Политика сертификације Агенције

Правила о електронском потпису која је утврдила Агенција као овлашћено тијело за пружање услуга од повјерења

Идентификациони број	
Верзија	1.0
Предлаже:	Генерални директор

Верзија	Датум	Припремио:	Кратак опис измјена
1.0	2021-09-20	Службеник за безбједност	Почетна верзија

Цонтентс

1. УВОДНИ ДИО 9

1.1. Преглед 9

1.2. Назив документа и идентификација 10

1.3. Учесници у инфраструктури јавног кључа (ПКИ) 10

1.3.1. Сертификациона тијела 10

1.3.1.1. Тијело за управљање политиком (ПМА) 12

1.3.1.2. Оперативно тијело (ОА) 13

1.3.2. Регистрациона тијела Сертификационог тијела Агенције (РА) 13

1.3.3. Корисници 14

1.3.4. Треће стране 14

1.3.5. Остали учесници 14

1.4. Употреба сертификата 14

1.4.1. Прихватљиво коришћење сертификата 14

1.4.2. Забрана коришћење сертификата 15

1.5. Администрирање политике сертификације 15

1.5.1. Администрирање документа 15

1.5.2. Контакт особа 15

1.5.3. Особа која одређује погодност Изјаве о сертификационој пракси 15

1.5.4. Процедура одобравања Изјаве о сертификационој пракси 15

1.6. Дефиниције и скраћенице 15

2. ОДГОВОРНОСТ ЗА ПУБЛИКОВАЊЕ И РЕПОЗИТОРИЈЕ 19

2.1. Репозиторији 19

2.2. Објављивање информација о сертификатима 19

2.3. Вријеме и учесталост објављивања 19

2.4. Контроле приступа репозиторијима 19

3. ИДЕНТИФИКАЦИЈА И АУТЕНТИКАЦИЈА КОРИСНИКА 20

3.1.1. Врсте имена 20

3.1.2. Имена треба да буду смислена 20

3.1.3. Анонимност или псеудонимност корисника 20

3.1.4. Правила за тумачење различитих облика имена 20

3.1.5. Јединственост имена 20

3.1.6. Препознавање, аутентикација и улога заштитних знакова 21

3.2. Иницијална провјера идентитета 21

3.2.1. Метод за доказивање посједовања приватног кључа 21

3.2.2. Аутентикација идентитета појединца 21

3.2.3. Непровјерене информације о кориснику 21

3.2.4. Критерији за међуоперацију 21

3.3. Идентификација и аутентикација захтјева за обнављање кључева 21

3.3.1. Идентификација и аутентикација приликом рутинске обнове кључева 21

3.3.2. Идентификација и аутентикација приликом обнове кључа након опозива 22

3.4. Идентификација и аутентикација приликом подношења захтјева за опозив 22

4. ОПЕРАТИВНИ ЗАХТЈЕВИ У ВЕЗИ ЖИВОТНОГ ЦИКЛУСА СЕРТИФИКАТА 23

4.1. Захтјев за добијање сертификата 23

4.1.1. Ко може предати захтјев за добијање сертификата 23

4.1.2. Процес уписа и одговорности 23

4.2. Обрада захтјева за добивање сертификата 23
4.2.1. Обављање функција идентификације и аутентикације 23
4.2.2. Одобравање или одбијање захтјева за сертификацију 24
4.2.3. Вријеме потребно за обраду захтјева за сертификацију 24

4.3. Издавање сертификата 24
4.3.1. Активности ТСП-а током издавања сертификата 24
4.3.2. Обавјештавање корисника о издавању сертификата 24

4.4. Прихватање сертификата 24
4.4.1. Поступак којим се прихвата сертификат 24
4.4.2. Обавјештење других лица о издавању сертификата које издаје ТСП 25

4.5. Коришћење пара кључева и сертификата 25
4.5.1. Коришћење корисничког приватног кључа и сертификата 25
4.5.2. Коришћење јавног кључа и сертификата треће стране 25

4.6. Обнављање сертификата (без генерисања новог кључа) 26
4.6.1. Услови за обнављање сертификата 26
4.6.2. Ко може тражити обнављање захтјева 26
4.6.3. Обрада захтјева за обнављање сертификационог кључа 26
4.6.4. Обавјештавање корисника о новом издавању сертификата 26
4.6.5. Поступак који представља прихватање сертификата са обновљеним кључем 26
4.6.6. Објављивање обновљеног сертификата које обавља ТСП 26
4.6.7. Обавјештавање других лица о издавању сертификата које обавља ТСП 26

4.7. Обнављање сертификата генерисањем новог кључа (обнављање генерисањем новог пара кључева) 26
4.7.1. Услови за обнову сертификата генерисањем новог кључа 26
4.7.2. Ко може тражити сертификацију са новим јавним кључем 26
4.7.3. Обрада захтјева за обнављање сертификата генерисањем новог кључа 27
4.7.4. Обавјештавање корисника о издавању новог сертификата 27
4.7.5. Поступак прихватања сертификата са новим кључем 27
4.7.6. Објављивање сертификата са новим кључем које обавља ТСП 27
4.7.7. Обавјештавање других лица о издавању сертификата које обавља ТСП 27

4.8. Измјене сертификата 27
4.8.1. Услови за измјене сертификата 27
4.8.2. Ко може тражити измјене сертификата 27
4.8.3. Обрада захтјева за измјену сертификата 27
4.8.4. Обавјештавање корисника о издавању новог сертификата 27
4.8.5. Поступак прихватања измијењеног сертификата 27
4.8.6. Објављивање измијењеног сертификата које обавља ТСП 27
4.8.7. Обавјештавање других лица о издавању сертификата које обавља ТСП 27

4.9. Опозив и суспензија сертификата 28
4.9.1. Услови за опозив 28
4.9.2. Ко може тражити опозив 28
4.9.3. Процедура за подношење захтјева за опозив 28
Опозив због измјене података у самом сертификату 28
Опозив због компромитованог приватног кључа 29
Опозив сертификата због неиспуњавања обавеза корисника 29
4.9.4. Одложени опозив сертификата 29
4.9.5. Рок у којем ЦА мора завршити обраду захтјева за опозив 29
4.9.6. Захтјев за провјеру опозива за треће стране 29
4.9.7. Учесталост објављивања списка опозваних сертификата (ако је примјењиво) 30
4.9.8. Максимално кашњење списка опозваних сертификата (ако је примјењиво) 30
4.9.9. Доступност електронског опозива/провјере статуса 30
4.9.10. Услови за електронску провјеру опозива 30

4.9.11. Остали начини оглашавања опозива 30
4.9.12. Посебни услови везани за компромитовање кључа 30
4.9.13. Суспензија сертификата 30
4.9.14. Ко може тражити суспензију 30
4.9.15. Процедура за подношење захтјева за суспензију 30
4.9.16. Ограничење периода суспензије 31

4.10. Сервиси провјере статуса сертификата 31
4.10.1. Оперативне карактеристике 31
4.10.2. Доступност услуга 31
4.10.3. Опционе карактеристике 31

4.11. Престанак важења сертификата 31

4.12. Депоновање и опоравак кључева 31
4.12.1. Политика и пракса депоновања и опоравка кључева 31
4.12.2. Политика и пракса енкапсулације и опоравка сесијског кључа 31

5. УПРАВНЕ, ОПЕРАТИВНЕ И ФИЗИЧКЕ БЕЗБЈЕДНОСНЕ КОНТРОЛЕ 32

5.1. Физичке контроле 32
5.1.1. Локација објекта и конструкција 32
5.1.2. Физички приступ 32
5.1.3. Електрично напајање и климатизација 32
5.1.4. Опасност од поплаве 32
5.1.5. Превенција и заштита од пожара 32
5.1.6. Чување медија 32
5.1.7. Одлагање отпада 32
5.1.8. Резервне копије на другој локацији 33

5.2. Процедуралне контроле 33
5.2.1. Повјерљиве улоге 33
5.2.2. Број особа које се захтјевају по сваком задатку 34
5.2.3. Идентификација и аутентикација за сваку улогу 34
5.2.4. Улоге које захтијевају раздвајање дужности 35

