



Правила на издавачот на сертификати

Верзија: 1.2

Датум: 29.05.2006

КИБС АД Скопје

© 2003 КИБС АД Скопје, сите права задржани

<http://ca.kibs.com.mk>



Содржина

1.	Општи одредби	7
1.1	КИБС	7
1.2	Електронски сертификати	7
1.3	Примена на правилата	8
1.4	Селектирање на сертификациона услуга	9
1.5	Идентификација на документот	9
1.6	КИБС Регистрациона канцеларија	9
1.7	КИБС Локални регистрациони канцеларии	10
1.8	Претплатници	10
1.9	Засегнати страни	10
1.10	Употреба на сертификат	11
1.11	Политика на администрација	11
1.12	Одговорност за објавување и сместување	11
2.	Технички аспекти	12
2.1	Профили на КИБС сертификатите	12
2.2	Коренски сертификат на КИБС	13
2.3	Оперативни сертификати	14
2.4	Сертификати на крајните корисници	16
2.4.1	КИБС Верба	16
2.4.2	КИБС Верба Про	17
2.4.3	КИБС Верба Сервер	18
2.5	Управување со електронски сертификати	19
2.6	КИБС директориуми и складиште	19
2.7	Идентификација на претплатникот	20
2.8	Доверливи системи	20
2.9	Ограничувања на опсегот на КИБС сертификатите	20
2.10	Проширувања и именување	20
2.10.1	Проширувања на електронските сертификати	20
2.10.2	Повикување на референца за проширувања и подобро именување	20
2.11	Процес на генерирање на приватен клуч	21
2.11.1	Употреба на приватниот клуч на КИБС	21
2.11.2	Тип на приватниот клуч на КИБС	21
2.11.3	Генерирање на приватниот клуч на КИБС	21
2.11.4	Уреди за генерирање на клучот	21
2.11.5	Контроли на генерирањето на клучот	21



2.11.6	Чување на приватниот клуч	21
2.11.7	Поделба на тајност	22
2.11.8	Безбедно чување на токен	22
2.12	Контроли на физичката безбедност	22
2.13	Процедурални котроли	23
2.14	Контрола на безбедната мрежа	23
3.	Организација	25
3.1	Инфраструктура на КИБС	25
3.2	Усогласување со овие ПИС	25
3.3	Престанување на дејноста на ИС	25
3.4	Форма на записите	25
3.5	Чување на записите	25
3.6	Логови за основните функции	26
3.7	Контрола на основните функции	26
3.8	Планови за настанување на непредвидени ситуации и нивно враќање во првобитна состојба	27
3.9	Компромитување и враќање во првобитна состојба	27
3.10	Расположивост на КИБС сертификатите	27
3.11	Објавување на информации за издадени сертификати	27
3.12	Доверливи информации	27
3.13	Безбедност на капацитетите	28
3.14	Управување со кадрите и постапки	28
3.14.1	Доверливи информации	28
3.15	Безбедносни контроли на персоналот	28
3.15.1	Квалификации, искуства и образложенија (разјаснувања)	28
3.15.2	Проверка на биографските податоци	29
3.15.3	Потребна обука и процедури	29
3.15.4	Периодични обуки и процедури	29
3.15.5	Казни против вработените	29
3.15.6	Контроли на независни изведувачи	29
3.15.7	Документација за обука и повторна обука	29
3.16	Објавување на информации	29
4.	Постапки и процедури	30
4.1	Барање на сертификат	30
4.1.1	Овластување	30
4.1.2	Генерирање на пар клучеви	30
4.1.3	Заштита на парот клучеви	30
4.1.4	Користење на безбедни средства и продукти	30
4.1.5	Доделување одговорности за приватни клучеви	30



4.2	Информации за валидација на барањата за сертификат.....	31
4.2.1	Именување	31
4.2.2	Иницијална валидација на идентитетот	31
4.2.3	Информации за аплицирање на деловни субјекти.....	31
4.2.4	Информации добиени од индивидуален барател	32
4.3	Валидација на барањата за сертификат	32
4.3.1	Лично присуство.....	32
4.3.2	Потврда од трето лице за информациите за деловниот субјект	32
4.3.3	Потврда за името на доменот и доделување на сериски број.....	33
4.4	Време за потврда на поднесените податоци	33
4.5	Одобрување и одбивање на барањата за сертификати.....	33
4.6	Издавање на сертификат и согласност на претплатникот.....	33
4.7	Валидација на сертификат.....	33
4.8	Прифаќање на сертификатот од страна на претплатникот	34
4.9	Објавување на издадените сертификати	34
4.10	Верификација на електронските потписи.....	34
4.11	Потпирање на електронските потписи.....	34
4.12	Суспендирање и поништување на сертификат	34
4.12.1	Ефект од отстранување или поништување.....	35
4.12.2	Известување пред истекување на периодот на важење	35
4.13	Обновување	35
5.	Законски услови на издавање	36
5.1	Претставување на КИБС.....	36
5.2	Податоци со повикување на референца во електронскиот сертификат	36
5.3	Показатели за повикување на референца	36
5.4	Изложување на ограничена одговорност, изјави за гаранција.....	36
5.5	Објавување на податоците од сертификатите	36
5.6	Обврска за следење на поднесените информации.....	37
5.7	Објавување на информациите	37
5.8	Интервенирање со КИБС имплементацијата	37
5.9	Стандарди	37
5.10	Ограничувања на КИБС партнерските врски	37
5.11	Ограничување на одговорноста на КИБС за КИБС партнерите.....	37
5.12	Одговорност на коренскиот потпис	38
5.13	Избор на криптографски методи	38
5.14	Потпирање на непотврдени електронски потписи.....	38
5.15	Издадени но неприфатени сертификати.....	38
5.16	Одбивање за издавање на сертификат	38



5.17	Обврски на претплатникот	38
5.18	Претставување од страна на претплатникот по прифаќање на сертификат	39
5.19	Обештетување од претплатникот	40
5.20	Обврски на КИБС РК	41
5.21	Обврски на засегнатата страна	41
5.22	Законитост на информациите	41
5.23	Користење на застапници	41
5.24	Одговорност на претплатникот кон засегнатите страни	41
5.25	Обврска за надзор над застапниците	41
5.26	Услови за употреба на КИБС складиштето и веб сајтот	42
5.27	Потпирање на сопствен ризик	42
5.28	Точност на информациите	42
5.29	Непочитување	42
5.30	Обврски на КИБС	42
5.31	Способност за посебна цел	43
5.32	Други гаранции	43
5.33	Неверифицирана информација на претплатник	43
5.34	Исклучување од одредени елементи на штети	43
5.35	Ограничувања на штета и загуба	44
5.36	Спротивставеност на правила	44
5.37	Права на интелектуална сопственост	44
5.38	Прекршителен и друг штетен материјал	44
5.39	Право на сопственост	45
5.40	Важечка регулатива	45
5.41	Судска надлежност	45
5.42	Решавање на спор	45
5.43	Наследници и назначени	45
5.44	Ништавност	46
5.45	Толкување	46
5.46	Отстапување	46
5.47	Известување	46
5.48	Надоместоци	47
5.49	Обврски по раскинување на договорот	47
6.	Општи процедури за издавање	48
6.1	Општо	48
6.2	Индивидуи и организации	48
6.3	Содржина	48
6.4	Поднесување на документи за идентификавање на барателот	49



6.5	Време на потврдување на поднесените податоци	49
6.6	Процедура за издавање	49
6.7	Осигурување	50
6.8	Процедури за КИБС ВЕРБА сертификатите	50
6.9	Процедури за КИБС Верба Про сертификатите	51
6.10	Процедури за КИБС Верба Сервер сертификатите	52
7.	Дефиниции	54



1. Општи одредби

Во овој дел се дава преглед на услугите за сертифицирање.

1.1 КИБС

КИБС е издавач на сертификати (ИС) кој издава високо квалитетни и високо доверливи електронски сертификати на физички и правни лица вклучувајќи субјекти од приватниот и јавниот сектор. КИБС работи како ИС во Република Македонија. Иако основната употреба на КИБС сертификатите е да се користат за трансакции при финансиски услуги во Република Македонија, КИБС не ја исклучува можноста и од други потенцијални употреби, во области во кои тие можат да се применуваат, и во било кои други земји.

ИС е деловен субјект кој издава електронски сертификати кои се употребуваат во јавниот домен, во деловната комуникација или за трансакции.

ИС креира политика за издавање на одредени видови или класи на сертификати. Во тој поглед, ИС е исто така авторитет за политиката на издавање на своите сертификати.

Работењето на ИС е под надзор и акредитација, согласно со одредбите од Законот за податоци во електронски облик и електронски потпис („Службен весник на РМ“ бр. 34/2001, 6/2002) и согласно сите подзаконски акти донесени врз основа на овој закон.

За да им се обезбеди известување или да им се даде на знаење на засегнатите страни за поништените и/или одложените сертификати, потребно е соодветно објавување во Регистар на поништени сертификати. ИС води таков регистар.

Врвот на коренот (Top Root) на КИБС ИС е дел од признатиот ‘Top Root’ издавач (познат како Trust anchor) кој е нашироко вграден во апликациите кои подржуваат сертификати. Во овој случај КИБС е дел од хиерархијата на коренот на GlobalSign.

Во посебниот домен на одговорност на ИС се вклучува целокупното управување со животниот циклус на сертификатот опфаќајќи:

- издавање
- суспендирање/активирање
- поништување
- обновување
- верификација на статус (сервис за статусот на сертификатот)
- објавува директориум на издадени сертификати

1.2 Електронски сертификати

Електронскиот сертификат му овозможува на лицето кое учествува во електронска трансакција да го докаже својот идентитет на другите учесници во таа трансакција. Електронските сертификати се користат како електронски еквивалент на лична карта.

КИБС издава персонални електронски сертификати и серверски електронски сертификати:

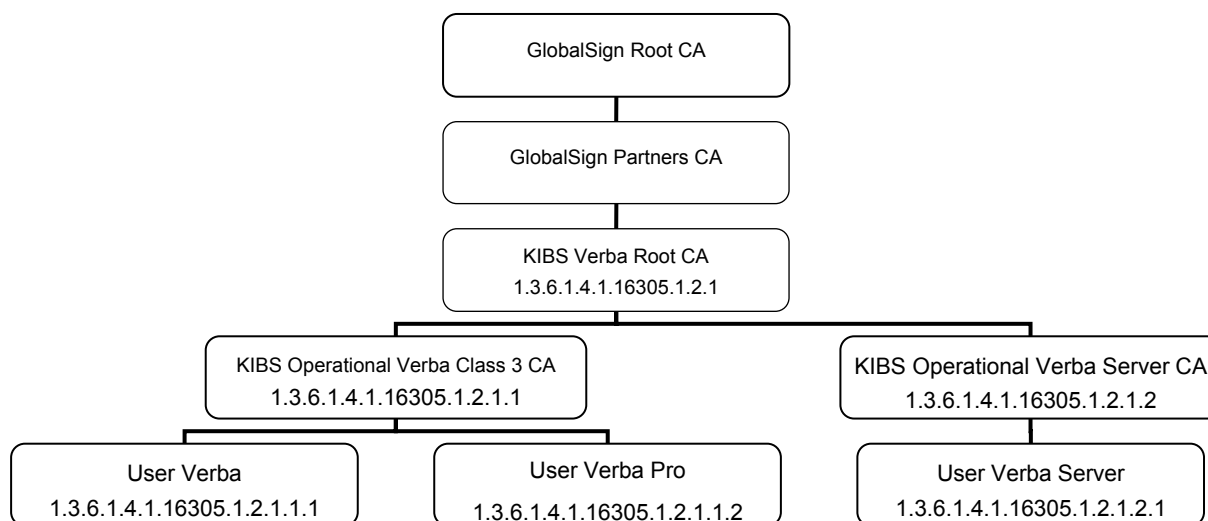
- **Верба**, персонален сертификат за автентикација и потпишување
- **Верба Про**, персонален сертификат за автентикација и потпишување при вршење на професионална дејност и
- **Верба Сервер**, сертификат за автентикација на сервер.

КИБС нуди електронски сертификати со ниво на сигурност од трета класа, кое бара лична идентификација на физичкото лице кое е барател на сертификат. КИБС ги следи општо прифатените нивоа на сигурност за електронско сертифицирање.

1.3 Примена на правилата

PKI (Public Key Infrastructure) е акроним за систем на криптографија со јавен клуч (Public Key cryptography) комбиниран со инфраструктура (Infrastructure) која е така дизајнирана да обезбеди ниво на безбедност за комуницирање и складирање на електронски информации доволно за да ја оправда довербата во таквите информации од страна на претпријатијата, потрошувачите, владите и судовите. PKI е технологија која се користи за доставување на електронски потписи одредена со Европската Директива 99/93/ЕС *Заедничка рамка за електронски потпис*. (European Directive 99/93/EC *On a common framework for electronic signature*).

Правилата на издавачот на сертификати (ПИС) уредуваат постапки кои ги користи ИС при издавање на сертификатите. ПИС го опфаќаат целокупното работење на ИС за тоа како ги става на располагање неговите сервиси. Овие ПИС се користат во доменот на ИС, исклучувајќи било кој друг. Овие ПИС имаат за цел да го ограничат доменот за обезбедување на PKI сервиси само за претплатниците и засегнатите страни во доменот на ИС. Овие ПИС ја скицираат врската помеѓу КИБС ИС и другите ИС во GlobalSign хиерархијата.



Слика 1. Хиерархија на клучевите на издавачот на сертификати КИБС



Овие ПИС се применуваат на ИС, Регистрационата канцеларија (РК) и Локалните регистрациони канцеларии (ЛРК) во доменот на КИБС ИС. Овие ПИС ги уредуваат улогите, одговорностите и постапките на ИС, РК и ЛРК. Овие ПИС се применуваат исто така, и за сите претплатници и засегнати страни кои користат или се потпираат на КИБС сертификатите. Овие ПИС се применуваат и на други ентитети кои одржуваат организациона врска со ИС, како на пример за супервизија, акредитација во рамките на Република Македонија и во меѓународни рамки. Конечно, овие ПИС потврдуваат одредени услови поставени во Политиката за сертификати на GlobalSign објавени на www.globalsign.net/repository во врска со коренското потпишување и со ограничувањата на одговорноста.

Одредбите од овие ПИС во поглед на постапките, нивото на услуги и одговорностите ги обврзуваат сите инволвирани страни и тоа: ИС, РК и ЛРА, претплатниците и засегнатите страни.

Овие ПИС го уредуваат издавањето на сертификати на ИС во текот на периодот на вршење на оваа дејност. Период на вршење на дејност е времето во кое одреден ИС може да издава сертификати.

Овие ПИС се ставени на располагање во складиштето на ИС под <http://ca.kibs.com.mk/repository>.

