



Правила на КИБС за издавање на квалификувани сертификати

Верзија 2.0

Дата на стапување на сила: април 2010 година

КИБС АД
К.Ј. Питу 1
1000, Скопје
Република Македонија
Тел. +389 2 3297 400
www.kibs.com.mk

Правила на КИБС за издавање на квалификувани сертификати

Објавено на дата: Април 2010

Белешки за трговската марка

КИБС е регистрирана марка на КИБС АД. ADACOM е регистрирана марка на ADACOM SA. VeriSign е регистрирана трговска марка на VeriSign, Inc. VeriSign логото, VeriSign доверливата мрежа и NetSure се трговски марки и сервисни марки на VeriSign, Инс. Другите трговски марки и услужни марки во овој документ се сопственост на нивните релевантни сопственици.

Без да се ограничуваат погоре заштитените права, освен онаму каде што е дозволено подолу, ниеден дел од оваа публикација не смее да се репродуцира, складира или воведе во систем од кој може да биде преземена, или да се пренесува, во било која форма или на било кој начин (електронски, механички, со фотокопирање, снимање или на друг начин) без претходна писмена дозвола од КИБС АД.

Барања за било каква друга дозвола за репродуцирање на овие Правила на КИБС за издавање на квалификувани сертификати (како и барања за копии од КИБС АД) мора да се адресираат на КИБС АД, К.Ј. Питу 1, 1000, Скопје, Република Македонија, тел: ++389 2 3297 400 факс: +389 2 3297 497 e-mail: ca-info@kibs.com.mk .

Содржина

| | | |
|-----------|--|-----------|
| 1 | ВОВЕД | 10 |
| 1.1. | Преглед | 11 |
| 1.2. | Име на документот и идентификација | 12 |
| 1.3. | Учесници | 12 |
| 1.3.1. | Издавачи на сертификати | 12 |
| 1.3.2. | Регистрациска канцеларија | 13 |
| 1.3.3. | Претплатници | 13 |
| 1.3.4. | Засегнати страни | 14 |
| 1.3.5. | Други учесници | 14 |
| 1.4. | Користење на сертификатите | 14 |
| 1.4.1. | Дозволена употреба на сертификатите | 14 |
| 1.4.2. | Забранета употреба на сертификатите | 15 |
| 1.5. | Администрирање на Правилата | 15 |
| 1.5.1. | Организација што го администрира документот | 15 |
| 1.5.2. | Лице за контакт | 15 |
| 1.5.3. | Соодветност на овие Правила со СР | 15 |
| 1.5.4. | Процедури за одобрување на Правилата | 15 |
| 1.6. | Дефиниции и кратенки | 16 |
| 2 | ОДГОВОРНОСТИ ПОВРЗАНИ СО ОБЈАВУВАЊЕ И СМЕСТУВАЊЕ | 17 |
| 2.1 | Складишта | 17 |
| 2.2 | Објавување на информации за сертификати | 17 |
| 2.3. | Време и периодичност на објавување | 17 |
| 2.4. | Контрола на пристап во складиштата | 18 |
| 3. | ИДЕНТИФИКАЦИЈА И ПРОВЕРКА НА АВТЕНТИЧНОСТА | 19 |
| 3.1 | Именување | 19 |
| 3.1.1 | Типови на имиња | 19 |
| 3.1.2 | Потреба имињата да имаат значење | 20 |
| 3.1.3 | Анонимност или псевдоними на претплатниците | 20 |
| 3.1.4 | Правила за интерпретирање на различни именски форми | 20 |
| 3.1.5 | Единственост на имињата | 20 |
| 3.1.6 | Признавање, проверување и улога на трговските марки | 20 |
| 3.2 | Првична потврда на идентитетот | 21 |
| 3.2.1 | Метод за докажување на сопственоста врз приватен клуч | 21 |
| 3.2.2 | Потврдување на идентитетот на личноста | 21 |
| 3.2.3 | Информација за претплатникот што не се проверува | 21 |
| 3.2.4 | Потврдување на овластување | 21 |
| 3.3 | Идентификација и автентикација за барања за обнова на пар на клучеви | 22 |
| 3.3.1. | Идентификација и автентикација за рутинска обнова на пар на клучеви | 22 |
| 3.3.2. | Идентификација и автентикација за обнова на пар на клучеви после поништување | 22 |
| 3.4 | Идентификација и автентикација за барање за поништување | 22 |
| 4. | ОПЕРИРАЊЕ СО ЖИВОТНИОТ ЦИКЛУС НА СЕРТИФИКАТОТ | 24 |

| | | |
|--------|--|----|
| 4.1. | Барање за сертификат | 24 |
| 4.1.2. | Процес на регистрирање и одговорности | 24 |
| 4.2 | Обработка на барањето за сертификат | 25 |
| 4.2.1. | Извршување на функциите за идентификација и автентикација | 25 |
| 4.2.2. | Одобрување или одбивање на барањата за сертификати | 25 |
| 4.2.3. | Време на обработка на апликациите за сертификат | 25 |
| 4.3. | Издавање на сертификат | 25 |
| 4.3.1. | Активности на КИБС ИС за време на издавање на сертификатот | 25 |
| 4.3.2. | Известување на претплатникот од страна на КИБС ИС за издавање на сертификатот | 25 |
| 4.4. | Прифаќање на сертификатот | 26 |
| 4.4.1. | Однесување кое означува прифаќање на сертификат | 26 |
| 4.4.2. | Објавување на сертификатот од страна на КИБС ИС | 26 |
| 4.4.3. | Известување за издавање на сертификатот од страна на КИБС ИС до други ентитети | 26 |
| 4.5. | Користење на парот клучеви и сертификатот | 26 |
| 4.5.1. | Користење на претплатничкиот приватен клуч и сертификатот | 26 |
| 4.5.2. | Користење на јавниот клуч и сертификатот од страна на засегнатите страни | 26 |
| 4.6. | Обновување на сертификат | 27 |
| 4.6.1. | Околности за обновување на сертификатот | 27 |
| 4.6.4. | Известување за издавањето на сертификатот до претплатникот | 27 |
| 4.6.6. | Објавување на обновување на сертификат од страна на КИБС ИС | 27 |
| 4.6.7. | Известување за издавање на сертификатот од страна на СА до други ентитети | 27 |
| 4.7. | Обновен сертификат со нов пар клучеви (Certificate Re-Key) | 27 |
| 4.7.1. | Околности за обновување на сертификатот со нов пар клучеви | 27 |
| 4.7.2. | Кој може да побара сертифицирање на нов јавен клуч | 28 |
| 4.7.3. | Обработка на барања | 28 |
| 4.7.4. | Известување за издавање на новиот сертификат до претплатникот | 28 |
| 4.7.5. | Однесување кое означува прифаќање на сертификат | 28 |
| 4.7.6. | Објавување на обновен сертификат со нов пар клучеви | 28 |
| 4.7.7. | Известување за издавање на сертификатот од страна на КИБС ИС до други ентитети | 28 |
| 4.8. | Изменување на сертификат | 28 |
| 4.8.1. | Околности за изменување на сертификат | 28 |
| 4.8.2. | Кој може да побара измени во сертификатот | 28 |
| 4.8.3. | Обработка на барањата за измени во сертификатот | 29 |
| 4.8.4. | Известување за издавање на нов сертификат | 29 |
| 4.8.5. | Однесување кое означува прифаќање на изменетиот сертификат | 29 |
| 4.8.6. | Објавување на новиот сертификат од страна на КИБС ИС | 29 |
| 4.8.7. | Известување за издавање на сертификатот од страна на СА до други ентитети | 29 |
| 4.9. | Поништување и суспендирање на сертификати | 29 |
| 4.9.1. | Околности за поништување | 29 |
| 4.9.2. | Кој може да побара поништување | 30 |
| 4.9.3. | Процедура за барање за поништување | 30 |
| 4.9.4. | Греис период за барање за поништување | 30 |
| 4.9.5. | Време за кое ИС мора да го процесира барањето за поништување | 30 |
| 4.9.6. | Барања за проверка на поништувањето за засегнатите страни | 31 |
| 4.9.7. | Интервали на издавање на РПС | 31 |
| 4.9.8. | Максимално доцнење на РПС | 31 |

| | | |
|-----------|---|-----------|
| 4.9.9. | Достапност на електронска проверка на статусот во врска со поништување | 31 |
| 4.9.10. | Барања за електронска проверка за поништување | 31 |
| 4.9.11. | Други достапни облици на огласување за поништување | 31 |
| 4.9.12. | Посебни барања во врска со компромитирање на клуч | 31 |
| 4.9.13. | Околности за суспендирање | 32 |
| 4.9.14. | Кој може да побара суспендирање | 32 |
| 4.9.15. | Процедура за барање за суспендирање | 32 |
| 4.9.16. | Ограничувања за периодот на суспензија | 32 |
| 4.10. | Услуги во врска со статусот на сертификатите | 32 |
| 4.10.1. | Оперативни карактеристики | 32 |
| 4.10.2. | Достапност на услугите | 32 |
| 4.10.3. | Опционални карактеристики | 32 |
| 4.11. | Крај на претплатата | 32 |
| 4.12. | Давање на чување кај трето лице и повторно преземање | 32 |
| 4.12.1. | Политика и практики за давање на чување кај трето лице и повторно преземање | 32 |
| 4.12.2. | Политика и практики за инкапулирање на сесиски клуч и повторно преземање | 32 |
| 5. | КОНТРОЛИ НА ПОСТРОЈКИТЕ, МЕНАЏМЕНТОТ И ОПЕРАТИВНИ КОНТРОЛИ | 33 |
| 5.1. | Физички контроли | 33 |
| 5.1.1. | Локација и конструкција | 33 |
| 5.1.2. | Физички пристап | 33 |
| 5.1.3. | Електрична енергија и климатизација | 34 |
| 5.1.4. | Изложување на вода | 34 |
| 5.1.5. | Превентива и заштита од пожар | 34 |
| 5.1.6. | Складирање на медиумите | 34 |
| 5.1.7. | Отстранување на отпадот | 34 |
| 5.1.8. | Резервни копии надвор од деловните простории | 34 |
| 5.2. | Процедурални контроли | 34 |
| 5.2.1. | Доверливи улоги | 34 |
| 5.2.2. | Број на лица потребни за една работна задача | 35 |
| 5.2.3. | Идентификација и автентикација за секоја позиција | 35 |
| 5.2.4. | Позиции за кои е потребно одвојување на должностите | 36 |
| 5.3. | Контроли на персоналот | 36 |
| 5.3.1. | Предуслови за квалификации и искуство | 36 |
| 5.3.2. | Процедури на проверка на биографијата | 36 |
| 5.3.4. | Услови и период на повторна обука | 37 |
| 5.3.5. | Период и редослед на ротирање на работните места | 37 |
| 5.3.6. | Санкции за неовластени дејствија | 37 |
| 5.3.7. | Предуслови за независни лица по договор | 37 |
| 5.3.8. | Документација што му се обезбедува на персоналот | 37 |
| 5.4. | Процедури за ревизорска трага (Audit logging Procedures) | 38 |
| 5.4.1. | Видови на настани што се евидентираат | 38 |
| 5.4.2. | Интервал на преглед на ревизорски траги | 38 |
| 5.4.3. | Период на зачувување на ревизорските траги | 39 |
| 5.4.4. | Заштита на ревизорските траги | 39 |
| 5.4.5. | Процедури за правење безбедносни копии на ревизорските траги | 39 |

| | | |
|-------------|--|-----------|
| 5.4.6. | Систем за логирање на податоците..... | 39 |
| 5.4.7. | Известување до субјектот што го предизвикал настанот | 39 |
| 5.5. | Архивирање на записите..... | 39 |
| 5.5.1 | Видови на записи кои се архивираат | 39 |
| 5.5.2 | Период на зачувување на архивата | 40 |
| 5.5.3. | Заштита на архивата | 40 |
| 5.5.4. | Процедури за архивирање | 40 |
| 5.5.5. | Предуслови за временски печат на документацијата | 40 |
| 5.5.6. | Систем за правење на архивата | 40 |
| 5.5.7 | Процедури за добивање и верификување на интегритет на архивски податоци..... | 40 |
| 5.6. | Промена на клучеви..... | 40 |
| 5.7. | Опоравување од компромитирање и од кризни ситуации | 41 |
| 5.7.1. | Процедури за справување со инциденти и компромитирање..... | 41 |
| 5.7.2. | Компромитирани компјутерски ресурси, софтвер и/или податоци..... | 41 |
| 5.7.3. | Процедури при компромитирање на приватниот клуч на ентитети..... | 41 |
| 5.7.4. | Способност за продолжување на деловните активности по кризна ситуација | 42 |
| 5.8. | Прекин на дејноста на КИБС ИС..... | 43 |
| 6. | КОНТРОЛИ НА ТЕХНИЧКАТА БЕЗБЕДНОСТ | 45 |
| 6.1. | Генерирање и инсталирање на пар на клучеви | 45 |
| 6.1.1. | Генерирање на пар клучеви | 45 |
| 6.1.2. | Испорака на приватниот клуч на претплатникот..... | 45 |
| 6.1.3. | Испорака на јавниот клуч на издавачот на сертификати..... | 45 |
| 6.1.4. | Испорака на јавниот клуч на засегнатите страни..... | 45 |
| 6.1.5. | Големина на клучевите | 46 |
| 6.1.6. | Параметри на генерирање јавен клуч и проверка на квалитетот | 46 |
| 6.2. | Заштита на приватен клуч и инженерски контроли на криптографскиот модул..... | 46 |
| 6.2.1. | Стандарди и контроли за криптографски модули | 46 |
| 6.2.2. | Контрола на приватен клуч од повеќе лица (м од н) | 47 |
| 6.2.3. | Давање на чување на приватните клучеви | 47 |
| 6.2.4. | Резервно складирање на приватните клучеви | 47 |
| 6.2.5. | Архивирање на приватните клучеви | 47 |
| 6.2.6. | Префрлување на приватните клучеви во или од криптографскиот модул..... | 47 |
| 6.2.7. | Складирање на приватниот клуч на криптографски модул | 48 |
| 6.2.8. | Метод на активирање на приватниот клуч | 48 |
| 6.2.9. | Метод на деактивирање на приватен клуч | 49 |
| 6.2.10. | Метод на уништување на приватен клуч | 49 |
| 6.2.11. | Рангирање на криптографскиот модул | 49 |
| 6.3. | Други аспекти на управување на пар клучеви | 49 |
| 6.3.1. | Архивирање на јавни клучеви | 49 |
| 6.3.2. | Оперативни периоди на сертификатите и периоди на користење на паровите на клучеви..... | 49 |
| 6.4. | Податоци за активирање | 50 |
| 6.4.1. | Генерирање и инсталирање на податоци за активирање | 50 |
| 6.4.2. | Заштита на податоци за активирање | 51 |
| 6.4.3. | Други аспекти на податоците за активирање | 51 |
| 6.5. | Контроли за безбедност на компјутерите | 51 |

| | | |
|-----------|--|-----------|
| 6.5.1. | Посебни технички услови за компјутерска безбедност | 51 |
| 6.5.2. | Рангирање на безбедноста на компјутерите..... | 52 |
| 6.6. | Технички контроли на животниот циклус | 52 |
| 6.6.1. | Контроли за развој на системот | 52 |
| 6.6.2. | Контроли за управување на безбедноста | 52 |
| 6.6.3. | Безбедносни контроли на животниот циклус | 52 |
| 6.7. | Контроли за безбедност на мрежата | 52 |
| 6.8. | Временски печат..... | 53 |
| 7. | ПРОФИЛИ НА СЕРТИФИКАТИ, РПС И ОСРР | 54 |
| 7.1. | Профили на сертификати | 54 |
| 7.1.1. | Нумерирање на верзии..... | 54 |
| 7.1.2. | Екстензии за сертификати..... | 55 |
| 7.1.3. | Алгоритамски предметни идентификатори..... | 57 |
| 7.1.4. | Форми на имиња | 57 |
| 7.1.5. | Ограничувања на имињата | 57 |
| 7.1.6. | Предметен идентификатор на Политика за сертификати | 57 |
| 7.1.7. | Користење на екстензијата за ограничувања на политиката | 57 |
| 7.1.8. | Синтакса и семантика на квалификаторите на политиката | 58 |
| 7.1.9. | Процесирачка семантика за критичните екстензии за сертификациските политики | 58 |
| 7.2. | Профил на РПС..... | 58 |
| 7.2.1 | Нумерирање на верзии..... | 58 |
| 7.2.2. | РПС и проширувањата на записот во РПС..... | 58 |
| 7.3. | ОСРР Профил | 58 |
| 7.3.1. | Нумерирање на верзии..... | 58 |
| 8. | НАДЗОР ВО ВРСКА СО УСОГЛАСЕНОСТА И ДРУГИ ПРОЦЕНКИ | 59 |
| 8.1. | Интервали и околности на оценките | 59 |
| 8.2. | Идентитет и квалификации на оценителот..... | 59 |
| 8.3. | Прашања на кои се однесува оценката..... | 59 |
| 8.4. | Дејствија што се преземаат како резултат на пропустите | 59 |
| 8.5. | Соопштување на резултатите..... | 60 |
| 9 | ОСТАНАТИ ДЕЛОВНИ И ПРАВНИ РАБОТИ | 61 |
| 9.1. | Надоместоци | 61 |
| 9.1.1. | Надоместоци за издавање и обновување на сертификати | 61 |
| 9.1.2. | Надоместоци за пристап до сертификатите | 61 |
| 9.1.3. | Надоместоци за пристап до информациите за поништување или за статусот на сертификатот..... | 61 |
| 9.1.4. | Надоместоци за други услуги..... | 61 |
| 9.1.5. | Политика на рефундирање (поврат на средства) | 61 |
| 9.2. | Финансиска одговорност | 61 |
| 9.2.1. | Покривање на осигурувањето..... | 61 |
| 9.2.2. | Други средства | 61 |
| 9.3. | Доверливост на деловните информации..... | 62 |
| 9.3.1. | Опсег на доверливи информации | 62 |
| 9.3.2. | Информации што не се во доменот на доверливи информации..... | 62 |
| 9.3.3. | Одговорност за заштитата на доверливите информации | 62 |

| | |
|---|----|
| 9.4. Приватност на личните информации | 62 |
| 9.4.1. План за лични податоци | 62 |
| 9.4.2. Лични податоци што се третираат како приватни..... | 62 |
| 9.4.3. Лични податоци што не се сметаат за приватни..... | 62 |
| 9.4.4. Одговорност за заштита на приватните податоци..... | 62 |
| 9.4.5. Известување и согласност за користење на лични податоци | 63 |
| 9.4.6. Откривање што произлегува од судски или административен процес..... | 63 |
| 9.4.7. Откривање по барање на сопственикот..... | 63 |
| 9.4.8. Други околности на откривање информации..... | 63 |
| 9.5. Права на интелектуална сопственост | 63 |
| 9.5.1. Права на сопственост во сертификатите и информациите за поништување | 63 |
| 9.5.2. Права на сопственост на Правилата | 63 |
| 9.5.3. Права на сопственост во имиња | 63 |
| 9.5.4. Права на сопственост на клучевите и материјалот со клучеви | 64 |
| 9.6. Претставувања и гаранции | 64 |
| 9.6.1. ИС Претставувања и гаранции | 64 |
| 9.6.2. РК претставувања и гаранции | 64 |
| 9.6.3. Претставувања и гаранции на претплатникот..... | 64 |
| 9.6.4. Претставувања и гаранции на засегнатата страна | 65 |
| 9.6.5. Претставувања и гаранции на други учесници | 65 |
| 9.7. Одредување на гаранциите | 65 |
| 9.8. Обврски за ИС којшто издава квалификувани сертификати | 66 |
| 9.9. Ограничувања на одговорноста | 67 |
| 9.10. Обесштетувања..... | 67 |
| 9.10.1. Обесштетување од страна на претплатниците..... | 67 |
| 9.10.2. Обесштетување од страна на засегнатите страни | 67 |
| 9.11. Период и прекин на важност | 68 |
| 9.11.1. Период на важност | 68 |
| 9.11.2. Прекин на важност..... | 68 |
| 9.11.3. Ефекти од прекин на важност и преживување | 68 |
| 9.12. Индивидуални известувања и комуникација со учесниците | 68 |
| 9.13. Амандмани | 68 |
| 9.13.1. Процедура за амандмани | 68 |
| 9.13.2. Механизам и период на известување..... | 68 |
| 9.13.3. Околности под кои OID мора да се промени | 68 |
| 9.14. Одредби за решавање на спорови | 69 |
| 9.14.1. Спорови помеѓу VeriSign, филијали и клиенти | 69 |
| 9.14.2. Спорови со претплатниците - крајни корисници и засегнатите страни | 69 |
| 9.15. Закон кој ќе се применува | 69 |
| 9.16. Усогласеност со законот што ќе се применува | 69 |
| 9.17. Збирни одредби | 69 |
| 9.17.1. Договорот во целост..... | 69 |
| 9.17.2. Припишување | 69 |
| 9.17.3. Разделивост..... | 69 |
| 9.17.4. Присилно извршување (надоместок за адвокат и откажување од правата) | 69 |
| 9.17.5. Виша сила | 69 |

| | |
|--|-----------|
| 9.18. Други одредби..... | 70 |
| Додаток А. Табела на кратенки и дефиниции | 71 |
| Табела на кратенки..... | 71 |
| Дефиниции | 71 |

1 ВОВЕД

Овој документ претставува Правила на КИБС за издавање на квалификувани сертификати (во понатамошниот текст Правила). Во нив се наведени практиките што ги користи КИБС при обезбедување на сертификациските услуги за квалификуваните сертификати уредени според Директивата 1999/93/ЕС на Европскиот парламент и на Советот од 13 декември 1999 година за рамките на заедницата во врска со Електронските потписи („Директивата“) и македонската регулатива. Обезбедувањето на сертификациските услуги вклучува, покрај другото, издавање, управување, поништување и обновување на квалификуваните сертификати, според специфичните барања на Политиките за издавање сертификати на Доверливата мрежа на VeriSign (VeriSign Trust Network Certificate Policies – во понатамошниот текст: CP) и Политики за издавање сертификати на доверливата мрежа на Верисајн согласно Европската директива (VeriSign Trust Network European Directive Policies - во понатамошниот текст: EDP), кои ја дополнуваат CP.