5.3. Кадровске контроле 35
5.3.1. Квалификације, искуство и сигурносне провјере 35
5.3.2. Процедуре провјере биографије 35
5.3.3. Захтјеви за обуке 35
5.3.4. Фреквенција и захтјеви за поновну обуку 36
5.3.5. Фреквенција и редослијед ротације послова 36
5.3.6. Казне за неовлаштене радње 36
5.3.7. Услови за спољне сараднике 36
5.3.8. Документација која се доставља запосленима 36

5.4. Процедуре ревизијских записа 36
5.4.1. Типови забиљежених догађаја 36
5.4.2. Фреквенција процесирања записа 37
5.4.3. Период чувања ревизијских записа 37
5.4.4. Заштита ревизијских записа 37
5.4.5. Процедуре резервних копија ревизијских записа 37
5.4.6. Систем прикупљања ревизија (интерне или екстерне) 37
5.4.7. Обавјештавање субјекта који је проузроковао догађај 38
5.4.8. Оцјена рањивости система 38

5.5. Архивирање записа 38
5.5.1. Типови архивираних записа 38
5.5.2. Период чувања архиве 39
5.5.3. Заштита архиве 39

5.5.4. Процедуре резервних копија архиве 39
5.5.5. Захтјеви за временску ознаку записа 39
5.5.6. Систем прикупљања архива (интерни или екстерни) 39
5.5.7. Процедуре за добијање и верификацију информација из архиве 39
5.6. Замјена кључева 39
5.7. Компромитација и опоравак у случају катастрофе 39
5.7.1. Процедуре за поступање у инцидентним и компромитујућим ситуацијама 39
5.7.2. Рачунарски ресурси, софтвер и/или подаци који су оштећени 39
5.7.3. Процедуре које се спроводе код компромитације приватног кључа корисника 39
5.7.4. Управљање капацитетом пословања након катастрофе 40
5.8. Завршетак рада ТСП-а или Регистрационог тијела 40
6. ТЕХНИЧКЕ БЕЗБЈЕДНОСНЕ КОНТРОЛЕ ТСП-А 41
6.1. Генерисање и инсталација пара кључева 41
6.1.1. Генерисање пара кључева 41
6.1.2. Испорука приватног кључа кориснику 41
6.1.3. Достава јавног кључа до издаваоца сертификата 41
6.1.4. Достава јавног кључа ТСП-а трећим странама 41
6.1.5. Дужине кључева 41
6.1.6. Генерисање јавних кључева и провјера квалитета 42
6.1.7. Намјене екстензије “Key usage” (дефинисано у X.509 v3 пољу употребе кључа) 42
6.2. Заштита приватног кључа и контрола криптографског хардверског модула 42
6.2.1. Стандарди и контроле криптографског модула 42
6.2.2. Контрола приватних кључева од стране више особа (н од м) 43
6.2.3. Чување (енгл. Escrow) приватног кључа код трећих лица 43
6.2.4. Сигурносне копије приватног кључа 43
6.2.5. Архивирање приватног кључа 43
6.2.6. Пренос приватних кључева са и на криптографски модул 43
6.2.7. Чување приватног кључа у криптографском модулу 43
6.2.8. Поступак активације приватног кључа 43
6.2.9. Поступак деактивирања приватног кључа 43
6.2.10. Поступак уништавања приватног кључа 44
6.2.11. Оцјењивање криптограског модула 44
6.3. Други аспекти управљања паром кључева 44
6.3.1. Архивирање јавног кључа 44
6.3.2. Периоди валидности сертификата и парова кључева 44
6.4. Активациони подаци 44
6.4.1. Генерисање и инсталација активационих података 44
6.4.2. Заштита активационих података 44
6.4.3. Други аспекти који се односе на активационе податке 45
6.5. Безбједносне контроле рачунара 45
6.5.1. Специфични технички захтјеви за безбједност рачунара 45
6.5.2. Оцјењивање безбједности рачунара 45
6.6. Животни циклус и безбједносне контроле 45
6.6.1. Контроле развоја система 45
6.6.2. Провјере управљања безбједношћу 45
6.6.3. Провјера безбједности животног циклуса 45
6.7. Контроле мрежне безбједности 45
6.8. Временски печат 46
7. ПРОФИЛИ СЕРТИФИКАТА, СПИСКА ОПОЗВАНИХ СЕРТИФИКАТА И ОЦСП 47

7.1. Профили сертификата 47
7.1.1. Број верзије сертификата 47
7.1.2. Екстензије сертификата 47
7.1.2.1. Екстензије приватних сертификата 48
7.1.3. Идентификатор објекта алгоритама 48
7.1.4. Облици назива 48
7.1.5. Ограничења имена 48
7.1.6. Идентификатор објекта политике сертификације 48
7.1.7. Употреба „Policy Constraints" екстензија 48
7.1.8. Синтакса и семантика квалификатора политике 48
7.1.9. Семантика процесирања критичне екстензије „Certificate Policies" 48
7.2. Профил списка опозваних сертификата 48
7.2.1. Број верзије сертификата 48
7.2.2. Списак опозваних сертификата и „entry" екстензије списка опозваних сертификата 49
7.3. ОЦСП профил 49
7.3.1. Број верзије сертификата 49
7.3.2. Екстензије ОЦСП 49
8. РЕВИЗИЈА УСКЛАЂЕНОСТИ И ДРУГА ОЦЈЕЊИВАЊА 50
8.1. Учесталост или услови оцјењивања 50
8.2. Идентитет/квалификације процјењивача (интерна ревизија) 50
8.3. Однос ревизора с предметом ревизије 50
8.4. Теме које су обухваћене ревизијом 50
8.5. Активности предузете као резултат утврђених недостатака 50
8.6. Саопштавање резултата 50
9. ДРУГИ ПОСЛОВНИ И ПРАВНИ АСПЕКТИ 51
9.1. Накнаде 51
9.1.1. Накнаде за издавање или обнову сертификата 51
9.1.2. Накнаде за приступ сертификату 51
9.1.3. Накнаде за опозив и приступ информацијама о статусу сертификата 51
9.1.4. Накнаде за остале услуге 51
9.1.5. Повратак накнаде 51
9.2. Финансијска одговорност 51
9.2.1. Покривање осигурања 51
9.2.2. Остала средства 51
9.2.3. Осигурање или гаранције за крајње кориснике 51
9.3. Заштита личних података 51
9.3.1. Опсег повјерљивих информација 51
9.3.2. Информације које нису у опсегу поверљивих информација 52
9.3.3. Одговорност за заштиту повјерљивих информација 52
9.4. Приватност личних информација 52
9.4.1. План приватности 52
9.4.2. Опсег приватних информација 52
9.4.3. Информације које се не сматрају приватним 52
9.4.4. Одговорност за заштиту повјерљивих информација 52
9.4.5. Обавјештење и сагласност за употребу приватних информација 52
9.4.6. Откривање информација у складу са правним и административним процесима 52
9.4.7. Друге околности за откривање информација 52
9.5. Права интелектуалног власништва 52

9.6. Обавезе и одговорности 53
9.6.1. Обавезе и одговорности ТСП-а 53
9.6.2. Одговорности и обавезе регистрационог тијела 53
9.6.3. Корисничке одговорности и обавезе 54
9.6.4. Обавезе и одговорности трећих страна 54
9.6.5. Одговорности и обавезе других учесника 55
9.7. Непризнавање гаранција 55
9.8. Ограничења одговорности 55
9.9. Накнада штете 55
9.10. Трајање и престанак важења 56
9.10.1. Трајање 56
9.10.2. Престанак важења 56
9.10.3. Посљедице престанка важења и наставак дјеловања 56
9.11. Појединачна обавјештења и комуникација са учесницима 56
9.12. Измјене и допуне 56
9.12.1. Поступак измјена и допуна 56
9.12.2. Механизам и период обавјештавања 56
9.12.3. Околности под којима се мора мијењати идентификатор објекта OID 56
9.13. Поступак рјешавања спорова 56
9.14. Важећи прописи 57
9.15. Усклађеност са важећим прописима 57
9.16. Остале одредбе 57
9.16.1. Комплетан уговор 57
9.16.2. Додјељивање 57
9.16.3. Случајеви непримјењивости одредби (раздвојеност) 57
9.16.4. Извршење (адвокатске накнаде и одрицање од права) 57
9.16.5. Виша сила 57
9.17. Остале одредбе 57

1. УВОДНИ ДИО

1.1. Преглед

- Агенција за идентификациона документа, евиденцију и размјену података БиХ (у даљем тексту: Агенција) управља инфраструктуром јавног кључа за пружање сљедећих квалификованих услуга од повјерења:

  1) Издавање квалификованих сертификата за електронски потпис.