Одржувањето на овие ПИС се под единствена одговорност на КИБС, согласно Законот во Република Македонија. Овие ПИС ја опишуваат политиката за барањата за издавање, управување и употреба на сертификатите во доменот на ИС.

ИС ги прифаќа коментарите во врска со ПИС адресирани на:

КИБС АД, Скопје

К.Ј.Питу 1,

1000 Скопје, Република Македонија

URL: <http://ca.kibs.com.mk>

email: ca-pravila@kibs.com.mk

1.4 Селектирање на сертификационата услуга

КИБС нуди неколку видови на сертификати. Иако КИБС нуди сертификати, тој не гарантира дека одбраниот модел е потполно сигурен. Пред да побараат сертификат, претплатниците се залагаат соодветно да ги проучат своите потреби за нивната специфична примена и да употребат сопствена проценка за безбедни комуникации.

1.5 Идентификација на документот

КИБС ИС применува OID за идентификување на овие ПИС: 1.3.6.1.4.1.16305.1.2.2.1.0

kibs-verba-cps-v1.0 OBJECT IDENTIFIER:= {iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1) KIBS(16305) PKI (1) VerbaCA(2) CPS(2) version(1) revision(0) }

1.6 КИБС Регистрационата канцеларија

КИБС ги става на располагање своите услуги на претплатниците преку одредена Регистрационата канцеларија (РК). КИБС РК:

- прифаќа, проценува, одобрува или одбива регистрација на барањата за сертификат,
- ги регистрира претплатниците на услугите на КИБС за сертифицирање,
- ги надгледува сите фази на идентификација на претплатниците, уредени од страна на КИБС, во согласност со типот на сертификатот кој го издава КИБС,
- користи званични, заверени документи и други документи заради оценка на барањето на претплатникот,
- ги проследува одобрувањата на барањата до ИС да издаде сертификат.
- го започнува процесот на поништување на сертификат и бара поништување на сертификат,
- врши надзор на ЛРК-и.

1.7 КИБС Локални регистрациони канцеларии

Преку мрежата на Локалните регистрациони канцеларии (ЛРК) КИБС ги става на располагање своите услуги на претплатниците на локално ниво. КИБС ЛРК:

- прифаќа, проценува, одобрува или одбива регистрација на барањата за сертификат,
- ги регистрира претплатниците на услугите на КИБС за сертифицирање,
- користи званични, заверени документи и други документи заради оценка на барањето на претплатникот,
- ги проследува документите од барањата до КИБС РК за да побара издавање на сертификат,
- го започнува процесот на поништување на сертификат и бара поништување на КИБС сертификат.

КИБС ЛРК ја извршува својата дејност на локално (географско и деловно) ниво, по одобрување и овластување од КИБС и во согласност со постапките и процедурите на КИБС. КИБС ЛРК извршува задачи на регистрација во корист на КИБС РК. КИБС ЛРК е под надзор на КИБС РК.

1.8 Претплатници

Претплатници на КИБС услугите за сертифицирање се физички или правни лица кои користат електронски сертификати. Претплатниците се страни кои:

- поднеле барање за сертификат и истото им е одобрено,
- се идентификувани како субјекти во сертификатот,
- поседуваат приватен клуч кој кореспондира со јавниот клуч, содржан во сертификатот на претплатникот.

1.9 Засегнати страни

Засегнати страни се физички или правни лица кои се потпираат на КИБС сертификат и/или електронски потпис, кој може да се провери со јавниот клуч содржан во сертификатот на претплатникот.

За проверка на валидноста на електронскиот сертификат кој го примаат, засегнатите страни мора да се упатат до Регистарот на поништени сертификати (РПС) на КИБС ИС, пред да се потпрат на информацијата наведена во сертификатот.



Иако КИБС, кој врши дејност како ИС, работи во секторот на финансиските услуги во Република Македонија, засегнатите страни можат да се потпираат на информациите од КИБС сертификатите кога тие се користат и во други сектори или други земји.

1.10 Употреба на сертификат

Сертификатите издадени од ИС можат да се користат за посебни електронски трансакции кои подржуваат PKI, и тоа за потпишување на електронски формулари и електронски документи, пристап на веб сајтови и друга online содржина, електронска пошта и тн. Одредени организувања на примена на употребата на сертификатите издадени од ИС се наведени во овие ПИС.

1.11 Политика на администрација

КИБС со овие ПИС ја поставува интерната политика на управување како овластен ИС и работи согласно истата. ИС е одговорен за изготвувањето, објавувањето, OID регистрацијата, одржувањето и толкувањето на овие ПИС.

Било која политика која е одобрена од страна на ИС мора да биде во согласност со одредбите од овие ПИС.

1.12 Одговорност за објавување и сместување

ИС ги објавува информациите за електронските сертификати кои ги издава, во складиште кое е јавно достапно. ИС ги задржува сите права за објавување на информациите за статусот на сертификатите во складиштата на трети страни.



2. Технички аспекти

Овој дел се однесува на одредени технички аспекти на инфраструктурата на КИБС и услугите на сертифицирање.

2.1 Профили на КИБС сертификатите

ИС во овие ПИС го објавува изгледот на сертификатите кои ги издава. Издадените сертификати од КИБС се согласно барањата од IETF RFC 2459 и IETF RFC 3039.

Персоналните сертификати издадени од КИБС се според Директивата 99/93/ЕС *Заедничката рамка за електронски потписи* (Directive 99/93/EC *On a Common framework for electronic signatures*) и регулативата во Република Македонија, посебно Законот за податоци во електронски облик и електронски потпис („Службен весник на РМ“ бр. 34/2001, 6/2002) кој ја поставува правната рамка за електронските потписи.



2.2 Коренски сертификат на КИБС

KIBS Verba Root CA	
Signature Algorithm	Sha-1/RSA
Version	Version of the certificate X.509v3
Serial Number	Unique serial Number of the certificate: assigned by OnlineGuardian Certificate Management system.
Issuer	CN GlobalSign Partners CA
	OU Partners CA
	O GlobalSign nv-sa
	C BE
Validity	From: 21.03.2003
	To: 28.01.2009
Subject	CN KIBS Verba Root CA
	OU Verba CA
	O KIBS AD Skopje
	C MK
Public Key Length/Type	RSA 2048 Bits
Key Usage (Critical)	Certificate Signing, CRL Signing (06)
Basic Constraints (Critical)	Subject Type = CA
	Path Length Constraint = None
AuthorityKeyIdentifier (Noncritical)	[Identifier of GlobalSign Partner Root]
SubjectKeyIdentifier (Noncritical)	[Identifier of the Public Key]
Certificate Policy (Noncritical)	PolicyIdentifier = 1.3.6.1.4.1.16305.1.2.1
	Policy Qualifier Info: Policy Qualifier Id = CPS Qualifier: http://ca.kibs.com.mk/repository
CRL distribution point (Noncritical)	http://crl.globalsign.net/partners.crl



2.3 Оперативни сертификати

KIBS Operational Verba Class 3 CA	
Signature Algorithm	Sha-1/RSA
Version	Version of the certificate X.509v3
Serial Number	Unique serial Number of the certificate: assigned by OnlineGuardian Certificate Management system.
Issuer	CN KIBS Verba Root CA
	OU Verba CA
	O KIBS AD Skopje
	C MK
Validity	From: 21-03-2003
	To: 21-03-2008
Subject	CN KIBS Verba Class 3 CA
	OU Verba CA
	O KIBS AD Skopje
	C MK
Public Key Length/Type	RSA 1024 Bits
Key Usage (Critical)	Certificate Signing, CRL Signing (06)
NetscapeCertType (Noncritical)	SSL CA, SMIME CA (06)
Basic Constraints (Critical)	Subject Type = CA Path Length Constraint = 0
AuthorityKeyIdentifier (Noncritical)	[Identifier of KIBS Operational X Public Key]
SubjectKeyIdentifier (Noncritical)	[Identifier of Subject Public Key]
Certificate Policy (Noncritical)	PolicyIdentifier= 1.3.6.1.4.1.16305.1.2.1.1 Policy Qualifier Info: Policy Qualifier Id = CPS Qualifier: http://ca.kibs.com.mk/repository
CRL distribution point (Noncritical)	http://crl.Globalsign.net/KIBS-ROOT.crl



KIBS Operational Verba Server CA		
Signature Algorithm	Sha-1/RSA	
Version	Version of the certificate X.509v3	
Serial Number	Unique serial Number of the certificate: assigned by OnlineGuardian Certificate Management system.	
Issuer	CN	KIBS Verba Root CA
	OU	Verba CA
	O	KIBS AD Skopje
	C	MK
Validity	From:	21-03-2003
	To:	21-03-2008
Subject	CN	KIBS Verba Server CA
	OU	Verba CA
	O	KIBS AD Skopje
	C	MK
Public Key Length/Type	RSA 1024 Bits	
Key Usage (Critical)	Certificate Signing, CRL Signing (06)	
NetscapeCertType (Noncritical)	SSL CA (04)	
Basic Constraints (Critical)	Subject Type = CA	
	Path Length Constraint = 0	
AuthorityKeyIdentifier (Noncritical)	[Identifier of KIBS Operational X Public Key]	
SubjectKeyIdentifier (Noncritical)	[Identifier of Subject Public Key]	
Certificate Policy (Noncritical)	PolicyIdentifier= 1.3.6.1.4.1.16305.1.2.1.2	
	Policy Qualifier Info: Policy Qualifier Id = CPS Qualifier: http://ca.kibs.com.mk/repository	
CRL distribution point (Noncritical)	http://crl.Globalsign.net/KIBS-ROOT.crl	



2.4 Сертификати на крајните корисници

2.4.1 КИБС Верба

Version	2*	
Serial number	100000000000	
Signature algorithm	RSA /SHA-1	
Issue date	notBefore (UTC)	
Validity period	notfter (UTC) 1 year	
Issuer RDN	CN	KIBS Verba Class 3 CA
	OU	Verba CA
	O	KIBS AD Skopje
	C	MK
Subject	CN	Common Name (GivenName + SurName)
	GivenName	First Name
	SurName	Last Name
	E	Email address
	SerialNumber	Reserved Field
	C	Country
Public key	RSA 1024 bits	
Extensions		
AuthorityKeyIdentifier (Noncritical)		
Subject Key Identifier (SKI)		
KeyUsage (Critical)	Digital signature, Non-Repudation, Key Encipherment, Data Encipherment (F0)	
NetscapeCertType (Noncritical)	SSL Client, S/MIME (A0)	
CertificatePolicies (Noncritical)	PolicyIdentifier = 1.3.6.1.4.1.16305.1.2.1.1.1 Policy Qualifier Info: Policy Qualifier Id = CPS Qualifier: http://ca.kibs.com.mk/repository	
CRL distribution point (Noncritical)	http://ca.kibs.com.mk/crl/KIBSC3.crl	
Authority Info Access (AIA)	URL=ldap://ldap-ca.kibs.com.mk/cn=KIBS%20Verba%20Class%203%20CA%2Cdc=kibs%2Cdc=com%2Cdc=mk?certificateRevocationList?base?(objectClass=*)	

* Забелешка: 2 е трета верзија, бидејќи првата верзија е референцирана со 0, а втората верзија е референцирана како 1



2.4.2 КИБС Верба Про

Version	2*	
Serial number	100000000000	
Signature algorithm	RSA /SHA-1	
Issue date	notBefore (UTC)	
Validity period	notfter (UTC) 1 year	
Issuer RDN	CN	KIBS Verba Class 3 CA
	OU	Verba CA
	O	KIBS AD Skopje
	C	MK
Subject	CN	Common Name (GivenName + SurName)
	GivenName	First Name
	SurName	Last Name
	E	Email address
	OU	Organization Unit Name
	O	Organization Name
	C	Country
	SerialNumber	Reserved Field
Public key	RSA 1024 bits	
Extensions		
AuthorityKeyIdentifier (Noncritical)		
Subject Key Identifier (SKI)		
KeyUsage (Critical)	Digital signature, Non-Repudation, Key Encipherment, Data Encipherment (F0)	
NetscapeCertType (Noncritical)	SSL Client, S/MIME (A0)	
CertificatePolicies (Noncritical)	PolicyIdentifier = 1.3.6.1.4.1.16305.1.2.1.1.2 Policy Qualifier Info: Policy Qualifier Id = CPS Qualifier: http://ca.kibs.com.mk/repository	
CRL distribution point (Noncritical)	http://ca.kibs.com.mk/crl/KIBSC3PRO.crl	
Authority Info Access (AIA)	URL=ldap://ldap-ca.kibs.com.mk/cn=KIBS%20Verba%20Class%203%20CA%2Cdc=kibs%2Cdc=com%2Cdc=mk?certificateRevocationList?base?(objectClass=*)	

* Забелешка: 2 е трета верзија, бидејќи првата верзија е референцирана со 0, а втората верзија е референцирана како 1

2.4.3 КИБС Верба Сервер

Version	2*	
Serial number	100000000000	
Signature algorithm	RSA /SHA-1	
Issue date	notBefore (UTC)	
Validity period	notfter (UTC) 1 year	
Issuer RDN	CN	KIBS Verba Server CA
	OU	Verba CA
	O	KIBS AD Skopje
	C	MK
Subject	CN	Common Name (Domain Name)
	OU	Organization Unit Name
	O	Organization Name
	C	Country
Public key	RSA 1024 bits	
Extensions		
AuthorityKeyIdentifier (Noncritical)		
Subject Key Identifier (SKI)		
KeyUsage (Critical)	Digital signature, Non-Repudiation, Key Encipherment, Data Encipherment (F0)	
NetscapeCertType (Noncritical)	SSL Server (40)	
CertificatePolicies (Noncritical)	PolicyIdentifier = 1.3.6.1.4.1.16305.1.2.1.2.1 Policy Qualifier Info: Policy Qualifier Id = CPS Qualifier: http://ca.kibs.com.mk/repository	
CRL distribution point (Noncritical)	http://ca.kibs.com.mk/crl/KIBSServer.crl	
Authority Info Access (AIA)	URL=ldap://ldap-ca.kibs.com.mk/cn=KIBS%20Verba%20Server%20CA%2Cdc=kibs%2Cdc=com%2Cdc=mk?certificateRevocationList?base?(objectClass=*)	

* Забелешка: 2 е трета верзија, бидејќи првата верзија е референцирана со 0, а втората верзија е референцирана како 1



2.5 Управување со електронски сертификати

Управувањето со електронски сертификати од страна на КИБС, во поширока смисла се однесува на следните функции:

- Идентификација на барателот на сертификат,
- Барање за издавање на сертификати
- Издавање на сертификати,
- Обновување на сертификати,
- Поништување на сертификати,
- Евентуално чување на сертификатите на портабл медиум,
- Обезвластување на приватниот клуч преку поништување на сертификатот,
- Евидентирање на сертификатите,
- Дистрибуирање на сертификатите,
- Објавување на сертификатите.