CP е основен документ за политиката што се спроведува во Доверливата мрежа на VeriSign (VeriSign Trust Network – во понатамошниот текст: VTN). Тој ги востановува деловните, правните и техничките предуслови за одобрување, издавање, управување, користење, поништување и обновување на дигиталните сертификати во рамките на VTN и обезбедување на придружни доверливи услуги. Овие предуслови наречени „VTN стандарди“ обезбедуваат заштита на безбедноста и интегритетот на VTN, и се однесуваат на сите учесници во VTN и според тоа обезбедуваат потврда за подеднаква доверба низ целата VTN. Информациите за VTN и VTN Стандардите се достапни во CP¹.

Покрај тоа, EDP ја дополнуваат CP со дополнителни информации за тоа како VTN ги задоволува специфичните предуслови на политиките поставени од страна на Европскиот институт за телекомуникациски стандарди (European Telecommunications Standards Institute - во понатамошниот текст: ETSI). Целта на EDP е да го олесни усогласувањето со Директивата бр. 1999/93/ЕС на Европскиот парламент и советот од 13.12.1999 за заедничка рамка за електронски потписи (во понатамошниот текст: Директива).

1. Директивата има за цел да го олесни користењето на електронските потписи и да постави предуслови за „квалификувани сертификати“ кои поддржуваат одредени типови на електронски потписи. EDP ги опишува двете политики за сертификати наведени во Техничката спецификација на Европскиот институт за телекомуникациски стандарди 101 456 (во понатамошниот текст: „ETSI Документ за политиките“)

2. EDP дефинира две политики кои што ја дополнуваат CP во однос на квалификуваните сертификати, а овде ќе се нарекуваат „Ниво 1 од Директивата“ (во понатамошниот текст: DL1) и „Ниво 2 од Директивата“ (во понатамошниот текст: DL2). DL1 и DL2 соодветно кореспондираат со „QCP јавна“ сертификациска политика и „QCP јавна + SSCD²“ сертификациска политика уредени во ETSI документот за политиките.

3. EDP го дополнува профилот на сертификатите развиен од ETSI („Профил на квалификуван сертификат“), кој го дефинира техничкиот формат на сертификатите, а кој ги задоволува предусловите на Директивата („квалификувани сертификати“). Издавачите на сертификати што издаваат квалификувани сертификати можат да го користат профилот на квалификувани сертификати при издавањето на сертификати кои ќе бидат во согласност со анекс I и II од Директивата. Копија од EDP може да се најде на: <https://ca.kibs.com.mk/repository/cps>.

¹ Важечката верзија на VTN CP, може да се најде на <https://ca.kibs.com.mk/repository/cps>

² Secure Signature Creation Device, безбедно средство за електронско потпишување - БСЕП

КИБС има овластување врз дел од VTN наречен “Поддомен“ на VTN. КИБС Поддоменот ги вклучува ентитетите што му се подредени, како што се клиентите и засегнатите страни.

Додека CP и EDP ги уредуваат предусловите што VTN учесниците мораат да ги задоволат, овие Правила опишуваат како КИБС ги задоволува овие предуслови во рамките на КИБС ИС како поддомен од VTN. Уште позначајно е што овие Правила ги опишуваат и практиките што КИБС ги применува за:

- безбедно управување со основната инфраструктура што ја поддржува VTN, и
- издавањето, управувањето, поништувањето и обновувањето на VTN квалификуваните сертификати.

Овие Правила се усогласени со RFC 3647 на Инженерскиот стручен тим на Интернет (Internet Engineering Task Force - IETF) за конструкција на Политики за сертификати и Сертификациски практики.

1.1. Преглед

КИБС делува како издавач на сертификати (во понатамошниот текст: ИС) во рамките на VTN и ги врши сите услуги од животниот циклус на сертификатите, како издавање, управување, поништување и обновување. КИБС нуди:

- Квалификувани сертификати (идентификација на физички лица) и
- Сертификати за веб страници (безбедна серверска идентификација и глобална серверска идентификација).

Сертификатите за веб страници се нудат од страна на КИБС како посебна соработка со VeriSign, а не во рамките на КИБС ИС. За овие сертификати ќе важат Правилата на VeriSign, објавени на <http://www.verisign.com/repository/cps/>.

Правилата на КИБС особено се однесуваат на:

- Примарниот јавен издавач на сертификати (во понатамошниот текст: PCA) на VeriSign, како коренски издавач на сертификати за квалификуваните сертификати на КИБС.
- Јавните сертификати на КИБС ИС, како дел од сертификацискиот ланец на квалификуваните сертификати на КИБС.

Генерално, овие Правила ја одредуваат и употребата на VTN услугите во врска со квалификуваните сертификати во рамките на КИБС поддоменот на VTN, од страна на сите поединци и ентитети во КИБС поддоменот (Учесници во КИБС поддоменот).

КИБС нуди квалификувани сертификати (DL1 и DL2) во рамките на поддоменот на VTN. Овие Правила опишуваат како КИБС ги задоволува предусловите од CP и EDP за квалификуваните сертификати што ги издава во рамките на својот поддомен. Така, овие Правила, како единствен документ, ги покрива практиките и процедурите во однос на издавање и управување со квалификуваните сертификати што ги обезбедува КИБС.

КИБС може да објавува дополнителни Правила за издавање на сертификати со цел за усогласување со правната регулатива, стандардите и барањата во индустријата. Овие дополнителни Правила ќе им бидат ставени на располагање на претплатниците на сертификати кои се издадени согласно истите, како и на нивните засегнати страни.

Овие Правила се само еден од збирката документи кои се однесуваат на КИБС, поддоменот на VTN. Останатите документи се следниве:

- Подредени доверливи безбедносни и оперативни документи³ што ги надополнуваат CP и Правилата со тоа што подетално ги наведуваат условите, како на пр.:
 - Политиката за физичка безбедност на VeriSign, која ги наведува безбедносните принципи што ја регулираат VTN инфраструктурата.
 - Прирачникот за условите на безбедност и надзор на VeriSign, кој детално ги опишува предусловите на VeriSign и придружните компании во однос на безбедноста на персоналот, физичката, телекомуникациската и логичката безбедност, како и безбедноста на управување на криптографските клучеви.
 - Референтен прирачник за церемонијата на клучевите, кој детално ги презентира оперативните предуслови за управување со клучеви.
 - Политиката за физичка и просторна сигурност на КИБС, која ги поставува принципите според кои се раководи КИБС поддоменот.
- Подредени договори наметнати од КИБС. Овие договори ги обврзуваат клиентите, претплатниците и засегнатите страни на КИБС. Помеѓу останатото, ги пренесуваат VTN Стандардите на овие VTN учесници и во некои случаи, ги наведуваат специфичните практики за тоа како тие да ги задоволат VTN стандардите.

Во одредени случаи Правилата се повикуваат на овие подредени документи за специфични, детални практики што ги наметнуваат VTN стандардите.

1.2. Име на документот и идентификација

Овој документ се именува како Правила на КИБС за издавање на квалификувани сертификати. VTN сертификатите содржат предметен идентификатор (OID) кој соодветствува со соодветна VTN класа на сертификати. Според тоа, КИБС на овие Правила не им доделува предметен идентификатор.

Идентификаторите на квалификуваните сертификати се користат во согласност со Дел 0.од овие Правила.

1.3. Учесници

1.3.1. Издавачи на сертификати

Терминот издавач на сертификати (ИС) се однесува на сите субјекти овластени да издаваат сертификати за јавен клуч во рамките на VTN. Терминот ИС ја опфаќа и подкатегијата на издавачи наречени Примарни издавачи на сертификати (во понатамошниот текст: ПИС, англ. Primary Certification Authority - PCA). ПИС делуваат како корени на домени. Секој ПИС е VeriSign ентитет. Подредени на ПИС се издавачите на сертификати кои издаваат сертификати на претплатници крајни корисници или на други ИС. КИБС, покрај другите, е ИС кој управува со квалификувани сертификати.

Еден VTN ИС кој е технички надвор од хиерархијата на ПИС е издавачот на сертификати за безбеден сервер (Secure Server Certification Authority). Овој ИС нема надреден, како корен или ПИС. Издавачот на сертификати за безбеден сервер делува како свој сопствен корен и си има издадено на себе си само-потпишан коренски сертификат. Тој исто така издава сертификати и на клиентите - крајни корисници. На тој начин хиерархијата на безбеден сервер се состои само од ИС за безбеден сервер.

³ Иако овие документи не се јавно достапни, нивните спецификации се вклучени во годишниот WebTrust-ов извештај за надзор на Издавачите на сертификати на VeriSign и можат да се стават на располагање во согласност со посебен Договор.

Во овие Правила под издавачи на сертификати ќе се мисли на издавачите кои се содржат во синџирот на квалификувани сертификати на КИБС. Поконкретно, тоа се:

- VeriSign Class 2 Public Primary Certification Authority – G3, како коренски ПИС,
- KIBS Verba CA, како посреднички ИС и
- KIBS Qualified Certificate Services CA, како издавач на сертификати за крајни корисници (издавачки ИС).

1.3.2. Регистрациска канцеларија

Регистрациска канцеларија (РК) е субјект кој врши идентификација и автентикација на барателите на сертификати за крајни корисници, иницира или проследува барања за поништување на сертификати на крајните корисници и одобрува барања за обновување на сертификати или повторно издавање на клучеви, во име на издавачот. КИБС делува како РК за квалификуваните сертификати што ги издава.

КИБС може да воспостави договорни односи со трети страни, во однос на прием на документација и потврда на идентитет на барателите. Во тој случај, третото лице претставува Локална регистрациска канцеларија (ЛРК). ЛРК е должна да ги извршува своите обврски во согласност со условите на договорот и овие Правила.

1.3.3. Претплатници

Претплатник е ентитет што е именуван како краен корисник на сертификат. Претплатници може да бидат физички лица или организации. За квалификувани сертификати претплатници можат да бидат само правно подобни физички лица, во согласност со македонските закони.

Во одредени случаи сертификатите се издаваат директно на физичките или на правните лица за нивна сопствена употреба. Меѓутоа, се јавуваат и случаи во кои страната што бара сертификат е различна од субјектот за кој се однесува барањето. На пример, некоја организација може да бара сертификати за своите вработени за да им овозможи тие да ја застапуваат организацијата во електронските трансакции/бизнис. Во такви случаи ентитетот што се претплатува за издавање на сертификатите (т.е., плаќа за нив, или преку претплата за специфична услуга) е различен од ентитетот кој е субјект на сертификатот (главо, носител на сертификатот). Во Овие Правила се користат два различни термини за да се направи разлика помеѓу овие две улоги. „Претплатник“ е ентитетот кој прави договор со КИБС за издавање на сертификат, а „Субјект“ е лицето кое е поврзано со сертификатот. Претплатникот ја понесува крајната одговорност за користењето на сертификатот, но Субјектот е лице-индивидуа чија автентичност се потврдува кога ќе се презентира сертификатот.

Кога се користи терминот „Субјект“ тоа треба да значи дека е различен од Претплатникот. Кога се користи „Претплатник“, тоа може да значи само Претплатник како посебен ентитет, но терминот исто така може да се користи и за да ги опфати обете значења. Контекстот на неговата употреба во овие Правила ќе доведе до неговото точно толкување.

ИС технички, исто така се претплатници на сертификати во рамките на VTN, било како ПИС кој си издава само-потпишан сертификат на себе си, или како ИС кому му е издаден сертификат од страна на надреден ИС. Референците „крајни ентитети“ и „претплатници“ во овие Правила се однесуваат само на крајните корисници претплатници на квалификуваните сертификати.

1.3.4. Засегнати страни

Засегнатата страна е физичко или правно лице кое делува потпирајќи се на сертификат и/или дигитален потпис издаден под VTN. Засегнатата страна може, но не мора да биде претплатник во рамките на VTN.

1.3.5. Други учесници

Не се применува.

1.4. Користење на сертификатите

1.4.1 Дозволена употреба на сертификатите

Индивидуалните сертификати обично се користат од страна на физичките лица за потпишување и шифрирање на електронска пошта, како и за автентикација кон апликации (автентикација на клиентот). Иако најчестите употреби на квалификуваните сертификати на КИБС се наведени подолу во Табела 1, сертификатите DL1 и DL2 можат да се користат и за други цели, за кои засегнатата страна може до разумна мерка да се потпре на таков сертификат и ако употребата не е забранета со закон или од страна на VTN CP, VTN EDP, овие Правила и Претплатничкиот договор.

DL1 сертификатите може да се користат за дигитално потпишување, онаму каде што за користење на дигиталните потписи се бараат електронски потписи на кои “не е (и нема да им биде) негирана правната полноважност и прифатливост како доказ во законски процедури” во согласност со член 5(2) од Директивата. Користењето на DL1 сертификатите соодветствува со употребата на сертификатите идентификувани во QCP политика на јавни сертификати во ETSI Документот за политиките.

DL2 сертификатите може да се користат за дигитално потпишување, онаму каде за користење на дигиталните потписи се бараат напредни електронски потписи⁴ „ги задоволуваат барањата за потпис во врска со податоците во електронска форма на ист начин на кој што своерачниот потпис ги задоволува овие барања во врска со податоците на хартија“ во согласност со член 5(1) од Директивата. Употребите на DL2 сертификатите соодветствуваат со употребите на сертификатите идентификувани во QCP политиката на јавни сертификати + БСЕП, во ETSI документот за политиките.

DL1 и DL2 сертификатите се сертификати со висока гаранција кои обезбедуваат високо ниво на сигурност на идентитетот на претплатникот.

| Класа на сертификат | Ниво на безбедност | | Користење | | |
|---------------------|--------------------|-------|-------------|-----------|-------------------------|
| | низок | висок | потпишување | шифрирање | автентикација на клиент |
| DL1 сертификати | | ✓ | ✓ | ✓ | ✓ |
| DL2 сертификати | | ✓ | ✓ | ✓ | ✓ |

Табела 1: Користење на сертификатите

⁴ Според Законот за податоци во електронски облик и електронски потпис се користи терминот општо прифатен електронски потпис

1.4.2. Забранета употреба на сертификатите

Сертификатите на КИБС не се дизајнирани, наменети или авторизирани за користење или за препродажба како контролна опрема во ризични околности или за користење во услови кои бараат неопходни безбедносни изведби, како што е функционирањето на нуклеарни постројки, навигациски или комуникациски системи за воздушна пловидба, системи за контрола на воздушниот сообраќај или системи за контрола на оружје, каде што неуспехот може да доведе директно до смрт, лична повреда или сериозна штета во однос на заштита на околината.

DL1 и DL2 сертификатите се наменети за користење од страна на клиентите и нема да се користат како сертификати за сервери или за организациски сертификати ниту пак како ИС сертификати.

ИС сертификатите не смеат да се користат за никакви функции освен за функциите на ИС.

1.5. Администрирање на Правилата

1.5.1 Организација што го администрира документот

КИБС АД
К.Ј. Питу 1,
1000, Скопје
Република Македонија
тел: ++389 2 3297 400
факс: +389 2 3297 497
e-mail: ca-info@kibs.com.mk

1.5.2 Лице за контакт

Раководител на група за развој на практики на КИБС ИС
К.Ј. Питу 1,
1000, Скопје
Република Македонија
тел: ++389 2 3297 400
факс: +389 2 3297 497
e-mail: ca-info@kibs.com.mk

1.5.3. Соодветност на овие Правила со CP

Организацијата идентификувана под 1.5.1 и Adacom се одговорни за определување дали овие Правила и другите документи од типот на Правила за сертификациските практики што ја дополнуваат или се подредени на овие Правила соодветствуваат со VTN CP, ADACOM CPS и овие Правила.

1.5.4 Процедури за одобрување на Правилата

Одобрувањето на овие Правила и другите последователни амандмани се врши од страна на Групата за развој на практики на КИБС и Авторитетот за управување на политиката на VeriSign (VeriSign Policy Management Authority (PMA)). Амандманите се или во форма на документ кој ја содржи изменетата верзија или како забелешка за ревидиран текст. Изменетите верзии или ревидираните забелешки се сместуваат во складиштето на КИБС кој се наоѓа на:

<http://www.kibs.com.repository/cps>. Ажурираните одредби заменуваат определени одредби или противречни одредби од референтната верзија на CPS.

1.6. Дефиниции и кратенки

Види го Додаток А за списокот на кратенки и дефиниции.

2 ОДГОВОРНОСТИ ПОВРЗАНИ СО ОБЈАВУВАЊЕ И СМЕСТУВАЊЕ

2.1 Складишта

КИБС ИС е одговорен за функциите на складиште за своите сопствени ИС сертификати. КИБС ги објавува DL1 и DL2 сертификатите во складиштето согласно Дел 2.2 од овие Правила.

По поништување на претплатнички сертификат, КИБС го објавува поништувањето во складиштето, како и во Регистарот на поништени сертификати (РПС⁵).

2.2 Објавување на информации за сертификати

КИБС одржува веб-базирано складиште кое е на располагање на засегнатите страни, од каде по електронски пат може да побараат информации за поништување или некој друг статус на сертификат. КИБС им дава на засегнатите страни информации за тоа како да го пронајдат складиштето за да го проверат статусот на некој сертификат.

КИБС ја објавува и става на постојано располагање во своето складиште последната верзија од:

- VTN CP,
- VTN EDP,
- овие Правила,
- Претплатничките договори,
- Договорите со засегнатите страни,
- својата политика за заштита на лични податоци.

КИБС објавува и одредени информации за ИС во делот на складиштето од веб-страницата <http://ca.kibs.com.mk/repository/rpa> како што е опишано подолу.

КИБС ги објавува и сертификатите наведени во Табелата 2:

| Тип на сертификат | Барања за објавување |
|---|---|
| VeriSign PCA коренски сертификат | Достапен на засегнатите страни преку вклучување во тековниот софтвер за интернет пребарување. |
| КИБС посреднички и оперативен ИС сертификат | Достапен на засегнатите страни како дел од синцирот на сертификати, којшто може да се добие од сертификатот на крајниот корисник преку функцијата на пребарување опишана подолу. |
| Сертификати на крајните претплатници | Достапен на засегнатите страни преку функција на пребарување во складиштето на КИБС на адреса: http://ca.kibs.com.mk/repository/rpa . Исто така, достапен е и преку пребарање во LDAP директориумот на серверот на КИБС на адреса ldap-ca.kibs.com.mk. |

Табела 2: Објавување на сертификатите

2.3. Време и периодичност на објавување

Ажурираните верзии на овие Правила се објавуваат согласно Дел 9.13 од овие Правила. Обновените верзии на претплатнички договори и договори со засегнатите страни, исто така, се

⁵ Certificate Revocation List - CRL

објавуваат. Сертификатите се објавуваат веднаш по издавањето. Информациите за статусот на сертификатот се објавуваат во согласност со одредбите на овие Правила.

2.4. Контрола на пристап во складиштата

Информациите објавени во делот на складиштето од веб-страницата на КИБС се јавно достапни информации. КИБС бара лицата да се согласат со одредбите на Договорот со засегнатата страна како услов за пристап до сертификатите, до информациите за статусот на сертификатите или до РПС. КИБС применува мерки на логичка и физичка безбедност за да се спречи неовластени лица да додаваат, бришат или менуваат содржини во складиштето во согласност со политиките за безбедност на КИБС.

3. ИДЕНТИФИКАЦИЈА И ПРОВЕРКА НА АВТЕНТИЧНОСТА

3.1 Именување

Имињата што се појавуваат во сертификатите издадени во рамките на VTN се подложуваат на потврдување на автентичност, освен ако поинаку е назначено во VTN CP, VTN EDP, овие Правила или во содржината на дигиталниот сертификат.