- Ова Политика сертификације је јавни документ који представља дио прописа које дефинише Агенција који се односе се на квалификоване услуге од повјерења које пружа Агенција као тијело овлашћено за пружање услуга од повјерења. Сврха овог документа је да појасни техничке, процедуралне и организационе активности, као и примјену инфраструктуре јавног кључа (ПКИ Агенције) и проведене процедуре сертификације које показују повјерљивост Агенције као квалификованог пружаоца услуга од повјерења (ТСП).

  Овај документ је усклађен са захтјевима Закона о електронским документима, електронској идентификацији и услугама од повјерења у Босни и Херцеговини и подзаконским актима донесеним на основу наведеног закона.

  Овај документ садржи Политику сертификације Агенције. Документ је израђен у складу са оквирним документом IETF RFC 3647 “Интернет X.509 Инфраструктура јавног кључа: Оквирна политика сертификације и сертификационе праксе” који садржи оквир са свеобухватном листом тема које треба да буду обрађене у политици сертификације и/или изјави о пракси сертификације. Садржај је усклађен са:

- ETSI EN 319 401 Општи услови политике за пружаоце услуга од повјерења
- ETSI EN 319 411-1 Политика и безбједносни услови за пружаоце услуга повјерења који издају сертификате; Дио 1: Општи услови
- ETSI EN 319 411-2 Политика и безбједносни услови за пружаоце услуга повјерења који издају сертификате; Дио 2: Услови које морају да испуне пружаоци услуга од повјерења који издају квалификоване сертификате ЕУ;
- ETSI EN 319 412-1 Профили сертификата; Дио 1: Преглед и заједничка структура података
- ETSI EN 319 412-2 Профили сертификата; Дио 2: Профили сертификата за физичка лица
- ETSI EN 319 412-3 Профили сертификата; Дио 3: Профили сертификата за правна лица
- ETSI EN 319 412-5 Профили сертификата; Дио 5: Профил квалификованог електронског сертификата (QCStatement)
- ЕТСИ ТС 119 495 Услови карактеристични за сектор; Профили квалификованог сертификата и Услови политике ТСП-а у складу са Директивом о платним услугама (ЕУ) 2015/2366

- Овај документ описује јавна правила за категорије квалификованих и нормализованих сертификата који су наведени у табелама испод.

Табела 1: Списак квалификованих сертификата

Категорија сертификата	Опис
Квалификовани ДС за квалификовани е-потпис	Квалификовани ДС за квалификовани електронски потпис издат физичком лицу гдје се приватни кључ и припадајући сертификат налазе на смрт картици/токену

Табела 2: Списак нормализованих сертификата

Категорија сертификата	Опис
Нормализовани ДС – ОЦСП	Нормализовани ОЦСП

1.2. Назив документа и идентификација

- Овај документ представља Политику сертификације Агенције, (у даљем тексту Политика или ПС). Политика је објављена на сљедећем URL-у:
    - https://www.iddeea.gov.ba/PKI/CP и јавно је доступан.
- Документ под називом Изјава о откривању инфраструктуре јавног кључа Агенције, састављен у складу са ETSI EN 319 411-1, Анекс А.1, у даљем тексту ПДС, објављен је на сљедећим URL-овима:
    - https://www.iddeea.gov.ba/PKI/CP
- Сљедећи идентификатори објекта (ОИД) се додјељују категоријама сертификата који се издају у складу са овом Политиком.

Категорија сертификата	Идентификација сертификационе политике
Квалификовани ДС за квалификовани електронски потпис	0.4.0.194112.1.2
Нормализовани ДС-ОЦСП	0.4.0.194112.1.2

- Агенција може издати различите сертификате, који морају бити јасно означени с посебном политиком или додатним идентификатором објекта политике у екстензији X.509 *certificatePolicies*. Идентификатор објекта има префикс 1.3.6.1.4.1.*18560*. *Identifier* и требао би бити јединствен за овај префикс.

1.3. Учесници у инфраструктури јавног кључа (ПКИ)

1.3.1. Сертификациона тијела

- Сертификационо тијело Агенције дјелује као јавни пружалац услуга од повјерења (ТСП) и издаје сертификате јавног кључа физичким и правним лицима.
- Сертификационо тијело Агенције дјелује као централно сертификационо тијело које издаје самопотписане сертификате у процесу церемоније генерисања коријенског кључа и унакрсног сертификата једном хијерархијски подређеном сертификационом тијелу. Агенција користи једно сертификационо тијело (сертификационо тијело за издавање сертификата) за издавање свих врста квалификованих и нормализованих сертификата крајњим корисницима.
- Сертификационо тијело Агенције управља сљедећим сертификационим тијелима:
    - Централним сертификационим тијелом Агенције са мандатом од 20. септембра 2021. до 20. септембра 2041. које има самопотписни сертификат који издаје сертификационим тијелима Агенције.
    - Сертификационим тијелима Агенције која издају квалификоване сертификате крајњег идентитета са мандатом од 29. септембра 2021. до 29. септембра 2031. које потписује Централно сертификационо тијело Агенције.
- Садржај дигиталног сертификата “ IDDEEA-RootCA-2021”:

Серијски број	449FFCA0B7E0AFE2DC4C5D9754F945677B9028AC
Издаје	IDDEEA
Субјекат	CN=IDDEEA-RootCA-2021, O=IDDEEA, emailAddress=eid@iddeea.gov.ba, L=Banja Luka, street=Kralja Petra I Karadjordjevica 83A, postalCode=78000, C=BA
Рок важења: не прије	20.09.2021
Рок важења: не послије	20.09.2041
Јавни кључ PCA	82:D0:61:16:28:EE:51:49:DF:40:C5:51:AA:DD:59:F8 66:B9:9D:1A:86:FB:7E:A8:37:33:54:B1:97:3C:72:26 C3:B8:B6:6C:0F:B0:35:CD:42:40:8A:87:22:DE:3A:90 5A:AA:29:52:AD:39:8E:C5:76:99:54:3B:3E:E1:00:12 DB:7E:0F:21:B1:31:EA:6B:87:5E:FC:B2:5B:AC:D7:FC F0:3C:BE:C3:BB:25:52:A5:C4:46:0B:94:8F:EF:C8:BE 25:4F:E2:F2:DC:69:60:F9:69:44:F7:2F:9A:01:2E:9E EE:88:A7:5D:7A:77:45:36:7F:70:ED:E9:A9:2C:2F:98 91:92:0B:FA:FB:B3:7F:62:C9:BA:EE:EE:60:60:26:65 66:FB:A6:7F:6A:F5:F7:2D:F6:39:50:68:68:EC:33:DD 4C:F8:35:42:92:57:0C:5E:8F:4A:DD:D4:83:2F:39:C3 D5:C7:68:CD:99:49:16:7F:1A:A8:F4:50:34:BF:5B:2C 10:C5:21:34:92:DF:35:AB:B6:4C:EF:32:12:EA:8B:AC CC:EE:71:06:1E:FF:46:53:DC:3B:32:F1:20:45:62:CC 50:39:DC:4F:14:7E:6D:2E:A1:D4:3A:82:45:61:4D:50 1B:91:06:35:C8:28:88:8B:26:FF:5C:40:DD:B5:42:08 C6:D8:AF:6D:02:B6:ED:EC:80:65:14:6F:AC:5D:E0:FB BC:B8:54:C3:F9:45:00:C4:F1:83:34:F8:2A:84:56:E8 DC:A3:37:FD:E2:1A:B9:9C:51:CC:37:20:BB:53:4D:64 37:BB:67:AD:85:D5:43:F7:80:60:C3:6E:F2:E5:51:5B B6:77:77:36:B0:03:45:33:06:2E:23:72:54:25:31:09 79:9C:05:4B:DF:D1:E2:E9:11:FE:2E:4D:93:B0:06:3D F0:84:02:56:D0:E7:FC:DE:11:6E:EE:F9:63:52:48:C6 68:6B:D4:76:E6:BB:A0:D5:96:A5:2B:DB:E7:58:99:16 47:37:90:13:1F:FF:F7:EA:9B:75:9A:7B:40:B2:FC:46 C7:5E:BA:96:C9:09:E9:74:FC:88:7E:B9:3E:73:2A:3D 2A:33:06:95:28:4B:68:86:78:D1:FF:32:CB:57:26:BE D3:C9:17:47:B8:26:A1:1C:03:77:C7:EE:57:FA:CE:E4 59:2E:BC:FD:43:AB:C1:56:8B:66:7D:28:58:A5:00:E8 B4:45:08:AB:25:5E:51:94:81:07:C2:67:8A:27:55:36 0E:D0:45:94:F5:17:1F:D2:52:E0:DA:38:78:99:AA:9A 79:7B:E3:04:B2:DF:6B:92:09:C2:A5:95:85:70:4F:8B
Алгоритам потписа	sha512WithRSAEncryption
Идентификатор кључа	09:8C:2D:66:7C:81:74:91:54:E5:85:59:42:E0:97:5F:0F:A2:B2:B2
Идентификатор кључа овлаштења	09:8C:2D:66:7C:81:74:91:54:E5:85:59:42:E0:97:5F:0F:A2:B2:B2
SHA-1 hash	A2:4E:6B:E6:78:98:AE:DD:5E:E9:5B:09:82:34:E5:80:48:37:E5:DD
SHA-256 hash	57:75:50:3D:A6:29:84:27:01:5B:33:79:6B:13:44:C2