Во рамките на сертификационите услуги на КИБС, целокупното управување со сертификатите е доверено на КИБС.

2.6 КИБС директориуми и складиште

Со цел да го зголеми нивото на доверба на своите услуги, КИБС ги става на располагање и управува со директориумите кои содржат податоци за издадени, одложени и поништени сертификати. Корисниците и засегнатите страни се посебно заинтересирани за консултирање на директориумите за издадени и поништени сертификати секогаш пред да се потпрат на информација која е наведена во сертификатот. КИБС почесто го ажурира директориумот на поништени сертификати.

КИБС ги објавува складиштата кои содржат правна регулатива за своите РКI услуги, вклучувајќи ги и овие ПИС, како и други информации, кои се суштински за услугите кои тој ги нуди.

Регистарот на поништени сертификати (РПС) се потпишува и се евидентира времето од страна на ИС.

РПС се издава на секои 3 часа.

ИС на својот веб сајт ги става на располагање сите РПС издадени последните 3 месеци.

Корисникот добива информација за статусот на сертификат преку едноставен веб интерфејс.

2.7 Идентификација на претплатникот

Пред да издаде сертификат КИБС задолжително го контролира идентитетот на претплатникот. Оваа контрола е во надлежност на КИБС РК, која исто така ги надгледува сите процедури, согласно упатствата за процедурите донесени од страна на КИБС, а кои се применуваат online и/или offline.

РК или ЛРК работат по овластување од ИС, кој донесува упатства за постапките и процедурите за автентикација на идентитетот и/или други атрибути на крајниот корисник-барател на сертификат. Пред да побара издавање на сертификат, РК го верификува идентитетот на барателот на сертификат со документите на барателот, кои ги прима, или приемот на истите и проверката ги врши ЛРК.



РК ги одржува соодветните процедури кои се однесуваат на постапките, вклучувајќи го препознавањето на правата на заштитниот знак на одредени имиња.

ЛРК одлучуваат при издавањето во однос на идентификацијата и автентикацијата на барателите на сертификати, меѓутоа РК единствено е одговорна за одобрувањата.

ИС врши автентикација на барањата на страните кои сакаат поништување на сертификати согласно овие ПИС.

2.8 Доверливи системи

За вршење на своите услуги КИБС користи доверливи системи.

2.9 Ограничувања на опсегот на КИБС сертификатите

КИБС нуди опсег на електронски сертификати и соодветни производи и услуги кои можат да се користат на начин согласно потребите на корисниците за безбедни лични и деловни комуникации.

КИБС може да ја ажурира или да ја прошири листата на производи, вклучувајќи ги видовите на сертификати кои тој ги издава, доколку смета дека тоа е соодветно. Објавувањето или ажурирањето на листата на КИБС производите се креира без барање од било која трета страна.

2.10 Проширувања и именување

2.10.1 Проширувања на електронските сертификати

КИБС користи стандард X.509, верзија 3 за креирање на електронски сертификати, за неговите РК1 производи и услуги. Согласно X.509 v3, ИС може на основната структура на сертификатот да додаде одредени проширувања на сертификатот. Јавните услуги на КИБС користат одреден број на контроли за целите наменети од X.509 спрема Додатокот 1 за ISO/IEC 9594-8, 1995.

2.10.2 Повикување на референца за проширувања и подобро именување

Проширувањата и подобреното именување обично се изразени во претплатничките сертификати. Тие исто така можат делумно да бидат дефинирани во сертификатот на претплатникот, додека остатокот може да биде посебен документ, на кој што се повикува со референца во сертификатот на претплатникот. Вклучената информација во таков посебен документ може да биде расположива на страните кои тоа го бараат.

2.11 Процес на генерирање на приватен клуч

КИБС извршува безбедно генерирање на своите коренски приватни клучеви на доверлив начин. КИБС е сопственик на приватните клучеви кои ги користи за управување со сертификатите. КИБС може да изврши генерирање на својот приватен клуч директно или индиректно преку овластена трета страна. Делувајќи спрема инструкции од КИБС, застапниците се соодветно овластени да извршуваат задачи кои се поврзани со управувањето со коренскиот приватен клуч. Операциите за управување со клучот секогаш се извршуваат согласно документираните и по можност контролирани постапки.

2.11.1 Употреба на приватниот клуч на КИБС

Приватниот клуч на КИБС се користи за потпишување на: издадените сертификати, регистарот на поништени сертификати и други овластени издавачи на сертификати. Ограничен е за друга употреба.

2.11.2 Тип на приватниот клуч на КИБС

За својот коренски клуч КИБС употребува MD5/RSA алгоритам со должина од 2048 бита и период на важење од 10 години.

За своите оперативни клучеви КИБС употребува MD5/RSA алгоритам со должина од 1024 бита и период на важење од 5 години.

2.11.3 Генерирање на приватниот клуч на КИБС

КИБС безбедно ги генерира и заштитува своите приватни клучеви, користејќи доверлив систем, и преземајќи неопходни мерки за заштита од компромитирање и неовластено користење на истите. КИБС ги спроведува и ги документира процедурите за генерирање на клуч, согласно овие ПИС. КИБС ги прифаќа јавните меѓународни и европски стандарди за доверливи системи и се залага да се придржува кон нив до степен на дозволена примена или обврзан на Законот во Република Македонија. КИБС ги чува генерираните клучеви на безбедни токени. Безбедните токени се ставени под надзор на овластен застапник.

2.11.4 Уреди за генерирање на клучот

Генерирањето на приватниот клуч на КИБС се извршува на безбеден криптографски уред исполнувајќи ги соодветни барања кои вклучуваат ISO 15782 140-1 ниво 3, ANSI X9.66.

2.11.5 Контроли на генерирањето на клучот

Генерирањето на приватниот клуч на КИБС бара контрола на повеќе од еден овластен вработен кој работи на доверливо работно место. Генерирањето на клучот е со писмено овластување.

2.11.6 Чување на приватниот клуч

КИБС употребува безбеден криптографски уред за чување на сопствениот приватен клуч, исполнувајќи ги соодветните ISO 15782-1/FIPS 140-1/ANSI X9.66 барања.

2.11.7 Поделба на тајност

КИБС користи трета страна за поделба на тајноста и повеќе овластени држатели на тајните делови на приватните клучеви, за да ја обезбеди и подобри сигурноста на своите приватни клучеви, како и да обезбеди повторно обновување на клучот.

Тајните делови се чуваат од страна на застапник овластен од КИБС на повеќе уреди, кои се потребни за пристап и активирање на приватниот клуч на КИБС ИС. Застапникот на КИБС ги чува тајните делови на повеќе токени за да се обезбеди и подобра доверливоста кон приватните клучеви.

Најмалку три овластени лица (држатели на тајни делови) кои се вработени на доверливи работни места мораат да работат истовремено за да го активираат приватниот клуч на КИБС ИС.



2.11.7.1 Прифаќање на тајните делови

Пред да ги прифатат тајните делови држателите на тајните делови мора лично да присуствувале на создавањето, ресоздавањето и дистрибуцијата на делот или нивниот следен ланец на држатели на тајни делови.

Тајните држатели примаат тајни делови на физички медиум, каков што е хардеверскиот криптографски модул одобрен од ИС. ИС ги чува пишаните записи на дистрибуцијата на тајниот дел.

2.11.8 Безбедно чување на токен

КИБС користи безбедни токени и овластени држатели на безбедни токени, за да се заштити и подобри доверливост на своите сопствени приватни клучеви и за да се обезбеди обновување на клучот.

КИБС ги чува своите сопствени приватни клучеви на отпорни од упад уреди. Активирањето на приватниот клуч на КИБС ИС настанува само согласно објавената процедура и со употреба на податоците за активирање, складирани во тајните делови, како што е погоре опишано.

Приватните клучеви на КИБС ИС не можат да бидат заложени. ИС презема интерни мерки за враќање во првобитна состојба, за заштита од несакани случаи од несреќи кои можат да пречат на интегритетот на неговите сопствени приватни клучеви.

2.12 Контроли на физичката безбедност

ИС спроведува физичка контрола на своите простории. Оваа контрола го вклучува следното:

Просториите на ИС се лоцирани на простор кој е соодветен за високо безбедни операции. Овие простории се нумерирани зони и заклучени соби, кафези, сефови и кабинети.

Физичкиот пристап е ограничен со воспоставени механизми за контрола на пристап до опремата или пристап внатре во зоните со висока безбедност, како што е одредувањето на местото за вршењето на работите на ИС во соба со безбеден компјутер надгледуван физички и обезбеден со сигурносни аларми и движењето од зона во зона се извршува користејќи токен и листи за контрола на пристап.

Електричното напојување и уредите за одржување на температура да работат со висок степен на редуванција.

Просториите се заштитени од поплави.

ИС спроведува спречување и заштита како и презема мерки против пожар.

Медиумите безбедно се чуваат. Исто така, бекап медиумите се чуваат на одделно место така што тие се безбедни и заштитени од штети кои можат да настанат од пожар и поплави.

За да се спречи несакано откривање на чувствителни податоци, тие се распоредуваат на безбеден начин.

ИС спроведува делумен off-site бекап.

Положбата на инфраструктурата на сајтовите на ИС е таква за да се обезбедат услугите на КИБС. ИС спроведува соодветни контроли на безбедност, вклучувајќи контрола на пристап, откривање на упад и надзор. Пристапот на сајтовите е ограничен на овластени лица наведени во списокот за контрола на пристап, кој е предмет на контрола.



2.13 Процедурални котроли

ИС применува кадровски и управувачки постапки кои обезбедуваат соодветно осигурување на доверливост и способност на вработените, како и задоволително извршување на нивните обврски на полето на технологии поврзани со електронскиот потпис.

Вработените се советуваат за воздржување од конфликт на интереси со ИС, како и за одржување на доверливоста и заштита на личните податоци.

Сите вработени кои работат на управување со клучевите, администраторите, службениците од безбедност и контролорите на системот или било кои други кои материјално влијаат на таквите операции се смета дека имаат доверлива позиција.

ИС посебно ги испитува сите вработени кои се кандидати да извршуваат доверлива улога со намера да ја одреди нивната доверливост и способност.

Кога е потребна двојна контрола, потребно се најмалку двајца доверливи работници од вработените на ИС да поседуваат особени и пооделни знаења за да можат во тек да ја изведат операцијата.

ИС осигурува дека сите активности во поглед на ИС можат да бидат припишани на системот на ИС и на вработените на кои ја извршиле активноста.

Критичните функции на ИС се спроведуваат со двојна контрола.

ИС ги дели следните работни групи:

- оперативна група која управува со сертификатите,
- административна група која работи на платформата за подршка на ИС,
- Вработени за безбедност кои применуваат безбедносни мерки.

2.14 Контрола на безбедната мрежа

ИС одржува високо ниво на мрежа од безбедносни системи вклучувајќи и огнени ѕидови.

Упадите на мрежата се под надзор и се откриваат. Посебно:

- ИС ги шифрира конекциите со РК,
- Веб сајтот на ИС обезбедува шифрирани конекции преку Secure Socket Layer (SSL) протокол и анти-вирус заштита,
- Мрежата на ИС е заштитена со управуван огнен ѕид и систем за откривање на напади,
- Забранет е пристап до чувствителните ресурси на ИС, вклучувајќи пристап до базата на податоци од надвор ,
- Сесиите на интернет за барање и испорака на информации се шифрирани.

3. Организација

Овој дел ја опишува организацијата и условите за доверба кон сертификациските услуги на КИБС.

3.1 Инфраструктура на КИБС

КИБС ја одржува цврста организациона, технолошката состојба и рамката на објавените постапки и процедури.

3.2 Усогласување со овие ПИС

КИБС ги извршува своите услуги во согласност со овие ПИС и другите обврски кои ги презема со договор.

3.3 Престанување на дејноста на ИС

КИБС благовремено обезбедува известување, пренесување на одговорностите на следбениците, чувањето на записите и исправките. Пред да заврши со својата дејност како ИС, КИБС:

- Во рок од 90 дена ги известува претплатниците кои имаат важечки сертификати дека престанува со работа.
- Ги поништува сите сертификати кои не се поништени или на кои не им е истекнат рокот на важење по 90 дена од известувањето, без согласност на претплатникот.
- Благовремено дава известување за поништување на секој засегнат претплатник.
- Организира заштита на записите согласно овие ПИС.
- Доколку е возможно, обезбедува следбеникот на ИС при ре-издавањето на наследените сертификати да ги примени овие ПИС.
- Обезбедува правен следбеник за да ги преземе и сите релевантни податоци за издавањето на сертификатите или доколку таков нема, тогаш да ги предаде на Министерството за финансии.
- Да го известува Министерството за финансии, кој врши надзор на работењето на издавачите на сертификати во Република Македонија, за намерата за престанок на работењето со сертификати.

Барањата од оваа точка може да варираат со договор, но таквите измени да влијаат само на договорените страни.

3.4 Форма на записите

КИБС ги чува записите во електронска форма или на хартија. КИБС може да побара од своите РК, претплатниците или своите застапници да поднесат соодветни документи заради обезбедување на ова барање.

3.5 Чување на записите

КИБС на доверлив начин ги чува записите кои се однесуваат на издавањето на електронските сертификати во период и тоа:

- КИБС ИС за период кој не е помал од 5 години,

- КИБС РК за период кој не е помал од 5 години
- КИБС ЛРК за период кој не е помал од 2 години.

Времето на чување започнува од датумот на изминување на рокот на важење или на поништување. Овие записи можат да се чуваат во електронска форма или на хартија или во друг формат за кој КИБС смета дека е погоден.

За електронските сертификати, КИБС обезбедува чување на записите и тоа:

- податоците поврзани со верификацијата на идентитетот на барателот, вклучувајќи ги поднесените документи и нивните копии,
- времето, датумот и начинот на издавање на сертификат,
- причините, времето, датумот и начинот на поништување на сертификат,
- периодот на важење на сертификатот,
- сите пораки кои се однесуваат на валидноста на сертификатот настанати помеѓу издавачот и имателот на сертификат.

3.6 Логови за основните функции

КИБС на доверлив начин ги чува логовите за следните настани:

- генерарање на клучеви,
- управување со клучеви,
- прекин на услугата,
- контролите во врска со просториите на ИС и РК дејноста,
- примените барања на сертификати од барателите на КИБС услугите.

3.7 Контрола на основните функции

КИБС може да ја стави својата расположива инфраструктура на контрола на инспектори и ревизори во врска со извршувањето на оперативните и деловните потреби. КИБС не е должен да потврди или одобри било каква содржина, наоди и препораки од записниците на ревизорите, а може да ги разгледа записниците во поглед на заштитата на КИБС услугите. КИБС не се презема на одговорност за било која штета која е резултат на потпирањето на КИБС на основа на записниците или од непримената на наодите од тие записници.