3.1.1 Типови на имиња

Сертификатите на КИБС ИС содржат X.501 карактеристични имиња (Distinguished Names) во полињата за Издавач (Issuer) и Субјект (Subject). Карактеристичните имиња на КИБС ИС се состојат од компоненти наведени во Табела 3.

| Атрибут | Вредност | | | | | |
|----------------------------|---|---|-------------------------------|---|-------------------------------------|---|
| | Поле на издавачот | | | Поле на субјектот | | |
| | Коренски ИС (Root CA) | Посреднички ИС (Intermediate CA) | Издавачки ИС (Issuing CA) | Коренски ИС (Root CA) | Посреднички ИС (Intermediate CA) | Издавачки ИС (Issuing CA) |
| Country (C) = | US | US | MK | US | MK | MK |
| Organization (O) = | VeriSign, Inc. | VeriSign, Inc. | Clearing House KIBS AD Skopje | VeriSign, Inc | Clearing House KIBS AD Skopje | Clearing House KIBS AD Skopje |
| Organizational Unit (OU) = | <ul style="list-style-type: none"> VeriSign Trust Network © 1999 VeriSign, Inc. – For authorized use only | <ul style="list-style-type: none"> VeriSign Trust Network © 1999 VeriSign, Inc. – For authorized use only | VeriSign Trust Network | <ul style="list-style-type: none"> VeriSign Trust Network © 1999 VeriSign, Inc. – For authorized use only | VeriSign Trust Network | <ul style="list-style-type: none"> VeriSign Trust Network Terms of use at http://ca.kibs.com.mk/repository/rpa (c)09 Class 2 Managed PKI Individual Subscriber CA |
| Common Name (CN) = | <ul style="list-style-type: none"> VeriSign Class 2 Public Primary Certification Authority – G3 | <ul style="list-style-type: none"> VeriSign Class 2 Public Primary Certification Authority – G3 | KIBS Verba CA | <ul style="list-style-type: none"> VeriSign Class 2 Public Primary Certification Authority – G3 | KIBS Verba CA | KIBS Qualified Certificate Services CA |

Табела 3: Атрибути за карактеристични имиња во CA сертификатите

Сертификатите за крајни корисници содржат X.501 карактеристично име во полето за субјектот (Subject Name) и се состои од компоненти наведени во Табела 4.

| Атрибут | Вредност |
|------------------------------|--|
| Држава (C) | ISO ознаката од 2 букви на државата на крајниот корисник |
| Организација (O) = | Името на организацијата на крајниот корисник |
| Организациска единица (OU) = | Овој атрибут е опционален и може да содржи назив |

| | |
|--------------------------|---|
| | на организационен дел или слично. |
| Општо име (CN) = | Овој атрибут го вклучува полното име (име и презиме) на крајниот корисник |
| Електронска адреса (E) = | Електронската адреса на крајниот корисник |

Табела 4: Атрибути за карактеристично име во сертификати за крајни корисници

Атрибутот Општо име (Common Name (CN=)) од карактеристичното име на субјектот на крајниот корисник се подложува на потврдување на автентичност. Вредноста Општо име вклучена во карактеристичното име на субјектот на индивидуалните сертификати го претставува вистинското лично име на физичкото лице.

3.1.2 Потреба имињата да имаат значење

DL1 и DL2 сертификатите содржат имиња со вообичаено разбирлива семантика која дозволува определување на идентитетот на индивидуата што е субјект на сертификатот.

КИБС ИС сертификатите содржат имиња со вообичаено разбирлива семантика која дозволува определување на идентитетот на ИС што е субјект на сертификатот.

3.1.3 Анонимност или псевдоними на претплатниците

За КИБС Квалификуваните сертификати (DL1 и DL2) не е дозволено користење на псевдоними.

3.1.4 Правила за интерпретирање на различни именски форми

Не постои одредба.

3.1.5 Единственост на имињата

КИБС потврдува со сигурност дека карактеристичните имиња на претплатникот се единствени во доменот за определен ИС преку автоматизирани компоненти на процесот на запишување на Претплатникот. Возможно е еден претплатник да има два или повеќе сертификати со слични карактеристични имиња на субјектот.

3.1.6 Признавање, проверување и улога на трговските марки

На подносителите на барања за сертификати им е забрането во своите барања за сертификати да користат имиња што ги прекршуваат правата на интелектуална сопственост на други. Сепак, КИБС не проверува дали подносителот на барање за сертификат има права на интелектуална сопственост во името што се појавува во барањето за сертификат, ниту пак арбитража, посредува или на било кој друг начин разрешува спорови во врска со било кое име на домен, трговско име, трговска марка или сервисна марка. КИБС има право, без да понесе одговорност кон било кој подносител на барање за сертификат, да одбие или суспендира барање за сертификат заради таков спор.

3.2 Првична потврда на идентитетот

3.2.1 Метод за докажување на сопственоста врз приватен клуч

Подносителот на барање за сертификат мора да покаже дека има право да го поседува приватниот клуч кој кореспондира со јавниот клуч што ќе биде наведен во сертификатот.

Начинот на докажување на сопственоста врз приватен клуч ќе биде PKCS#10 или друга криптографски еквивалентна демонстрација.

3.2.2 Потврдување на идентитетот на лицето

За DL1 и DL2 сертификатите автентикацијата на идентитетот се базира на личното (физичко) присуство на Подносителот на барање за сертификат пред овластено лице на КИБС или пред нотар или друго службено лице со слично овластување во рамките на надлежноста на Подносителот на барање за сертификат. Овластеното лице на КИБС, нотарот или другите службени лица го проверуваат идентитетот на подносителот на барање за сертификат со користење на лична карта или пасош. Кога потврдувањето на идентитетот е засновано на лично (физичко) присуство на подносителот на барање за сертификат пред овластено лице на КИБС, КИБС заверува копија од личната карта или пасошот за цели на архивирање. Кога потврдувањето на идентитетот е засновано на личното (физичко) присуство на подносителот на барање за сертификат пред нотар или друго службено лице со слични овластувања, подносителот на барање мора да испрати до РК на КИБС ИС заверена копија од неговата лична карта или пасош во која е наведена датата на заверката.

Потврдата на личната карта или пасошот мора да биде на македонски или англиски јазик. Во случај личната карта или пасошот да се издадени на некој друг јазик различен од погоре наведените, заверката мора да биде на еден од овие јазици или да биде приложен превод на еден од погоре наведените јазици.

3.2.3 Информација за претплатникот што не се проверува

Содржината на атрибутот Организациска единица (OU) за претплатникот не се проверува.

3.2.4 Потврдување на овластување

Секогаш кога име на некое лице е поврзано со име на Организација во сертификат на таков начин што покажува поврзаност на лицето или негово овластување да делува во име на Организацијата, КИБС РК:

- потврдува дека организацијата постои преку користење на најмалку еден сервис за потврдување или база на податоци на трето лице, или алтернативно, со документација на организацијата издадена од или пополната кај соодветна надлежна институција која го потврдува постоењето на таа организација, и
- користи информации што се содржани во деловната документација или базата на податоци на деловни информации (вработени или партнери) на некоја РК која им одобрува сертификати на физичките лица поврзани со неа или добива поштенска пратка со потврда или во слична процедура, од организацијата, за тоа дека лицето кое го поднесува барањето за сертификат има овластување да делува во име на Организацијата.

3.3 Идентификација и автентикација за барања за обнова на пар на клучеви

Пред истекот на постоечки претплатнички сертификат, неопходно е претплатникот да добие нов сертификат за да го одржи континуитетот на користење на сертификатот. КИБС обично бара на Претплатникот да му се генерира нов пар на клучеви за да се замени парот на кој му истекува важноста, технички дефинирано како “обнова на парот на клучеви” (re-key) . Сепак, во одредени случаи (т.е., за сертификати за веб-сервери) Претплатниците можат да побараат нов сертификат за постоечкиот пар на клучеви (технички дефинирано како “обновување”).

Во општи црти, и “Обнова на парот на клучеви” и “Обновувањето” обично се опишуваат како “Обновување на сертификат”, фокусирајќи се на фактот дека стариот сертификат е заменет со нов сертификат, а не потенцирајќи дали се генерира нов пар на клучеви или не. За DL1 и DL2 сертификатите оваа дистинкција не е значајна, бидејќи секогаш се генерира нов пар на клучеви како дел од КИБС процесот на замена на сертификат на краен корисник Претплатник.

3.3.1. Идентификација и автентикација за рутинска обнова на пар на клучеви

Процедурите за обнова на парот на клучеви потврдуваат со сигурност дека лицето што побарува обнова на парот на клучеви за сертификат е навистина претплатникот на сертификатот.

Претплатникот поднесува барање за обнова на парот на клучеви до КИБС или до РК поднесувајќи го дигитално потпишаното барање со својот постоечки сертификат. РК на тој начин повторно го потврдува идентитетот на Претплатникот. За DL1 и DL2 сертификатите личното (физичко) присуство на Подносителот на барање за сертификат пред овластено лице на КИБС или пред нотар или друго службено лице со слично овластување во рамките на надлежноста на Подносителот на барање за сертификат не е неопходно, доколку верификуваните регистарски податоци вклучени во сертификатот или во личната карта или пасош кои биле поднесени во првичното барање не се променети.

Во секој случај, барателот мора повторно да поднесе заверена на нотар копија од личната карта или пасошот што биле поднесени во првичното барање.

3.3.2. Идентификација и автентикација при обнова на пар на клучеви после поништување

Обнова на парот на клучеви после поништување не е дозволена.

3.4 Идентификација и автентикација за барање за поништување

Пред да поништи сертификат КИБС проверува дали поништувањето е побарано од Претплатникот на сертификатот.

Прифатливите процедури за потврдување на автентичноста на барање за поништување од Претплатникот вклучуваат еден или повеќе од следниве наводи:

- Да се побара од Претплатникот да ја достави лозинката за проверка и поништувањето на Сертификатот се врши автоматски ако таа соодветствува со лозинката за проверка што е документирана.
- Добивање на порака од Претплатникот во која се бара поништување, а која содржи дигитален потпис којшто може да се верификува со сертификатот што треба да се поништи.
- Комуникација со Претплатникот што ќе обезбеди разумни уверувања кои потврдуваат со сигурност дека лицето или организацијата која бара поништување е навистина

Претплатникот или има прописно овластување да го побара тоа. Таквата комуникација, во зависност од околностите, може да вклучува едно или повеќе од следново: телефон, факс, електронска пошта, по пошта или по курир.

Администраторите на КИБС ИС имаат право да побараат поништување на сертификати на крајни корисници Претплатници во рамките на КИБС Поддоменот. КИБС го утврдува идентитетот на администраторот преку контрола на пристапот со користење на SSL и автентикација на администраторот пред да му дозволи да ги изведе функциите на поништување или друга процедура одобрена од VTN.

4. ОПЕРИРАЊЕ СО ЖИВОТНИОТ ЦИКЛУС НА СЕРТИФИКАТОТ

4.1. Барање за сертификат

4.1.1. Кој може да поднесе барање за сертификат?

Барање за сертификат може да ја поднесе физичко лице кое е субјект на сертификатот, доколку е полнолетно и од правен аспект има основа за тоа според македонските прописи.

4.1.2. Процес на регистрирање и одговорности

4.1.2.1. Претплатници на сертификати за крајни корисници

Претплатниците се согласуваат со Претплатничкиот договор, кој содржи претставување и гаранции опишани во Делот 9.6.3 од овие Правила и поминуваат низ процес кој се состои од:

- Пополнување и потпишување на барање за сертификат и давање на точни и вистинити информации;
- Генерирање или организирање да се генерира пар клучеви;
- Испорачување на својот јавен клуч до КИБС ИС;
- Показување на поседување на приватниот клуч кој соодветствува со јавниот клуч испорачан до КИБС.

Процесот на регистрирање за квалификуваните сертификати е во согласност со Дел 4.1.2 од СР, а предмет на следниве разјаснувања:

- Претплатничките договори со кои барателите на сертификати се согласуваат се според дел 2.1.1, 2.1.2 од EDP,
- Барателите на сертификати ќе презентираат доказ за идентитетот согласно со Делот 3.1.9 од EDP и
- Информациите за регистрација наведени во сертификатот вклучуваат адреса или други атрибути што му овозможуваат на КИБС да контактира со Барателот на сертификат.

Записите кои се чуваат согласно дел 5.4.1 од овие Правила, вклучуваат информации користени за потврдување на автентичноста на идентитетот на барателот на сертификат, вклучувајќи го и референтниот број на документот употребен за автентикација и роковите за неговата важност, како и запис за потпишан претплатнички договор во електронска форма, каде Претплатникот се согласува КИБС ИС да ги чува информациите кои се користени во регистрацијата и ги дава сите согласности што се потребни според ETSI Документот за Политиката.

Во случај на барање за обнова на пар клучеви:

- Било какви промени во условите на Претплатничкиот договор што ќе следат по првичната или повторната регистрација ќе бидат согласно со Дел 2.1.1, 2.1.2 од EDP,
- Документацијата што се задржува согласно Дел 5.5.1 од CPS исто така ја вклучува согласноста на Претплатникот за било која од тие промени.

4.1.2.2. ИС и РК Сертификати

Адаком, како филијала на VeriSign, може да издава дополнителни РК сертификати за издавање на DL1 и DL2 сертификати.

4.2 Обработка на барањето за сертификат

4.2.1. Извршување на функциите за идентификација и автентикација

КИБС РК извршува идентификација и автентикација на сите потребни информации за Претплатникот согласно Дел 3.2 од овие Правила.

4.2.2. Одобрување или одбивање на барањата за сертификати

КИБС РК одобрува барање за сертификат само доколку се задоволени следниве критериуми:

- Успешна е идентификацијата и автентикацијата на сите потребни информации за Претплатникот согласно Дел 3.2 од Овие Правила.
- Уплатен е надоместокот за сертификатот.

КИБС РК го одбива барањето за сертификат ако:

- Не може целосно да се изврши идентификацијата и автентикацијата на сите потребни информации за Претплатникот во смисла на Дел 3.2 од Овие Правила, или
- Претплатникот не ги доставил потребните документи по барањето, или
- Претплатникот не одговорил на забелешките во рокот определен за тоа, или
- Не е уплатен надоместокот за сертификатот, или
- оцени дека издавањето на сертификатот на Претплатникот може да и донесе лоша репутација на VTN.

4.2.3. Време на обработка на барањата за сертификат

КИБС започнува со обработка на барањето за сертификат во разумен рок по приемот. Барањето за сертификат останува активно се до моментот додека не биде одбиено.

4.3. Издавање на сертификат

4.3.1. Активности на КИБС ИС за време на издавање на сертификатот

Сертификатот се креира и издава од страна на КИБС ИС по одобрување на барањето за сертификат или по добивање на потврда од РК за издавање на сертификат. КИБС го креира и го издава сертификатот на барателот на сертификат врз основа на податоците во барањето.

Квалификуваните сертификати генерирани и издадени во согласност со 4.2.1 од EDP се издаваат од страна на системи кои користат заштита против фалсификување, која е детално опишана во делот 6 од CP и делот 6 од EDP и обезбедува со сигурност сертификатот да биде издаден на барателот на сертификат, кој го поседува приватниот клуч што кореспондира со јавниот клуч во сертификатот кој што треба да се издаде.

Издавањето на сертификат согласно дел 3.3 од овие Правила, во техничка смисла, повеќе значи обновување на парот клучеви, отколку ресертификација на претходно сертифициран клуч.

4.3.2. Известување на претплатникот од страна на КИБС ИС за издавање на сертификатот

КИБС ИС директно или преку РА, го известува претплатникот дека му издал сертификат и му обезбедува пристап до него. Сертификатите се ставаат на располагање на Претплатниците -

крајни корисници со нивно информирање да ги преземат од веб-страницата, преку електронска порака испратена до Претплатникот.

4.4. Прифаќање на сертификатот

4.4.1. Однесување кое означува прифаќање на сертификат

Сертификатот се смета за прифатен кога:

- Претплатникот ќе го преземе сертификатот или ќе го инсталира сертификатот.
- Претплатникот нема да достави приговор за сертификатот или неговата содржина.

4.4.2. Објавување на сертификатот од страна на КИБС ИС

КИБС ги објавува Сертификатите што ги издава во јавно достапно складиште.

4.4.3. Известување за издавање на сертификатот од страна на КИБС ИС до други ентитети

Не се применува.

4.5. Користење на парот клучеви и сертификатот

4.5.1. Користење на претплатничкиот приватен клуч и сертификатот

Користењето на приватниот клуч што кореспондира со јавниот клуч во сертификатот е дозволено, само откако Претплатникот ќе се согласи со Претплатничкиот договор и ќе го прифати сертификатот. Сертификатот ќе се користи во согласност со Претплатничкиот договор на КИБС ИС, со условите на СР и овие Правила. Користењето на сертификатот мора да биде конзистентно со полето за користење на клучот (KeyUsage) вклучено во сертификатот.

Претплатниците ќе ги заштитат своите приватни клучеви од неовластена употреба и ќе престанат да ги употребуваат своите приватни клучеви по истекот на важноста или повлекувањето на сертификатот.

4.5.2. Користење на јавниот клуч и сертификатот од страна на засегнатите страни

Засегнатите страни ќе се согласат со условите во Договорот за засегнати страни како услов за да можат да се потпрат на сертификатот.

Потпирањето врз сертификатот мора да биде соодветно на дадените околности. Ако околностите наложат потреба за дополнителни уверувања, засегнатите страни мора да ги добијат такви уверувања за да може да се потпрат на сертификатот.

Засегнатите страни самостојно ќе проценат:

- дали користењето на сертификат е соодветно за одредена цел, а истовремено не е забранета или на друг начин ограничена со овие Правила. КИБС ИС не е одговорен за проценката на соодветноста на користењето на сертификатот.
- Дека сертификатот се користи согласно наведеното во полето за употреба на клучот (KeyUsage) од сертификатот.
- За статусот на сертификатот и на останатите сертификати во синцирот на сертификати. Ако некој од сертификатите во синцирот бил поништен, единствено засегнатата страна е одговорна да истражува дали потпирањето на дигиталниот потпис изведено од

сертификатот на Претплатникот - краен корисник, пред поништувањето на сертификат во Синџирот на сертификати било разумно. Ризикот од потпирањето е исклучиво на засегнатата страна.

Под претпоставка дека користењето на сертификатот е соодветно, засегнатите страни ќе применуваат соодветен софтвер и/или хардвер за да извршат проверка на дигиталниот потпис или други криптографски операции што сакаат да ги изведат, како услов за потпирање врз сертификатите поврзани со секоја таква операција. Овие операции вклучуваат и идентификување на синџирот на сертификати и проверување на дигиталните потписи за сите сертификати во синџирот на сертификати.

4.6. Обновување на сертификат

Обновување на сертификат е издавање на нов сертификат на претплатникот без менување на јавниот клуч или било која друга информација во сертификатот. Обновувањето на DL1 и DL2 сертификатите не се врши на овој начин.

4.6.1. Околности за обновување на сертификатот

Не се применува.

4.6.2. Кој може да побара обновување

Не се применува.

4.6.3. Обработка на барањата за обновување на сертификат

Не се применува.

4.6.4. Известување за издавањето на сертификатот до претплатникот

Не се применува.

4.6.5. Однесување кое означува прифаќање на обновениот сертификат

Не се применува.

4.6.6. Објавување на обновување на сертификат од страна на КИБС ИС

Не се применува.

4.6.7. Известување за издавање на сертификатот од страна на СА до други ентитети

Не се применува.

4.7. Обновен сертификат со нов пар клучеви (Certificate Re-Key)

Обновен сертификат со нов пар на клучеви претставува сертификат за новиот јавен клуч од новогенерираниот пар на клучеви, а со исто карактеристично име од претходниот сертификат. Обновувањето за DL1 и DL2 сертификати се врши на овој начин.

4.7.1. Околности за обновување на сертификатот со нов пар клучеви

Пред истекот на важноста на постоечкиот сертификат, неопходно е претплатникот да изврши обнова на сертификатот со нов пар клучеви, за да го одржи континуитетот на користење на

сертификатот. Ваква обнова на сертификатот може да се изврши и по истекот на неговата важност.

4.7.2. Кој може да побара сертифицирање на нов јавен клуч

Само претплатник на сертификат може да побара обновување на сертификатот со нов пар на клучеви.

4.7.3. Обработка на барања

Процедурата на обновување на сертификат утврдува со сигурност дека лицето што бара да се обнови сертификатот е навистина е претплатникот.

Претплатникот поднесува барање за обновување до КИБС ИС, кое е дигитално потпишано со својот постоечки и важечки сертификат. КИБС повторно го потврдува идентитетот на Претплатникот, согласно со условите за идентификација и автентикација опишани во дел 3.3.1 од овие Правила.

4.7.4. Известување за издавање на новиот сертификат до претплатникот

Известувањето на Претплатникот за издавањето на сертификатот е во согласност со дел 4.3.2 од овие Правила.

4.7.5. Однесување кое означува прифаќање на сертификат

Однесувањето кое означува прифаќање на обновениот сертификат е во согласност со дел 4.4.1 од овие Правила.

4.7.6. Објавување на обновен сертификат со нов пар клучеви

Објавувањето на обновениот сертификат се врши во складиштето на КИБС ИС.

4.7.7. Известување за издавање на сертификатот од страна на КИБС ИС до други ентитети

Не се применува.

4.8. Изменување на сертификат

4.8.1. Околности за изменување на сертификат

Изменувањето на сертификат се однесува на барање за издавање на нов сертификат заради промена на податоците во постоечкиот сертификат.

Изменувањето на сертификат се смета како барање за сертификат во смисла на дел 4.1 од овие Правила.

4.8.2. Кој може да побара измени во сертификатот

Види дел 4.1.1 од овие Правила.

4.8.3. Обработка на барањата за измени во сертификатот

КИБС ИС врши идентификација и автентикација на сите потребни информации согласно дел 3.2 од овие Правила.

4.8.4. Известување за издавање на нов сертификат

Види дел 4.3.2 од овие Правила.

4.8.5. Однесување кое означува прифаќање на изменетиот сертификат

Види дел 4.4.1 од овие Правила.

4.8.6. Објавување на новиот сертификат од страна на КИБС ИС

Види дел 4.4.2 од овие Правила.

4.8.7. Известување за издавање на сертификатот од страна на СА до други ентитети

Види дел 4.4.3 од овие Правила.

4.9. Поништување и суспендирање на сертификати

4.9.1. Околности за поништување

Претплатничкиот договор им дава обврска или/и право на страните да бараат поништување на сертификат. Само во подолу наведените околности сертификатот за краен корисник ќе биде поништен од страна на КИБС ИС или од претплатникот и објавен во РПС. По барање од претплатник кој повеќе не може, или не сака да го користи сертификатот од причина што е различна од подолу наведените, КИБС ќе го означи сертификатот како неактивен (суспендиран) во својата база на податоци, но нема да го објави сертификатот во РПС.