- Дигитални сертификат сертификационог тијела за издавање сертификата *IDDEEA-IssuingCA* са роком важења од 29. септембра 2021. до 29. септембра 2031.” садржи:

Серијски број	27AF82049AC3D91AE8664A4A6FFFB991AE89B66C
Издаје	IDDEEA
Субјекат	CN=IDDEEA-IssuingCA
Рок важења: не прије	29.09.2021
Рок важења: не послије	29.09.2031
Јавни кључ PCA	B0:DC:AF:AD:C5:1E:14:97:AC:A9:DA:77:C1:06:6A:61 D1:28:DA:45:78:93:B4:A6:70:8B:DE:82:37:EF:4B:61 7D:37:A8:C0:0E:A1:15:7E:D7:CB:9C:3D:43:7A:89:7C B6:FC:A5:93:12:CE:74:00:1B:5E:F7:C6:25:E8:C8:F0 DF:C9:D6:DF:EB:5C:B3:A2:A4:33:6C:54:D6:A4:EA:72 3D:D5:E2:38:F8:74:4C:B7:2F:4E:B4:92:13:3A:D5:07

	50:34:57:BC:18:26:90:58:97:EA:BA:E1:17:DF:22:CA 3B:F3:2B:2C:5E:8D:77:93:BC:C8:75:3F:30:99:1C:87 D2:3A:36:80:6F:BC:D3:9D:D2:28:36:8E:84:51:DC:A1 80:FD:75:64:7E:D1:8E:E2:B0:9A:79:C6:36:9D:CB:3B 81:8D:90:E0:4C:D2:16:5F:F3:0A:4A:B9:39:04:B3:20 39:8B:DF:50:A5:22:64:54:27:C8:56:CC:C3:6E:5C:F0 D8:6D:2B:7B:09:13:FE:E9:6F:9A:16:29:3B:E4:A5:3B F2:74:68:39:88:4C:49:48:3A:35:A9:96:A6:D1:CC:22 B2:99:10:8F:05:C6:A3:A2:76:5A:DA:36:9E:7C:97:C2 4F:50:AA:A4:02:65:AA:34:53:56:0A:14:2A:A3:F4:BC 30:5E:E6:6A:71:71:1C:AF:E8:9B:2A:EB:5E:42:62:AD 39:2B:CA:C2:5F:02:7C:00:4F:D5:AE:F0:94:61:2D:B3 DF:D1:D1:50:96:3F:A9:63:2D:CC:B5:88:DD:FE:A3:AC 45:51:0E:76:D2:E7:E3:19:B0:EC:B3:06:DB:D9:FE:BD 2A:4C:5B:A9:77:AF:11:C1:1E:52:A8:3C:AD:BF:B5:86 9B:E5:B5:98:1D:94:CE:E2:7C:65:67:FF:D4:EF:51:0E 49:96:82:6B:FF:35:C6:08:8F:0E:7F:83:39:EE:15:2C 6A:A0:EF:3C:F9:88:1D:13:5C:22:EA:1F:A6:73:4C:41 B9:04:F5:B6:76:1F:46:A3:75:75:A6:D4:D6:31:54:0B 3D:C6:8C:67:A3:4B:0E:93:4B:81:9B:5B:86:3E:DB:57 76:F1:0A:B8:ED:75:E9:1C:95:1C:E4:45:15:09:93:E4 12:CD:91:D7:44:4A:9C:1E:AE:A1:4D:13:DB:70:F3:15 59:BA:56:EF:76:C4:21:41:3B:C5:D5:16:58:1D:57:04 71:6D:CB:97:46:A8:7A:9A:4F:7B:1E:E3:9A:C7:3C:60 0A:5D:FB:A4:E9:83:15:49:11:23:21:B1:B4:34:2A:68 DF:9F:6F:C6:16:8B:F0:E9:0F:E6:24:5A:7C:5C:50:DF
Алгоритам потписа	sha512WithRSAEncryption
Идентификатор кључа	55:4D:EF:8B:87:48:55:BA:DD:AA:0E:41:D6:B6:CB:7D:77:1A:11:DA
Идентификатор кључа овлаштења	09:8C:2D:66:7C:81:74:91:54:E5:85:59:42:E0:97:5F:0F:A2:B2:B2
SHA-1 hash	C2:A7:DF:30:66:40:D0:7E:D1:BF:E6:98:37:48:5E:32:E7:4A:60:5A
SHA-256 hash	71:27:C8:24:E2:47:5C:B8:A9:25:E0:53:83:91:41:6C 2D:F0:0B:B9:C1:B6:85:95:1D:98:F3:A1:D0:AD:CE:EF

- Сертификационо тијело Агенције је као пружалац услуга од повјерења дужно проводити мјере и поступке којима се осигурава управљање сертификатима, у складу са важећим прописима у Босни и Херцеговини и интерним правилима пружаоца услуга сертификовања. Сертификационо тијело Агенције запошљава особе које су одговорне за:
    - цјелокупни рад ТСП-а (Тијела за управљање политиком Агенције – ПМА Агенције);
    - особе које управљају и одржавају инфраструктуру ТСП-а, приватне криптографске кључеве сертификационог тијела, сервере и софтвер (Тијело за оперативне послове – ОА); и
    - особе које су одговорне за идентификацију корисника (Тијело за регистрацију – РА) и координацију са спољним РА.
- Када је потребно, ова правила политике праве разлику између различитих корисника и улога оних који приступају функцијама ТСП-а. Када ова разлика није потребна, термин ТСП се користи за означавање укупног ТСП ентитета, укључујући софтвер и његове операције.

1.3.1.1. Тијело за управљање политиком (ПМА)

Тијело за управљање политиком у оквиру Агенције одговорно је за:

- израду и одржавање Политике сертификације Сертификационог тијела Агенције;
- израду и одржавање јавних докумената Сертификационог тијела Агенције (Уговор са крајњим корисницима, итд.)

- предају Политике сертификације Сертификационог тијела Агенције надлежном управном органу на одобрење;
- регистрацију и акредитовање Сертификационог тијела Агенције;
- ангажовање особља у тијелима за оперативне послове и регистрацију (ОА и РА);
- контролу и ревизију усклађености операција Сертификационог тијела Агенције и активности како би се осигурало да ТСП ради у складу са Политиком и релевантним законодавством;
- контролу и одобравање Политике сертификације или Изјаве о пракси сертификације (ЦПС документ) спољњих унакрсно сертификованих тијела за сертификацију;
- рјешавање спорова између учесника Сертификационог тијела Агенције.