Системот на ИС ги запишува настаните кои вклучуваат но не се ограничуваат на:

- издавање на сертификат,
- поништување на сертификат,
- обновување на сертификат,
- одложување на сертификат,
- автоматско поништување,
- објавување на РПС или промените на РПС.

ИС го контролира секој настан-логиран запис.

Записникот од контролата содржи:

- идентификација на операцијата,
- датумот и времето на операцијата,
- идентификација на сертификатот, вклучен во операцијата,
- идентитетот на барателот на трансакцијата.

3.8 Планови за настанување на непредвидени ситуации и нивно враќање во првобитна состојба

За да одржи интегритетот на услугите, КИБС спроведува, документира и периодично тестира планови и процедури во случај на настанување на непредвидени ситуации и решавање на истите.

3.9 Компромитурање и враќање во првобитна состојба

Во посебен интересен документ ИС го евидентира инцидентот, го запишува компромитурањето и применетите процедури. ИС ги евидентира користените процедури за враќање во првобитна состојба доколку компјутерските извори, софтверот и/или податоците се корумпирани или заради настанатото корумпирање се сомнителни.

Постојаниот деловен план се спроведува за да обезбеди конитнуетет во работењето од настанатата природна или друг вид на катастрофа.

Сите мерки се согласно ISO 1-7799.

ИС воспоставува:

- Извори за враќање во првобитна состојба на две локации кои се доволно оддалечени една од друга.
- Брза комуникација помеѓу двете страни заради осигурување на интегритет на податоците.
- Комуникациска инфраструктура од две страни за поддршка на РК интернет комуникациските протоколи.

Инфраструктурата за враќање во првобитна состојба и процедурите се тестираат најмалку еднаш годишно.

3.10 Расположивост на КИБС сертификатите

За да се овозможи проверка на потписот со референца на електронскиот сертификат, КИБС става на располагање на страните копии од сертификатите во кои КИБС е субјект како и податоците за поништување.

3.11 Објавување на информации за издадени сертификати

КИБС ги објавува сите издадени електронски сертификати, податоци за поништување или податоци за истекување на рокот на електронските сертификати, како и овие ПИС.

3.12 Доверливи информации

КИБС се придржува кон правилата за приватност на личните податоци. Исто така, КИБС на доверлив начин и како што е пропишано со закон, постапува со:

- претплатничките договори,
- записите за примените сертификати,
- записите за трансакции,
- записите и извештаите од надворешни и внатрешни контроли,
- планови за непредвидени ситуации и планови за враќање во работна состојба после катастрофа,

- интерна евиденција и записи од работењето на КИБС инфраструктурата, управувањето со сертификати и запишување на услуги и податоци.

КИБС не издава ниту пак од него се бара да издаде било каква доверлива информација без потврдено, евидентирано барање од овластена страна и тоа посебно:

- од страна за која КИБС е должна да ги чува доверливите информации,
- од страна која бара таква информација или
- по судски налог.

КИБС може да наплатува надоместок по овој основ.

3.13 Безбедност на капацитетите

Физичкиот пристап до безбедниот дел на капацитетите на КИБС е ограничен само за овластени лица. Средствата за издавање на сертификати се заштитени од надворешна опасност. Губитоците, штетите или компромитирањето на имотот и упадот во работењето се откриваат и соодветно се спречуваат. Компромитирањето или кражба на информации и средствата за процесирање на информациите се откриваат и соодветно се заштитуваат.

3.14 Управување со кадрите и постапки

При доследното извршување на овие ПИС, КИБС применува кадровски постапки и постапки за управување со кои се осигурува доверливост и способност на неговите вработени успешно да ги извршуваат нивните обврски. Доверливоста се евидентира преку административни контроли или еднострани изјави за почитување, обезбедени од вработените или од агенти од трета страна.

3.14.1 Доверливи информации

Лицата кои се на доверливи работни места сите информации ги чуваат како строго доверливи. Посебно вработените во РК/ЛРК се должни да ги применуваат општите барања наведени во Европската директива 95/46/ЕС за заштита на лицата во врска со обработката на личните податоци и слободното движење на тие податоци и Законот за заштита на личните податоци („Службен весник на РМ“ бр. 7/2005).

3.15 Безбедносни контроли на персоналот

ИС имплементира одредени безбедносни контроли во поглед на обврските и извршувањето на работата на своите вработени. Овие контроли се документираат во правилник и ги вклучуваат доле наведените области.

3.15.1 Квалификации, искуства и образложенија (разјаснувања)

ИС, РК и ЛРК вршат проверка на биографијата, квалификации и искуството кое е неопходно за успешно извршување на специфична работа. Проверката на биографијата вклучува:

- осудувања за тешки кривични дела,
- лажно претставување на кандидатот,
- несоодветни препораки,
- било какви образложенија кои се сметаат како соодветни.

3.15.2 Проверка на биографските податоци

ИС извршува одредени проверки на кандидатот врз основа на решение за статусот издадено од надлежен орган, изјави од трети страни или лично потпишана изјава.

3.15.3 Потребна обука и процедури

ИС врши обука на своите вработени за вршење на функциите на ИС.

3.15.4 Периодични обуки и процедури

Исто така, можат да се изведуваат и периодични обуки заради воспоставување на континуитет и обновување на знаењето на вработените како и ажурирање на процедурите.

3.15.5 Казни против вработените

ИС ги казнува вработените за неовластено работење, неовластено користење на овластување и неовластено користење на системите, така што ги изложува на одговорност вработените на ИС, соодветно на дадените околности.

3.15.6 Контроли на независни изведувачи

Независните изведувачи и нивните вработени се исто така, предмет на проверка на биографските податоци, како што се вработените на ИС. Проверката на биографијата вклучува:

- осудувања за сериозни кривични дела,
- лажно претставување на кандидатот,
- соодветни препораки,
- било какви образложенија кои се сметаат како соодветни,
- заштита на приватноста,
- услови за доверливост.

3.15.7 Документација за обука и повторна обука

ИС, РК и ЛРК им даваат на располагање документација на вработените за времетраење на обуката, повторната обука или во други прилики.

3.16 Објавување на информации

Услугите за сертификати на КИБС и КИБС складиштето се пристапни преку:

- веб: <http://ca.kibs.com.mk/repository/>
- е-пошта: ca-info@kibs.com.mk, ca-pravila@kibs.com.mk
- пошта: КИБС АД Скопје, К.Ј.Питу 1, 1000 Скопје, Македонија

4. Постапки и процедури

Овој дел ги претставува постапките и процедурите на услугите за сертификарање на КИБС.

4.1 Барање на сертификат

Пред, по и за време на барањето на електронски сертификат, барателите на сертификати (наречени претплатници) ги преземаат следните чекори во врска со барањето на КИБС сертификат:

- поднесуваат барање за сертификат преку online процедурата за барање, и се согласуваат со условите од претплатничкиот договор и овие ПИС,
- генерираат пар клучеви и покажуваат на КИБС дека приватниот клуч кој го поседуваат одговара со јавниот клуч кој го испраќаат до КИБС за да биде внесен во КИБС сертификатот и издаден на претплатникот,
- го поднесуваат до КИБС јавниот клуч од генерираниот пар клучеви,
- обезбедуваат доказ за нивниот идентитет, согласно процедурите на КИБС или други стандардно пропишани процедури, кои се прифатени од КИБС,
- го заштитуваат интегритетот на приватниот клуч од генерираниот пар клучеви. Тоа е постојана обврска на претплатникот.

4.1.1 Овластување

Зависно од типот на сертификатот, барањето за КИБС електронски сертификат може да биде направено лично или преку застапник. Барањата за електронски сертификати мора да бидат проследени преку веб базирани процедури кои се ставени на располагање од страна на КИБС.

4.1.2 Генерирање на пар клучеви

Претплатниците се исклучиво одговорни за безбедно генерирање на нивниот сопствен пар на клучеви, користејќи безбеден систем како што е предвидено со продуктот или апликацијата.

4.1.3 Заштита на парот клучеви

Претплатниците се исклучиво одговорни за преземање на сите неопходни мерки за да се спречи компромитирање, губење, откривање, менување, кражба или друга неовластена употреба на нивниот приватен клуч.

4.1.4 Користење на безбедни средства и продукти

Освен ако поинаку не е дадено во овие ПИС, претплатниците користат безбедни средства и продукти кои обезбедуваат заштита на нивните клучеви.

4.1.5 Доделување одговорности за приватни клучеви

Претплатниците се исклучиво одговорни за постапките и пропустите на партнерите и застапниците кои тие ги користат за генерирање, задржување, заложување или уништување на нивните приватни клучеви.

4.2 Информации за валидација на барањата за сертификат

Кон барањата за КИБС сертификатите се приложува соодветна документација за да се утврди идентитетот на подносителот на барањето како што е подолу опишано.

Повремено, КИБС може да ги менува барањата за претплатниците кои се однесуваат на информациите за применување за да можат да одговорат на барањата на КИБС, во врска со употребата на електронски сертификат, или тоа може да биде пропишано со закон.

Документите треба содржат елементи за идентификација, како што се следните:

4.2.1 Именување

За идентификување на претплатник, ИС пропишува одредени правила за именувања и идентификација кои вклучуваат видови на имиња доделени на субјектот.

Имињата доделени на претплатниците на сертификат се единствени во доменот на ИС така што тие секогаш се употребуваат заедно со единствениот последователен број.

ИС не прифаќа заштитни марки, логоа или други заштитени авторски права, графички или текст материјал за вклучување во неговите сертификати

4.2.2 Иницијална валидација на идентитетот

Согласно процедурите за идентификација и автентикација од иницијалната регистрација на претплатникот, ИС ги проследува барањата од РК во поглед на идентификација и автентикација на барателите за сертификати. ИС целосно се потпира на РК во поглед на содржината, соодветноста, точноста и доверливоста на трансмисијата на личните податоци на барателите.

4.2.3 Информации за аплицирање на деловни субјекти

Потребните информации за издавање на КИБС сертификат на правно лице, може да содржат некоја или сите од следните елементи. Сервер сертификатите се издаваат на правни лица. КИБС може да ги менува потребните информации доколку смета дека тоа е соодветно, во деловен контекст на сертификатот, или тоа може да биде пропишано со закон:

- Име на барателот.
- Име на правниот застапник и доказ за овластувањето.
- Име на доменот.
- IP адреса.
- Назив на субјектот.
- Организациона единица
- Улица, град, поштански број, земја
- Лица за технички и сметководствени контактни и правниот претставник
- Даночен број
- Број од Трговски регистар
- Софтвер на серверот
- Податоци за плаќање
- Доказ за право за користење на име
- Доказ за постоење на субјектот
- Доказ за организациониот статус како на пример: акти за основање на друштвото, писмо од Деканот или Директорот (за образовни институции), официјално писмо од овластен претставник на владина организација.
- Формулар за регистрација потпишан и правилно пополнет
- Потпишан претплатнички договор.

4.2.4 Информации добиени од индивидуален барател

Податоците потребни за да се поткрепи барањето за КИБС сертификат се наведени подолу. КИБС може да ги менува потребните податоци доколку смета дека тоа е соодветно, во деловниот контекст на сертификатот, или доколку е пропишано со закон:

- E-mail адреса на барателот;
- Законско име
- Земја
- Јавен клуч на барателот
- Податоци за идентификација
- Лозинка
- Податок за плаќање
- Претплатнички договор и формулар за регистрација потврден од страна на РК/ЛРК, кој е соодветен на потребниот званичен формулар за идентификација од барателот.
- Доказ за професионален контекст (каде што е применливо).

4.3 Валидација на барањата за сертификат

По прием на барањето за електронски сертификат и согласно доставените информации, КИБС го потврдува следното:

- Барателот на сертификат е истото лице како лицето утврдено во барањето за сертификат;
- Барателот на сертификат поседува приватен клуч кој одговара на јавниот клуч кој треба да биде вклучен во сертификатот;
- Податоците кои ќе се објават во сертификатот се точни, освен не-потврдените податоци за претплатникот;
- Застапниците кои поднесуваат барање за сертификат во кое е наведен јавниот клуч на барателот на сертификат се овластени да го сторат тоа.

КИБС ја контролира точноста на објавените податоци доставени од барателот во моментот кога сертификатот се издава.

Во сите случаи и за сите видови на КИБС сертификати, претплатникот има постојана обврска да ја следи точноста на доставените информации и да го извести КИБС за евентуалните промени.

4.3.1 Лично присуство

За да се воспостави поврзаност помеѓу барателот и јавниот клуч на барателот, КИБС бара лично присуство на барателот пред РК/ЛРК за одредени типови или класи на електронски сертификати, но го резервира своето право да ги менува условите за регистрација доколку смета дека е потребно или доколку тоа е пропишано со закон.

4.3.2 Потврда од трето лице за информациите за деловниот субјект

КИБС може да побара од трети лица да ја потврдат информацијата за деловниот ентитет кој поднесува барање за КИБС електронски сертификат. КИБС ја прифаќа потврдата од страните како што се трговските комори, други бази податоци на трети лица и владините ентитети, доколку тоа може да се провери од друга трета страна, од вешти лица обезбедно во рамките на нивната дејност.

На одредени ентитети може да им биде побарано да обезбедат доказ за нивните активности пред да им се издадат електронски сертификати, со цел да се овозможи деловни активности или на поинаков начин дозволени или контролирани функции.

КИБС може да употреби средства за комуникација кои му се на располагање за да го утврди идентитет на правното лице.

4.3.3 Потврда за името на доменот и доделување на сериски број

Само КИБС има право да доделува Единствени карактеристични имиња - (Relative Distinguished Name) и сериски броеви на сертификати кои се појавуваат на сертификатите на КИБС. Доколку е потребно, КИБС може да го користи Сервисот за име на домен како решение за доделување на единствени карактеристични имиња.

4.4 Време за потврда на поднесените податоци

КИБС ги потврдува податоците содржани во барањето за сертификат и издава електронски сертификат во разумен временски рок.

4.5 Одобрување и одбивање на барањата за сертификати

По успешното завршување на сите потребни валидации на барањето за сертификат, КИБС го одобрува барањето за електронски сертификат.

Доколку не се изврши валидација на барањето за сертификат, КИБС го одбива барањето за сертификат. По одбивањето КИБС веднаш го известува барателот на начин кој смета дека е најприкладен и ја наведнува причината за одбивање, согласно со закон.

КИБС го резервира своето право да го одбие барањето за издавање на сертификат доколку има сопствена проценка дека со издавањето на сертификатот може да му се одземе или смали угледот и довербата или да му се намали вредноста. КИБС го резервира своето право да одбие барања за издавање сертификати на баратели, доколку смета дека е оправдано, без да предизвика одговорност за загуби или трошоци што произлегуваат како резултат на одбивањето.

Барателите чии барања биле отфрлени, можат повторно да аплицираат.

4.6 Издавање на сертификат и согласност на претплатникот

КИБС издава сертификат по одобрувањето на барањето за сертификат. Електронскиот сертификат се смета за валиден по неговото прифаќање од страна на претплатникот. Издавањето на електронскиот сертификат значи дека КИБС го прифаќа барањето за сертификат.