Сертификатот за краен корисник се поништува ако:

- КИБС ИС или крајниот корисник имаат причина да веруваат или да се сомневаат дека се случило компромитирање на приватниот клуч на претплатникот.
- КИБС ИС има причина да верува дека претплатникот прекршил материјална обврска, претставување или гаранција од важечкиот Претплатнички договор.
- Претплатничкиот договор со претплатникот е истечен.
- КИБС ИС има причина да верува дека сертификатот е издаден спротивно на процедурите од овие Правила, сертификатот е издаден на лице друго од она што е наведено во сертификатот, или сертификатот е издаден без овластување на лицето наведено како субјект во сертификатот.
- КИБС ИС има причина да верува дека некој од податоците во барањето за сертификат е погрешен.
- КИБС утврди дека материјалниот предуслов за издавање на сертификатот не е задоволен.
- Во случај претплатникот да ја изгуби правната подобност, да биде прогласен за исчезнат или мртов, имајќи предвид дека сертификатот е во секој случај непренослив.
- Во случај на судска одлука без право на жалба која наложува поништување или откажување на сертификатот.

- Во случај приватниот клуч на КИБС ИС за издавање на сертификати е компромитиран.
- Информациите во сертификатот, освен не-верификуваните информации за претплатникот, се неточни или се промениле, или околностите во кои сертификатот е издаден се промениле (т.е. во случај кога вработен добил сертификат, но не е веќе вработен во таа компанија).
- Понатамошното користење на тој сертификат е штетно за VTN.

Кога се разгледува дали користењето на сертификат е штетно за VTN, КИБС ИС го разгледува, меѓу другото, и следново:

- Природата и бројот на примените поплаки;
- Идентитетот на оној што ги искажал поплаките;
- Релевантните прописи што се во сила;
- Одговорите на наводното штетно користење од страна на претплатникот.

КИБС ИС може исто така, да поништи администраторски сертификат ако овластувањето на администраторот да делува како администратор, е прекинато или на друг начин завршило.

Согласно претплатничкиот договор, крајниот корисник должен е веднаш да го извести КИБС ИС за сознанието или претпоставката дека неговиот приватен клуч е компромитиран.

По одобрување на барањето за поништување од страна на КИБС ИС, поништениот сертификат не може повторно да се стави на сила.

4.9.2. Кој може да побара поништување

Претплатникот или лицето кое што е наведено како субјект во сертификатот може да побараат поништување на своите сертификати.

КИБС има право да побара поништување на сертификатите издадени за своите сопствени СА. КИБС има право да побара или иницира поништување на сертификатите издадени на неговите сопствени РК за квалификуваните сертификати.

4.9.3. Процедура за барање за поништување

4.9.3.1. Процедура за барање за поништување на претплатнички сертификат за краен корисник

Претплатник – краен корисник кој бара поништување треба да го упати барањето по електронска пошта на sa-romos@kibs.com.mk, по што ќе биде иницирано поништување на сертификатот.

4.9.3.2. Процедура за барање за поништување на ИС или РК сертификат

КИБС може да иницира поништување на ИС или РК сертификат.

4.9.4. Греис период за барање за поништување

Барањата за поништување се поднесуваат во што е можно пократко време, кое е комерцијално разумно.

4.9.5. Време за кое ИС мора да го процесира барањето за поништување

КИБС ИС презема разумни чекори за да ги процесира барањата за поништување на сертификатот без одложување.

Веднаш по одобрувањето на барањето за поништување ИС го поништува сертификатот и го известува субјектот по електронска пошта.

4.9.6. Барања за проверка на поништувањето за засегнатите страни

Засегнатите страни ќе го проверат статусот на сертификатот на кој сакаат да се потпрат. Еден од начините на кој засегнатите страни може да го проверат статусот на некој сертификат е да го консултираат најновиот РПС од ИС. Како друга можност, засегнатите страни можат да го проверат статусот на сертификатот со користење на КИБС веб-базираното складиште. ИС ќе им обезбеди на засегнатите страни информација како да го пронајдат соодветниот РПС и/или веб-базираното складиште за да го проверат статусот на поништените сертификати.

4.9.7. Интервали на издавање на РПС

РПС за сертификатите за крајни корисници се издаваат најмалку еднаш во денот. РПС за ИС сертификатите се издаваат барем еднаш годишно, но исто така и секогаш кога ИС сертификат ќе биде поништен. Ако на сертификат што е запишан во РПС му истече важноста, тој може да биде отстранет во следно издадениот РПС по истекот на важноста на сертификатот. КИБС не ги отстранува сертификатите што се истечени од подоцна-издадените РПС. КИБС има право да го менува овој начин на работа.

4.9.8. Максимално доцнење на РПС

РПС се поставува во складиштето во разумно време откако ќе биде генериран. Ова главно се прави автоматски неколку минути по генерирањето.

4.9.9. Достапност на електронска проверка на статусот во врска со поништување

Информациите за статусот во врска со поништувањето, како и други информации за статусот на сертификатот се достапни преку веб-базираното складиште. Покрај издавањето на РПС, КИБС обезбедува информации за статусот на сертификат и преку функциите за пребарување во складиштето.

Информации за статусот на сертификатот се достапни на:

<https://secure-ca.kibs.com.mk/services/qcen/client/search.htm>

4.9.10. Барања за електронска проверка за поништување

Засегнатата страна мора да го провери статусот на сертификатот на кој сака да се повика. Ако засегнатата страна не го провери статусот на сертификатот преку консултирање на најновиот релевантен РПС, ќе го провери консултирајќи го складиштето на КИБС.

4.9.11. Други достапни облици на огласување за поништување

Не се применува.

4.9.12. Посебни барања во врска со компромитирање на клуч

КИБС вложува комерцијално разумни напори да ги извести потенцијалните засегнати страни ако открие, или има причини да верува, дека приватниот клуч на некој од неговите сопствени ИС бил компромитиран.

4.9.13. Околности за суспендирање

КИБС не обезбедува услуги на суспендирање за сертификатите што ги издава.

4.9.14. Кој може да побара суспендирање

Не се применува.

4.9.15. Процедура за барање за суспендирање

Не се применува.

4.9.16. Ограничувања за периодот на суспензија

Не се применува.

4.10. Услуги во врска со статусот на сертификатите

4.10.1. Оперативни карактеристики

Статусот на јавните сертификати е достапен преку РПС на веб-страницата на КИБС и во LDAP директориумот.

4.10.2. Достапност на услугите

Услугите за статусот на сертификатите се достапни 24 x 7 без однапред планиран прекин.

4.10.3. Опционални карактеристики

Не се применува.

4.11. Крај на претплатата

Претплатата завршува:

- со истекувањето на важноста на сертификатот;
- со поништување на сертификатот пред истекувањето на неговата важност.

4.12. Давање на чување кај трето лице и повторно преземање

ИС приватните клучеви и приватните клучеви на крајните корисници не се даваат на чување кај трето лице.

4.12.1. Политика и практики за давање на чување кај трето лице и повторно преземање

Не се применува.

4.12.2 Политика и практики за инкапулирање на сесиски клуч и повторно преземање

Не се применува.

5. КОНТРОЛИ НА ПОСТРОЈКИТЕ, МЕНАЏМЕНТОТ И ОПЕРАТИВНИ КОНТРОЛИ

5.1. Физички контроли

КИБС има имплементирано сет од безбедносни политики, кои ги поддржуваат барањата за безбедност од овие Правила. Придржувањето кон овие политики е вклучено во условите за надзор опишани во Дел 8 од овие Правила. Безбедносните политики на КИБС содржат осетливи податоци за безбедноста и се ставаат на располагање само по потпишување на договор со КИБС. Преглед на овие услови е даден подолу.

5.1.1. Локација и конструкција

КИБС ИС и РК операциите се изведуваат во рамките на физички заштитена средина која одбива, спречува и забележува неовластено користење на пристап до или откривање на осетливи информации, било да е тоа притаено или отворено.

ИС операциите ги извршува ADACOM SA. ADACOM одржува локации за опоравување од кризи за своите ИС операции. Локацијата за опоравување од кризи на ADACOM е во согласност со безбедносните барања за складирање настрана од деловните простории, кои се наведени во „План за надминување кризи на ADACOM“.

5.1.2 Физички пристап

КИБС системите се заштитени со пет нивоа на физичка заштита, при што е потребно да се има пристап до пониското ниво пред да се добие дозвола за пристап во повисокото ниво.

КИБС ги користи системите на ADACOM SA кои се заштитени со седум нивоа на физичка заштита, при што потребно е да се има пристап најнапред до пониското ниво за да се добие дозвола за пристап до повисокото ниво.

Прогресивно рестриктивниот пристап претставува контрола на пристапот на секое ниво. Осетливите оперативни активности, било каква активност поврзана со животниот циклус во сертификацискиот процес, како што се автентикација, верификација и издавање, се случуваат во рамките на многу рестриктивни физички нивоа. За влез во секое ниво потребна е бец картичка за пристап на вработениот. Физичкиот пристап автоматски се запишува и се снима на видео. Некои нивоа применуваат индивидуална контрола на пристапот со истовремено користење и на картичка и на биометрика (два фактори на идентификација). Доколку посетител или вработено лице кое нема овластување или пак не е придружувач од лице на кое му е доверено овластување за пристап, не се дозволува влез во таквите обезбедени простори.

Системот за физичка безбедност кој го употребува ADACOM вклучува нивоа за безбедност а управувањето на клучевите со цел заштита на електронското и неелектронското складирање на ЦСУ-те и материјалот со клучеви. За просториите што се користат за креирање и складирање на криптографски материјал се применува двојна контрола, секоја од нив со истовремено користење на картичка и биометриски карактеристики. Онлајн ЦСУ се заштитени со користење на заклучени кабинети. Офлајн ЦСУ се заштитени со користење на заклучени сефови, кабинети и контејнери. Пристапот до ЦСУ и материјалот со клучеви е ограничен во согласност со условите на ADACOM за сегрегација на должностите. Отварањето на кабинетите и контејнерите во овие слоеви се логира за да може да се надгледува.

5.1.3. Електрична енергија и климатизација

Безбедните простории на КИБС и ADACOM се опремени со примарни и резервни:

- системи за електрична енергија кои ќе обезбедуваат континуирано и непрекинато напојување со електрична енергија и
- системи за греење/ вентилација/ климатизација, со кои ќе се контролира температурата и релативната влажност.

5.1.4. Изложување на вода

ADACOM и КИБС имаат превземено разумни мерки на претпазливост со цел да го минимизираат негативното влијание од изложување на вода врз системите.

5.1.5. Превентива и заштита од пожар

ADACOM и КИБС ги имаат превземено сите разумни мерки за спречување и гасење на пожар или други драматични изложувања на оган или чад. Превентивните и заштитните мерки на КИБС се дизајнирани на таков начин да се во согласност со локалните барања за безбедност од пожари.

5.1.6. Складирање на медиумите

Сите медиуми кои содржат продукциски софтвери и податоци за надзор, архивски информации или резервни копии на податоци се складираат во рамките на просториите на КИБС и ADACOM во безбедни згради надвор од деловните простории со соодветни контроли за физички и логички пристап дизајнирани на таков начин што ќе го ограничи пристапот само на овластениот персонал и ќе ги заштити тие медиуми од евентуални штети (пр., вода, оган и електромагнетни бранови).

5.1.7. Отстранување на отпадот

Осетливите документи и материјали се уништуваат со сецкање пред да се исфрлат. Медиумите што се користат за чување или пренос на осетливи податоци се прават нечитливи пред да се исфрлат. Криптографските направи физички се уништуваат или онеспособуваат во согласност со инструкциите на производителот пред да се исфрлат. Останатиот отпад се исфрла во согласност нормалните барања на ADACOM и КИБС за ослободување од отпадот.

5.1.8. Резервни копии надвор од деловните простории

ADACOM и КИБС вршат рутинско складирање на клучните системски податоци, податоците од логовите за надзор и другите осетливи информации. Медиумите со резервни копии се чуваат надвор од просториите на физички безбеден начин.

5.2. Процедурални контроли

5.2.1. Доверливи улоги

Доверливи лица се вработените лица кои имаат пристап до или го контролираат потврдувањето на автентичноста и криптографските операции кои можат материјално да влијаат на:

- Потврдувањето на информациите во барањата за сертификати,

- Прифаќањето, одбивањето или друг вид на обработка на барањата за сертификати, барањата за поништување, барањата за обновување, или информации за регистрацијата,
- Издавањето или поништувањето на сертификати, вклучително и персоналот кој има пристап до ограничените делови од складиштето,
- Ракувањето со информациите или барањата на претплатниците.

Како доверливи лица се сметаат оние:

- кои даваат услуги на клиентите,
- што работат на криптографски деловни операции,
- кои се задолжени за безбедност,
- кои се задолжени за администрација на системот,
- кои се дел од инженерскиот тим
- извршни раководни лица кои се назначени да ја управуваат доверливоста на инфраструктурата.

КИБС ги смета категориите на вработени лица наведени во овој дел за доверливи лица кои имаат доверливи позиции. Вработените кои сакаат да станат доверливи лица со добивање на доверливи позиции мораат sukcesивно да ги задоволат безбедносните барања наведени во овие Правила.

На лицата со договор и консултантите кои имаат пристап до или го контролираат потврдувањето на автентичноста и криптографските операции не им е дозволено да ги извршуваат овие операции без придружба.

5.2.2. Број на лица потребни за една работна задача

КИБС воспостави, одржува и применува ригорозни контролни процедури за да обезбеди издвојување на должностите врз основа на работните одговорности и согласно потребите да обезбеди повеќе доверливи лица да ги извршуваат осетливите задачи.

Политиката и контролните процедури треба да обезбедат одвојување на должностите врз основа на работните одговорности. Најосетливите задачи, бараат ангажирање на повеќе доверливи лица.

Валидацијата и издавањето на квалификувани сертификати наложува потреба од најмалку 2 доверливи лица, или комбинација од барем едно доверливо лице и процес за автоматско валидација и издавање.

5.2.3. Идентификација и автентикација за секоја позиција

За вработените лица кои бараат да станат доверливи лица, се врши проверка на идентитетот со нивно лично присуство пред доверливите лица на КИБС, кои работат во одделот за човечки ресурси или ги вршат безбедносните функции и презентирање на документ за идентификација (пасош или лична карта). Идентитетот потоа се потврдува преку процедурите на проверка на биографијата, на начин уреден во делот 5.3.1. од овие Правила.

Откако ќе се потврди дека лицата стекнале доверлив статус, соодветниот оддел дава одобрување пред да им бидат:

- издадени уреди за влез за дозволен пристап во потребните простории, и
- издадени електронски акредитиви за пристап и за изведување на специфични функции во КИБС ИС, РК или други системи на информатичка технологија.

5.2.4. Позиции за кои е потребно одвојување на должностите

Позициите за кои е потребно одвојување на должностите вклучуваат, но не се ограничени на:

- Потврдување на информациите во барањата за сертификати,
- Прифаќање, одбивање и друг вид на обработка на барањата за сертификати, барањата за поништување, или за обновување, или информациите за регистрација;
- Издавање или поништување на сертификати, вклучувајќи ги и лицата кои имаат пристап до ограничените делови на просторот за складирање;
- Ракување со информациите и барањата на претплатниците;
- Генерирање, издавање или поништување на ИС сертификат.

5.3. Контроли на персоналот

Вработените лица кои бараат да станат доверливи лица мораат да презентираат доказ за биографските податоци, квалификациите и искуството што се потребни за извршување на нивните идни работни задачи во целост и на задоволителен начин. Проверки на биографските податоци се вршат најмалку на 5 години за доверливите лица.

5.3.1. Предуслови за квалификации и искуство

КИБС бара од вработените кои сакаат да станат доверливи лица да презентираат доказ за неопходните биографски податоци, квалификациите и искуството што им се потребни за да ги извршуваат своите идни работни обврски целосно и на задоволителен начин.

5.3.2. Процедури на проверка на биографијата

КИБС, пред да вработи лице на доверлива позиција, спроведува проверка на биографијата, која вклучува:

- проверка на претходните вработувања, доколку постојат,
- потврда на највисокиот или најрелевантниот степен на образование што е стекнат,
- потврда за неосудуваност.

Онаму каде што некои од овие предуслови наведени во овој дел не можат да бидат задоволени заради забрани или ограничувања, согласно пропис или поради други околности, КИБС ќе примени алтернативни техники дозволени со пропис, кои ќе обезбедат суштествено слични информации.

Фактите од проверката на биографијата што можат да се сметаат како основа за одбивање на кандидатите за доверливи позиции или за преземање дејствија против веќе вработено доверливо лице главно го вклучуваат, но не се ограничени на:

- Погрешно претставување од страна на кандидатот или доверливото лице,
- Крајно неповолни професионални референци,
- Одредени пресуди за криминални дејствија.

Извештаите кои содржат такви информации се разгледуваат од страна на одделот за човечки ресурси и безбедност, кои ги определуваат понатамошните насоки на делување во зависност од видот, големината и зачестеноста на однесувањето до кое е дојдено со проверката на биографијата. Тие дејствија може да вклучуваат мерки и до откажување на понудата за вработување на кандидати за доверливи позиции или до прекин на работниот однос на постојното доверливо лице.

Користењето на информациите утврдени со проверката на биографијата за преземање на одредени активности е предмет на важечките прописи.

5.3.3. Неопходна обука

КИБС обезбедува обука на вработените веднаш по вработувањето или обуката ја врши на самото работно место што е им е потребно за да ги извршуваат своите работни обврски целосно и на задоволителен начин. КИБС води евиденција за таквите обуки. На одредени временски периоди КИБС ги ревидира и надградува своите програми за обука според потребите.

Програмите на КИБС за обука се сочинети според индивидуалните работни одговорности и како релевантно го вклучуваат следново:

- Основи на ПКИ,
- Работните одговорности,
- Безбедносните и оперативните политики и процедури на КИБС,
- Користењето и оперирањето со хардверот и софтверот што е дистрибуиран,
- Пријавување и справување со инциденти и компромитирања.

5.3.4. Услови и период на повторна обука

КИБС обезбедува обновена и осовременета обука за својот персонал до онаа мерка и со онаа периодичност што е потребна за да го одржи потребното ниво на стручност за извршување на работните задачи компетентно и на задоволувачки начин.

5.3.5. Период и редослед на ротирање на работните места

Не се применува.

5.3.6. Санкции за неовластени дејствија

За неовластени дејствија и други прекршувања на политиките и процедурите на КИБС се превземаат соодветни дисциплински мерки. Дисциплинските дејствија може да вклучуваат различни мерки се до прекин, вклучително и прекин на работниот однос и соодветствуваат со зачестеноста и сериозноста на неовластените дејствија.

5.3.7. Предуслови за независни лица по договор

Само во одредени околности може да се користат самостојни лица по договор или консултанти за да се пополнат доверливи позиции. Таквите лица по договор или консултанти се подложни на истите функционални и безбедносни критериуми кои што важат за вработените на КИБС на слична позиција. На независните лица по договор и на консултантите кои не ги завршиле или поминале процедурите на проверка на биографски податоци наведени во делот 5.3.2 од овие Правила, пристапот до безбедните простори на КИБС им е дозволен само доколку се придружувани и директно надгледувани од страна на доверливо лице.

5.3.8. Документација што му се обезбедува на персоналот

КИБС на својот персонал ја обезбедува потребната обука, како и документацијата што им е потребна за да ги извршуваат своите работни обврски целосно и на задоволителен начин.

5.4. Процедури за ревизорска трага (Audit logging Procedures)

5.4.1. Видови на настани што се евидентираат

КИБС ги евидентира, мануелно или автоматски, следниве значајни настани:

- Настани од управувањето на животниот циклус на ИС клучевите, вклучувајќи ги:
 - Генерирањето на клучеви, резервна копија, складирање, повторно активирање, архивирање и уништување,
 - Настаните поврзани со управување на животниот циклус на криптографските направи.
- Настани од управувањето на животниот циклус на ИС сертификатите и претплатничките сертификати, кои ги вклучуваат:
 - Барања за издавање сертификати, обновување и поништување,
 - Успешната или неуспешната обработка на барањата,
 - Генерирање и издавање на РПС.
- Настани поврзани со безбедноста, кои вклучуваат:
 - Успешни или неуспешни обиди за пристап до ПКИ системот,
 - ПКИ и безбедносни системски дејствија,
 - Безбедносно осетливи документи или записи што се прочитани, напишани или избришани,
 - Промени на безбедносниот профил,
 - Испади на системот, откажување на хардверот и други аномалии,
 - Активности поврзани со огнен ѕид и мрежен упатувач,
 - Влез/излез на посетители во просториите на КИБС ИС.

Записите во евиденцијата ги вклучува следниве елементи:

- Датум и време,
- Сериски или редоследен број на автоматскиот запис,
- Идентитет на ентитетот што извршува внес во евиденцијата,
- Вид на записот.

КИБС ИС ги евидентира информациите од барањата за сертификати, вклучувајќи ги:

- Видот на документот(ите) за идентификација презентирани од барателот на сертификат,
- Единствените идентификациски податоци од документот за идентификација,
- Локацијата на складирање на барањата и копии на документите за идентификација,
- Идентитетот на субјектот што го прифаќа барањето,
- Методот што е применет за потврдување на валидноста на документот за идентификација,
- Име на канцеларијата која ги прима барањата.

5.4.2. Интервал на преглед на ревизорски траги

Ревизорската трага се прави најмалку еднаш неделно во однос на значајните безбедносни или оперативни настани. Покрај тоа, КИБС ИС ги прегледува своите ревизорски траги на сомнителни или невообичаени активности, како одговор на тревоги што се појавуваат заради неправилности или инциденти во рамки на системите на КИБС ИС.

Обработката на ревизорската трага се состои од прегледување на ревизорските траги и документацијата на сите значајни настани во прегледот на евиденцијата. Прегледите на евиденцијата за контрола вклучува и проверка дека во евиденцијата не е интервенирано неовластено, како и увид во сите записи во евиденцијата и испитување на било какви тревоги или неправилности во записите. Покрај тоа, се документираат и сите дејствија што се преземаат врз основа на прегледите на ревизорските траги.