1.3.1.2. Оперативно тијело (ОА)

- Оперативно тијело Сертификационог тијела Агенције надлежно је за:
- генерисање тсп пара кључева, безбједно управљање приватним тсп кључевима, и дистрибуцију јавних тсп кључева;
- успостављање окружења и процедуре за подношење захтјева за сертификацију;
- идентификацију и аутентикацију појединаца или лица који се пријављују за сертификат;
- одобравање и одбијање захтјева за издавање сертификата;
- потписивање и издавање X.509 сертификата који кориснике обавезује својим јавним кључем, као одговор да је захтјев за издавање сертификата одобрен;
- слање X.509 сертификата путем директорија;
- покретање опозива сертификата, било на захтјев корисника или на сопствену иницијативу субјекта;
- опозив сертификата, укључујући издавање и објављивање Списка опозваних сертификата и одржавање сервиса Протокола о електронској провјери сертификата;
- управљање ТСП-ом у складу са законима у Босни и Херцеговини и овом Политиком;
- одобравање и ангажовање особа како би се попуниле радне позиције за ПКИ службенике;
- контролу и ревизију послова РА и ЛРА у оквиру своје надлежности;
- иницирају опозив сертификата запослених у ТСП-у и РА.

1.3.2. Регистрациона тијела Сертификационог тијела Агенције (РА)

- Министарство унутрашњих послова (МУП) је надлежни орган за издавање личних карата са уграђеним меморијским елементом (е-ОИ/е-ЛК).
- Министарство унутрашњих послова је регистрационо тијело (у даљем тексту: пружалац услуга регистрације или РА) које потврђује идентитет и идентификационе податке физичких лица, на основу чега сертификационо тијело Агенције издаје, обнавља, опозива и суспендује сертификате.
- Министарство унутрашњих послова независно руководи својим запосленим у полицијским управама и полицијским станицама (ПУ/ПС) који дјелују у својству локалних регистрационих тијела (ЛРА), а врше регистрацију особа у складу са Законом о личним картама држављана Босне и Херцеговине.
- ПУ/ПС послови су:
    - информисање особа о процесима регистровања и издавања (е-ОИ/е-ЛК),
    - примање захтјева за издавање, опозив и суспензију сертификата (е-ОИ/е-ЛК),
    - утврђивање идентитета особа и подносилаца захтјева,
    - омогућавање потписивања уговора са физичким лицима,
    - издавање сертификата (еОИ/еЛК).

- МУП и Агенција су склопили споразум којим се МУП обавезује да ће обезбиједити провођење безбиједносних прописа и процедура који су описани у овом документу, у поглављу 5, у одјељцима 5.3 Кадровске контроле и 5.5 Архивирање записа.

- РА користи двије опште категорије регистрационих тијела. Прва категорија регистрационих тијела (Локална регистрациона тијела или ЛРА) обухвата регистрациона тијела која су надлежна за обављање верификације идентитета лицем у лице и сакупљање корисничких података како би се обезбиједило уписивање корисника и рутинска обнова сертификата са новим кључем. Друга категорија регистрационих тијела (примарно регистрационо тијело или ПРА) подразумијева службенике именоване за контролу корисничких података и одобравање захтјева за регистрацију.

1.3.3. Корисници

- Лице подразумијева физичко лице коме се издаје е-ОИ/е-ЛК, и које добива сертификат на личној карти и потписује споразум са Агенцијом о пружању услуга сертификације у складу са Законом о личној карти држављана Босне и Херцеговине. Лице је директно одговорно за поступање у складу са Условима сертификационих услуга.

- Лице је и оно лице које је наведено у сертификату и потписник који креира електронски потпис и користи сертификат у његово/њено име.

- Корисник је лице, укључујући и физичко лице (појединце), које користи услуге.

- Субјекат је лице које је идентификовано у сертификату као носилац приватног кључа који је повезан са јавним кључем датим у сертификату.

- Корисник је лице које сноси крајњу одговорност за кориштење приватног кључа који је повезан са сертификатом јавног кључа, док је субјекат особа чија је аутентикација извршена помоћу приватног кључа.

1.3.4. Треће стране

- Треће стране су ентитети, укључујући и физичка лица (особе), која користе сертификат и/или електронски потпис који се може провјерити у односу на јавни кључ наведен у сертификату субјекта;

- Прије него што се ослоне на информације које су дате у сертификату, треће стране се увијек морају позвати на Списак опозваних сертификата Сертификационог тијела Агенције или Протокол о електронској провјери сертификата како би се потврдила валидност сертификата који су добили.

1.3.5. Остали учесници

- Није примјењиво.

1.4. Употреба сертификата

1.4.1. Прихватљиво коришћење сертификата

Сертификати Сертификационог тијела Агенције могу се користити за:

- Апликације које захтијевају коришћење квалификованог сертификата у складу са Законом о електронским документима, електронској идентификацији и услугама од повјерења Босне и Херцеговине;
- Верификацију електронски потписаних докумената;
- Верификацију електронски издатих докумената за правна лица;
- Идентификовање носиоца сертификата;
- Безбједну комуникацију е-поштом;
- Шифровање и дешифровање докумената у електронском облику;

Напомена: Не чувати копију приватних кључева за дешифровање корисника за опоравак кључа. Одговорност корисника је да одржава безбједну копију приватних кључева за дешифровање.

- Друге намјене на захтјев корисника и у складу са Законом о електронским документима, електронској идентификацији и услугама од повјерења и другим релевантним законима у Босни и Херцеговини.

1.4.2. Забрана коришћење сертификата

- Сви сертификати које издаје сертификационо тијело Агенције користе се у складу са важећим законодавством Босне и Херцеговине.

1.5. Администрирање политике сертификације

1.5.1. Администрирање документа

- Сертификационом политиком Агенције руководи сама Агенција.

1.5.2. Контакт особа

Адреса:	Агенција за идентификациона документа евиденцију и размјену података Босне и Херцеговине- IDDEEA; Краља Петра I Карађорђевића 83А; Бања Лука
E-adresa:	eid@iddeea.gov.ba
Интернет:	https://www.iddeea.gov.ba

1.5.3. Особа која одређује погодност Изјаве о сертификационој пракси

- Није примјењиво.

1.5.4. Процедура одобравања Изјаве о сертификационој пракси

- Сертификациону политику Сертификационог тијела Агенције израђује и одржава Тијело за управљање Сертификационом политиком Агенције, а одобрава је генерални директор.

1.6. Дефиниције и скраћенице

Дефиниције:

Електронски потпис је скуп података у електронском облику који су придружени или су логички повезани са другим подацима у електронском облику, а користи га потписник за потписивање.

- **Потписник** је физичко лице које креира електронски потпис.
- **Информациони систем** је систем који се користи за прикупљање, слање, примање, чување или другу врсту обраде електронских података.
- **Подаци за креирање потписа** су јединствени подаци који се користе у процесу израде електронског потписа, као што су кодови или приватни криптографски кључеви.
- **Средства за креирање потписа** су конфигурисани програми или техничка опрема која се користи за израду електронског потписа.
- **Средства за формирање квалификованог потписа (смарт картица/токен) -** су средства која обезбјеђују јединствене, безбједне и повјерљиве податке који се односе на електронски потпис, спречавају могућност добивања података о електронском потпису у разумном року и путем оправданих средстава од података за провјеру електронског потписа, обезбјеђују заштиту од фалсификовања електронског потписа коришћењем тренутно доступне технологије и омогућавају потписнику да безбједно заштити податке у електронском потпису од неовлашћеног приступа.

Подаци за провјеру електронског потписа су јединствени подаци који се користе за провјеру електронског потписа, као што су кодови или јавни криптографски кључеви.

Средства за провјеру електронског потписа су конфигурисани софтвери или хардвери који се користе да би потврдили да је неки електронски потпис валидан.

