repudiation), механизмы которых определены в стандарте ИСО/МЭК 13888-2008 [2]. Спецификация таких сервисов лежит вне области применения *СТ РК ИСО/МЭК 9798-2008*.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие стандарты:

СТ РК ИСО/МЭК 10181-1-2008 Информационная технология. Взаимодействие открытых систем. Основы безопасности для открытых систем. Часть1.Обзор.

СТ РК ИСО/МЭК 10181-2-2008 Информационная технология. Взаимодействие открытых систем. Основы безопасности для открытых систем. Часть 2. Основы аутентификации

СТ РК ИСО/МЭК 11770-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Управление ключами. Часть 2. Механизмы с использованием симметричных методов.

СТ РК ИСО/МЭК 13888-2-2008 Информационная технология. Методы и средства обеспечения безопасности. Неотказуемость. Часть 2. Механизмы, использующие симметричные методы.

СТ РК ИСО/МЭК 14888-2-2006 Информационная технология. Методы защиты информации. Цифровые подписи с приложением. Часть 2. Механизмы, основанные на идентичности.

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

3 Термины и определения

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

3.1 Асимметричный криптографический метод (asymmetric cryptographic technique) - криптографический метод, который использует два взаимосвязанных преобразования: открытое преобразование (определяемое открытым ключом) и секретное преобразование (определяемое секретным ключом). Данная пара преобразований обладает свойством, благодаря которому, используя только открытое преобразование блока данных, неосуществимо вычислительным путем получить секретное преобразование того же блока данных.

Примечание. Система, основанная на асимметричных криптографических методах, может быть системой шифрования, системой подписи, комбинированной системой шифрования и подписи, либо системой распределения ключей. В асимметричных криптографических методах предусмотрены четыре элементарных преобразования: подписывание и проверка подписи для систем подписи, шифрование и расшифрование для систем шифрования. Секретность преобразований подписывания и расшифрования должна сохраняться применяющими их сущностями, тогда как соответствующие преобразования проверки подписи и расшифрования являются открытыми. Существуют асимметричные криптосистемы (например, RSA), в которых все четыре элементарные функции могут быть реализованы только двумя преобразованиями: одного секретного преобразования достаточно и для подписи, и для расшифрования сообщения, а одного открытого преобразования достаточно и для проверки подписи и для шифрования сообщения. Однако, поскольку подобный пример не является общим случаем, в *СТ РК ИСО/МЭК 9798-2008* все четыре элементарных преобразования и соответствующие ключи считаются различными.

3.**2 Система асимметричного шифрования** (asymmetric cryptographic system) - система, основанная на асимметричных криптографических методах, в которой открытое преобразование используется для шифрования и секретное преобразование используется для расшифрования.

3.3 Пара асимметричных ключей (asymmetric key pair) - пара взаимосвязанных ключей, где секретный ключ определяет секретное преобразование, а открытый ключ определяет открытое преобразование.

3.4 Система асимметричной подписи (asymmetric signature system) - система, основанная на методах асимметричной криптографии, которые используют секретное преобразование для подписывания, а открытое – для проверки подлинности подписи.

3.5 Вызов (challenge) - элемент данных, выбранный произвольно и посланный верификатором претенденту, который используется претендентом в совокупности с известной претенденту секретной информацией для формирования ответа, посылаемого верификатору.

3.6 Зашифрованный текст (ciphertext) - данные, преобразованные по алгоритму шифрования в зашифрованный вид для сокрытия своего информационного содержимого.

3.7 Криптографическая контрольная функция (cryptographic check function) - криптографическое преобразование, которое, получая на входе секретный ключ и произвольную строку, вычисляет криптографическое контрольное значение на выходе. Вычисление правильного контрольного значения без знания секретного ключа должно быть неосуществимо.

3.8 Расшифрование (decipherment) - преобразование, обратное соответствующему преобразованию шифрования.

3.9 Отличительный идентификатор (distinguishing identifier) - информация, которая однозначно определяет аутентифицируемую сущность.

3.10 Шифрование (encipherment) - (обратимое) преобразование данных криптографическим алгоритмом для получения зашифрованного текста, то есть для сокрытия информации, содержащейся в данных.

3.11 Аутентификация сущности (entity authentication) - подтверждение того, что сущность является тем, что она заявляет.

3.12 Атака вставками (interleaving attack) - разновидность атаки с подменой, при которой используется информация, перехваченная из информационного обмена, осуществляющегося или осуществившихся ранее процессов аутентификации.