КИБС издава сертификат согласно согласноста на барателот. Согласноста за издавање на сертификат се демонстрира со поднесувањето на барањето, и покрај фактот што прифаќањето на сертификат сеуште не е настанато.

4.7 Валидација на сертификат

Сертификатите стануваат валидни со издавањето од страна на КИБС и прифаќањето од страна на претплатникот.

4.8 Прифаќање на сертификатот од страна на претплатникот

Претплатникот се смета дека го прифатил сертификатот кога одобрувањето се манифестира на начин како што е подолу опишан:

- On-line: преку безбедна Интернет врска (https). Претплатникот мора да го извести КИБС за евентуалните неточности или недостатоци во сертификатот веднаш по прием на сертификатот или со претходно известување за содржина која треба да се вклучи во сертификатот.
- E-mail (S/MIME): За одредени класи на сертификати КИБС може да поддржи e-mail базирани барања. Барателот на сертификат поднесува потпишано барање за сертификат до КИБС за прифаќање на сертификат. По завршувањето на процедурата за верификација КИБС го испраќа сертификатот до барателот по e-mail. Барателот за сертификат мора веднаш да го информира КИБС за било која неточност или ако во сертификатот пронајде грешка или предходна забелешка за било која содржина, која мора да биде вклучена во сертификатот.

Претплатниците мора веднаш да го известат КИБС доколку има грешка во сертификатот.

Сертификатот може да биде поништен во рок од 5 работни дена по издавањето и претплатникот може да побара нов сертификат без обврска за плаќање на надоместок. Доколку не се добие известување за прифаќање се смета дека сертификатот е прифатен по истекот од 5 дена од издавањето.

4.9 Објавување на издадените сертификати

По прифаќање на сертификатот од страна на претплатникот и проверка од КИБС, КИБС објавува копија во складиштето на КИБС или во било кои други складишта кои можат да бидат утврдени од страна на КИБС. Претплатниците можат исто така да ги објават своите КИБС сертификати во други складшта.

4.10 Верификација на електронските потписи

Верификацијата на електронскиот потпис има за цел да се утврди дека:

- електронскиот потпис е креиран со приватен клуч што одговара на јавниот клуч заведен во сертификатот на потписникот;
- содржаната порака не е изменета по креирањето на електронскиот потпис.

4.11 Потпирање на електронските потписи

Конечната одлука за тоа дали треба или не треба да се потпира на верификуваниот електронски потпис останува исклучиво да ја донесе верификаторот. На електронскиот потпис може да се потпреме доколку:

- Електронскиот потпис е креиран во текот на оперативниот период на валиден сертификат, што може да се потврди со повикување на истиот сертификат;
- Потпирањето е разумно согласно дадените околности.

4.12 Суспендирање и поништување на сертификат

Да се поништи сертификат значи трајно да се стави крај на оперативниот период од одреденото време па натаму. Да се суспендира сертификат значи привремено да се одстрани сертификат. По барање на претплатник КИБС ќе суспендира или ќе поништи електронски сертификат ако:

- тоа го бара претплатникот;



- се јави губење, кражба, менување, неовластено откривање или друго компромитирање на приватниот клуч поврзан со јавниот клуч од сертификатот на субјектот;
- субјектот на сертификатот ја нарушил материјалната обврска, согласно овие ПИС;
- извршувањето на обврските на лицето согласно овие ПИС доцни или е спречено од природни несреќи, компјутерски или комуникциски испади или друга причина вон контролата на лицето и како резултат на други лични податоци кои доведуваат до материјално загрозување или компромитирање;
- е извршена измена на податоците содржани во сертификатот;
- во случај на смрт или неспособност на субјектот наведен во сертификатот;
- по судски налог.

Претплатниците кои не се субјекти (иматели) на КИБС сертификати, се залагаат да презамат потребни мерки на предострожност тие да можат да ја преземат контролата за барање на поништување на КИБС сертификати, доколку имателот на сертификат е неспособен или без воља тоа да биде извршено од негова страна.

4.12.1 Ефект од отстранување или поништување

Во периодот на отстранувањето, или по поништувањето на сертификатот, оперативниот период на тој сертификат веднаш се смета за завршен.

4.12.2 Известување пред истекување на периодот на важење

За да се сочува способноста на корисниците на електронски сертификати електронски да потпишуваат, триесет (30) дена, односно седум (7) дена пред истекот на електронскиот сертификат, КИБС ќе вложи реални напори да ги известат претплатниците преку електронска пошта за престојниот истек на електронскиот сертификат.

4.13 Обновување

Барањата за обновување на издадените и сеуште важечките електронски сертификати се поинакви од првобитните барања за претплата на услугата. КИБС ќе го потсети претплатникот 30 дена односно 7 дена пред истекувањето на рокот на важење на неговиот сертификат. Сите информации на сеуште важечките сертификати за кои се бара обновување мора да бидат валидни. Обновувањето се прави преку веб страната користејќи го истиот јавен клуч од парот клучеви кој е на сертификат за кој се бара обновување. Не е потребна дополнителна верификација за регистрација при обновувањето.

5. Законски услови на издавање

Овој дел ги обработува правните аспекти, гаранции и ограничувања во врска со КИБС електронските сертификати.

5.1 Претставување на КИБС

КИБС на сите претплатници и засегнати стани ги презентира своите јавни услуги, кои се опишани подолу. КИБС има право да ги менува одредбите доколку смета дека тоа е потребно илитоколку тоа се бара со закон.

5.2 Податоци со повикување на референца во електронскиот сертификат

КИБС се повикува со референца на следните податоци во секој електронски сертификат што го издава и тоа:

- термините и условите во овие ПИС,
- друга политика за сертификати која може да биде содржана на издаден сертификат од КИБС,
- задолжителни елементи од стандардот X.509,
- сите незадолжителни но побарани елементи од стандардот X.509,
- содржина на екстензијата и проширеното именување кое не е одредено на друго место,
- друг податок кој е насочен да биде содржан во поле на сертификатот.

5.3 Показатели за повикување на референца

За вградување податок со референца КИБС користат компјутерски и текстуални показатели кои вклучуваат URL-и (Universal Resource Locator), OID-и (Object Identifier) или било кое друго средство за повикување на референца, со цел да можат да бидат ставени на располагање.

5.4 Изложување на ограничена одговорност, изјави за гаранција

КИБС сертификатите можат да содржат кратка изјава во која се опишани ограничувањата на одговорноста, ограничувања на вредноста на трансакциите кои треба да се извршат, период на валидација и наменета цел на сертификатот, како и одрекувањата за гаранција која би можела да биде применета. Таквите информации можат алтернативно да се прикажуваат преку хипертекст врска. За комуникација на информациите КИБС може да користи:

- атрибут на организациона единица,
- стандардно средство на КИБС одредено во политиката на сертификати,
- сопствени проширувања.

5.5 Објавување на податоците од сертификатите

КИБС го резервира правото да објавува сертификат и податоци поврзани со сертификат во својата РПС или на некои други пристапни складишта, како што е наведено.



Со оглед дека КИБС работи со директориуми, за да го подигне нивото на доверба на своите услуги, на корисниците и засегнатите страни им препорачува да ги консултираат директориумите на издадени и сторнирани сертификати секогаш пред да се потпрат на информацијата содржана на сертификатот.

5.6 Обврска за следење на поднесените информации

Во сите случаи за сите видови на КИБС сертификати, претплатникот (а не КИБС) има постојана обврска да ја следи точноста на доставената информација и да го извести КИБС за било кои измени.

5.7 Објавување на информациите

Објавените критични информации можат да бидат повремено ажурирани како што е пропишано во овие ПИС. Таквото ажурирање ќе биде индицирано преку соодветна верзија со нумерирање и објавување на податоците во нова верзија.

5.8 Интервенирање со КИБС имплементацијата

Претплатниците, засегнатите страни и други страни ќе се воздржат од надзор, интервенција или спротивставување на инженерска техничката имплементација на РКІ услугите на КИБС, вклучувајќи го процесот на генерирање на клуч, јавниот веб сајт и КИБС складиштата, освен како што е недвосмислено дозволено со оваа ПИС или по претходна писмена согласност на КИБС.

5.9 Стандарди

КИБС претпоставува дека корисничкиот софтвер, кој бара да биде во согласност со X.509 и друг соодветен стандард, ги применува барањата поставени во овие ПИС. КИБС не може да гарантира дека таквиот кориснички софтвер ќе подржи и примени потребни контроли од страна на КИБС доколку корисникот бара соодветен совет.

5.10 Ограничувања на КИБС партнерските врски

Партнерите во КИБС мрежата треба да се воздржат од преземање на активности кои можат да го загорзат, да го стават под сомневање или да ја намалат довербата на продуктите и услугите на КИБС. КИБС партнерите посебно треба да се воздржат од барањата на партнерските врски со други коренски овластувања или примена на процедури настанати од таквите авторитети.

5.11 Ограничување на одговорноста на КИБС за КИБС партнерите

Со оглед дека КИБС мрежата може да ги вклучи ЛРК кои работат спред КИБС постапките и процедурите, КИБС го гарантира интегритетот на сертификатите издадени под неговиот сопствен корен во границите на политиката за осигурување на КИБС и други ограничувања на гаранција кои се наведени во овие ПИС.



5.12 Одговорност на коренскиот потпис

За време на периодот во кој КИБС е коренски потпишан од друг коренски издавач на сертификати познат како Trust Anchors КИБС потврдува, дека е единствено одговорен кон претплатниците и засегнатите страни за стекнатата доверба со таквата врска. Издавачот на сертификат за потпишување на коренот има единствена обврска да осигура правилно вршење и интегритет на сертификатот за коренскиот потпис.

5.13 Избор на криптографски методи

Страните потврдуваат дека се единствено одговорни и независни во изборот на безбедносен софтвер, хардвер и алгоритми за криптографски/електронски потпис, вклучувајќи ги нивните соодветни параметри, процедури, техники како и PKI како решение за нивните потреби за безбедност.

5.14 Потпирање на непотврдени електронски потписи

Страните кои се потпираат на електронски сертификат мора да го потврдат електронскиот потпис во секое време со проверка на важноста на електронскиот сертификат според РПС или друг расположив директориум објавен од страна на КИБС. Засегнатите страни се предупредени дека непотврден електронски потпис не може да бидат одреден како потпис на претплатникот.

Доколку се потпира на непотврден потпис ризикува засегнатата страна, но не и КИБС.

Со помош на овие ПИС КИБС соодветно ги информираат засегнатите страни за употребата и потврдувањето на електронските потписи и друга документација објавена во неговото јавно складиште.

5.15 Издадени но неприфатени сертификати

Барателот на сертификат чие барање нема да биде прифатено како валидно, никогаш нема да може да креира електронски потписи користејќи приватен клуч кој соодветствува со јавниот клуч во сертификатот.

5.16 Одбивање за издавање на сертификат

КИБС го задржува своето право да одбие да издаде сертификат доколку смета дека тоа е соодветно, без навлекување врз себе одговорност за некаква загуба или трошоци настанати таквото одбивање.

5.17 Обврски на претплатникот

Доколку поинаку не е предвидено со овие ПИС претплатникот на КИБС, а не КИБС, треба да биде исклучиво одговорен за следното:

- Да поседува знаења или ако е потребно да побара обука за употребата на електронските сертификати и PKI.
- Безбедно да го генерира неговиот пар клучеви, со користење на безбеден систем.
- Да обезбеди точна и прецизна информација во неговата комуникација со КИБС.
- Да генерира нов пар клучеви со цел да ги користи со сертификат кој тој го бара од КИБС.

- Да ги прочита, разбере и да се согласи со сите термини и услови со овие ПИС и во врска со ова објавените политики во КИБС складиштето.
- Да се воздржи од фалсификување на КИБС сертификатот.
- Да го користи КИБС сертификатот за законски и овластени цели согласно овие ПИС на КИБС.
- Да го извести КИБС или КИБС РК за било која измена на поднесените информации;
- Да престане да го користи КИБС сертификатот доколку некоја информација во него доведува во заблуда, е застарена или е неважечка;
- Да престане да го користи КИБС сертификатот доколку сертификатот е со изминат рок и да го отстрани од апликациите и/или од средствата на кој бил инсталиран;
- Да се воздржи од употребата на приватниот клуч кој е соодветен на јавниот клуч во сертификат издаден од КИБС под негово име, за издавање на други сертификати;
- Да го користи КИБС сертификатот совесно, како што налагаат околностите;
- Да спречи компромитирање, губење, откривање, менување или неовластена употреба на неговиот приватен клуч;
- Да користи безбедни средства и продукти кои обезбедуваат соодветна заштита на клучевите;
- Работењето и пропустите на партнерите или застапниците кои тој ги користи за генерирање, чување, заложување или уништување на неговиот приватен клуч;
- Да се воздржи од поднесување до КИБС или на некој директориум на КИБС било каков материјал кој содржи изјави кои се клеветнички, колебливи, непристојни, пронографски, навредливи, нетрпеливи, одвратни, дискриминаторски, активности кои се нелегални или активности од нелегални дискусии, со намера со нив да се изврши или да се овозможи нарушување на закон.
- да гарантира дека јавниот клуч кој е поднесен до КИБС одговара со приватниот клуч кој го употребува,
- да гарантира дека јавниот клуч кој е поднесен до КИБС е точен,
- да бара суспендирање или поништување на сертификатот во случај на настан кој материјално влијае на интегритетот на КИБС сертификатот.

5.18 Претставување од страна на претплатникот по прифаќање на сертификат

По прифаќањето на сертификатот претплатникот се претставува на КИБС и на засегнатите страни дека од моментот на прифаќањето и до следното известување:

- Електронскиот потпис креиран со употреба на приватниот клуч кој одговара со јавниот клуч вклучен во сертификатот е електронски потпис на претплатникот и сертификатот е прифатен и оперативно подготвен од времето кога електронскиот потпис е креиран;
- Наовластено лице никогаш не пристапило до приватниот клуч на претплатникот;
- Сите претставувања кои се направени од страна на претплатникот до КИБС во врска со информациите содржани во сертификатот се точни и вистинити;
- Сите информации содржани во сертификатот се точни и вистинити со најдоброто знаење на претплатникот или до степен кога претплатникот известува за таквата информација, односно претплатникот треба веднаш да го извести КИБС за некоја материјална неточност во таа информација;



- Сертификатот се користи исклучиво за овластени и за законски цели, кои се содржани во овие ПИС;
- Употребува КИБС сертификат само во врска само со именуваниот ентитет во организационото поле на електронскиот сертификат (ако е применливо).
- Претплатникот ја задржува контролата на неговиот приватен клуч, употребува доберлив систем, и презема соодветни мерки на претпазливост за да го заштити од губење, откривање, менување или неовластено користење.
- Претплатникот е краен корисник, а не издавач на сертификат и нема да го користи приватниот клуч кој е соодветен со јавниот клуч наведен во сертификатот со цел да потпишува на некој сертификат (или некој друг формат од потврден јавен клуч) или РПС, како ИС или друго, освен ако изрично не е писмено договорено помеѓу претплатникот и КИБС;
- Претплатникот се согласува со термините и условите во овој ПИС и другите спогодби и политики на КИБС;
- Претплатникот се согласува со законите кои се во сила во неговата земја или територија вклучувајќи ги оние кои се однесуваат на заштитата на интелектуалната сопственост, вирусите, пристапувањето на компјутерските системи и тн;
- Претплатникот се согласува со сите надворешни закони и регулирања за двојна употреба на добрата, доколку е применливо.