5.4.3. Период на зачувување на ревизорските траги

Ревизорските траги се зачувуваат на локацијата најмалку два (2) месеци по обработката, а потоа се архивираат во согласност со Дел 5.5.2. од овие Правила.

5.4.4. Заштита на ревизорските траги

Ревизорските траги се заштитуваат со систем за електронска евиденција, кој вклучува механизми за заштита на датотеките за евиденција, од неовластено прегледување, изменување, бришење или друго интервенирање.

5.4.5. Процедури за правење безбедносни копии на ревизорските траги

Секојдневно се прави дополнителна заштита на ревизорските траги.

5.4.6. Систем за логирање на податоците

Автоматските податоци за логирање се генерираат и се забележуваат на ниво на апликација, мрежа и оперативен систем.

5.4.7. Известување до субјектот што го предизвикал настанот

Кога некој настан се евидентира од страна на системот за евиденција, физичкото лице, организацијата, направата или апликацијата што го предизвикала тој настан не се известува.

5.4.8. Проценка за ранливост

Настаните во процесот на контролата се евидентираат делумно и заради надгледување на ранливоста на системот. Логичката проценка за ранливост во безбедноста (ЛПРБ) се извршува, прегледува и проверува преку испитување на овие записи. Овие ЛПРБ се базираат на автоматско логирање на податоците во реално време и се изведуваат на дневна, месечна и годишна основа. Годишниот ЛПРБ е влез за годишната контрола на сообразност.

5.5. Архивирање на записите

5.5.1 Видови на записи кои се архивираат

КИБС ИС ги архивира:

- Сите податоци прибрани во согласност со дел 5.4. од овие Правила,
- Информациите за барањата за сертификати,
- Документацијата приложена кон барањата за сертификати,
- Информациите за животниот циклус на сертификатот како на пример, информации за барања за поништување и обновување.

КИБС ИС ја чува следнава документација што се однесува на идентитетот на претплатниците, а во врска со барањата за квалификувани сертификати:

- Видовите на документи поднесени од барателите на сертификати, во врска со нивните барања за сертификати.
- Доказите за единствени идентификациски податоци (пр. матичен број, број на документ за идентификација) од документите за идентификација, ако е применливо,
- Идентитетот на ентитетот што го прима и прифаќа барањето за сертификат,
- Планот за валидација во кој се прикажани методите што се користат за валидација на документите за идентификација.

Покрај тоа, КИБС задржува записи за локацијата на складирање на барањата за сертификати и документите за идентификација.

5.5.2 Период на зачувување на архивата

Документацијата поврзана со квалификуван сертификат се чува најмалку пет (5) години од поништувањето или истекот на важноста на конкретниот квалификуван сертификат.

5.5.3. Заштита на архивата

КИБС ИС ја заштитува архивата на тој начин, што само овластени доверливи лица имаат можност да добијат пристап до неа. Архивата е заштитена од неовластено разгледување, изменување, бришење или друг вид на упад во рамките на доверливиот систем. Медиумот на кој се чуваат архивските податоци и барањата што се потребни за обработка на архивските податоци ќе се одржува со цел да се обезбеди пристап до архивските податоци во временскиот период наведен во овие Правила.

5.5.4. Процедури за архивирање

КИБС ИС за електронските архиви на информациите за своите издадени сертификати и прави целосна сигурносна копија дневно и неделно. Копии од документацијата на хартија ќе се чуваат со користење на безбедни простории на друга локација оддалечена од деловната зграда.

5.5.5. Предуслови за временски печат на документацијата

Сертификатите, РПС-ите и другите записи за поништување во базата на податоци содржат информации за времето и датумот.

5.5.6. Систем за архивирање

Системите на КИБС ИС за архивирање се интерни.

5.5.7 Процедури за добивање и верификување на интегритет на архивски податоци

Само овластени доверливи лица можат да добијат пристап до архивата, а интегритетот на добиениот архивски податок се верификува.

5.6. Промена на клучеви

Парот на клучеви на КИБС ИС се повлекува од употреба на крајот на нивниот животен циклус, согласно овие Правила. Сертификатите на КИБС ИС можат да се обноват, доколку кумулативниот животен циклус на парот на клучеви, не го надмине максималниот животен циклус на парот на клучеви на наредениот ИС. Доколку е неопходно, се генерира нов пар на

ИС клучеви, на пример, за да се заменат паровите на клучеви што се повлекуваат, за да се надополнат постоечките, активни парови на клучеви и за да се поддржат нови услуги.

Пред истекот на сертификатот на надредениот ИС, се активираат процедури за промена на клучеви со цел да се овозможи полесен премин за субјектите во рамките на хиерархијата на надредениот ИС од стариот пар на клучеви кон нов(и) пар(ови) на клучеви. Процесот на промена на КИБС ИС клучевите претпоставува дека:

- Надредениот ИС престанува да издава нови сертификати за подредени ИС најдоцна 60 дена пред даден момент (“Датата за престанок на издавање”), при што остатокот од животниот циклус на парот на клучеви на надредениот ИС е еднаков со периодот на важност на одобриениот сертификат за специфичен(и) тип(ови) на сертификати што се издаваат од страна на подредени ИС во хиерархијата на надредените ИС.
- По успешната валидација на барањата за сертификат на подредените ИС (или претплатниците - крајни корисници) што се примени после “Датата за престанок на издавање”, сертификатите ќе бидат потпишани со новиот пар на клучеви на ИС.

Надредениот ИС продолжува да издава РПС-и со оригиналните приватни клучеви на Надредениот ИС се до истекот на датата на последниот сертификат што е издаден со користење на оригиналниот пар клучеви.

5.7. Опоравување од компромитирање и од кризни ситуации

5.7.1. Процедури за справување со инциденти и компромитирање

Информациите за кои КИБС ИС прави сигурносна копија во простории надвор од локацијата на деловната зграда и се расположливи во случај на компромитирање и кризни ситуации се следниве: податоци од барањата за сертификати, евиденции и бази на податоци со документација за издадените сертификати. Сигурносна копија на приватните клучеви на ИС се генерира и се одржува во согласност со дел 6.2.4. од овие Правила. КИБС ИС одржува сигурносна копија за ИС информации за своите сопствени ИС.

5.7.2. Компромитирани компјутерски ресурси, софтвер и/или податоци

Во случај на корумпирање на компјутерските ресурси, софтверот и/или податоците, таков настан се пријавува на одделот за безбедност на ADACOM и се активираат процедурите за справување со инциденти. Таквите процедури претпоставуваат соодветна ескалација, истражување на инцидентот и одговор на инцидентот. Доколку е неопходно, ќе се применат процедурите за справување со компромитиран клуч или кризна ситуација.

5.7.3. Процедури при компромитирање на приватниот клуч на ентитети

По претпоставено или познато компромитирање на ADACOM ИС, инфраструктурата на ADACOM или на приватниот клуч на КИБС ИС, се применуваат процедурите за Реакција на компромитирање на клуч од страна на Тимот за справување со безбедносен инцидент на ADACOM SA. Овој тим, во кој се вклучени вработени лица од безбедноста, криптографските деловни операции, производните услуги и други претставници на управата на ADACOM ја проценува ситуацијата, прави акционен план и го спроведува акциониот план со одобрение од страна на извршната управа на ADACOM.

Ако е потребно поништување на ИС сертификат, се изведуваат следниве процедури:

- За статусот на поништениот сертификат се информираат засегнатите страни преку КИБС складиштето, во согласност со дел 4.4.9 од овие Правила,

- Се вложуваат комерцијално разумни напори за да се достави дополнителна информација за поништувањето, на сите загрозени VTN Учесници и
- ИС генерира нов пар на клучеви во согласност со дел 4.7 од овие Правила, освен кога се укинува ИС во согласност со дел 4.9 од овие Правила.

5.7.4. Способност за продолжување на деловните активности по кризна ситуација

5.7.4.1. Verisign

VeriSign има на располагање постројки за опоравување од катастрофи поставени на локација на оддалеченост од повеќе од 1600 км од VeriSign главните безбедни простории. VeriSign има развиено, применето и тестирано план за надминување на катастрофи за да ги ублажи ефектите од било какви природни катастрофи или катастрофи предизвикани од човечки фактор. Овој план редовно се тестира, верификува и надградува за да биде оперативен во случај на катастрофа.

Деталните планови за надминување на катастрофи имаат за цел да се насочат кон повторно ставање во функција на услугите на информатичките системи и клучните деловни активности. Локацијата на VeriSign за опоравување од катастрофи има поставено заштита за физичка безбедност и оперативни контроли согласно „VeriSign Водичот за предуслови за безбедност и надзор“ за да обезбедат цврста поставеност на оперативни сигурносни копии.

Во случај на природна катастрофа или катастрофа предизвикани од човечки фактор заради која е потребен прекин на операциите од VeriSign примарните постројки, се активира VeriSign процесот за справување со катастрофи од страна на VeriSign Тимот за делување во итни ситуации.

VeriSign има капацитет повторно да ги воспостави или да ги поврати неопходните операции во рок од 24 часа по катастрофата со поддршка барем на следниве функции:

- Издавање на сертификати,
- Поништување на сертификати,
- Објавување на информации за поништување
- Обезбедување на информации за повторно добивање на клучеви за Клиентите - Претпријатија кои користат МПКИ менаџер за клучеви.

VeriSign базата на податоци за опоравување од катастрофа редовно се синхронизира со базата на податоци од производството со временски рокови наведени во Водичот за предуслови за безбедност и надзор. VeriSign опремата за опоравување од катастрофи е обезбедена со заштита за физичка безбедност кои можат да се споредат со нивоата за физичка безбедност наведени во дел 5.1.2 од овие Правила.

VeriSign Планот за надминување на катастрофи е сочинет на начин за да обезбеди потполно опоравување во рок од една седмица од катастрофата што се случила во примарните простории на VeriSign. VeriSign ја тестира својата опрема во своите примарни простории за да ги поддржи ИС/ПК функциите што би следеле по сите кризни ситуации, освен голема катастрофа која што би ги ставила надвор од функција сите постројки на таа локација. Резултатите од таквите тестови се прегледуваат и се чуваат за цели на надзор и планирање. До колку е тоа возможно, операциите што е можно поскоро се обновуваат на примарната локација на VeriSign после поголема катастрофа.

VeriSign одржува резервен хардвер и сигурносни копии на своите ИС и инфраструктурни системски софтвери во своите постројки за надминување на катастрофи. Покрај тоа, СА приватните клучеви резервно се чуваат и одржуваат за цели на опоравување од катастрофи во согласност со дел 6.2.4. од овие Правила.

VeriSign одржува сигурносна копија од значајните информации за VeriSign ИС, како и од сервисните центри на ИС и клиентите - претпријатија, во рамките на поддоментот на VeriSign на локација оддалечена од главните постројки. Таквите информации вклучуваат, но не се и ограничени на: податоците од барањата за сертификати, податоците од надзорот (дел 5.4) и документацијата од базата на податоци за сите сертификати што се издадени.

5.7.4.2. ADACOM

ADACOM има воспоставено план за надминување на катастрофи со цел да ги ублажи последиците од било какви природни катастрофи или катастрофи предизвикани од човечки фактор. Овој план редовно се тестира, верификува и надградува за да биде оперативен во случај на катастрофа.

Деталните планови за надминување на катастрофи имаат за цел да се насочат кон повторно ставање во функција на информатичките системи и клучните деловни активности.

Во случај на природна катастрофа или катастрофа предизвикана од човечки фактор заради која е потребен прекин на операциите на примарната локација, се активира процесот за справување со катастрофи од страна на раководниот тим на ADACOM.

ADACOM има капацитет повторно да ги воспостави или да ги поврати операциите, со врвен приоритет на поддршката на функциите за поништување на сертификати и објавување на информации за поништување.

ADACOM прави сигурносна копија на системите на ИС и инфраструктурните системски софтвери на безбедна локација подалеку од главните простории. ADACOM исто така одржува и резервно складирање на значајни информации за ADACOM ИС.

Покрај тоа, се прави сигурносна копија и на ИС приватните клучеви и тајните удели со цел за надминување на катастрофи во согласност со дел 6.2.4. од овие Правила, „Планот за надминување на кризи за времено складирање на криптографските материјали на одвоена локација на ADACOM” и „Планот за надминување на кризи на ADACOM”, со што се овозможува обновување на деловните активности подоцна.

5.8. Прекин на дејноста на КИБС ИС

Во случај да е неопходно КИБС ИС да ги прекине активностите, КИБС ги известува претплатниците, засегнатите страни и другите ентитети. Доколку КИБС престане да ја извршува дејноста на ИС, ќе го активира документиранiot „План за прекинување на активностите на КИБС” за да го минимизира дисконтинуитетот кај клиентите, претплатниците и засегнатите страни. Овој план за прекинување на работење се однесува на следново:

- Доставување известување до страните засегнати со прекинувањето, како што се клиентите, претплатниците, засегнатите страни, информирајќи ги за статусот на ИС,
- Поднесување на трошоците за таквото известување,
- Поништувањето на сертификатот на ИС,
- Чувањето на архивите и документацијата на ИС во периодот што е предвиден во овие Правила,
- Продолжување на услугите на поддршка на претплатниците и клиентите,
- Продолжување на услугите на поништување, како што е издавање на РПС или одржување на услугата за електронска проверка на статусот,
- Поништување на неистечени непоништени сертификати на претплатниците крајни корисници, доколку е неопходно,

- Рефундирање на претплатниците чии неистечени непоништени сертификати се поништуваат во рамките на планот за прекинување или обезбедување, или друга алтернатива, на издавање на сертификат како замена, од страна на ИС што ќе ја наследи дејноста.
- Дислокација на приватниот клуч на ИС и хардверските токени што го содржат тој приватен клуч.
- Одредбите што се потребни за пренесување на услугите, на ИС што ги продолжува активностите.
- Доставување на известување до надлежната институција во Република Македонија.

Во случај да е неопходно КИБС да ги прекине активностите, КИБС дополнително ќе ги направи сите неопходни чекори согласно закон. Ова вклучува, но не се ограничува на предавање на архивите и документацијата на КИБС ИС на друг обезбедувач на сертификациски услуги за квалификувани сертификати, во временски период предвиден со закон.

6. КОНТРОЛИ НА ТЕХНИЧКАТА БЕЗБЕДНОСТ

6.1. Генерирање и инсталирање на пар на клучеви

6.1.1. Генерирање на пар клучеви

Генерирањето на парот на клучеви за ИС се изведува од страна на неколку избрани, обучени и доверливи лица користејќи доверливи системи и процеси кои обезбедуваат безбедност и потребна криптографска снага за генерираните клучеви. Криптографските модули што се користат и издавањето на клучеви за ПИС и за коренските ИС за издавање ги задоволуваат условите од CC EAL 4+ и FIPS 140-1 Ниво 3.

Сите парови на клучеви за ИС се генерираат со претходно планирана церемонија на генерирање клучеви, во согласност со условите на следните документи: „Референтен водич за церемонија на генерирање клучеви“, „Кориснички водич за алатки за управување со ИС клучеви“ и „VeriSign Водичот за услови за безбедност и надзор“. Активностите што се изведуваат при секоја церемонија на генерирање на клучеви се документираат, датираат и потпишуваат од лицата што се вклучени. Оваа документација се чува со цел за надзор и пребарување во временски период што се смета за соодветен од страна на Управата на КИБС.

Генерирањето на РК пар на клучеви главно се изведува од страна на РК со користење на криптографски модул сертифициран според CC EAL 4+ и FIPS 140-1 Ниво 1.

Генерирањето на парот на клучеви за претплатникот - краен корисник главно се изведува од страна на претплатникот.

6.1.2. Испорака на приватниот клуч на претплатникот

Паровите на клучеви за претплатникот - краен корисник се генерираат од страна на претплатникот - краен корисник, така што испораката на клучеви на претплатникот не може да се примени.

6.1.3. Испорака на јавниот клуч на издавачот на сертификати

Претплатниците - крајни корисници го поднесуваат својот јавен клуч до КИБС ИС за да биде електронски сертифициран со користење на PKCS#10 Барање за потпишување на Сертификат (Certificate Signing Request -CSR) или друг дигитално потпишан пакет во сесија обезбедена со протоколот Secure Sockets Layer (SSL).

6.1.4. Испорака на јавниот клуч на засегнатите страни

КИБС ги става ИС Сертификатите за VeriSign ПИС и за своите коренски ИС на располагање на претплатниците и засегнатите страни преку нивно вклучување во софтверот за веб-прелистување. Кога новите ПИС и коренски сертификати ќе бидат генерирани, VeriSign им ги доставува тие нови сертификати на производителите на веб-прелистувачи за да ги вклучат во новите изданија.

КИБС вообичаено им обезбедува целосен синџир на ИС сертификати на своите претплатници - крајни корисници по издавањето на сертификатот.

Корисниците за време на процесот на подигнување на сертификатот автоматски го преземаат и го инсталираат на својот компјутер јавниот клуч на посредничкиот ИС и на издавачкиот ИС. Во секој случај, доколку корисникот има потреба да го верификува и/или преземе јавниот клуч

на ИС, тој може да го стори тоа пристапувајќи до КИБС веб-базираното складиште (ca.kibs.com.mk/repository).

6.1.5. Големина на клучевите

Парот на клучеви треба да биде со должина доволна да ги спречи другите да го откријат приватниот клуч од парот од клучеви со користење на криптоанализа за време на периодот кога се очекува да се користи тој пар клучеви. Третата генерација (G3) на VeriSign има пар клучеви за ПИС од 2048 бита. КИБС ИС за квалификуваните сертификати има RSA пар клучеви од 2048 бита.

КИБС РК употребува пар на клучеви од 1024 или повеќе. КИБС препорачува претплатникот - краен корисник да генерира RSA пар на клучеви од 1024 бита. КИБС може да не одобри издавање на сертификати на крајни корисници кои имаат генерирано пар на клучеви со големина од 512 бита или помала.

6.1.6. Параметри на генерирање јавен клуч и проверка на квалитетот

Не се применува.

6.2. Заштита на приватен клуч и инженерски контроли на криптографскиот модул

ADACOM има имплементирано комбинација од физички, логички и процедурални контроли за да ја обезбеди сигурноста на КИБС ИС приватните клучеви. Од претплатниците со договор се бара тие да ги преземат сите неопходни мерки на претпазливост за да спречат губење, откривање, измена или неовластена употреба на сопствениот приватен клуч.

6.2.1. Стандарди и контроли за криптографски модули

За генерирање на пар клучеви за ПИС и за издавачките ИС сертификати, како и за складирање на приватните клучеви за ИС, VeriSign користи хардверски криптографски модули кои се сертифицирани за или ги задоволуваат предусловите од CC EAL 4+ и FIPS 140-1 Ниво 3. За останатите КИБС ИС, се користат хардверски криптографски модули кои се сертифицирани за или ги задоволуваат предусловите наведени во дел 6.1.1 од овие Правила.

Покрај одредбите наведени во овие Правила, КИБС дистрибуира БСЕП за DL2 претплатниците - крајни корисници кое мора да ги задоволи следниве предуслови.

Пред се, БСЕП со соодветни технички и процедурални мерки го обезбедува најмалку следново:

- приватниот клуч во рамките на БСЕП практично може да се појави само еднаш и дека неговата тајност е во разумна мерка гарантирана,
- таквиот приватен клуч не може, со разумна гаранција, да биде произведен и дека потписот е заштитен од фалсификување со користење на во моментално достапната технологија, и
- приватниот клуч може да биде заштитен од страна на претплатникот против неговата употреба од други

Второ, дека БСЕП не ги менува податоците што треба да бидат потпишани или/и не спречува таквите податоци да му бидат презентирани на потписникот пред процесот на потпишување.

БСЕП што ги користи КИБС се сертифицирани и ги задоволуваат условите од CC EAL 4 +.

6.2.2. Контрола на приватен клуч од повеќе лица (м од н)

КИБС применува технички и процедурални механизми кои предвидуваат повеќе доверливи лица да ги изведуваат осетливите криптографски операции. КИБС користи “Споделување на тајните удели” за да ги раздели податоците за активирање што се потребни за да се користи ИС приватниот клуч на одвоени делови наречени “Тајни удели”, кои се чуваат од страна на обучени и доверливи лица наречени “Чувари на уделите”. За да се активира приватниот клуч на ИС, складиран во модулот, потребен е минимален број (м) на Тајни удели од целосниот број (н) на Тајните удели коишто се креирани и дистрибуирани за конкретниот криптографски модул.

Минималниот број на удели што се потребни за да се потпише сертификат на ИС е три (3). Тајните удели се заштитени во согласност со овие Правила.

6.2.3. Давање на чување на приватните клучеви

Приватните клучеви на КИБС ИС и на крајните корисници не се даваат на чување кај трето лице.

6.2.4. Резервно складирање на приватните клучеви

ADACOM прави резервни копии на приватните клучеви на КИБС ИС заради рутинско обновување и со цел за надминување на катастрофи. Таквите клучеви се складираат во шифрирана форма во рамките на криптографски модули и слични направи за складирање. Криптографските модули што се користат за складирање на приватните клучеви на ИС ги задоволуваат критериумите на овие Правила. Приватните клучеви на ИС се копираат на резервни хардверски криптографски модули во согласност со овие Правила.

Модули што содржат резервни копии на приватни клучеви на ИС на главната локација се подложни на условите на овие Правила. Модули што содржат копии за надминување на катастрофи, исто така се предмет на условите на овие Правила.

ADACOM не складира копии од приватните клучеви на РК. За складирање на приватните клучеви на претплатниците - крајни корисници, види дел 6.2.3 и дел 4.1.2.