Сертификат је сертификат у електронском облику који потврђује везу између података за провјеру електронског потписа и одговарајућег лица, субјекта сертификата и идентитета тог лица.

Квалификовани сертификат је сертификат који садржи име и државу пребивалишта, односно сједиште тијела, име, односно псеудоним субјекта, односно псеудоним информационог система који носи ознаку субјекта, податке за верификацију електронског потписа који се односе на податке о електронском потпису, почетак и престанак важења сертификата, идентификациони број сертификата, напредни електронски потпис органа и могућа ограничења у коришћењу сертификата.

Нормализовани сертификат је сертификат који има иста техничка својства и нуди исти ниво повјерљивости као и квалификовани сертификат, али без правних ограничења његове намјене.

Напредни електронски потпис је електронски потпис који испуњава сљедеће захтјеве:

a) на јединствен начин је повезан са потписником;

b) може идентификовати потписника;

c) формиран је коришћењем података за формирање електронског потписа који се користе под искључивом контролом потписника уз висок степен повјерљивости;

d) повезан је с подацима потписаним тако да се свака наредна промјена података може открити.

Квлификовани електронски потпис је напредни електронски потпис који се креира примјеном средства за креирање квалификованог електронског потписа, који је заснован на квалификованом сертификату електронског потписа.

Сертификационо тијело је свако физичко или правно лице које издаје сертификате или пружа друге услуге које су повезане са сертификатима, односно са електронским потписом.

Субјекат је свако физичко или правно лице које је идентификовано у сертификату као закупац приватног кључа који се односи на јавни кључ који је укључен у сертификат.

Уговарач/апликант је лице које подноси захтјев за издавање сертификата од сертификационог тијела у име једног или више субјеката. Уговарач/апликант може бити и субјекат, када се сертификат издаје појединцу за лично кориштење.

Трећа страна је лице које има оправдано повјерење у сертификат.

Кориснички налог рачунара је кориснички налог који означава скуп карактеристика које одређеној особи омогућавају приступ рачунарском систему. Сваки кориснички налог је јединствен за сваки рачунарски систем, што се реализује помоћу интерних функција рачунарског система. Основа за приступ корисничком налогу је пар корисничког имена и лозинке. Корисничко име је низ алфанумеричких знакова који се састоји од идентификационог имена корисника у датом рачунарском систему. Такво идентификационо име мора бити јединствено на нивоу рачунарског система. Лозинка је такође низ алфанумеричких знакова, који је познат искључиво власнику корисничког рачуна. Корисничка лозинка за оне рачунарске системе који захтевају висок ниво безбједности може се допунити или замијенити чип картицом.

Пар кључева за шифровање је пар симетричних кључева који се састоје од јавног кључа за шифровање и помоћног приватног кључа за дешифровање. Назива се још и повјерљиви пар кључева.

Приватни кључ за дешифровање. Види Пар кључева за шифровање.

Приватни кључ за потписивање. Види Пар кључева за шифровање

Јавни кључ за шифровање. Види Пар кључева за шифровање

Сертификат јавног кључа за шифровање је сертификат који садржи јавни кључ за шифровање.

Кључ за провјеру јавног потписа Види Пар кључева за шифровање.

- **Сертификат кључа за провјеру јавног потписа** је сертификат који садржи јавни кључ за потпис.
- **Пар кључева за потпис** је пар асиметричних кључева који се састоје од приватног кључа за потпис и помоћног јавног кључа за провјеру потписа.
- **QSCD (Смарт картица/токен)** је средство за израду квалификованог електронског потписа/печата у облику смарт картице/токена на којем се приватни кључеви могу чувати.
- **ХСМ (Хардверски сигурносни модул)** је физички уређај за безбједно чување дигиталних кључева.
- **Пружалац услуга повјерења** је физичко или правно лице које пружа једну или више услуга од повјерења, било као квалификовани или неквалификовани пружалац услуга од повјерења.

Квалификовани пружалац услуга од повјерења је пружалац услуга од повјерења који пружа једну или више квалификованих услуга од повјерења и коме надзорни орган додјељује статус квалификованог пружаоца услуга.

Скраћенице:

Списак скраћеница, које се користе у овом документу и у Политици дат је у сљедећој табели:

Скраћеница	**Објашњење**
ARL	Списак опозива овлаштења (Authority Revocation List)
CA	Сертификационо тијело (Certificate Authority)
CN	Име и презиме (Common Name - Name X.500)
CPS	Изјава о пракси сертификације (Certification Practice Statement)
ЦРЛ	Списак опозваних сертификата (Certificate Revocation List)
DC	Дигитални сертификат (Digital Certificate)
DN	Јединствени назив (Distinguished Name X.500)
EAL	Ниво процијењене сигурности (Evaluation Assurance Level)
EKU	Продужена употреба кључа (Extended Key Usage)
PA	Регистрационо тијело (Registration Authority)
ЛРА	Локално регистрационо тијело (Local Registration Authority)

ПРА	Примарно регистрационо тијело (Primary Registration Authority)
ПМА	Примарни управни орган (Primary Management Authority)
ОА	Оперативно тијело (Operation Authority)
FIPS 140-1	Федерални стандарди за обраду информација http://csrc.nist.gov/publications/fips/fips140-1/fips1401.pdf
PKCS #10	Стандарди криптографије јавног кључа (Public-Key Cryptography Standard #10)
ПКИ	Инфраструктура јавног кључа (Public Key Infrastructure)
PKIX	ПКИ заснован на X.509 (X.509 based PKI)
PKIX-CMP	PKIX Протоколи за управљање сертификатима (PKIX-Certificate Management Protocols), описани у RFC 4510
X.509	Стандарди сертификата описани у RFC 5280
QSCD	Средства за провјеру квалификованог електронског потписа, смарт картица/токен (Qualified Signature Creation Device) Средство за формирање квалификованог или напредног електронског потписа и квалификованог или напредног печата у складу са захтјевима eIDAS
ТСП	Пружалац услуга од повјерења (Trust Service Provider)

2. ОДГОВОРНОСТ ЗА ПУБЛИКОВАЊЕ И РЕПОЗИТОРИЈЕ

2.1. Репозиторији

- Сертификационо тијело Агенције објављује информације везане за сертификационе услуге у репозиторијима на сљедећим адресама:

Јавни веб-сајт: https://www.iddeea.gov.ba/PKI/CPS

2.2. Објављивање информација о сертификатима

Сертификационо тијело Агенције објављује:

- Списак опозваних сертификата (ЦРЛ)
- Статус сертификата путем Протокола за електронску провјеру сертификата
- Сертификате сертификационих тијела
- Политику сертификата и Изјаву о достави ПКИ
- Списак регистрационих тијела
- Корисничка упутства
- Сертификационо тијело Агенције обавјештава и оглашава о осталим услугама сертификације које се односе на јавно информисање.

2.3. Вријеме и учесталост објављивања

- Сертификати се објављују одмах по издавању, као што је наведено у одјељку 4.4. Спискови опозваних сертификата се објављују одмах након издавања, како је наведено у одјељку 4.9.7. Све информације се објављују одмах након што се измијене или постану доступне ТСП-у.

2.4. Контроле приступа репозиторијима

- Све јавне информације су доступне у документу који је само за читање без ограничења. Репозиторијуми су додатно заштићени од неовлашћених измјена.

3. ИДЕНТИФИКАЦИЈА И АУТЕНТИКАЦИЈА КОРИСНИКА

3.1.1. Врсте имена

- Поље са именом субјекта у сертификатима које је издало сертификационо тијело Агенције садржи аутентиковано име корисника како је дефинисано у табели у одјељку 3.1.4 Правила за тумачење различитих облика имена. Поље са именом субјекта у сертификату сертификационог тијела и у сертификатима издатим корисницима је у облику X.501 Distinguished Name (DN). Јединствено име је кодирано као Printable String или UTF8String и мора бити наведено у свим издатим сертификатима.

3.1.2. Имена треба да буду смислена

- Скуп карактеристика јединственог имена субјекта сертификата јединствено идентификује сваког власника сертификата и има значајне вриједности. Серијски број се наводи ради разликовања оних имена за која би поље субјекта иначе било идентично.