5.19 Обештетување од претплатникот

Со прифаќањето на сертификатот, претплатникот се согласува да го обештети КИБС, како и неговите застапници и изведувачи, за постапки или пропусти кои произлегуваат од одговорност, и загуби или штети, судски постапки и трошоци од било каква природа, вклучувајќи трошоци за адвокатски услуги, кои што КИБС и напред наведените страни можат да ги претрпат, кои се причинети заради употреба или објавување на сертификат, и кои се настанати од:

- Лажни и погрешно презентирани податоци доставени од претплатникот или неговиот застапник(ци);
- Било каков пропуст на претплатникот да открие материјални докази, доколку погрешното презентирање или пропуст бил направен од негрижа или со намера да се измами ИС, или друго лице кое го прима или се потпира на сертификатот;
- Пропуст да го заштити приватниот клуч на претплатникот, да користи соодветен безбеден систем или да преземе потребни мерки на претпазливост за да се заштити од компромитирање, губење, откривање, менување или неовластена употреба на приватниот клуч на претплатникот;
- Кршење на закони кои се во сила во неговата земја или територија вклучувајќи ги и оние кои се однесуваат на заштитата на интелектуалната сопственост, вируси, пристапување кон компјутерските системи и тн.

5.20 Обврски на КИБС РК

КИБС РК работејќи во мрежата на КИБС се обврзува:

- да прима барања за КИБС сертификатите во согласност со овие ПИС ;
- да врши верификација пропишана со процедурите на КИБС и овие ПИС;
- да ги прима, верификува и пренесува до КИБС сите барања за поништување на КИБС сертификат во согласност со КИБС процедурите и овие ПИС.

5.21 Обврски на засегнатата страна

Страната засегната од КИБС сертификат се обврзува:

- да има познавања и доколку е потребна соосветна обука околу употребата на електронските сертификати и РКИ,
- да ги прочита и да се согласни со условите на ПИС на КИБС и со договорот со засегнатата страна или изјавата за откривање,
- да го проверува КИБС сертификатот со користење помеѓу другото и на РПС (вклучувајќи го РПС на КИБС) во согласност со процедурата за валидација на сертификат,
- верува на КИБС сертификатот само доколку сите содржани информации кои можат да бидат верификувани се коректни и ажурирани.
- се потпира на КИБС сертификатот, колку што е тоа разумно во дадените околности.

5.22 Законитост на информациите

Единствено претплатниците треба да бидат одговорни за законитоста на информациите кои тие ги презентираат, за да се употребат во сертификати издадени согласно овие ПИС, во надлежност во која таквата содржина може да биде употребена или разгледана.

5.23 Користење на застапници

За сертификатите издадени по барање на застапник на претплатникот, и застапникот и претплатникот треба заедно и посебно да го обештетат КИБС и неговите застапници и изведувачите.

5.24 Одговорност на претплатникот кон засегнатите страни

Без ограничување на други обврски на претплатникот наведени во овие ПИС, претплатниците се одговорни за сите лажни претставувања кои тие ги прават спрема трети лица, кои се потпираат на содржината во сертификатите и верифицирале еден или повеќе електронски потписи со сертификатот.

5.25 Обврска за надзор над застапниците

Претплатникот треба да ги контролира податоците кои застапникот може да ги поднесе до КИБС. Претплатникот мора веднаш да го извести издавачот за било какви лажни изјави или пропушти причинети од застапникот додека оваа должност трае.

5.26 Услови за употреба на КИБС складиштето и веб сајтот

Страните (вклучувајќи ги претплатниците и засегнатите страни) пристапувајќи до КИБС складиштето и веб сајтот се согласуваат со одредбите од овие ПИС и другите услови на употреба кои КИБС може да ги стави на располагање. Страните го покажуваат прифаќањето на условите за употреба на овие ПИС со тоа што поднесуваат барање во врска со статусот на електронски сертификат или било кој начин на употреба или потпирање на информациите или услугите. Условите за употреба на КИБС складиштата вклучуваат:

- Информации кои се обезбедуваат со пребарување за електронски сертификат;

- Верификација на статусот на електронските потписи креиран со приватен клуч кој одговара на јавниот клуч содржан во сертификатот;
- Информации објавени на веб сајтот на КИБС;
- Други услуги кои КИБС може да ги огласи или обезбеди преку неговиот веб сајт.

5.27 Потпирање на сопствен ризик

Ова е единствена одговорност на страните кои пристапуваат до информациите сместени во КИБС складиштата и веб сајтот за да проценат и да се потпрат на информациите наведени во истите.

Страните потврдуваат дека примиле соодветни информации за да одлучат дали да се потпрат на некоја информација обезбедена во сертификат.

КИБС ќе ги преземе сите потребни чекори за да ги ажурира записите и директориумите во поглед на статусот на сертификатите и ќе издаде предупредувања.

5.28 Точност на информациите

КИБС познавајќи ја својата позиција на доверба ги прави сите напори за да осигура дека страните пристапувајќи до складиштата добиваат прецизни, ажурирани и точни информации. КИБС, сепак, не може да прифати одговорност над лимитите поставени во овие ПИС и КИБС политиката на осигурување.

5.29 Непочитување

Непочитувањето на условите на употреба на КИБС складиштата и веб сајтот може да резултира во прекинување на врската помеѓу КИБС и страната.

5.30 Обврски на КИБС

Во рамките на содржаното во оддлни делови на овие ПИС, КИБС:

- ќе се придржува кон овие ПИС;
- ќе обезбедува инфраструктура и услуги за сертифицирање, вклучувајќи ги воспоставувањето и работењето на КИБС складиштето и веб сајтот за работа на РК услугите;
- ќе обезбедува механизми на доверба, вклучувајќи механизам за генерирање на клуч, заштита на клуч, и процедурите за тајно делење во врска со својата сопствена инфраструктура;
- веднаш ќе извести во случај на компромитирање на неговите приватни клучеви;
- ќе обезбедува и ќе ги потврдува процедурите за апликација за различните типови на сертификати кои може да ги направи јавно достапни;
- ќе издава електронски сертификати во согласност со овие ПИС и ги извршува обврските наведени во истите;
- по прием на барање од РК, која работи во мрежата на КИБС, веднаш ќе издаде КИБС сертификат во согласност со овие КИБС ПИС;
- по прием на барање за поништување од РК, која работи во мрежата на КИБС, веднаш ќе го поништи КИБС сертификат во согласност со овие КИБС ПИС;
- ќе ги објавува прифатените сертификати во согласност со овие ПИС;
- ќе обезбедува поддршка на претплатниците и засегнатите страни како што е опишано во овие ПИС;
- ќе ги поништува сертификатите во согласност со овие ПИС;

- ќе е грижи за периодот на важноста на и обновувањето на сертификатите согласно овие ПИС;
- ќе ги почитува одредбите објаснети и содржани во овие ПИС;
- по барање на страните, ќе стави на располагање копија од овие ПИС и политиките кои ги применува.

КИБС потврдува дека нема други обврски наведени во овие ПИС.

5.31 Способност за посебна цел

КИБС ги откажува сите гаранции и обврски за било кој тип, вклучувајќи ја и гаранцијата за погодност за посебна цел, и било која гаранција за точноста на непроверена информација.

5.32 Други гаранции

КИБС не гарантира:

- За точноста, автентичноста, комплетноста или погодноста од некои непотврдени информации содржани во сертификатите или на друг начин составени, објавени или дисеминирани за или во корист на КИБС, освен како што тоа може да биде изнесено во релевантниот продукт подолу опишан во овие ПИС и во КИБС политиката за осигурување;
- Нема да ја преземе одговорноста на себе за претставување на информација содржана во сертификат, освен како што тоа може да биде изнесено во релевантниот продукт подолу опишан во овие ПИС.
- Не гарантира за квалитетот, функциите или можностите на било кој софтвер.

5.33 Неверифицирана информација на претплатник

Покрај ограничувањето на гаранциите наведено во одделот за продуктите од овие ПИС, КИБС нема да биде одговорен за непроверените информации поднесени од претплатникот до КИБС, или КИБС директориумот или поднесени на поинаков начин со намера истите да бидат вклучени во сертификатот.

5.34 Исклучување од одредени елементи на штети

Во никој случај (освен во случај на измама или намерно лошо управување) КИБС нема да биде одговорен за:

- индиректни, случајни или последични штети;
- изгубена добивка;
- губење на податоци;
- други индиректни, последични или казнени штети настанати од или во врска со употребата, испораката, дозволата, можноста или неможноста на сертификатите или електронските потписи;
- други трансакции или услуги понудени или во рамките на овие ПИС;
- други штети освен оние настанати со потпирање на информации наведени во сертификат, на проверени информации во сертификат;
- одговорност настаната во случај кога вината во непроверената информација е настаната со измата или намерно лошо управување на барателот.



5.35 Ограничувања на штета и загуба

Во никој случај (освен во случај на измама или намерно лошо управување) КИБС нема да ја понесе одговорноста за сите страни, вклучувајќи ги без ограничување претплатникот, барателот, примачот или засегнатата страна за сите електронски потписи и трансакции кои се во врска со сертификат кој може да го надмине нивото на применливата одговорност за таков сертификат, како што е наведено во КИБС Планот за осигурување.

5.36 Спротивставеност на правила

Во случај кога овие ПИС се во спротивност со други правила, упатства, договори, овие ПИС ќе имаат предност и ќе го обврзуваат претплатникот и другите страни, освен во однос на други договори кои:

- По датум се склучени порано од првото јавно објавување на сегашната верзија на оваие ПИС;
- Недвосмислено ги заменуваат овие ПИС за што таквиот договор ќе биде раководен од договорните страни и во рамките дозволени со закон.

5.37 Права на интелектуална сопственост

КИБС или неговите партнери или здруженија ги поседуваат сите права на интелектуална сопственост кои се поврзани со нивните бази на податоци, веб сајтови, КИБС дигитални сертификати и други публикации кои потекнуваат од КИБС вклучувајќи ги и овие ПИС.

КИБС треба да ги обештети партнерите или здруженијата за било кој прекшок на нивните права на интелектуална сопственост.

5.38 Прекршителен и друг штетен материјал

КИБС претплатниците се претставуваат и гарантираат дека со поднесувањето до КИБС и употребата на доменот и карактеристично име (и сите други информации за аплицирање на сертификат) тие не пречат и не ги крашат правата на трети страни во ни една јуриisdикација од аспект на нивните трговски жигови, трговски имиња, имиња на друштвото, или други права на интелектуална сопственост и дека тие не бараат да го употребат доменот и карактеристичното име за незаконска цел вклучувајќи без ограничување, заобиколени пречки со договор или можна деловна предност, нелојална конкуренција, штетна репутација на друг и забуна или лажење на лице, било да е физичко или правно.

Претплатниците на сертификати ќе го штитат, обештетат и да го држат нештетен КИБС од загуба или штета кои се како резултат на пречка или прекршок.

5.39 Право на сопственост

Сертификатите се сопственост на КИБС. КИБС дава дозвола за репродуцирање и дистрибуирање на сертификати на неисклучив, на основа на royalty-free, обезбедени така што тие во потполност ги репродуцираат и ги дистрибуираат, освен оние сертификати кои не треба да бидат објавени во било кое јавно пристапно складиште или директоруим без изрично напишана дозвола од КИБС.

Ова ограничување има намера да ги заштити претплатниците од неовластени републикации на нивните лични податоци наведени во сертификатот.

Приватните и јавните клучеви се сопственост на претплатниците кои правилно ги издаваат и ракуваат со истите.



Приватниот клуч на КИБС ја задржува сопственоста на КИБС.

5.40 Важечка регулатива

Овие ПИС се изготвени согласно законите во Република Македонија. Овој избор на закон е направен за да се осигура единственоста во интерпретацијата на овие ПИС, безоглед на местото на престој или местото на употреба на КИБС електронските сертификати или други продукти и услуги. Законот во Република Македонија се применува во сите комерцијални или договорни односи на КИБС во кои овие ПИС можат да се применат или се наведени имплицитно или експлицитно во врска со КИБС производите и услугите каде КИБС работи како обезбедувач, снабдувач, корисник примач или друго.

5.41 Судска надлежност

Секоја страна, вклучувајќи ги и партнерите на КИБС, претплатниците и засегнатите страни, неотповикливо се согласуваат дека судот во Скопје има исклучива надлежност да сослушува и одлучува во некој процес, акција или постапки, и да решава спорови кои можат да настанат надвор од или во врска со овие ПИС или одредба во врска со КИБС сертификационите услуги.

5.42 Решавање на спор

Пред да се пристапи кон механизмот за решавање на спор, кој вклучува пресуда или друг вид на Алтернативно решавање на спор (вклучувајќи без исклучок мини судења, арбитража задолжителен стручен совет, набљудување во соработка и редовен стручен совет) страните се согласуваат да го известат КИБС за спорот со цел да се бара решавање на спорот.

5.43 Наследници и назначени

Овие ПИС се обврзувачки за наследниците, извршителите, следбениците, застапниците, администраторите и назначените, било да е изрична, да се подразбира или очигледна за страните. Правата и должностите кои се разработени во овие ПИС се однесуваат за страните, согласно со закон (вклучување кое е резултат на спојување или трансфер на контролиран интерес со тајни гласања) или друго, обезбедено такво доделување кое доследно е задржана со членовите за завршување или престанок на работа во овие ПИС, и обезбедува такво доделување кое нема ефект на обновување на други долгови или обврски одредената страна ги задолжува другите страни во време на таквото доделување.

5.44 Ништавност

Доколку некоја одредба од овие ПИС, или апликација која произлегува од истите, се утврди дека од некоја причина и во некој обем е неточна или неприменлива, останатиот дел од овие ПИС (и апликацијата од неточната или неприменливата одредба за други лица или околности) треба да биде интерпретирана на начин што ќе има ефект на оригиналната намера на страните.

Секоја одредба од овие ПИС кои обезбедуваат ограничување на одговорност, одрекување од или ограничување на некои гаранции или други обврски, или исклучување на штети е со намера да биде поделена и независна од друга одредба и да биде применета како таква.