6.2.5. Архивирање на приватните клучеви

По истекот на периодот на важност на КИБС ИС сертификатот, парот на клучеви што е поврзан со сертификатот безбедно се зачувува одреден временски период од најмалку 5 години со користење на хардверски криптографски модули кои ги задоволуваат критериумите на овие Правила. Овие ИС парови на клучеви не треба да се користат за потпишување, освен ако ИС Сертификатот не се обнови согласно овие Правила.

КИБС не архивира копии на приватните клучеви на РК и на Претплатници.

6.2.6. Пренос на приватните клучеви во или од криптографскиот модул

ADACOM генерира КИБС ИС парови на клучеви на хардверските криптографски модули од кои клучевите ќе се користат. Покрај тоа, ADACOM прави копии на тие ИС парови на клучеви заради рутинско обновување и со цел за надминување на катастрофи. Во случаи кога ИС паровите на клучеви се резервно складираат во друг хардверски криптографски модул, таквите парови на клучеви се пренесуваат помеѓу модулите во шифрирана форма.

6.2.7. Складирање на приватниот клуч на криптографски модул

ИС и РК приватните клучеви кои се поставени на хардверски криптографски модули се складираат во шифрирана форма.

6.2.8. Метод на активирање на приватниот клуч

Сите учесници во КИБС поддоменот ќе ги заштитуваат податоците за активирање на нивните приватни клучеви од губење, кражба, изменување, неовластено откривање или неовластена употреба.

6.2.8.1. Приватни клучеви на квалификуваните сертификати

VTN Стандардите за заштита на приватни клучеви предвидуваат претплатниците да преземаат комерцијално разумни мерки за физичка заштита на своите работни станици за да го спречат користењето на тие работни станици и на приватните клучеви поврзани со нив без овластување на претплатникот. Покрај тоа, КИБС препорачува претплатникот да користи лозинка во согласност со дел 6.4.1 или еквивалентно обезбедување за автентикација на претплатникот пред активирање на приватниот клуч, кое вклучува, на пример, лозинка за оперирање со приватниот клуч, лозинка за најавување на Windows или заштита на заклучување на мониторот.

Покрај претходно наведеното:

- За претплатниците на DL 1 Сертификатите не постои услов за користење на БСЕП во врска со користењето и активирањето на нивниот приватен клуч.
- Претплатниците на DL 2 Сертификатите ќе користат БСЕП во врска со користењето и активирањето на нивниот приватен клуч.

6.2.8.2. Приватни клучеви на администраторите

Стандардот за заштита на приватните клучеви на администраторите предвидува тие да:

- Користат смарт картичка, биометриска направа за пристап, лозинка во согласност со дел 6.4.1 или обезбедување со еквивалентна снага за потврдување на идентитетот на администраторот пред да се активира приватниот клуч, кое вклучува, на пример, лозинка за оперирање со приватниот клуч, лозинка за најавување на Windows или заштита на заклучување на мониторот; и
- Превземаат комерцијално разумни мерки за физичка заштита на администраторската работна станица за да го спречат користењето на таа работна станица и на приватните клучеви поврзани со неа, без овластување на администраторот.

КИБС препорачува администраторите да користат смарт картичка, биометриска направа за пристап или обезбедување со еквивалентна снага со користењето на лозинка во согласност со дел 6.4.1, за потврдување на идентитетот на администраторот пред да се активира приватниот клуч.

Откако ќе бидат деактивирани, приватните клучеви се чуваат само во шифрирана форма.

6.2.8.3. Приватните клучеви што ги имаат центрите за обработка

Приватниот клуч на Издавачкиот ИС ќе биде активиран со користење на минимален број на чуварите на уделите, како што е дефинирано во дел 6.2.2 со давање на своите податоци за активирање (складирани на безбеден медиум). Откако приватниот клуч еднаш ќе биде активиран, тој може да биде активен на неопределен период на време, се до неговото деактивирање, кога ИС ќе престане со оперирање. На сличен начин, ќе биде потребно

минималниот број на Чувари на удели да ги дадат своите податоци за активирање со цел да биде активиран приватниот клуч на Посредничкиот ИС. Откако приватниот клуч еднаш ќе биде активиран, тој ќе биде активен само во еден наврат.

6.2.9. Метод на деактивирање на приватен клуч

КИБС ИС приватните клучеви се деактивираат со нивно отстранување од читачот на токен. КИБС РК приватните клучеви (кои се користат за автентикација на РК апликацијата) се деактивираат со одјавување од системот. Кога администраторите на РК го напуштаат работното место, потребно е да се одјават од работните станици.

Приватните клучеви на администраторите, на РК и на претплатниците - крајни корисници можат да се деактивираат после секоја операција, по одјавувањето од системот или со вадењето на смарт картичката од читачот за смарт картички, во зависност од механизмот за автентикација кој го применува корисникот. Во секој случај, претплатниците - крајни корисници имаат обврска на соодветен начин да го заштитуваат својот приватен клуч во согласност со овие Правила.

6.2.10. Метод на уништување на приватен клуч

По завршувањето на оперативниот животен циклус на КИБС ИС, една или повеќе копии од ИС приватниот клуч се архивира во согласност со дел 6.2.5 од овие Правила. Преостанатите копии од ИС приватните клучеви безбедно се уништуваат. Покрај тоа, архивираниите ИС приватни клучеви безбедно се уништуваат на крајот на периодот за архивирање. Активностите за уништување на ИС клучевите предвидуваат учество на повеќе доверливи лица.

Онаму каде што е потребно, КИБС ги уништува ИС приватните клучеви на начин кој обезбедува разумни уверувања дека нема остатоци од клучот кои би можеле да доведат до реконструкција на клучот. Ова уништување се изведува само откако ќе помине минималниот неопходен период за активирање на ИС во согласност со дел 5.5.5, после повлекување на ИС Сертификатот. КИБС ја користи функцијата на анулирање на своите хардверски криптографски модули и други соодветни средства за да обезбеди со сигурност целосно уништување на ИС приватните клучеви. За време на уништување на ИС клучевите се прави евиденција од активностите.

6.2.11. Рангирање на криптографскиот модул

Види Дел 6.2.1

6.3. Други аспекти на управување на пар клучеви

6.3.1. Архивирање на јавни клучеви

Од сертификатите на ИС, РК и на претплатниците - крајни корисници се прават резервни копии кои се архивираат како дел од рутинските процедури на резервно складирање.

6.3.2. Оперативни периоди на сертификатите и периоди на користење на паровите на клучеви

Оперативниот период на сертификатот завршува по истекот на неговата важност или по неговото поништување. Оперативниот период за паровите клучеви е подеднаков како и оперативниот период на со нив поврзаните сертификати, само што тие можат да продолжат да

се користат за шифрирање и верификување на потписот. Максималниот оперативен период за сертификатите на КИБС се наведени во Табела 5 подолу.

Покрај тоа, КИБС ИС престануваат да издаваат сертификати на соодветна дата пред истекот на важноста на ИС сертификатите, така што ниеден сертификат издаден од Подредениот ИС не истекува после истекот на сертификатите на било кој надреден ИС.

| Издаден сертификат од: | Период на важност |
|-----------------------------------|--|
| Само-потпишан ПИС (1024 bit) | 30 години |
| Од ПИС до Посреднички ИС | 15 години |
| Од Посреднички ИС до Издавачки ИС | 10 години |
| Од Издавачки ИС до краен корисник | Нормално до 2 години, но под услови опишани подолу, до 5 години ⁶ |

Table 5: Оперативен период на сертификатите

Учесниците во поддоменот на КИБС ќе прекинат да го користат својот пар на клучеви по истекот на периодот на нивното важење.

Сертификатите издадени за крајните корисници може да имаат оперативен период подолг од 2 години, најмногу до 5 години, ако се исполнети следните услови:

- Сертификатите се индивидуални сертификати,
- Парот на клучеви на претплатникот е сместен на БСЕП,
- Претплатниците треба да се подложуваат на ре-автентикација најмалку на секои 25 месеци согласно со дел 3.2.2,
- Претплатниците ќе докажат дека го поседуваат приватниот клуч што кореспондира со јавниот клуч во сертификатот најмалку на секои 25 месеци согласно со дел 3.2.2,
- Ако претплатникот не може да ја изврши процедурата на ре-автентикација или не може да го докаже поседувањето на приватниот клуч со претходно наведеното, ИС ќе го поништи сертификатот на претплатникот.

6.4. Податоци за активирање

6.4.1. Генерирање и инсталирање на податоци за активирање

Податоците за активирање (Тајните удели) што се користат за заштита на криптографскиот модул кој го содржи приватниот клуч на КИБС ИС се користат во согласност со условите од дел 6.2.2 и Референтниот водич за Церемонија на генерирање клучеви. Креирањето и дистрибуирањето на Тајните удели се евидентира.

Од КИБС РК се бара да користат силни лозинки за заштита на своите приватни клучеви. Одредбите на КИБС за одбирање на лозинката предвидуваат лозинките да:

- бидат генерирани од корисникот;
- имаат најмалку осум карактери;
- имаат најмалку еден карактер од букви и еден нумерички карактер;
- имаат барем една мала буква;
- не содржат многу повторувања на една буква;

⁶ Доколку се издаваат петгодишни договори за претплатници - крајни корисници, оперативен период за издавачкиот ИС ќе биде 10 години, без можност да се обнова. Обнова на клуч ќе се бара после 5 години.

- не се исти како профил името на операторот; и
- не содржат долг под-збор на профил името на корисникот.

КИБС РК користи, а КИБС силно препорачува претплатниците - крајни корисници да одбираат лозинки кои ги задоволуваат истите услови. КИБС исто така препорачува користење на механизми за автентикација од два чинители (пр. токен и лозинка, биометрика и токен или биометрика и лозинка) за активирање на приватните клучеви.

6.4.2. Заштита на податоци за активирање

Потребно е Чуварите на удели на КИБС ИС да ги чуваат своите Тајни удели и да потпишат договор во кој ќе бидат јасно изразени нивните одговорности.

КИБС РК ги складираат своите Администраторски/РК приватни клучеви во шифрирана форма со користење на лозинка како заштита и со користење на опцијата "висока безбедност" на нивните веб прелистувачи.

КИБС РК и нивните администратори ги складираат своите приватни клучеви во шифрирана форма и ги заштитуваат своите приватни клучеви со користење на хардверски токен и/или силна лозинка и КИБС препорачува претплатниците - крајни корисници да ги складираат своите приватни клучеви во шифрирана форма и ги заштитуваат своите приватни клучеви со користење на хардверски токен и/или силна лозинка. Се поттикнува користење на механизми за автентикација од два чинители (пр. токен и лозинка, биометрика и токен или биометрика и лозинка).

6.4.3. Други аспекти на податоците за активирање

6.4.3.1. Пренос на податоци за активирање

Кога податоците за активирање на приватните клучеви се пренесуваат, VTN учесниците треба да го заштитат преносот користејќи методи кои обезбедуваат заштита од губење, кражба, изменување, неовластено откривање или неовластена употреба на таквите приватни клучеви. Кога кај претплатникот - краен корисник како податок за активирање се користи комбинацијата име/лозинка на корисникот на Windows или најава на мрежа, лозинките што се пренесуваат преку мрежата треба да бидат заштитени од неовластени корисници.

6.4.3.2. Уништување на податоци за активирање

Податоците за активирање на приватните клучеви на ИС се повлекуваат од употреба со применување на методи кои обезбедуваат заштита од губење, кражба, изменување, неовластено откривање или неовластена употреба на таквите приватни клучеви. Откако ќе помине периодот за чување на документација согласно дел 5.5.2, податоците за активирање се бришат со наснимување преку нив или со физичко уништување.

6.5. Контроли за безбедност на компјутерите

ADACOM и КИБС ги изведуваат функциите на ИС и РК со користење на доверливи системи кои ги задоволуваат условите на Водичот за предуслови за безбедност и надзор на VeriSign.

6.5.1. Посебни технички услови за компјутерска безбедност

КИБС обезбедува системите кои го одржуваат софтверот и податоците да бидат доверливи системи заштитени од неовластен пристап. Покрај тоа, КИБС го ограничува пристапот до

продукцискиот сервер само на оние лица кои имаат оправдана деловна причина за таков пристап. Обичните корисници на апликации немаат пристап до продукциските сервери.

Продукциската мрежа на КИБС ИС е логички одвоена од другите делови на КИБС. Ова одвојување спречува пристап во мрежата, освен преку определени апликациски процеси. КИБС користи огнени ѕидови за да ја заштити продукциската мрежа од интерни и екстерни упади и ги ограничува видот и изворот на мрежни активности кои можат да влезат во продукциските системи.

КИБС предвидува користење на лозинки кои имаат минимум должина на карактери и комбинација од алфанумерички и специјални карактери. КИБС наложува лозинките да бидат менувани на одредени временски интервали.

Директниот пристап до базата на податоци која ги поддржува операциите на КИБС ИС е ограничен на овластените лица во групата за продукциски операции кои имаат оправдана деловна причина за таков пристап.

6.5.2. Рангирање на безбедноста на компјутерите

Нема одредби.

6.6. Технички контроли на животниот циклус

6.6.1. Контроли за развој на системот

Апликациите се развиваат и имплементираат од КИБС во согласност со КИБС стандардите за управување на развојот и промените на системите.

Софтверот развиен од VeriSign, кога за прв пат ќе биде поставен за користење, има обезбеден метод за верификување дека софтверот во системот е дизајниран од VeriSign, дека не бил модификуван пред инсталирањето и дека е тоа верзијата која е наменета за користење.

6.6.2. Контроли за управување на безбедноста

КИБС има механизми и/или политики за контролирање и надгледување на конфигурацијата на своите ИС системи. VeriSign креира хеш од сите софтверски пакети и од надградувањата на VeriSign софтверите. Хешот се користи за да се верификува таквиот софтвер мануелно. По инсталирањето и подоцна на определени интервали КИБС го потврдува интегритетот на своите ИС системи.

6.6.3. Безбедносни контроли на животниот циклус

Нема одредби.

6.7. Контроли за безбедност на мрежата

КИБС ги изведува сите свои ИС и РК функции со користење на мрежи обезбедени во согласност со Водичот за услови за безбедност и надзор на VeriSign со цел да спречи неовластен пристап и други злонамерни активности. КИБС го заштитува пренесувањето на осетливи информации со користење на шифрирање и дигитални потписи.

6.8. Временски печат

Сертификатите, РПС и другите записи за поништување во базата на податоци содржат податоци за времето и датумот. Тие информации поврзани со времето нема потреба да бидат криптографски базирани.

7. ПРОФИЛИ НА СЕРТИФИКАТИ, РПС И ОССР

7.1. Профили на сертификати

Сертификатите на КИБС главно се усогласени со (а) ITU-T Препораките X.509 (1997): Информатичка технологија - Меѓусебна поврзаност на отворени системи - Директориум: Рамка за автентикација, јуни 1997 и (б) RFC 5280: Профил на сертификат и РПС според X.509 интернет инфраструктура со јавен клуч, април 2002 („RFC 5280“).

X.509 сертификатите, како минимум, ги содржат основните полиња и однапред определени вредности или ограничувања, според Табела 6.

| Поле | Вредност или ограничување |
|---------------------|---|
| Serial Number | Единствена вредност во рамките на издавачот |
| Signature Algorithm | Ознака за идентификација на алгоритмот користен за потпишување на сертификатот (види дел 7.1.3) |
| Issuer DN | Види дел 7.1.4 |
| Valid From | Универзална временска координата (UTC). Кодирано во согласност со RFC 5280. |
| Valid To | Универзална временска координата (UTC). Кодирано во согласност со RFC 5280. |
| Subject DN | Види дел 7.1.4 |
| Subject Public Key | Кодирано во согласност со RFC 5280. |
| Signature | Генериран и кодиран во согласност со RFC 5280. |

Табела 6: Основни полиња на профил на сертификат

Покрај тоа, согласно профилот на квалификуваните сертификати, DL 1 и DL 2 сертификатите се усогласени со RFC 3739, онаму каде што тоа не е во контрадикција со профилот на квалификуваните сертификати. Исто така, основните полиња во сертификатите што се потребни согласно дел 7.1 од VTN CP се придржуваат кон условите на Директивата и во сертификатите треба да го вклучат следново:

- Назнака дека сертификатот што е издаден е квалификуван сертификат;
- Идентификацијата на ИС (давател на услуги за сертификација) и државата во која е основан;
- Име на потписникот;
- Податоци за верификување на потписот (јавен клуч на субјектот);
- Почеток и крај на периодот на важност (датуми на важење од - до);
- Кодот на идентитетот на сертификатот (серискиот број);
- Напредниот електронски потпис на издавачкиот КИБС ИС.

7.1.1. Нумерирање на верзии

Коренскиот сертификат на VeriSign е X.509 Верзија 1, посредничкиот и издавачкиот сертификат на КИБС ИС се X.509 Верзија 3, како и сертификатите на претплатниците - крајните корисници.

7.1.2. Екстензии за сертификати

КИБС ги дополнува сертификатите X.509 Верзија 3 со екстензии што се предвидени во 7.1.2.1 - 7.1.2.8.

7.1.2.1 Користење на клуч

Екстензијата за користење на клуч во X.509 Верзија 3 Сертификатите е конфигурирана на начин што ги поставува (1) и анулира(0) битовите и полето на критичност согласно Табела 7. Полето на критичност во екстензијата за користење на клуч е поставено на ТОЧНО (TRUE) за посредничките и издавачките сертификати на КИБС ИС, а е поставено на НЕТОЧНО (FALSE) за сертификатите на крајните корисници.

| | | посреднички и издавачки сертификати на КИБС ИС | DL1 и DL2 Сертификати за крајни корисници |
|------------|------------------|--|---|
| Критичност | | ТОЧНО | НЕТОЧНО |
| 0 | digitalSignature | 0 | 1 |
| 1 | nonRepudiation | 0 | 1 |
| 2 | keyEncipherment | 0 | 1 |
| 3 | dataEncipherment | 0 | 1 |
| 4 | keyAgreement | 0 | 0 |
| 5 | keyCertSign | 1 | 0 |
| 6 | CRLSign | 1 | 0 |
| 7 | encipherOnly | 0 | 0 |
| 8 | decipherOnly | 0 | 0 |

Табела 7: Поставеност на KeyUsage екстензијата

Забелешка: Не е потребно битот nonRepudiation⁷ (не одрекување) да биде поставен во овие сертификати, бидејќи PKI индустријата сè уште нема постигнато консензус за тоа што значи битот nonRepudiation. Додека да се постигне таков консензус, nonRepudiation битот можеби нема да има некое значење за потенцијалните засегнати страни. И повеќе од тоа, најчесто користените апликации не секогаш го респектираат nonRepudiation битот. Според тоа, поставувањето на битот можеби нема да им помогне на засегнатите страни да донесат одлука за доверба. Било каков спор поврзан со не-одрекување што ќе произлезе од користење на дигиталниот сертификат е прашање единствено помеѓу претплатникот и засегнатата страна(и). VeriSign не превзема никаква одговорност во врска со ова.”

7.1.2.2 Екстензија за сертификациски политики

Екстензијата за сертификациски политики во X.509 Верзија 3 сертификатите содржи предметен идентификатор за VTN CP во согласност со дел 7.1.6 од овие Правила и со квалификаторите на политики наведени во CP и во дел 7.1.8 од овие Правила. Оваа екстензија е означена како не-критична.

⁷ Битот за nonRepudiation може исто така да се нарече и ОпределеностЗаСодржината (ContentCommitment) согласно X.509 стандардот.

7.1.2.3 Приватна екстензија на Сертификатите (QCStatements)

DL 1 и DL 2 Сертификатите имаат приватна екстензија која содржи предметен идентификатор (OID) кој ја идентификува изјавата што тврди дека сертификатот се издава во согласност со Директивата. Таквата екстензија соодветствува со дефиницијата во дел 4.2.1(2) од Профилот на квалификувани сертификати. Оваа екстензија за КИБС DL 1 и DL 2 сертификатите е означена како не-критична.

7.1.2.4 Алтернативно име на субјектот

Екстензијата **subjectAltName** од X.509 Верзија 3 сертификатите е пополнета во согласност со RFC 5280. Оваа екстензија е означена како не-критична.

7.1.2.5 Основни ограничувања

Екстензијата **BasicConstraints** (БазичниОграничувања) на КИБС ИС сертификатите X.509 Верзија 3 го има CA полето поставено на TRUE. Екстензијата **BasicConstraints** на сертификатите на претплатниците - крајни корисници е поставена со вредност на празна секвенца. Полето на критичност од оваа екстензија е поставено на ТОЧНО за ИС сертификатите, а на НЕТОЧНО за сертификатите на претплатниците - крајни корисници.

КИБС ИС Сертификатите X.509 Верзија 3 го имаат полето "pathLenConstraint" од екстензијата ОсновниОграничувања поставено на максималниот број на ИС сертификати што можат да го следат овој сертификат на сертификацискиот пат.

7.1.2.6 Проширена употреба на клуч

КИБС ИС ја применува екстензијата **ExtendedKeyUsage** (ПроширенаУпотребаНаКлуч) за DL 1 и DL 2 сертификатите.

За овие сертификати, КИБС ја поставува екстензијата ExtendedKeyUsage согласно Табела 8:

| | DL1 и DL2 сертификати |
|-----------------|-----------------------|
| Критичност | НЕТОЧНО |
| ServerAuth | 0 |
| ClientAuth | 1 |
| CodeSigning | 0 |
| EmailProtection | 1 |
| ipsecEndSystem | 0 |
| ipsecTunnel | 0 |
| ipsecUser | 0 |
| TimeStamping | 0 |
| OCSP Signing | 0 |

Табела 8 – Поставеност на ExtendedKeyUsage екстензијата

7.1.2.7 Точки на дистрибуција на РПС

Сертификатите на КИБС за претплатници - крајни корисници, посредничките сертификати и сертификатите на ИС што издаваат вклучуваат екстензија **CRLDistributionPoints** (ТочкиНаДистрибуцијаНаРПС), која содржи URL локација од каде што засегнатите страни можат да добијат РПС за да го проверат статусот на сертификатите. Оваа екстензија е означена како не-критична.