3.13 Ключ (key) - последовательность символов, которая управляет процессом криптографического преобразования (например, шифрованием, расшифрованием, вычислением криптографической контрольной функции, созданием подписи или проверкой подписи).

3.14 Взаимная аутентификация (mutual authentication) - аутентификация сущностей, при которой обеим сущностям предоставляется гарантия подлинности друг друга.

3.15 Открытый текст (plaintext) - незашифрованная информация.

3.16 Секретный ключ расшифрования (private decipherment key) - секретный ключ, который определяет секретное преобразование расшифрования.

3.17 Секретный ключ (private key) - ключ из пары асимметричных ключей сущности, который должен быть использован только этой сущностью.

Примечание. В случае асимметричной системы подписи секретный ключ определяет преобразование подписывания. В случае асимметричной системы шифрования секретный ключ определяет преобразование расшифрования.

3.18 Секретный ключ подписи (private signature key) - секретный ключ, который определяет секретное преобразование подписывания.

Примечание. Иногда упоминается как личный ключ подписи.

3.19 Открытый ключ шифрования (public encipherment key) - открытый ключ, который определяет открытое преобразование шифрования.

3.20 Открытый ключ (public key) - ключ из пары асимметричных ключей сущности, который может быть общеизвестным.

Примечание. В случае системы асимметричной подписи открытый ключ определяет преобразование проверки подписи. В случае системы асимметричного шифрования этот ключ определяет преобразование шифрования. Ключ, который «общеизвестен», не обязательно общедоступен. Ключ может быть доступен только членам заранее определенной группы.

3.21 Сертификат открытого ключа/сертификат (public key certificate/certificate) - информация об открытом ключе сущности, подписанная удостоверяющим центром, вследствие чего рассматривается как неподдельная (см. также Приложение В). Эквивалентным этому термину является термин «регистрационное свидетельство», применяемый в законодательстве Республики Казахстан.

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

3.23 Открытый ключ проверки подлинности (public verification key) - открытый ключ, который определяет открытое преобразование проверки подлинности.

3.24 Случайное число (random number) - зависящий от времени параметр, значение которого непредсказуемо (см. также Приложение Б).

3.25 Атака отражением (reflection attack) - разновидность атаки с подменой, при которой используется посылка ранее переданного сообщения назад его отправителю.

3.26 Атака повтором (replay attack) - разновидность атаки с подменой, которая использует ранее переданные сообщения.

3.27 Последовательное число (sequence number) - зависящий от времени параметр, значение которого выбирается из заданной последовательности, которая не содержит повторных значений в пределах определенного периода времени (см. также приложение Б).

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

3.29 Алгоритм симметричного шифрования (symmetric encipherment algorithm) - алгоритм шифрования, основанный на использовании одного и того же секретного ключа для преобразования как со стороны отправителя, так и со стороны получателя сообщения.

3.30 Метка времени (time stamp) - зависящий от времени параметр, который обозначает, в общем случае, момент времени (см. также Приложение Б).

3.31 Параметр, зависящий от времени (time variant parameter) - элемент данных, который используется для проверки того, что сообщение не является переданным вторично; используется в определении случайного числа, последовательного числа, а также метки времени (см. также Приложение Б).

3.32 Маркер (token) - сообщение, состоящее из полей данных, имеющих отношение к конкретному сеансу связи, которое содержит информацию, преобразованную с использованием криптографического метода.

3.33 Односторонняя аутентификация (unilateral authentication) - аутентификация сущности, при которой гарантия подлинности предоставляется другой сущности и обратное не имеет места.

4 Обозначения

В настоящем стандарте используются следующие обозначения:

A	Отличительный идентификатор сущности *A*.
B	Отличительный идентификатор сущности *B*.
TP	Отличительный идентификатор доверенной третьей стороны.