3.1.3. Анонимност или псеудонимност корисника

- Не може се примијенити.

3.1.4. Правила за тумачење различитих облика имена

- Поље са именом субјекта је дефинисано као X.501 type Name (x.500 Distinguished Name), у складу са RFC 5280.
- Поље „Субјекат” и поље „Издавалац” у сертификатима сертификационог тијела за сертификационо тијело Агенције су као што је наведено у одјељку **Error! Reference source not found.**.
- X.500 *Јединствено име* (Субјекат) у сертификатима које издаје сертификационо тијело Агенције има сљедећи облик за:
- Физичко лице

Компонента јединственог имена	Вриједност
Country (C =)	BA
(O =) За физичка лица на која се односи	IDDEEA
organizationIdentifier За физичка лица	IDDEEA
Име	Име
Презиме	Презиме
Име и презиме (CN=)	Име и презиме носиоца сертификата за физичка лица 1.6
Серијски број (serialnumber=)	Јединствени серијски број

3.1.5. Јединственост имена

- Сертификационо тијело Агенције у субјекту сертификата додјељује комбинацију карактеристика *јединственог имена*, како је дефинисано у одјељку 3.1.2 и одјељку 3.1.4, да би се осигурала недвосмисленост и јединственост имена.

3.1.6. Препознавање, аутентикација и улога заштитних знакова

- Сертификационо тијело Агенције ће се строго придржавати правила за додјељивање имена датих у складу са одјељцима *Типови имена и Смислена имена*. Корисницима је забрањено да траже она имена лица, која би изазвала кршење интелектуалних и имовинских права других корисника.

- Сертификационо тијело Агенције улаже оправдане напоре да ријеши спорове који могу настати око додјеле имена, нпр. ТСП може контактирати са подносиоцем захтјева и усагласити да поље *име и презиме* (CN) које се односи на субјекат треба измијенити, како би се јединствено име (DN) разликовало од већ постојећег јединственог имена.

- Сертификационо тијело Агенције, може према свом нахођењу, одбити, промијенити, поново издати или опозвати сертификате у вези са било којим јединственим именом.

3.2. Иницијална провјера идентитета

3.2.1. Метод за доказивање посједовања приватног кључа

- Доказ о посједовању приватног кључа корисника доставља се путем безбједне размјене између ТСП захтјева и ПКИ захтјева клијената коришћењем протокола о управљању сертификатима у складу са стандардом PKCS#10 Certification Request Syntax Standard.

- Када ТСП генерише приватне кључеве и сертификате, картица са кључевима и ПИН се шаљу субјекту који је поднио захтјев за издавање сертификата и на тај начин се обезбјеђује да корисници добију приватне кључеве.

3.2.2. Аутентикација идентитета појединца

- За сваког појединца (физичко лице), које жели да постане корисник Сертификационог тијела Агенције, обављаће се провјера идентитета лицем у лице. Лице које је одговорно за послове регистрације идентификује физичко лице које подноси захтјев за сертификат или услугу прегледајући његову важећу личну карту или пасош.

- Сертификационо тијело Агенције води евиденцију о средствима којима је потврђен идентитет лица.

3.2.3. Непровјерене информације о кориснику

Није примјењиво.

3.2.4. Критерији за међуоперацију

- Процедуре и праксе свих унакрсно сертификованих тијела морају бити једнаке процедурама и праксама Сертификационог тијела Агенције које су дефинисане у овој Политици сертификације. Сертификационо тијело Агенције дефинише детаљније услове зависно од случаја до случаја.

3.3. Идентификација и аутентикација захтјева за обнављање кључева

3.3.1. Идентификација и аутентикација приликом рутинске обнове кључева

- Рутинска обнова кључева врши се онда када истекне рок важења сертификата или приватног кључа.

- Аутентикација корисника који подносе захтјев за обнову сертификата обављена је како је наведено у одјељку 3.2.2 Аутентикација идентитета и одјељку 3.2.3 Аутентикација идентитета појединца.

3.3.2. Идентификација и аутентикација приликом обнове кључа након опозива

- Аутентикација корисника који подносе захтјев за обнову кључева обављена је како је наведено у одјељку 3.2.2 Аутентикација идентитета и одјељку 3.2.3 Аутентикација идентитета појединца.

3.4. Идентификација и аутентикација приликом подношења захтјева за опозив

- Захтјев за опозив корисник или носилац сертификата може поднијети позивом на контакт телефон ТСП-а и идентификацијом са ПИН-ом/лозинком дефинисаном током процеса регистрације, лично у просторијама регистрационог тијела или дигитално потписаним захтјевом, који се потписује приватним кључем потписа лица које тражи опозив.

- Аутентикација овлашћених лица ТСП-а која траже опозив путем електронске комуникације обавља се на основу дигиталног потписа, чак и онда када се сумња да је коришћени приватни кључ за потписивање компромитован.

- У супротном, аутентикација овлашћених лица обавља се на основу информација садржаних у досјеу корисника или како је наведено у одјељку 3.2.2 Аутентикација идентитета појединца.

4. ОПЕРАТИВНИ ЗАХТЈЕВИ У ВЕЗИ ЖИВОТНОГ ЦИКЛУСА СЕРТИФИКАТА

4.1. Захтјев за добијање сертификата

4.1.1. Ко може предати захтјев за добијање сертификата

- Сертификациони захтјев за регистрацију јавног сертификата може поднијети:
- Свака особа (физичко лице) која испуњава услове наведене у Захтјеву за регистрацију дигиталног сертификата, Политици сертификације Сертификационог тијела Агенције и пратећим уговорима између ТСП-а и крајњег корисника.

4.1.2. Процес уписа и одговорности

- Сертификационо тијело Агенције издаје сертификате само након потврде идентитета корисника и успјешног завршетка процеса регистрације. Главни кораци процеса уписа сертификата су:
    - Корисник предаје потписан захтјев за регистрацију дигиталног сертификата и прилаже важећи идентификациони документ.
    - Корисник је сагласан са Политиком сертификације Сертификационог тијела Агенције и својим обавезама по потписивању Уговора са крајњим корисником.
    - Захтјев за регистрацију дигиталног сертификата одобрава регистрационо тијело Сертификационог тијела Агенције.
    - Регистрационо тијело подноси захтјев за регистрацију дигиталног сертификата путем одговарајуће апликације за регистрацију или директно у Оперативном тијелу Агенције.
    - Оперативно тијело Агенције креира корисника са одговарајућим профилом сертификата и генерише активационе кодове који се састоје од регистрационог броја и ауторизационог кода. Ако се захтјев шаље путем апликације, генерисање кода је аутоматско или ручно. Оба активациона кода су потребна крајњем кориснику да затражи сертификат од сертификационог тијела или ТЦП РА када кључеве или сертификате припрема Агенција на смарт картици/токену.

Уколико кључеве и сертификате припреми ТСП на смарт картици/токену, ПИН и ПУК се шаљу кориснику е-поштом и/или СМС-ом; достављају се регистрационом тијелу у запечаћеној коверти коју преузима лично корисник или се шаље на регистровану е-адресу.

- Активациони кодови за упис сертификата шаљу се носиоцу сертификата:
    - Регистрациони број се шаље кориснику на е-адресу која је наведена у захтјеву за регистрацију дигиталног сертификата.
    - Регистрациони број се шаље е-поштом претплатнику на е-адресу наведену у обрасцу захтјева за регистрацију дигиталног сертификата путем СМС-а
    - Корисник употребљава активациони код користећи корисничке апликације коју је обезбиједило сертификационо тијело Агенције или путем интернет претраживача. Списак подржаних клијентских апликација и интернет претраживача објављен је заједно са корисничким упутством на веб-сајту Сертификационог тијела Агенције који је наведен у одјељку 2.1 Репозиторији.

4.2. Обрада захтјева за добивање сертификата

4.2.1. Обављање функција идентификације и аутентикације

- Сертификационо тијело Агенције обавља функције идентификације и аутентикације на начин дефинисан у одјељку 3.2.2 Аутентикација идентитета појединца.