7.1.2.8 Идентификатор на клучот на издавачот

DL 1 и DL 2 сертификатите и сертификатот на ИС што издава содржат екстензија за **Authority Key Identifier** (идентификатор на клучот на издавачот). Идентификаторот на клучот на

авторитетот се состои од 160 битен SHA-1 хеш на јавниот клуч на ИС што го издава сертификатот. Оваа екстензија е означена како не-критична.

7.1.2.9 Идентификатор на клучот на субјектот

За DL 1 и DL 2 Сертификатите, посредничките и издавачките сертификати на ИС вклучена е екстензијата на Идентификатор на клучот на субјектот. **SubjectKeyIdentifier** базиран на јавниот клуч на субјектот на сертификатот се генерира во согласност со еден од методите опишани во RFC 5280. Оваа екстензија е означена како не-критична.

7.1.3. Алгоритамски предметни идентификатори

КИБС сертификатите се потпишани со:

```
sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840)
rsads(113549) pkcs(1) pkcs-1(1) 5}
(OID: 1.2.840.113549.1.1.5)).
```

Потписите направени со користење на овој алгоритам треба да бидат во согласност со RFS 3279.

7.1.4. Форми на имиња

Во КИБС сертификатите се вклучени и карактеристичното име на издавачот и на субјектот, согласно дел 3.1.1.

Покрај тоа, КИБС во сертификатите за претплатници - крајни корисници вклучува дополнително поле на Организациона единица (ou), кое содржи URL локација на која се наведени условите за користење на сертификатот, која всушност упатува на референтниот договор со засегнатата страна кој е на сила.

7.1.5. Ограничувања на имињата

Нема одредби.

7.1.6. Предметен идентификатор на Политика за сертификати

VeriSign, делувајќи како авторитет кој ја дефинира политиката, има наменето екстензија за вредност на предметниот идентификатор(OID) на секоја Класа на Сертификати издавани под VeriSign Доверливата мрежа (VTN).

Квалификуваните сертификати (DL 1 и DL 2) содржат два OID:

1. OID за Сертификациска политика за Класа 2:

VeriSign/pki/policies/vtn-cp/class2 (2.16.840.1.113733.1.7.23.2)⁸.

2. OID специфициран во документот ETSI Политики за квалификуваните сертификати (ETSI TS101 456):

- За DL 1 сертификати (0.4.0.1456.1.2)
- За DL 2 сертификати (0.4.0.1456.1.1)

7.1.7. Користење на екстензијата за ограничувања на политиката

Нема одредби.

⁸ Паради фактот дека квалификуваните сертификати се потпишуваат со коренски CA на VeriSign Класа 2.

7.1.8. Синтакса и семантика на квалификаторите на политиката

КИБС вклучува во сертификатите X.509 Верзија 3 квалификатор на политиката во рамките на екстензијата за Серификациските Полики. Таквите сертификати содржат квалификатор кој упатува на овие Правила.

7.1.9. Процесирачка семантика за критичните екстензии за сертифицирачките политики

Нема одредби.

7.2. Профил на РПС

РПС содржи основни полиња со содржина специфицирана во Табела 9:

| Поле | Вредност или ограничувачка вредност |
|-----------------------|--|
| Верзија | Види дел 7.2.1. |
| Алгоритам за потпис | Алгоритам што се користи за потпишување на РПС. За DL1 и DL2 се користи алгоритмот sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) |
| Издавач | Ентитетот што го издал и потпишал РПС. |
| Датум на издавање | Датум на издавање на РПС. |
| Следно ажурирање | Датум на следно издавање на РПС. Фреквенцијата на издавање на РПС е согласно дел 4.4.7. |
| Поништени сертификати | Преглед на поништени сертификати, коишто вклучува сериски број на поништениот сертификат и датум на поништување. |

Табела 9 – Профил на основни полиња на РПС

7.2.1 Нумерирање на верзии

КИБС издава РПС Верзија 2. За КИБС Класа 2 ИС (Посреднички ИС), VeriSign издава РПС Верзија 1.

РПС е во согласност со барањата на RFC 5280.

7.2.2. РПС и проширувањата на записот во РПС

Нема одредби.

7.3. OSCP Профил

OSCP (Протокол за онлајн проверка на статусот на сертификатот) е начин да се добие навремена информација за статусот дали одреден сертификат е поништен. КИБС не обезбедува OSCP услуги за DL 1 и DL 2 сертификатите.

7.3.1. Нумерирање на верзии

Не се применува.

8. НАДЗОР ВО ВРСКА СО УСОГЛАСЕНОСТА И ДРУГИ ПРОЦЕНКИ

Еднаш годишно се врши ревизија на операциите на центарот за податоци и операциите на управување со клучеви на ADACOM ИС поврзани со квалификуваните сертификати.

Покрај ревизиите за усогласеност, КИБС има право да врши и други проверки и истражувања за да се увери дека КИБС, како поддомен на VTN, ја заслужува довербата. Овие истражувања вклучуваат, но не се ограничени на:

- КИБС има право, по сопствена иницијатива, во било кое време да си изврши „Итна ревизија/истражување“, во случај КИБС да доживеал инцидент или компромитирање, или пак дејствувал или пропуштил да дејствува на начин кој претставува реална или потенцијална закана за безбедноста или интегритетот на VTN.
- КИБС има право да изврши „Дополнителна проверка на управување со ризикот“ во случај на наоди од Ревизијата за усогласеност или како дел од целосниот процес на управување со ризикот во вообичаениот тек на работењето.

КИБС има право да го довери извршувањето на овие ревизии, проверки и истражувања на ревизорска куќа како трето лице. Ентитетите што се предмет на овие ревизии, проверки или истражувања должни се да соработуваат со лицата што ги вршат ревизиите, проверките или истражувањата.

Покрај тоа, ревизија на усогласеноста со македонските закони и прописи се врши и од страна на надлежните органи.

8.1. Интервали и околности на оценките

Ревизија за усогласеност на КИБС ИС се изведува најмалку еднаш годишно. КИБС може да врши ревизија на трети лица, како на пример ЛРК/РК, со кои воспоставил договорни односи. Ревизија се изведува на трошок на ентитетот што е предмет на ревизијата.

8.2. Идентитет и квалификации на проценителот

Надзорот за усогласеност на ADACOM ИС се изведува од страна на:

- Интерно од квалификувани ревизори за ИТ на ADACOM,
- Контролни тела што се назначени од овластениот орган согласно закон, или
- Ревизорска куќа со потврдени познавања и способности за технологијата за инфраструктура со јавен клуч, алатките и техниките за информатичка безбедност и ревизијата на безбедност.

8.3. Прашања на кои се однесува оценката

Опсегот на годишните ревизии на ADACOM вклучува контроли на работните услови на ИС, операциите за управување со клучеви, административно/инфраструктурни контроли, управување на животниот циклус на сертификатите и на деловните практики на ИС.

8.4. Дејствија што се преземаат како резултат на пропустите

Во врска со ревизиите за усогласеност на операциите на ADACOM, доколку бидат идентификувани значителни исклучоци или недостатоци за време на Ревизијата за усогласеност, ќе бидат определени дејствијата што треба да се преземат. Ова определување ќе биде извршено од управата на ADACOM со информации што ќе ги добие од ревизорот.

Управата на КИБС ја има одговорноста за развивање и имплементирање на корективен акционен план. Доколку ADACOM одлучи дека таквите исклучоци или недостатоци претставуваат директна закана за безбедноста или интегритетот на VTN, корективниот акционен план ќе биде изготвен во рок од 30 дена и имплементиран во разумен период на време. Во врска со помалку сериозните исклучоци или недостатоци, управата на ADACOM ќе ги процени тие проблеми и ќе ја определи соодветната насока на дејствување.

8.5. Соопштување на резултатите

Резултатите од ревизиите за усогласеност на операциите на ADACOM можат да бидат објавени по дискреција на Управата на ADACOM.

9 ОСТАНАТИ ДЕЛОВНИ И ПРАВНИ РАБОТИ

9.1. Надоместоци

9.1.1. Надоместоци за издавање и обновување на сертификати

КИБС наплатува на претплатниците - крајни корисници надомест за издавање и обновување на сертификатите.

9.1.2. Надоместоци за пристап до сертификатите

КИБС ги става на располагање сертификатите во складиште или на друг начин, за да ги направи достапни на засегнатите страни. За оваа услуга КИБС не наплатува надоместок.

9.1.3. Надоместоци за пристап до информациите за поништување или за статусот на сертификатот

КИБС не наплатува надоместок за користењето на РПС уредени со овие Правила, а кои се ставени на располагање во складиштето или на друг начин да им ги направи достапни на засегнатите страни. КИБС не дозволува пристап до информациите за поништување, до информациите за статусот на сертификатите или временскиот печат кои ги сместува во своите складишта на трети лица кои обезбедуваат производи или услуги со користење на ваквите информации, без претходно јасно изразена писмена согласност од страна на КИБС.

9.1.4. Надоместоци за други услуги

КИБС не наплатува надоместоци за пристап и разгледување на овие Правила. Секое друго користење (пр. репродуцирање, редистрибуирање, изменување или креирање на текстови што ќе произлезат од нив) се предмет на договор за лиценца со КИБС.

9.1.5. Политика на рефундирање (поврат на средства)

Не се применува.

9.2. Финансиска одговорност

9.2.1. Покривање на осигурувањето

КИБС одржува комерцијално разумно ниво на покривање на осигурувањето за грешки и пропусти согласно Правилникот за осигурување јавно објавен на веб-локацијата: <http://ca.kibs.com.mk/repository>.

9.2.2. Други средства

КИБС има доволно финансиски средства да ги одржува своите операции и да ги извршува своите должности, како и разумна моќ да го понесе ризикот од одговорност спрема претплатниците и засегнатите страни. Доказите за финансиските средства не се јавно достапни.

9.3. Доверливост на деловните информации

9.3.1. Опсег на доверливи информации

Следниве документи за претплатниците, во согласност со 9.3.2, ќе бидат чувани во тајност и ќе се сметаат за приватни: („доверливи информации“):

- Формуларот за регистрација, без оглед дали е одобрен или одбиен,
- Прилозите кон формуларот за регистрација,
- Доказот за плаќањето (налог за плаќање, извод од состојбата на сметката и др.)
- Записите од ревизорските траги креирани или сочувани од КИБС или Клиентот,
- Ревизорските извештаи направени од КИБС или од ревизорите (било интерни или јавни),
- Безбедносните мерки со кои се контролираат операциите на хардверот и софтверот на КИБС, како и управувањето со сертификациските услуги и услугите за регистрирање.

9.3.2. Информации што не се во доменот на доверливи информации

Сертификатите, поништувањето и други информации за статусот на сертификатите, складиштето на КИБС и информациите што се содржани во нив, не се сметаат за доверливи информации. Информациите кои не наведени како доверливи информации во дел 9.3.1 не се доверливи. Овој дел е предмет на важечките прописи за тајност на личните податоци.

9.3.3. Одговорност за заштитата на доверливите информации

КИБС ги обезбедува доверливите информации од компромитирање и откривање на трети лица.

9.4. Приватност на личните информации

9.4.1. План за лични податоци

КИБС применува политика за заштита на личните податоци, која е поставена на <http://ca.kibs.com.mk/repository/> во согласност со македонските прописи за заштита на личните податоци.

9.4.2. Лични податоци што се третираат како приватни

Било каков податок за претплатникот кој не е јавно достапен преку содржината на издадениот сертификат, директориумот на сертификати и електронските РПС се третира како приватен.

9.4.3. Лични податоци што не се сметаат за приватни

Секоја информација што е јавно достапна во сертификатите не се смета за приватен податок.

9.4.4. Одговорност за заштита на приватните податоци

КИБС ќе ги обезбеди личните податоци од компромитирање и од откривање на трети лица и ќе се придржува до важечките законски и подзаконски акти за заштита на личните податоци.

9.4.5. Известување и согласност за користење на лични податоци

Согласно Законот за заштита на личните податоци, приватните податоци не се користат без согласност на страната на која се однесува информацијата, освен ако не е поинаку наведено во овие Правила, важечките Правила и принципи за заштита на личните податоци во КИБС или според договор.

9.4.6. Откривање што произлегува од судски или административен процес

КИБС има право да открие доверливи информации ако, со добра намера, КИБС верува дека:

- откривањето е неопходно како одговор на судска покана и налог за претрес;
- откривањето е неопходно како одговор на судски, административни и други правни процедури за време на истражни процеси во граѓански или административни дејствија, како на пример судска покана, распит, барање за адмисија и барање за продуцирање на документи.

9.4.7. Откривање по барање на сопственикот

Правилата и принципите за заштита на личните податоци во КИБС содржат одредби поврзани со откривање на лични податоци на лицето кое му ги доставило тие податоци на КИБС.

9.4.8. Други околности на откривање информации

Нема одредби.

9.5. Права на интелектуална сопственост

Припишувањето на правата на интелектуална сопственост помеѓу учесниците во поддоменот на КИБС, освен на претплатниците и засегнатите страни, е регулирано со договорите, склучени помеѓу тие учесници. Следниве подточки на дел 9.5 се однесуваат на правата на интелектуална сопственост поврзани со претплатниците и засегнатите страни.

9.5.1. Права на сопственост во сертификатите и информациите за поништување

КИБС ИС ги задржува сите права на интелектуална сопственост во и на сертификатите и РПС што ги издава. КИБС дава дозвола за репродуцирање и дистрибуирање на сертификатите на не-ексклузивна основа без плаќање на авторски права, под услов тие да бидат репродуцирани во целост и користењето на сертификатите да е регулирано со договор со засегнатата страна. КИБС дава дозвола на засегнатите страни да ги користат информациите за поништување за своите потреби, што е регулирано во соодветниот договор или некои други важечки договори.

9.5.2. Права на сопственост на Правилата

Претплатниците и засегнатите страни прифаќаат дека КИБС ги задржува сите права на интелектуална сопственост во и на овие Правила.

9.5.3. Права на сопственост во имиња

Барателот на сертификат ги задржува сите права што ги има (доколку ги има) на трговска марка, услужна марка или трговско име кое е содржано во формуларот за регистрација за сертификат и карактеристично име во сертификатот издаден на тој барател на сертификат.

9.5.4. Права на сопственост на клучевите и материјалот со клучеви

Паровите на клучеви што соодветствуваат со сертификатите на ИС и на претплатниците - крајни корисници се сопственост на ИС и на претплатниците - крајни корисници кои се субјекти на тие сертификати, без оглед на физичкиот медиум во кој тие се складираат и заштитуваат, и тие лица ги задржуваат сите права на интелектуална сопственост во и на овие парови на клучеви. Без да се ограничува воопштеноста на претходното, коренските јавни клучеви на VeriSign и коренските сертификати кои ги содржат нив, вклучително и ПИС јавните клучеви и самопотпишаните сертификати, се сопственост на VeriSign. VeriSign дава лиценци на производителите на хардвер и софтвер да ги репродуцираат ваквите коренски сертификати за да ги постават во безбедна хардверска опрема или во софтвер. Конечно, Тајните удели на приватните клучеви на КИБС ИС се сопственост на КИБС. КИБС ги задржува сите права на интелектуална сопственост на тие Тајни удели, иако не може да стекне физичка сопственост врз тие удели.

9.6. Претставувања и гаранции

9.6.1. ИС Претставувања и гаранции

КИБС ИС гарантира дека:

- не постојат материјални погрешни претставувања на факти во сертификатите што им се познати на или потекнуваат од ентитетите што вршат одобрување на барањето за сертификатот или го издаваат сертификатот,
- нема грешки во информациите во сертификатот што се внесени од ентитетите што вршат одобрување на барањето за сертификат или го издаваат сертификатот како резултат на неприменување на разумна грижа во управувањето на барањето за сертификат или креирањето на сертификатот,
- неговите сертификати ги задоволуваат сите материјални услови на овие Правила, и
- услугите на поништување и користење на складиштето се согласно овие Правила.

Претплатничкиот договор на КИБС може да вклучува дополнителни претставувања и гаранции.

9.6.2. РК претставувања и гаранции

КИБС РК гарантира дека:

- нема материјални погрешни претставувања на факти во сертификатите што им се познати на или потекнуваат од ентитетите што вршат одобрување на барањето за сертификат или го издаваат сертификатот,
- нема грешки во информациите во сертификатот што се внесени од ентитетите што вршат одобрување на барањето за сертификат или го издаваат сертификатот како резултат на неприменување на разумна грижа во управувањето со барањето за сертификат,
- неговите сертификати ги задоволуваат сите материјални услови на овие Правила,
- услугите за поништување (ако може да се примени) и користењето на складиштето се усогласени со овие Правила,
- се задоволуваат условите на овие Правила и EDP.

Претплатничкиот договор на КИБС може да вклучува дополнителни претставувања и гаранции.

9.6.3. Претставувања и гаранции на претплатникот

Претплатниците гарантираат дека:

- секој електронски потпис креиран со користење на приватниот клуч што кореспондира со јавниот клуч внесен во сертификатот е дигиталниот потпис на претплатникот и дека сертификатот е прифатен и оперативен (а не истечен или поништен) во моментот кога е креиран дигиталниот потпис,
- нивниот приватен клуч е заштитен и ни едно неовластено лице никогаш немало пристап до претплатничкиот приватен клуч,
- сите претставувања кои ги навел претплатникот во барањето за сертификат која ја поднел претплатникот се вистинити,
- сите информации што ги дал претплатникот, а се содржани во сертификатот, се вистинити,
- сертификатот се користи единствено за законски цели и цели за кои постои овластување, во согласност со овие Правила, и
- претплатникот е претплатник - краен корисник, а не ИС и не го користи приватниот клуч што кореспондира со било кој јавен клуч внесен во сертификатот за цели на дигитално потпишување на друг сертификат (или било кој формат на сертифициран јавен клуч) или РПС, како ИС или на друг начин.

Претплатничкиот договор на КИБС може да вклучува дополнителни претставувања и гаранции.

9.6.4. Претставувања и гаранции на засегнатата страна

Договорот со засегнатата страна предвидува засегнатата страна да стави на знаење дека поседува доволно информации за да донесе одлука заснована на информации за обемот до кој таа ќе одбере да се потпре на информациите во сертификатот, да прифати дека единствено таа е одговорна за одлуката дали ќе се потпре, или не, на тие информации, и дека таа ќе ја понесе законската одговорност за нејзиниот неуспех да ги изврши обврските на засегната страна согласно овие Правила.

Договорот со засегнатата страна содржи гаранција за засегнатите страни кои разумно се потпираат на квалификуваните сертификати за да верификуваат дигитален потпис, дека:

- квалификуваниот сертификат ги содржи сите детали пропишани за квалификуван сертификат според Директивата,
- претплатникот на таков квалификуван сертификат има приватен клуч што кореспондира со јавниот клуч во тој квалификуван сертификат во моментот кога квалификуваниот сертификат е издаден, и
- ИС и РК применуваат разумна грижа да достават известување за поништување на квалификуван сертификат согласно со деловите 4.9.7, 4.9.9.

Договорот со засегнатата страна може да вклучува дополнителни претставувања и гаранции. Претплатничкиот договор исто така ги содржи претходно споменатите гаранции и ќе важи доколку претплатникот покрај тоа делува и како засегната страна.

9.6.5. Претставувања и гаранции на други учесници

Нема одредби.

9.7. Одредување на гаранциите

Претплатничкиот договор и Договорот со засегнатата страна ги одрекуваат сите можни гаранции, вклучително и гаранција за можноста за трговија со нив и нивната адекватност за конкретна цел.

9.8. Обврски за ИС којшто издава квалификувани сертификати

КИБС како издавач на квалификувани сертификати исто така ги задоволува условите наведени во EDP.

Претплатничкиот договор е во писмена форма и на разбирлив јазик. Понатаму, Претплатничкиот договор ги содржи следниве услови предвидени во Директивата, со македонските прописи и со ETSI стандардот:

- Применлива политика, било да е за DL1 или DL2, која вклучува јасна изјава дали се бара користење на БСЕП,
- Потврда дека информациите содржани во сертификатот се точни, освен ако претплатникот не ги информира ИС и РК за поинаква информација,
- Применливи ограничувања на користењето, кои ги вклучуваат најмалку ограничувањата во делот 9.9 од овие Правила,
- Обврските на претплатниците наведени во овој дел и согласност да се исполнуваат тие обврски,
- Информации за тоа како да се валидира сертификат, вклучително и предусловот да се провери статусот на сертификатот, и условите под кои потпирањето на некој сертификат се смета за "разумно", кое се однесува на ситуации кога претплатниците делуваат како засегнати страни,
- Применливи ограничувања на одговорноста,
- Согласност за објавување на сертификатот што му е издаден на претплатникот и неговата достапност за да можат да го добијат засегнатите страни,
- Согласност за задржување на документацијата која се користела за упис, обезбедување на БСЕП на претплатникот, информациите за повлекување и пренесувањето на тие информации на трети лица во случај на укинување на ИС,
- Периодот за зачувување на документација од барањето за сертификат,
- Периодот за зачувување на документација на ИС ревизорските траги од настани,
- Применлива процедура за разрешување на спорови,
- Законот кој ќе се применува,
- Дали е сертифицирано дека ИС е усогласен со DL1 Политиките за сертификати или со DL2 Политиките за сертификати.