5.45 Толкување

Овие ПИС треба да бидат доследно толкувани, во границите на деловните обичаи, трговските разбирања во околности и со намера на употреба за продукт и услуги. При интерпретирањето на овие ПИС, страните треба да водат сметка и на меѓународно поле и примена на услуги и продукти од КИБС, како и принципите на доверба кои се применуваат во комерцијални трансакции.

Заглавијата, подзаглавијата, и другите наслови во овие ПИС се само со намера за соодветно упатување и немаат намера да се користат во интерпретирање, конструирање и применување на некои од одредбите од овие ПИС.

Дополнувањата и дефинициите од овие ПИС, се интегрален и обврзувачки дел од овие ПИС.

5.46 Отстапување

Овие ПИС ќе се применуваат во целост, додека неизвршувањето на одредба од страна на лице нема да значи отстапување и во идната примена на таа или некоја друга одредба.

5.47 Известување

КИБС ги прифаќа известувањата кои се однесуваат на овие ПИС со електронски потпишани пораки или во хартиена форма. По приемот на важечка, дигитално потпишана потврда за прием од КИБС, испраќачот на известувањето треба да смета дека комуникацијата е успешно спроведена. Испраќачот мора да добие потврда во рок од пет (5) дена, или поинаку напишано писмено известување мора потоа да се прати во хартиена форма преку курир со потврда на испораката или преку потврдена или препорачана пошта, платена поштарина, со барање за повратен прием, адресирана:

КИБС АД Скопје,

К.Ј.Питу 1, 1000 Скопје, Македонија

URL: <http://ca.kibs.com.mk>

e-mail: ca-pravila@kibs.com.mk

5.48 Надоместоци

КИБС може да ги менува надоместоците на претплатниците за употреба на КИБС продуктите и услугите, кои се објавени на неговиот веб сајт. КИБС го задржува своето право за ефектот од промените на надоместоците.

5.49 Обврски по раскинување на договорот

Обврските и органичувањата содржани во дадените точки: *Контрола, Доверливи информации, Обврски на КИБС, и Ограничувања на таквите обврски и Одредбите под разво* ќе важат и по завршувањето на овие ПИС.



6. Општи процедури за издавање

Општите процедури наведени подолу, се применуваат за сите издадени КИБС сертификати. Во оваа точка се наведени процедурите за секој тип на сертификат посебно.

6.1 Општо

КИБС сертификатите нудат сигурен идентитет кои бараат лично претставување пред регистрационата канцеларија.

КИБС сертификатите се издаваат на физички лица (индивидуи) или на правни лица.

КИБС можат да употребуваат PIN софтвер за заштитена енкрипција за издавање на КИБС сертификати. Се препорачува криптографски модул, но не е задолжителен.

Периодот на важност на КИБС сертификатите е 1 година, или онака како е наведено на КИБС веб сајтот.

6.2 Индивидуи и организации

Барателот за сертификат користи online врска за пристап за регистрација на веб страните на КИБС. Следејќи го издавањето на сертификатот претплатникот мора да го извести КИБС за одредена неточност или грешка во сертификатот веднаш по приемот или порано, со забелешка за содржината која треба да биде вклучена во сертификатот.

6.3 Содржина

Содржината на информациите објавени во КИБС сертификатот обично ги вклучува следните елементи:

- e-mail адреса на барателот,
- име на барателот,
- јавен клуч на барателот,
- кодот на земјата на барателот,
- издавач на сертификатот (КИБС),
- електронски потпис на издавачот (КИБС),
- тип на алгоритам,
- период на важење на електронскиот сертификат,
- сериски број на електронскиот сертификат.

6.4 Поднесување на документи за идентификаување на барателот

ДОКУМЕНТИ ПОТРЕБНИ ЗА ИДЕНТИФИКУВАЊЕ НА БАРАТЕЛОТ НА СЕРТИФИКАТОТ(*)			
	Верба	Верба Про	Верба Сервер
Формулар за регистрација	X	X	X
Претплатнички договор	X	X	X
Лична карта/Пасош/Возачка дозвола	X	X	
Доказ за постоење на деловниот субјект		X	X
Овластување за аплицирање за сертификат		X	X

(*) РК го користи правото да побара дополнителни барања и дополнителни документирани докази во поглед на утврдувањето на идентитетот на барателот.

6.5 Време на потврдување на поднесените податоци

КИБС вложува реални напори да ги потврди информациите од барањето за сертификат и да издаде електронски сертификат во разумни временски рамки. За Верба Про потребно време за верификација е од 1 до 5 дена.

6.6 Процедура за издавање

Следните чекори го опишуваат процесот на издавањето на персонален сертификат:

1. Барателот пополнува online барање кое се наоѓа на веб сајтот на КИБС.
2. Барателот поднесува барани информации.
3. КИБС ја верификува e-mail адресата на барателот со испраќањена e-mail со URL од каде барателот може да продолжи со процедурата за регистрација.
4. Барателот ги поднесува бараните информации: e-mail адреса, заедничкото име, информации за организацијата, кодот за земјата, методот за верификација, и информации за плаќање.
5. Барателот го прифаќа online претплатничкиот договор.
6. Пар клучеви се генерираат на средство на барателот (компјутер, смарт картичка и тн.)
7. Јавниот клуч и online барањето автоматски се испраќаат до КИБС.
8. КИБС верификува со личното појавување пред ЛРК, доказ за професионален контекст и плаќање.
9. ЛРК/РК може позитивно да го верификува барателот.
10. КИБС може да издаде сертификат на барателот.
11. КИБС го објавува издадениот сертификат во online базата на податоци.
12. Обновување: дозволено.
13. Поништување: дозволено.

6.7 Осигурување

КИБС прифаќа одговорност како што е соопштено на веб сајтот: ca.kibs.ca.com.mk/repository.

6.8 Процедури за КИБС ВЕРБА сертификатите

КИБС Верба сертификатите нудат високо ниво на осигурување на идентитетот за што се бара лично присуство пред ЛРК. ЛРК, на основа на личното присуство го верификува идентитетот на барателот.

КИБС Верба сертификатите можат да се употребуваат за извршување на електронски трансакции кои подржуваат автентикација и електронски потписи базирани на сертификати како што е потпишување на електронски формулари и електронски документи, пристапување на веб страни, а исто така и за комерцијални трансакции со високи вредности, како што е електронското банкарство и извршување на договори.

КИБС Верба сертификатите се издаваат исклучиво само на лица-граѓани.

КИБС Верба сертификатите не бараат верификација на професионалната дејност на барателот. КИБС може да прифати одговорност до максимално ниво по загуба за одредени случаи на загуба, кои се наведени во КИБС Правилата на издавачот на сертификати.

КИБС Верба сертификатот содржи некои информативни податоци, вклучувајќи: e-mail адреса, име, јавен клуч, код на земјата, назив на издавач на сертификати – КИБС, електронски потпис на КИБС, алгоритам за контрола на потписот, период на важење, единствен сериски број.

Барателот изготвува online барање за сертификат на web страната на КИБС, а потоа барањето и јавниот клуч ги испраќа online до КИБС ИС.

Барателот печати online формулар за регистрација со јавниот клуч и online претплатнички договор, ги потпишува овие документи и ги предава на ЛРК со неговиот доказ за идентитет.

Барателот по успешното завршување на барањето за сертификат мора лично да се појави пред ЛРК.

ЛРК ги прима документите и ги верификува:

- податоците наведени во документите,
- идентитетот на барателот,
- плаќањето за сертификатот.

Доколку верификацијата е позитивна ЛРК го потврдува тоа и потврдувањето го испраќа до регистрационата канцеларија.

ЛРК ги чува копиите од документите на барателот. Ова досие се чува 2 години.

РК откако ќе ги добие документите, го верификува потписот на овластеното лице од ЛРК кој е потпишан на формуларот за регистрација и го иницира издавањето на сертификатот.

ИС на барателот му испраќа e-mail со URL или Интернет адреса од каде ќе може да биде подигнат КИБС Верба сертификатот.

РК го печати сертификатот и го чува во архива заедно со примените документи од ЛРК. Ова досие се чува 5 години.

На крајот од секој месец ЛРК испраќа фактура до РК.

Подршка:

За подршка, корисникот може да оди на веб страната на КИБС, каде е центарот за подршка, кој содржи упатства, најчесто поставени прашања и тн.

Обновување:

Корисникот може да го обнови сертификатот со посетување на веб страната на КИБС ИС и користејќи го неговиот сеуште важечки сертификат.

Поништување:

Корисникот може да го поништи неговиот сертификат online користејќи ја лозинката, која ја внел online во моментот на барањето на сертификатот или со испраќање на потпишано барање за поништување.

6.9 Процедури за КИБС Верба Про сертификатите

КИБС Верба Про сертификатите нудат високо ниво на осигурување на идентитетот за што се бара лично присуство пред локалната регистрациона канцеларија. Локалната регистрациона канцеларија, на основа на личното присуство го верификува идентитетот.

КИБС Верба Про сертификатите се употребуваат за електронски трансакции кои поддржуваат РКI (Public Key Infrastructure), како што е потпишување на електронски формулари и електронски документи, пристап на веб сајтови, како и за комерцијални трансакции со високи вредности, како електронско банкарство и извршување на договори.

КИБС Верба Про сертификатите се издаваат на лица во рамките на нивниот професионален контекст.

Барателот по успешното завршување на барањето за сертификат мора лично да се појави пред ЛРК.

Се проверува организациониот контекст на основа на доказот за организациониот контекст. КИБС може да прифати одговорност до максимално ниво по загуба за одредени случаи на загуба, кои се наведени во КИБС Правилата на издавачот на сертификати.

КИБС Верба Про сертификатот содржи информативни податоци кои вклучуваат: e-mail адреса, име, јавен клуч, код на земјата, назив на издавачот на сертификати - КИБС, електронски потпис на КИБС, алгоритам за контрола на потписот, период на важење, единствен сервиски број.

Барателот изготвува online барање за сертификат на веб страната на КИБС, а потоа барањето и јавниот клуч ги испраќа online до КИБС.

Барателот печати online формулар за регистрација со јавниот клуч и online претплатнички договор, ги потпишува овие документи, а истите ги потпишува и лицето кое ја претставува организацијата каде барателот е вработен. Ова лице мора да биде наведено во актите на организацијата. Барателот ги поднесува овие документи до ЛРК заедно со неговиот доказ за идентитет и доказ за постоење на организацијата.

ЛРК ги прима документите и ги верификува и тоа:

- Верифицирање на идентитетот и професионалниот контекст. Доколку верификацијата е позитивна локалната регистрациона канцеларија го потврдува тоа и потврдата ја испраќа до регистрационата канцеларија.
- Верификација на плаќањето за сертификат
- Ги чува копиите од документите на барателот. Ова досие се чува 2 години..

Откако РК ќе ги добие документите, го верификува потписот на овластеното лице од ЛРК кој е потпишан на формуларот за регистрација и иницира издавање на сертификатот. КИБС на барателот му испраќа e-mail со URL или интернет адреса од каде ќе може да биде превземен КИБС Верба Про сертификатот.

РК го печати сертификатот и го чува во архива заедно со примените документи од ЛРК. Ова досие се чува 5 години.

На крајот на секој месец ЛРК испраќа фактура до РК.



Подршка:

За подршка, корисникот може да оди на веб страната на КИБС ИС, каде е центарот за подршка, кој содржи упатства, најчесто поставени прашања и тн.

Обновување:

Корисникот може да го обнови сертификатот користејќи го неговиот сеуште важечки сертификат.

Поништување:

Корисникот може да го поништи неговиот сертификат online користејќи ја лозинката, која ја внел online во моментот на барањето за сертификат или со испраќање на потпишано барање за поништување.

6.10 Процедури за КИБС Верба Сервер сертификатите

Верба Сервер сертификатите се користат за автентикација на сервер, SSL енкрипција и за други намени. Со нив се утврдува идентитетот и сопственоста на името на доменот и се овозможува безбедна комуникација помеѓу серверите и помеѓу веб серверот и корисниците.

Верба Сервер сертификат се издава на деловен субјект на основа на негово барање.

Верификацијата на идентитетот на барателот се врши на основа на податоци од соодветни извори зависно од намената за која тој сака да го користи Верба Сервер сертификатот и тоа :

- документација за упис во трговскиот регистар,
- бази на податоци за деловни субјекти,
- известување за име на доменот или известување за намената за која сака да го користи Верба Сервер сертификатот,
- телефонски разговор со деловниот субјект и др.

КИБС ја прифаќа одговорноста која е пропишана во овие ПИС.

Прво, барателот мора да изготви барање за сертификат, кое го содржи јавниот клуч, креирано со софтверот од неговиот веб сервер.

Потоа, барателот ја посетува веб страната на КИБС ИС и го внесува неговото барање заедно со потребните информации за деловниот субјект. Формуларот за регистрација и договорот се печатат, се пополнуваат, се потпишуваат од страна на законскиот застапник на деловниот субјект.

Целокупната документација се испраќа по пошта до РК или лично се носи во РК и тоа:

- Формулар за регистрација,
- Претплатнички договорот,
- Документација за деловниот субјект,
- Доказ за извршено плаќање за сертификатот.

Деловниот субјект кој бара Верба Сервер сертификат за безбедна комуникација со веб страна, покрај наведената документација доставува и документ со кој се потврдува дека името на доменот е во сопственост на барателот.

Деловниот субјект кој бара Верба Сервер сертификат за друга намена, покрај наведената документација, наместо документ за името на доменот доставува известување дека Верба Сервер сертификатот нема да го користи за безбедна комуникација со веб страна и ќе ја наведе намената на истиот.



РК ги верификува документите на барателот и плаќањето. Посебно РК верификува дека името на законскиот застапник на деловниот субјект која бара сертификат е лицето кое е наведено во соодветните документи.

РК го иницира издавањето на КИБС Верба Сервер сертификатот. КИБС ИС го издава КИБС Верба Сервер сертификатот и на барателот му испраќа електронска порака со URL или интернет адреса, од каде што може да го преземе својот КИБС Верба Сервер сертификат.

РК ја архивира оригиналната документација која се однесува на барањето заедно со отпечатениот сертификат.

РК испраќа фактура на барателот.

КИБС Верба Сервер сертификатот содржи име на доменот, име на организацијата и организационата единица, кодот на земјата, издавачот на сертификат КИБС, електронскиот потпис на КИБС, алгоритмот за контрола на потписот, период на важење, единствен сериски број.

РК може да побара од барателот да достави документација за сопственоста на името и правата на трговскиот знак односно за податоците кои се поднесени за да бидат вклучени во сертификатот.

Поддршка:

За поддршка, корисникот може да оди на веб страната на КИБС, каде е центарот за поддршка, кој содржи упатства, најчесто поставени прашања и т.н.

Обновување:

Корисникот може да го обнови сертификатот со употреба на неговата лозинка или со испраќање на потпишано барање за обновување до РК.