K_{XY}	Секретный ключ, известный сущностям X и Y; используется только в симметричных криптографических методах.
P_X	Открытый ключ проверки подлинности, связанный с сущностью X; используется только в асимметричных криптографических методах.
S_X	Секретный ключ подписи, связанный с сущностью X; используется только в асимметричных криптографических методах.
N_X	Последовательное число, предложенное сущностью X.
R_X	Случайное число, предложенное сущностью X.
T_X	Метка времени, предложенная сущностью X.
T_X N_X	Параметр, зависящий от времени, который был предложен сущностью X и является либо меткой времени T_X, либо последовательным числом N_X .
$Y\|\|Z$	Результат последовательного соединения элементов данных Y и Z в указанном порядке.
$eK(Z)$	Результат шифрования данных Z симметричным алгоритмом шифрования, использующим ключ K.
$dK(Z)$	Результат расшифрования данных Z симметричным алгоритмом шифрования, использующим ключ K.
$f_K(Z)$	Криптографическое контрольное значение, которое является результатом применения криптографической контрольной функции f, использующей в качестве входных параметров секретный ключ K и произвольную строку данных Z.
$CertX$	Сертификат, выданный доверенной третьей стороной сущности X.
$TokenXY$	Маркер, посланный от сущности X сущности Y.
TVP	Параметр, зависящий от времени.
$sS_X(Z)$	Подпись, полученная применением секретного преобразования подписывания к данным Z с использованием секретного ключа подписи S_X.

5 Модель аутентификации

Общая модель для механизмов аутентификации сущности показана на рисунке 1. Не обязательно присутствие всех сущностей и сторон обмена информацией в каждом конкретном механизме аутентификации.

Для механизмов аутентификации, подробно описываемых в других частях *СТ РК ИСО/МЭК 9798-2008*, при односторонней аутентификации сущность A рассматривается в роли претендента, а сущность B - в роли

верификатора. При взаимной аутентификации обе сущности, *A* и *B*, берут на себя функции как претендента, так и верификатора.

Для целей аутентификации сущности генерируют и обмениваются стандартизованными сообщениями, называемыми маркерами. Требуется обмен, по крайней мере, одним маркером при односторонней аутентификации и обмен, по крайней мере, двумя маркерами при взаимной аутентификации. Если для инициализации обмена данными процесса аутентификации должен быть послан вызов, то может потребоваться дополнительный проход. Также могут потребоваться дополнительные проходы, если в процесс аутентификационного обмена вовлечена доверенная третья сторона.

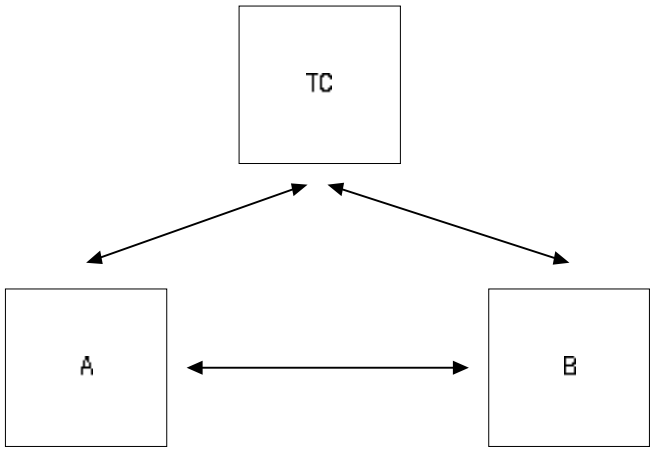


Рисунок 1. Модель аутентификации

На рисунке 1 стрелками обозначены возможные информационные потоки. Сущности *A* и *B* могут либо непосредственно взаимодействовать друг с другом, непосредственно взаимодействовать с доверенной третьей стороной ТС, опосредованно взаимодействовать с доверенной третьей стороной через *A* или *B* соответственно, либо использовать некоторую информацию, предоставленную доверенной третьей стороной.

Подробности механизмов аутентификации *СТ РК ИСО/МЭК 9798-2008* приведены в последующих частях стандарта.

6 Общие требования и ограничения

Чтобы одна сущность могла аутентифицировать другую, обе они должны использовать общий набор криптографических методов и параметров.

За все время существования ключа значения всех параметров, зависящих от времени, на которые распространяется действие ключа

(то есть, метки времени, последовательные и случайные числа), не должны повторяться, по крайней мере, с достаточно высокой вероятностью.

Предполагается, что в процессе использования механизма аутентификации, сущностям *A* и *B* известны заявленные, присущие только каждой из них, сведения друг о друге. Это может быть достигнуто включением идентификаторов в информацию, которой обмениваются эти две сущности, или это может быть очевидно из контекста применения механизма.

Подлинность сущности может быть установлена только на момент совершения аутентификационного обмена данными. Чтобы гарантировать подлинность данных, переданных позднее, процесс аутентификационного обмена должен использоваться в совокупности со средствами обеспечения информационной безопасности (например, в совокупности со средствами контроля целостности).