Претплатничкиот договор им се испраќа на барателите за сертификат пред тие да ги поднесат информациите за упис и на начин кој го зачувува интегритетот на претплатничкиот договор. Пред да се издаде нов сертификат или за време на обновување, за било какви промени во претплатничкиот договор имплементирани по моментот на последната регистрација или пре-регистрање, претплатникот се известува на начин кој ќе го заштити интегритетот на Претплатничкиот договор.

Договорот со засегнатата страна е во писмена форма и на разбирлив јазик. Понатаму, Договорот со засегнатата страна ги содржи следниве услови предвидени во ETSI Документот за политики:

- Применлива политика, било да е за DL1 или DL2, која вклучува јасна изјава дали од претплатниците се бара да користат БСЕП или не,
- Применливи ограничувања на користењето, кои ги вклучуваат најмалку ограничувањата во од делот 1.4.2 од овие Правила,

- Информации за тоа како да се валидира сертификат, вклучително и предусловот да се провери статусот на сертификатот, и условите под кои потпирањето на некој сертификат се смета за "разумно",
- Применливи ограничувања на одговорноста,
- Периодот за зачувување на документација од барањето за сертификат,
- Периодот за зачувување на ИС ревизорските траги од настани,
- Применливи процедури за решавање на спорови,
- Законот кој ќе се применува, и
- Дали е потврдено дека ИС е усогласен со DL1 Политиките за сертификати и DL2 Политиките за сертификати.

9.9. Ограничувања на одговорноста

Претплатничкиот договор и Договорот со засегнатата страна ја ограничуваат одговорноста на КИБС. Ограничувањата на одговорност вклучуваат изземање од одговорност за индиректни, специјални, случајни и последични штети. Тие исто така вклучуваат и максимална висина на одговорност во износ утврден со Правилникот за осигурување на КИБС, што ја ограничува отштетата од КИБС во врска со DL1 или DL2 Сертификат.

Одговорноста на Претплатниците е наведена во релевантните Претплатнички договори.

Одговорноста на Засегнатите страни е наведена во релевантните Договори со Засегнатите страни.

9.10. Обесштетувања

9.10.1. Обесштетување од страна на претплатниците

Од претплатниците се очекува да платат обесштетување на КИБС за:

- Фалсификување или погрешно интерпретирање на факти од страна на претплатникот во барањето за сертификат,
- Неприкажување на материјален факт во барањето за сертификат, од страна на претплатникот, ако погрешната интерпретација или пропустот се направени од небрежност или со намера да се залаже некоја од страните,
- Неуспехот на претплатникот да го заштити претплатничкиот приватен клуч, некористењето на доверлив систем или неуспевањето на било кој начин да се заштити од компромитирање, губење, откривање, изменување или неовластено користење на претплатничкиот приватен клуч, или
- Користењето од страна на претплатникот на име (вклучително и без ограничувања во рамките на вообичаеното име, името на доменот, или електронската адреса) кое ги прекршува правата на интелектуална сопственост на трето лице.

Претплатничкиот договор може да вклучува дополнителни обврски за обесштетувања.

9.10.2. Обесштетување од страна на засегнатите страни

Не се применува.

9.11. Период и прекин на важност

9.11.1. Период на важност

Овие Правила стапуваат на сила по објавувањето на веб страната на КИБС. Амандманите на овие Правила стапуваат на сила по објавувањето во веб страната на КИБС.

9.11.2. Прекин на важност

Измените на овие Правила остануваат на сила се додека не се заменат со нова верзија.

9.11.3. Ефекти од прекин на важност и преживување

По прекинувањето на важноста на овие Правила, учесниците во КИБС поддоменот и покрај тоа се обврзани со сите услови за сите издадени сертификати до крајот на периодот на важност на тие сертификати.

9.12. Индивидуални известувања и комуникација со учесниците

Доколку не е специфицирано поинаку со договорот помеѓу страните, учесниците во КИБС ќе користат комерцијално разумни методи кога ќе комуницираат помеѓу себе, имајќи ги предвид критичноста и темата на комуникацијата.

9.13. Амандмани

9.13.1. Процедура за амандмани

Амандманите на овие Правила ги прави групата за развој на практики на КИБС (ГРПК). Амандманите се вклучуваат во нова верзија на Правилата што се објавува на <http://ca.kibs.com.mk/repository/cps>.

Обновените верзии надвладуваат било која специфична или конфликтна одредба од претходната верзија на овие Правила.

9.13.2. Механизам и период на известување

КИБС го задржува правото да врши измени на овие Правила без известување за промените.

9.13.2.1. Период за коментари

Не се применува.

9.13.2.2. Механизам за третирање на коментарите

Не се применува.

9.13.3. Околности под кои OID мора да се промени

Ако ГРПК во соработка VeriSign, одреди дека е неопходна промена во некој предметен идентификатор од овие Правила, амандманот ќе содржи нов предметен идентификатор во Правилата соодветно за секоја класа на сертификати. Инаку, амандманите не бараат промена во предметниот идентификатор на Правилата.

9.14. Одредби за решавање на спорови

9.14.1. Спорови помеѓу VeriSign, филијали и клиенти

Не се применува.

9.14.2. Спорови со претплатниците - крајни корисници и засегнатите страни

КИБС Претплатничките договори и Договорите со засегнатите страни содржат клаузула за решавање на спорови. За споровите во кои е вмешан КИБС предвиден е почетен период на преговори од шеесет (60) дена, после кој ќе следи судски спор во надлежниот суд во Скопје.

9.15. Закон кој ќе се применува

Законите на Република Македонија ќе бидат надлежни за извршувањето, составувањето, интерпретирањето и важноста на овие Правила, без оглед на договорните или изборот на други законски одредби.

Надлежноста на законот важи само за овие Правила. Договорите кои ги вклучуваат овие Правила само како референца може да имаат свои сопствени одредби за надлежен закон, под услов делот 9.14 да го регулира извршувањето, сочинувањето, интерпретирањето и важноста на условите од овие Правила одделно и раздвоено од останатите одредби на било кој таков договор, предмет на било какви ограничувања што се појавуваат во применливиот закон.

9.16. Усогласеност со законот што ќе се применува

Овие Правила се во надлежност на законите на Република Македонија.

9.17. Збирни одредби

9.17.1. Договорот во целост

Не се применува.

9.17.2 Припишување

Не се применува.

9.17.3. Разделивост

Во случај некој член или клаузула од овие Правила, од соодветен суд или од друг надлежен авторитет бидат прогласени за ништовни, остатокот од овие Правила ќе остане во сила.

9.17.4. Присилно извршување (надоместок за адвокат и откажување од правата)

Не се применува.

9.17.5. Виша сила

Претплатничките договори на КИБС и Договорите со засегнатата страна може да содржат клаузула за виша сила која го заштитува КИБС.

9.18. Други одредби

Не се применува.

Додаток А. Табела на кратенки и дефиниции

Табела на кратенки

| Термин | Дефиниција |
|--------|--|
| ГРПК | Група за развивање практики на КИБС. |
| ИС | Издавач на сертификати. |
| СР | Политика за сертификати. |
| СРС | Изјава за сертификациските практики |
| РПС | Регистар на поништени сертификати. |
| EAL | Ниво на гаранција за проценката (согласно заедничките **општите, вообичаените** критериуми |
| FIPS | Федерални стандарди за обработка на информации. |
| LSVA | Проценка за ранливост на логичката безбедност. |
| OCSP | Протокол за електронско добивање на статусот на сертификат. |
| РСА | Примарен сертификациски авторитет. |
| PIN | Личен идентификациски број. |
| PKCS | Криптографски стандард за јавен клуч. |
| PKI | Инфраструктура на јавен клуч. |
| PMA | Авторитет за управување на политиката. |
| РА | Регистрациски авторитет. |
| RFC | Барање за коментар. |
| S/MIME | Протокол за безбедно пренесување на интернет пошта. |
| SSL | Протокол Secure Socket Layer |
| VTN | VeriSign Доверлива мрежа. |

Дефиниции

| Термин | Дефиниција |
|--|---|
| Администратор | Доверливо лице во организацијата на процесирачки центар, услужен центар или кај управуваниот ПКИ Клиент, кое врши валидација и други ИС или РК функции. |
| Група за развивање на практики КИБС (ГРПК) | Организација во рамките на КИБС одговорна за донесување на оваа политика. |
| Администраторски сертификат | Сертификат што му се издава на администраторот и кој може да се користи само за изведување на ИС или РК функции. |

| | |
|--|---|
| Партнерска фирма | Водечко доверливо трето лице, на пример, во технологијата, телекомуникациите или индустријата на финансиските услуги, кое склучува договор со VeriSign за да биде VTN канал за дистрибуција и услуги во рамките на определена територија. |
| Сертификат | Порака која како минимум наведува име или идентификува ИС или претплатник, го содржи јавниот клуч на претплатникот, го определува оперативниот период на сертификатот, го содржи серискиот број на сертификатот и е дигитално потпишан од ИС. |
| Барател на сертификат | Личност или организација што бара издавање на сертификат од ИС. |
| Барање за сертификат | Барање од барателот на сертификат (или од овластен застапник на барателот за сертификат) до ИС за издавање на сертификат. |
| Синцир на сертификати | Подредена листа на сертификати која го содржи сертификатот на претплатникот - краен корисник и сертификати на ИС, а завршува со коренски сертификат. |
| Политика за сертификати (CP) | Документ кој се нарекува "Политика за сертификати на VeriSign Мрежата на Доверба" и претставува главна изјава за политиката според која делува VTN. |
| Регистар на повлечени сертификати (РПС) | Периодично (или инцидентно) издаван регистар, дигитално потпишан од ИС, на сертификати кои биле повлечени пред датата на истекување на нивната важност. Листата обично го наведува името на издавачот на РПС, датата на издавање, датата на следното закажано издавање на РПС, серискиот број на повлечениот сертификат, како и точното време и причините за повлекувањето. |
| Барање за потпишување на Сертификат | Порака која го пренесува барањето за сертификат |
| Издавач на сертификати (ИС) | Ентитет овластен да издава, у повлекува, обновува и управува со сертификати во VTN |
| Правила на издавачот на сертификати (или Правила) | Овој документ кој ги наведува Правилата што КИБС ги применува при одобрување или одбивање на барањата за сертификати; издавање, управување и поништување на сертификати; бара од неговите корисници и да ги применуваат. |
| Фраза за проверка | Тајна фраза избрана од барателот на сертификат за време на барањето на сертификат. Кога сертификатот ќе му биде издаден, барателот на сертификат станува претплатник и ИС или РК може да ја користи оваа фраза за да го автентичира претплатникот кога тој сака да го поништи или обнови својот сертификат. |
| Класа | Одредено ниво на гаранции, како што е дефинирано во CP. Види го делот 1.1.1 од CP. |
| Центар за услуги на клиенти | Центар за услуги кој во името на КИБС обезбедува сертификати за физички лица или претпријатија. |

| | |
|--|---|
| Ревизија за усогласеност | Периодична ревизија на која подлежи центарот за обработка, центарот за услуги или МПКИ Клиентот, за да се определи нивната усогласеност со VTN стандардите кои важат за нив. |
| Компромитирање | Прекршување (или претпоставено прекршување) на безбедносната политика, при кое можело да се случи неовластено откривање или губење на контролата врз осетливи информации. Во врска со приватните клучеви, компромитирање претставува губење, кражба, откривање, изменување, неовластено користење или друг вид на компромитирање на безбедноста на тој приватен клуч. |
| Доверлива/лична информација | Информација која треба да се чува како доверлива и лична во согласност со дел 2.8.1 од овие Правила |
| Договор за користење на РПС | Договор кој ги поставува условите и термините под кои можат да се користи РПС или информациите во него. |
| Претпријатие, како во Центар за услуги на претпријатија | Линија на бизнис во кој ADACOM влегува за да обезбедува Менаџирани ПКИ услуги за Менаџирани ПКИ Клиенти. |
| Инцидентна ревизија/претражување | Ревизија или претражување од страна на VeriSign или ADACOM кога ADACOM има причина да верува дека настанало непридржување на некој ентитет кон VTN Стандардите, инцидент или компромитирање или дека постои реална или потенцијална опасност. |
| Права на интелектуална сопственост | Права кои потпаѓаат под некое од следново: авторски права, патент, трговска тајна, заштитена марка и било кои други права на интелектуална сопственост. |
| Посреднички сертификациски авторитет (Посреднички ИС) | Сертификациски авторитет чиј сертификат е лоциран во синцирот на сертификати помеѓу сертификатот на коренскиот ИС и сертификатот на сертификацискиот авторитет кој го издал сертификатот на претплатникот - краен корисник. |
| Церемонија на генерирање клуч | Процедура во која се генерира пар на клучеви за ИС или РА, нивниот приватен клуч се трансферира во криптографски модул, нивниот приватен клуч се складира резервно и/или нивниот јавен клуч се сертифицира. |
| Менаџиран ПКИ | Целосно интегрирана менаџирана ПКИ услуга на ADACOM која им овозможува на фирмите клиенти на ADACOM да дистрибуираат сертификати на физички лица, како на пример, членови на персоналот, партнери, добавувачи и клиенти. Менаџираниот ПКИ им овозможува на фирмите да ги обезбедат своите пораки или апликации во електронската трговија. |
| Рачна автентикација | Процедура при која барањата за сертификати се разгледуваат и одобруваат рачно една по една, од страна на администраторот со користење на веб-базирана апликација. |
| Неверификувана претплатничка информација | Информација поднесена од барател на сертификат до ИС или РК и вклучена во Сертификат, а која не била потврдена од ИС или РК и за која релевантниот ИС и РК не обезбедуваат други гаранции освен дека информацијата била поднесена од барателот на сертификат. |

| | |
|--|--|
| Не-одрекување | Атрибут на комуникацијата кој обезбедува заштита од : комуникација за која лажно се одрекува нејзиното потекло, се одрекува дека таа била поднесена или се одрекува нејзината испорака. Одрекнување на потеклото вклучува негирање дека комуникацијата потекнува од истиот извор како редослед од една или повеќе претходни пораки, дури и кога идентитетот поврзан со испраќачот е непознат. Забелешка: само судска одлука, арбитража или некој друг трибунал можат во крајна мерка да спречат одрекување. На пример, дигитален потпис верификуван во врска со VTN Сертификат може да обезбеди доказ во прилог на определувањето на Не-одрекување од страна на трибунал, но тоа само по себе не сочинува Не-одрекување. |
| Исклучени (Офлајн) ИС | VeriSign ПИС кои издават коренски сертификати и други посреднички ИС, кои се одржуваат исклучени (Офлајн) од безбедносни причини, со цел да бидат заштитени од можни напади од натрапници преку мрежата. Овие ИС не потпишуваат директно Сертификати на Претплатници - крајни корисници. |
| Издавачки (Онлајн) ИС | ИС кои потпишуваат Сертификати на Претплатници - крајни корисници и се одржуваат електронски за да овозможат континуирани услуги на потпишување. |
| Протокол за Електронски статус на Сертификат (OCSP) | Протокол со кој им се обезбедува на засегнатите страни информација за статусот на Сертификат во реално време. |
| Оперативен период | Период што започнува на датата и во времето на издавањето на сертификатот (или на подоцнежна дата и време ако е така наведено во Сертификатот), а завршува на датумот и во времето кога сертификатот истекува или е повлечен порано. |
| PKCS #10 | Криптографски стандард # 10, развиен од RSA, кој дефинира структура за барањето за сертификат. |
| PKCS #12 | Криптографски стандард # 12 испорачан од RSA, кој дефинира безбеден начин за трансфер на приватни клучеви. |
| Авторитет за Управување со Политиката (АМП) | Организација во рамките на VeriSign одговорна за ширење на оваа политика низ целата VTN. |
| Примарен Издавач на Сертификати (ПИС) | ИС што делува како коренски ИС за специфична класа на сертификати и им издава сертификати на ИС кои му се потчинети. |
| Центар за Обработка | Локација на ADACOM со безбедни простории за сместување, меѓу другото, и на криптографските модули што се користат за издавање на сертификати. Од клиентска гледна точка центарот за обработка делува како ИС во рамките на VTN и ги извршува сите услуги поврзани со животниот циклус на сертификатот, како издавање, управување, повлекување и обновување на сертификати. Од бизнис гледна точка, процесирачкиот центар обезбедува услуги поврзани со животниот циклус на сертификатите, во име на Менаџираните ПКИ Клиенти. |

| | |
|---|---|
| Инфраструктура на Јавен Клуч (ПКИ) | Архитектура, организација, техники, практики и процедури кои заеднички ги поддржуваат имплементацијата и функционирањето на криптографскиот систем на јавни клучеви базирани на сертификати. VTN ПКИ се состои од системи кои соработуваат за обезбедување и имплементирање на VTN. |
| Регистрациски Авторитет (РА) | Авторитет одобрен од ИС за да им помогне на баратели за сертификат во аплицирањето за сертификати, како и да одобри или одбие барање за сертификат, повлече Сертификат или обнови сертификат. |
| Доверлива страна | Личност или организација која делува со потпирање на сертификат и/или дигитален потпис. |
| Договор со засегната страна | Договор кој се користи на тој начин што ИС ги поставува условите и термините под кои физичко лице или организација делува како засегната страна. |
| РСА | Криптографски систем за јавен клуч дизајниран од Ривест, Шамир и Аделман. |
| Таен удел | Дел од приватен клуч на ИС или дел од активирачките податоци што се потребни за да функционира приватен клуч на ИС во рамките на аранжман на тајни удели. |
| Споделување на тајна | Практика на разделување на ИС приватен клуч или на активирачките податоци што се потребни за да функционира ИС приватен клуч со цел да се воспостави контрола од повеќе лица врз операциите на ИС приватниот клуч согласно CP § 6.2.2 |
| ИД на Безбеден сервер | Организациски Сертификат Класа 3 кој се користи за поддржување на SSL сесии помеѓу веб-пребарувачите и веб-серверите |
| Secure Sockets Layer (SSL) | Метод на индустриски стандарди за заштита на веб комуникации развиен од Нетскеип корпорација за комуникации. SSL безбедносниот протокол обезбедува шифрирање на податоци, серверска автентикација, интегритет на пораките и, по избор, автентикација на клиент за конекција на Протоколот за контрола на трансмисија/Интернет протоколот. |
| Водич за услови на безбедност и ревизија | VeriSign документ кој ги поставува условите и практиките за безбедност и ревизија за Центри за обработка и Центри за услуги. |
| Сервисен Центар | Сервис на КИБС која не вклучува единици за потпишување на сертификати со цел за издавање на сертификати од конкретна класа или тип, туку повеќе, се потпира на центарот за обработка за да извршува издавање, управување, повлекување и обновување на такви сертификати. |
| Поддомен | Дел од VTN под контрола на било кој ентитет и сите ентитети што му се потчинети нему во рамките на VTN хиерархијата. |

| | |
|---------------------------------------|---|
| Субјект | Сопственик на приватен клуч што кореспондира со јавен клуч. Терминот "субјект" може, во случај на сертификат за организации, да се однесува на опрема или направа во која е сместен приватниот клуч. На субјектот му се дава недвосмислено име, кое е поврзано со јавниот клуч што се содржи во сертификатот на субјектот. |
| Претплатник | Во случај на сертификат за физички лица, претплатник е лицето кое што е субјект на сертификатот и на кое му е издаден сертификатот. Во случај на сертификат за организации, претплатник е организацијата што ја поседува опремата или направата која што е субјект на сертификатот и на која што и е издаден сертификатот. Претплатникот е способен да го користи и има овластување да го користи приватниот клуч што кореспондира со јавниот клуч запишан во сертификатот. |
| Претплатнички договор | Договор кој се користи од ИС и РК за поставување на условите и термините под кои физичко лице или организација делува како претплатник. |
| Надреден ентитет | Ентитет надреден над некој друг ентитет во рамките на VTN хиерархијата (Класа 1 или Класа 3 хиерархија). |
| Доверливо лице | Вработен, соработник под договор или консултант на ентитет во рамките на VTN одговорен за инфраструктурната сигурност и безбедност на ентитетот, неговите производи, услуги, неговите простории и/или практики како што е поконкретно дефинирано во CP § 5.2.1 |
| Доверлива позиција | Позиции во VTN ентитет на кои мора да бидат поставени доверливи лица. |
| Сигурен и безбеден систем | Компјутерски хардвер, софтвер и процедури кои се разумно безбедни од упади и погрешна употреба, обезбедуваат разумно ниво на достапност, доверливост и коректно функционирање, во разумна мерка се адекватни за извршување на функциите што им се наменети и ја применуваат потребната безбедносна политика. Тоа не значи неопходно дека сигурниот и безбеден систем е и доверлив систем, во смисла на класифицираната владејачка номенклатура. |
| VeriSign | Значи, во врска со секој релевантен дел од овие Правила, VeriSign, Inc, и/или било која помошна фирма во целосна сопственост на VeriSign која е одговорна за специфични операции во издавањето. |
| КИБС Складиште | База на податоци на КИБС со сертификати и други релевантни информации за КИБС ИС достапни по електронски пат. |
| VeriSign Доверлива мрежа (VTN) | Инфраструктура на јавен клуч базирана на сертификати, која е водена од Политиките за сертификати на VeriSign Доверливата мрежа и овозможува распространување и користење на сертификати низ целиот свет од страна на VeriSign и компаниите поврзани со него, како и од нивните клиенти, претплатници и засегнати страни. |

| | |
|----------------------|--|
| VTN Учесник | Физичко лице или организација кои се едно или повеќе од следниве наводи во рамките на VTN: VeriSign, КИБС, Клиент, Универзален сервисен центар, препродавач, претплатник или засегната страна. |
| VTN Стандарди | Деловните, правните и техничките услови за издавање, управување, повлекување, обновување и користење на Сертификати во рамките на VTN. |