Поништување:

Корисникот може да го поништи неговиот сертификат користејќи ја лозинката која е внесена во моментот на барањето на сертификатот или со испраќање на потпишано барање за поништување.

7. Дефиниции

АВТЕНТИЧНОСТ

Процес што се користи за да се потврди идентитет на лице или да се докаже интегритетот на одредени податоци со нивно ставање во вистински контекст и потврда на таква врска.

АВТОРИЗАЦИЈА

Доделување права.

АКРЕДИТАЦИЈА

Званична изјава од овластен субјект дека одредена функција/ентитет ги исполнува пропишаните услови.

АРХИВА

Чување на записи за одреден период од време со цел да се обезбеди нивна безбедност, копија или ревизија.

БАРАЊЕ ЗА ПОТПИШУВАЊЕ НА СЕРТИФИКАТ (БПС)¹

Електронски читлив формулар за барање на електронски сертификат.

БАРАЊЕ НА СЕРТИФИКАТ

Барање испратено од барател на сертификат до ИС за да му се издаде електронски сертификат.

БЕЗБЕДЕН СИСТЕМ

Компјутерски хардвер, софтвер и процедури кои обезбедуваат прифатливо ниво на безбедносни ризици, обезбедуваат доволно ниво на расположивост, доверливост и правилно работење и ја спроведуваат политиката на безбедност.

ВЕБ – МРЕЖА НА СВЕТСКО НИВО ²(www)

Графички базирана средина за публикување на документи и пронаоѓање на податоци на Интернет.

ВЕРБА, ВЕРБА ПРО, ВЕРБА СЕРВЕР СЕРТИФИКАТ

Сертификат со посебно ниво на доверба дефинирано од страна на КИБС ИС.

ВРЕМЕНСКИ ЖИГ³

Електронски потпишана потврда за одредена содржина на податоци во точно одредено време и датум.

ГЕНЕРИРАЊЕ ПАР НА КЛУЧЕВИ

Безбеден процес за креирање приватен клуч во текот на аплицирање за сертификат чиј соодветен јавен клуч се доставува до релеватниот ИС во тек на барањето за сертификат, на начин кој ја одразува способноста на барателот да го користи приватниот клуч.

ДИРЕКТОРИУМ

Постојано јавно објавуван именик на сертификати кој овозможува пронаоѓање на сертификат врз основа на неговиот идентификатор.

¹ CERTIFICATE SIGNING REQUEST (CSR)

² World Wide Web (www)

³ дефиниција од Законот за податоци во електронски облик и електронски потпис (бр. 34/2001, 6/2002)



ДОВЕРЛИВОСТ

Услов на откривање податоци само на одбрани и овластени страни.

ДОВЕРЛИВА ПОЗИЦИЈА

Улога во рамките на ИС која вклучува пристап или контрола на криптографските операции кои можат да дозволат привилегиран пристап до издавањето, употребата, суспендирање или поништување на сертификати, вклучувајќи операции кои го ограничуваат пристапот кон складиштето.

ЕДИНСТВЕНО КАРАКТЕРИСТИЧНО ИМЕ⁴

Збир на податоци кои во компјутер-базиран контекст идентификуваат ентитет од реалниот свет, како на пример лице или домен.

ЕКСТЕНЗИИ

Дополнителни полиња во X.509 v. 3.0 сертификатите.

ЕЛЕКТРОНСКИ ПОТПИС

Кодирање на порака со употреба на асиметричен криптосистем и хеш функција, така што лицето кое ја има иницијалната порака и јавниот клуч на потпишувачот може автоматски да одреди дали трансформацијата е креирана со употреба на приватен клуч кој соодветствува со јавниот клуч на потпишувачот и дали иницијалната порака е променета за време на трансформацијата.

ЕЛЕКТРОНСКИ СЕРТИФИКАТ

Форматирани податоци кои го поврзуваат идентификуваниот претплатник со јавниот клуч кој тој го користи.

ЗАСЕГНАТА СТРАНА

Ентитет кој се потпира на сертификат заради извршување на некоја активност.

ИДЕНТИФИКАТОР НА ОБЈЕКТ⁵

Низа на нумерички компоненти кои можат да бидат доделени на регистриран објект, кој има особина да биде единствен меѓу сите идентификатори на објекти во рамките на одреден домен.

ИДЕНТИФИКУВАЊЕ

Процес со кој се потврдува идентитетот на одреден ентитет. Идентификацијата се олеснува во рамките на криптографија со јавен клуч со употреба на сертификати.

ИЗВЕСТУВА

Соопштување на одредени податоци до друго лице, како што е предвидено со овие ПИС и применливиот закон.

ИЗВЕСТУВАЊЕ

Резултат од соопштувањето на вклучените страни во примањето на услугите на ИС, во согласност со овие ПИС.

ИЗДАВАЧ НА СЕРТИФИКАТИ (ИС)

Овластен издавач, каков што е КИБС, кој издава, суспендира или поништува електронски сертификати.

ИЗДАВАЊЕ НА СЕРТИФИКАТ

Испорака на електронски сертификат X 509 v3 за автентикација и електронски потпис, кој се базира на лични податоци и јавен клуч согласно на RFC 2527 and RFC 3039.

⁴ Relative Distinguished Name (RDN)

⁵ OID (Object Identifier)



ИНФРАСТРУКТУРА СО ЈАВЕН КЛУЧ (PKI)

Архитектурата, организацијата, техниките, постапките и процедурите кои заедно го поддржуваат имплементирањето и работата на криптографски систем базиран на јавен клуч.

ИСТЕКУВАЊЕ НА СЕРТИФИКАТ

Крајот на периодот на важност на електронскиот сертификат.

ЈАВЕН КЛУЧ

Математички клуч кој може да биде јавно достапен и кој се користи за верифицирање на потписи креирани со неговиот соодветен приватен клуч. Во зависност од алгоритмот, јавните клучеви можат исто така да се користат за шифрирање на пораки или документи кои потоа можат да се дешифрираат со соодветниот приватен клуч.

ЈАВНИ СЕРТИФИКАЦИОНИ УСЛУГИ НА КИБС

Систем за електронско сертифицирање кој го нуди КИБС, како и ентитетите кои припаѓаат во доменот на КИБС, како што е опишано во овие ПИС.

КОМПРОМИТИРАЊЕ

Повреда на политиката на безбедност која има за резултат губење на контролата врз чувствителна информација.

КРАЕН КОРИСНИК - ПРЕТПЛАТНИК

Претплатник на сертификат, кој не е друг издавач.

КРИПТОГРАФИЈА НА ЈАВЕН КЛУЧ

Криптографија која користи пар на клучеви од математички поврзани криптографски клучеви.

ЛОКАЛНА РЕГИСТРАЦИОНА КАНЦЕЛАРИЈА (ЛРК)

Локалните регистрациони канцеларии ги евидентираат податоците аз претплатниот и личните податоци во корист на регистрационата канцелација (РК). Генерално кажано, ЛРК е субјект (организација) назначена од издавачот на сертификат, која треба да врши регистрација на барањата за електронски сертификати.

НЕПОТВРДЕНИ ПОДАТОЦИ ЗА ПРЕТПЛАТНИК

Податоци поднесени од страна на барател за сертификат до ИС, и објавени во сертификат, кој не е потврден од ИС и за кој ИС не дава гаранција освен дека податоците биле доставени од барателот на сертификатот. Таквите податоци вклучуваат титули, степен на професионално образование и др.

НОСИТЕЛ НА ТАЕН ДЕЛ

Лицето кое го чува тајниот дел.

ОБВРЗУВАЧКА ИЗЈАВА

Изјава од РК за поврзаноста помеѓу именуваниот ентитет и неговиот јавен клуч.

ОСИГУРУВАЊЕ

Комплет од изјави и однесувања кои имаат за цел да се пренесе општа намера.

ПАМЕТНА КАРТИЧКА

Хардверски дел кои содржи меѓу другото и чип за имплементирање на криптографски функции.

ПАР КЛУЧЕВИ

Приватен клуч и неговиот соодветен јавен клуч во асиметрично шифрирање.

ПОНИШТУВАЊЕ НА СЕРТИФИКАТ

Услуга која се користи да се оневозможи трајно (поништи) електронскиот сертификат пред неговата дата на истекување.



ПОВИКУВАЊЕ СО РЕФЕРЕНЦА

Да се направи еден документ да стане дел од друг со идентификување на документот кој треба да се вгради, со информација која овозможува примачот да пристапи и да ја добие вградената порака во целост и со изразување на намерата таа да биде дел од порака во која е вградена. Таквата вградена порака ќе го има истото значење како да била во целост наведена во пораката.

ПОДОБРЕНО ИМЕНУВАЊЕ

Користење на дополнително организациско поле (OU=) во X.509 v.3.0 сертификат.

ПОТПИРАЊЕ НА ЕЛЕКТРОНСКИ ПОТПИС

Прифаќање на електронски потпис и однесување на начин кој одразува доверба во него.

ПОТПИСНИК

Лице кои креира електронски потпис за порака, или потпис за документ.

ПРАВИЛА НА ИЗДАВАЧОТ НА СЕРТИФИКАТОТ (ПИС)

Правила за постапките на ИС и условите за издавање, суспендирање, поништување и др. на сертификат.

ПРЕТПЛАТНИК

Субјект од електронски сертификат кој го употребува приватниот клуч што соодветствува со јавниот клуч наведен во сертификатот.

ПРЕТПЛАТНИЧКИ ДОГОВОР

Договорот помеѓу претплатникот и ИС за давање јавни услуги на сертифицирање.

ПРИВАТЕН КЛУЧ

Математички клуч кој креира електронски потписи и понекогаш (во зависност од алгоритмот) кој дешифрира пораки во комбинација со соодветен јавен клуч.

ПРИФАЌАЊЕ (НА СЕРТИФИКАТ)

Прифаќање на електронски сертификат од страна на барател на сертификат во рамките на процесот на барање и добивање на сертификат.

ПРОЦЕДУРИ НА КИБС

Документ во кој се опишани процедурите за внатрешната безбедност и управувањето со сертификатите.

ПРОЦЕС НА ГЕНЕРИРАЊЕ ПАР НА КЛУЧЕВИ

Безбеден процес на креирање на пар приватен/јавен клуч. Јавниот клуч му се доставува на ИС во текот на процесот на барање на сертификат.

РАСПОЛОЖИВОСТ

Степенот на достапност на податоци или извори.

РЕГИСТАР НА ПОНИШТЕНИ СЕРТИФИКАТИ

Регистар издаден и електронски потпишан од ИС кој ги содржи поништените и суспендираните сертификати. Овие листи ги користат засегнатите страни за да се консултираат пред да се потпрат на податоците содржани во сертификатот.

РЕГИСТРАЦИОНА КАНЦЕЛАРИЈА (РК)

Субјект кој е одговорен да ги идентификува и автентичира претплатниците. РК не издава сертификати. Во рамките на доменот на КИБС, КИБС ја извршува функцијата на РК.

СЕРИСКИ БРОЈ НА СЕРТИФИКАТОТ

Последователен број кој единствено го дефинира сертификатот во рамките на доменот на ИС.



СЕРТИФИКАТ

Потврда која ги поврзува јавниот клуч и информациите за субјектот, електронски потпишана со приватен клуч од страна на издавачот на сертификати.

СЕРТИФИКАЦИЈА

Процес на поврзување на јавниот клуч со информациите за субјектот содржани во сертификатот.

СКЛАДИШТЕ

База на податоци и/или директориум со преглед на електронски сертификати и други релевантни информации кои се постојано пристапни.

СУБЈЕКТ НА ЕЛЕКТРОНСКИ СЕРТИФИКАТ

Имателот на приватниот клуч кој соодветствува со јавниот клуч од сертификатот.

СУСПЕНДИРАН СЕРТИФИКАТ

Привремено отстранет сертификат.

СУСПЕНДИРАЊЕ НА СЕРТИФИКАТ

Постојана услуга која се користи привремено да се оневозможи електронскиот сертификат и автоматски да се поништи доколку нема барање за реактивирање и истото не е поднесено во одреден временски период.

ТАЕН ДЕЛ

Дел од криптографска тајна која се дели меѓу одреден број физички токени, како што се смарт картичките и др.

УПРАВУВАЊЕ СО СЕРТИФИКАТИТЕ

Активности поврзани со управување со сертификатите кои вклучуваат чување, дисеминација, објавување, поништување и суспендирање на сертификати.

УСЛУГА ЗА СТАТУСОТ НА СЕРТИФИКАТОТ

Услуга, која овозможува на засегнатите страни и на други лица проверка на статусот на сертификатите.

ХЕШ

Алгоритам кој пресликува или преведува едно множество на битови во друго (обично помало) множество на таков начин што:

- пораката го дава истиот резултат секогаш кога се извршува алгоритмот со користење на истата порака како влезна информација.
- пресметковно е неизводливо пораката да биде добиена или повратена од резултатот добиен со алгоритмот.
- пресметковно е неизводливо да се најдат две различни пораки кои го даваат истиот хеш резултат со користење на истиот алгоритам.

ХИЕРАРХИЈА НА СЕРТИФИКАТИ

Подредена секвенца на сертификати кои го содржат сертификатот на претплатникот краен-корисник и сертификатите на ИС.

X.509

Стандард за дигитални сертификати на ITU-T (Интернационално Здружение за телекомуникации-Т).



Контрола на документот и референци

КИБС АД Скопје	К.Ј. Питу 1, 1000 Скопје, Македонија
URL:http://ca.kibs.com.mk	Тел : + 389 (0)2 3297 400
E-mail: ca-info@kibs.com.mk	Факс:+ 389 (0)2 3290 909

БЕЛЕШКА ЗА АВТОРСКИТЕ ПРАВА

Copyright © КИБС АД Скопје. Сите права се задржани.

Ни еден дел од оваа публикација не смее да се репродуцира, складира или воведе во некој информациски систем, ниту да се пренесе, во било каква форма и на било кој начин (електронски, механички, со фотокопирање, преснимување или со други средства), без претходна писмена дозвола од КИБС АД Скопје.

Барања за било каква друга дозвола за репродукција на овој документ на КИБС АД Скопје (како и барања за копии од КИБС АД Скопје) мора да бидат доставени на следнава адреса:

КИБС АД Скопје

К.Ј.Питу 1,

1000 Скопје, Македонија

E-mail: ca-pravilal@kibs.com.mk

Заштитениот знак “Верба” е регистрирана трговска марка на КИБС АД Скопје.

Промени во документот

Верзијата 1.0 е прва верзија на документот (28.11.2003)

Верзијата 1.1 е втора верзија на документот (02.11.2004) со измени и дополнувања на потпоглавјето 6.10

Верзијата 1.2 е трета верзија на документот (29.05.2006) со измени и дополнувања на преамбулата и во потпоглавјата 1.1, 2.4.1, 2.4.2 и 3.14.1.