Приложение А
(справочное)
Использование текстовых полей

Маркеры, приведенные в следующих частях *СТ РК ИСО/МЭК 9798-2008*, содержат текстовые поля. Фактическое применение и взаимозависимость между различными текстовыми полями при конкретном проходе механизма аутентификации зависит от приложения.

Текстовые поля могут содержать дополнительные параметры, зависящие от времени. Например, в текстовое поле(я) маркера может быть включена метка времени, если в маркере уже используются последовательные числа. Если получатель сообщения удостоверится, что любая содержащаяся в сообщении метка времени находится в пределах предопределенного интервала, это позволит обнаруживать принудительные задержки (см. также приложение Б).

При наличии нескольких действующих ключей, идентификатор ключа может быть включен в текстовое поле в открытом тексте. Если в процессе аутентификации участвуют несколько доверенных третьих сторон, то текстовые поля могут использоваться для включения в запрос отличительного идентификатора доверенной третьей стороны.

Текстовые поля могут также использоваться для распределения ключей (см. *СТ РК ИСО/МЭК 11770-2-200*8 и [1].

Даже если какой-либо из механизмов, описанных в следующих частях *СТ РК ИСО/МЭК 9798-2008*, встроен в приложение, которое позволяет любому пользователю запустить процесс аутентификации путем использования дополнительного сообщения до начала работы механизма, это не исключает возможных попыток нарушения безопасности. Для противодействия подобным попыткам, при которых нарушитель может многократно использовать незаконно полученный маркер, могут использоваться текстовые поля с целью выявления сущностей, запрашивающих аутентификацию (см. *СТ РК ИСО/МЭК 10181-2-2008*).

Вышеперечисленные примеры не являются исчерпывающими.

Приложение Б
(справочное)
Параметры, зависящие от времени

Параметры, зависящие от времени, используются для проверки уникальности/своевременности. Они позволяют обнаруживать повторную посылку ранее переданных сообщений. Для этого аутентификационная информация должна изменяться от одного процесса к другому.

Некоторые типы параметров, зависящих от времени, могут позволять обнаружение «принудительных задержек» (задержек, добавленных в коммуникационную среду злоумышленником). В механизмах, использующих более одного прохода, принудительные задержки также могут быть обнаружены другими средствами (например, «счетчик тайм-аутов» используется для ограничения максимально допустимых интервалов по времени между отдельными сообщениями).

В последующих частях используются три типа параметров, зависящих от времени: метки времени, последовательные числа и случайные числа. Требования конкретной реализации могут делать предпочтительными те или иные параметры, зависящие от времени, в различных приложениях. В некоторых случаях может быть целесообразно использование более одного параметра, зависящего от времени, (например, и метки времени, и последовательные числа). Детали относительно выбора параметров находятся вне области применения настоящего стандарта.

Б.1 Метки времени

Механизмы, использующие метки времени, опираются на общую систему отсчета времени, которая логически связывает претендента и верификатора. Рекомендуемое системное время - скоординированное всемирное время (UTC). Верификатор использует в качестве приемного окна некоторые временные рамки установленного размера. Верификатор проверяет своевременность, вычисляя разность между меткой времени в проверяемом полученном маркере и времени, считанного верификатором при получении маркера. Если разница по времени находится в пределах окна, то сообщение принимается. Уникальность может быть проверена регистрацией всех сообщений в пределах текущего окна, и отклонением повторных и последующих поступлений идентичных сообщений в пределах данного окна.

Для гарантии синхронизации часов сущностей, обменивающихся информацией, должны применяться определенные механизмы. Более того, точность синхронизации часов должна быть достаточно высокой, чтобы сделать вероятность подмены путем повторной посылки приемлемо малой. Следует также обеспечить гарантии того, что вся информация, связанная с проверками меток времени и, в особенности, с системными часами двух участвующих в процессе информационного обмена сущностей, надежно защищена от фальсификации.

Механизмы, использующие метки времени, позволяют обнаруживать принудительные задержки.

Б.2 Последовательные числа

Уникальность может проверяться посредством использования последовательных чисел, поскольку они позволяют верификатору обнаружить повторную передачу сообщений. Претендент и верификатор заранее особым образом договариваются

относительно политики нумерации сообщений. Общая идея должна быть такова, что сообщение с конкретным номером будет принято только однажды (или только однажды в пределах оговоренного периода времени). Номер, переданный с каждым сообщением, которое получил верификатор, проверяется на соответствие согласованной политике нумерации. Сообщение отклоняется, если сопровождающее его последовательное число не соответствует согласованной политике.

Применение последовательных чисел может потребовать ведения дополнительного списка. Претендент должен поддерживать записи, содержащие уже использованные последовательные числа, и/или последовательные числа, которые остаются допустимыми для последующего применения. Претендент должен вести такие записи для всех потенциальных верификаторов, с которыми возможна связь. Аналогично верификатор должен поддерживать такие записи, соответствующие всем потенциальным претендентам. Могут также требоваться особые процедуры для восстановления и/или сброса последовательного числа в ситуации (такой, как отказ системы), которая нарушает нормальную последовательность.

Применение последовательных чисел претендентом не гарантирует, что верификатор будет способен обнаружить принудительные задержки. Для механизмов, использующих два или более сообщений, принудительные задержки могут быть обнаружены, если отправитель сообщения измеряет временной интервал между передачей сообщения и получением ожидаемого ответа и отклоняет его, если задержка окажется больше, чем предопределенный временной интервал.

Б.3 Случайные числа

Случайные числа, используемые в механизмах, указанных в последующих частях, предотвращают атаки повтором или вставками. Поэтому требуется, чтобы все случайные числа, используемые в *СТ РК ИСО/МЭК 9798-2008*, были выбраны из достаточно большого диапазона так, чтобы при их использовании с тем же самым секретным ключом вероятность повторения была достаточно малой, и чтобы вероятность предсказания установленного значения третьей стороной была также достаточно малой. В контексте *СТ РК ИСО/МЭК 9798-2008* термин "случайные числа" также включает псевдослучайные числа, удовлетворяющие тем же самым требованиям.

Чтобы предотвратить атаки повтором или вставками, верификатор генерирует случайное число, которое посылается претенденту, а претендент отвечает включением полученного случайного числа в защищенную часть возвращаемого маркера (обычно эта процедура называется ответ на вызов.) Эта процедура соединяет два сообщения, содержащих конкретное случайное число. Если то же самое случайное число используется верификатором снова, третья сторона, которая сделала запись оригинального обмена при аутентификации, может послать записанный маркер верификатору и ложно подтвердить свою подлинность как претендента. Для предотвращения таких нарушений необходима высокая вероятность неповторяемости случайных чисел.

Применение случайных чисел претендентом не гарантирует, что верификатор будет способен обнаружить принудительные задержки.

Приложение В
(справочное)

Сертификаты

В следующих частях *СТ РК ИСО/МЭК 9798-2008* сертификаты открытого ключа (сертификаты) могут использоваться для гарантии подлинности открытых ключей. В этом случае сертификат содержит общедоступную информацию о ключе сущности, которая состоит, по крайней мере, из отличительного идентификатора сущности и открытого ключа. Сертификат может содержать прочие сведения, включенные в общедоступную информацию о ключе, где речь идет об органе по подтверждению соответствия, сущности и открытом ключе, такие как: срок действия открытого ключа, срок действия связанного с ним секретного ключа или идентификатор использованных в механизме алгоритмов. Сертификат состоит из общедоступной информации о ключе, подписанной доверенной третьей стороной.

Проверка сертификата заключается в подтверждении подписи доверенной третьей стороны и проверки, если требуется, других условий, связанных с действием сертификата, например, его аннулирования или срока действия.

Сертификаты не являются единственным способом гарантировать подлинность открытых ключей. Чтобы позволить сущности получать общедоступные ключи других сущностей при применении других средств, не обязательно использование сертификатов во всех механизмах, описываемых в следующих частях. Другие методы гарантии подлинности открытых ключей используют схемы, основанные на проверке подлинности подписи, аналогичные схемам, определенным в *СТ РК ИСО/МЭК 14888-2-2008*.

Приложение

(справочное)

Библиография

[1] ИСО/МЭК 11770-3-1999 Информационная технология. Методы защиты. Управление ключами. Часть 3. Механизмы, использующие асимметричные методы.

[2] ИСО/МЭК Информационная технология. Методы и средства обеспечения безопасности. Неотказуемость.

УДК 681.324:006.354 **МКС 35.040**

Ключевые слова: обработка данных, информационный обмен, защита информации, методы и средства защиты, аутентификация, коды аутентификации сообщений, модели.

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