4.2.2. Одобравање или одбијање захтјева за сертификацију

- Захтјев за регистрацију сертификата код Сертификационог тијела Агенције биће одобрен само уколико су испуњени сви наведени услови:
  - Корисник подноси захтјев за регистрацију дигиталног сертификата уз успјешну идентификацију и аутентикацију у складу са одјељком 3.2;
  - Корисник је овлашћен на одговарајући начин, уколико дјелује у нечије име (правног лица);
  - Образац дигиталног сертификата, достављена идентификациона документација и овлашћења су успјешно верификовани;
  - Корисник је потписао одговарајући уговор са Сертификационим тијелом Агенције.
- У случају да било који од наведених критерија није испуњен, или постоји основана сумња да подносилац захтјева крши одредбе овог документа, Уговора са крајњим корисником или важећег законодавства, службеник за регистрацију Сертификационог тијела Агенције одбија захтјев за сертификацију. Агенција задржава право да одбије било који захтјев за сертификацију без навођења разлога за одбијање.

4.2.3. Вријеме потребно за обраду захтјева за сертификацију

- Образац захтјева за сертификацију и идентификациони документ се провјеравају и обрађују у присуству подносиоца захтјева у просторијама регистрационог тијела Сертификационог тијела Агенције.
- Поднесени захтјев се даље обрађује у року од 30 дана.

4.3. Издавање сертификата

4.3.1. Активности ТСП-а током издавања сертификата

- систем за издавање сертификата Сертификационог тијела Агенције по пријему захтјева за сертификацију (PKCS#10):
- провјерава ваљаност активацијских кодова који се налазе у примљеним подацима;
- провјерава да ли корисник посједује приватни кључ повезан са јавним кључем који се шаље на сертификацију, као што је предвиђено у одјељку 3.2.1 Метод за доказивање посједовања приватног кључа;
- провјерава да ли сертификат захтијева усклађеност са техничком спецификацијом PKCS#10;
- издаје тражени сертификат, уколико је испуњено све претходно наведено.

4.3.2. Обавјештавање корисника о издавању сертификата

- Апликација Сертификационог тијела Агенције ће одмах уручити сертификат подносиоцу захтјева, тако да нема потребе за додатним обавјештавањем.
- За сертификате који се издају путем смарт картице/токена, кључ и сертификате припрема ТСП на смарт картици/токену, корисник се обавјештава током процеса достављања.

4.4. Прихватање сертификата

4.4.1. Поступак којим се прихвата сертификат

- Процедура уписивања сертификата зависи од врсте сертификата:
- Смарт картица/токен се доставља у затвореној коверти кориснику лично или препорученом поштом на адресу корисника ако се ради о физичком лицу; док се за правна лица доставља на адресу правног лица или се лично преузима;

- Сертификате који се не издају на смарт картици/токену носилац сертификата уноси кроз апликацију интернет претраживача.

- За сертификате који се не издају на смарт картици/токену:

- Упутство за унос сертификата може се пронаћи на веб-сајту Сертификационог тијела Агенције https://www.iddeea.gov.ba/PKI/CPS. Корисник ће, такође, добити упутство путем е-поште када добије регистрациони број. Сама упутства су подложна промјенама у складу са актуелним промјенама у оквиру ПКИ и нису саставни дио ове Политике. За успјешан упис сертификата релевантна су посљедња објављена упутства.

- Корисник може уписати сертификат само са важећим активационим подацима: регистрационим бројем и ауторизационим кодом. Вијек трајања података за активацију је ограничен на 30 дана. По истеку активационих података, потребно је поновити поступак регистрације.

- У случају неуспјешног процеса уписа, носилац сертификата пријављује проблем регистрационом тијелу (види контакт информације за регистрационо тијело у одјељку 1.5.2 Контакт особа).

- Подносилац захтјева добива све сертификате током електронског процеса уписа сертификата или на смарт картици/токену. Није потребна додатна потврда о прихватању сертификата.

4.4.2. Обавјештење других лица о издавању сертификата које издаје ТСП

- Сертификационо тијело Агенције не обавјештава друга лица.

4.5. Коришћење пара кључева и сертификата

4.5.1. Коришћење корисничког приватног кључа и сертификата

- Сертификационо тијело Агенције издаје сертификате који подржавају неколико коришћења кључа. Та подршка је обезбијеђена укључивањем одговарајућих екстензија за коришћење кључа.

- Корисници ће користити сертификате у складу с екстензијама сертификата keyUsage и extKeyUsage X.509 и у сврхе дефинисане у одјељку 1.4.1. Одговарајућа употреба сертификата. Корисници морају чувати свој приватни кључ на сигурном и предузети мјере предострожности како би спријечили компромитовање кључа и неовлашћено коришћење.

- По истеку важења сертификата или опозиву сертификата, пратећи приватни кључ се више не може користити.

4.5.2. Коришћење јавног кључа и сертификата треће стране

Трећа страна ће ограничити коришћење јавних кључева који се налазе у потврдама које је издало сертификационо тијело Агенције за одговарајућу употребу како је наведено у одјељку 1.4.1 Прихватљиво коришћење сертификата. Трећа страна је одговорна и да:

- буде свјесна ограничења сертификата и одговорности ТСП-а као што је детаљно наведено у овој Политици.

- обезбиједи да сертификат не буде опозван електронским приступом било којем и свим важећим Списковима опозваних сертификата (ЦРЛ списак) или Протоколу за електронску провјеру сертификата.

- одмах обавијести ТСП о свакој сумњи или познатој злоупотреби било ког сертификата који је ТСП издао.

4.6. Обнављање сертификата (без генерисања новог кључа)

- Обнављање сертификата је процес у којем ТСП издаје нови сертификат за истог корисника. Сертификационо тијело Агенције не дозвољава нити обезбјеђује обнављање сертификата.

4.6.1. Услови за обнављање сертификата

- Није примјењиво, као што је наведено у одјељку 4.6. Обнављање сертификата (без генерисања новог кључа).

4.6.2. Ко може тражити обнављање захтјева

- Није примјењиво, као што је наведено у одјељку 4.6. Обнављање сертификата (без генерисања новог кључа).

4.6.3. Обрада захтјева за обнављање сертификационог кључа

- Није примјењиво, као што је наведено у одјељку 4.6. Обнављање сертификата (без генерисања новог кључа).

4.6.4. Обавјештавање корисника о новом издавању сертификата

- Није примјењиво, као што је наведено у одјељку 4.6. Обнављање сертификата (без генерисања новог кључа).

4.6.5. Поступак који представља прихватање сертификата са обновљеним кључем

- Није примјењиво, као што је наведено у одјељку 4.6. Обнављање сертификата (без генерисања новог кључа).

4.6.6. Објављивање обновљеног сертификата које обавља ТСП

- Није примјењиво, као што је наведено у одјељку 4.6. Обнављање сертификата (без генерисања новог кључа).

4.6.7. Обавјештавање других лица о издавању сертификата које обавља ТСП

- Није примјењиво, као што је наведено у одјељку 4.6. Обнављање сертификата (без генерисања новог кључа).

4.7. Обнављање сертификата генерисањем новог кључа (обнављање генерисањем новог пара кључева)

- Обнављање сертификата генерисањем новог кључа је процес у коме ТСП издаје кориснику нови сертификат. Нови сертификат садржи исте информације о субјекту као и стари сертификат и нове јавне кључеве.

4.7.1. Услови за обнову сертификата генерисањем новог кључа

Обнављање кључа сертификата обавља се:

- по опозиву сертификата;
- по истеку рока важења или непосредно прије истека рока важења.

4.7.2. Ко може тражити сертификацију са новим јавним кључем

Корисник, носилац сертификата или овлашћени представник који је тражио првобитно издавање сертификата може тражити обнављање сертификата генерисањем новог кључа.

4.7.3. Обрада захтјева за обнављање сертификата генерисањем новог кључа

Обнављање сертификата генерисањем новог кључа врши се на исти начин као и првобитно издавање сертификата.

4.7.4. Обавјештавање корисника о издавању новог сертификата

Као што је наведено у одјељку 4.3.2 Обавјештавање корисника о издавању сертификата које обавља ТСП.

4.7.5. Поступак прихватања сертификата са новим кључем

- Као што је наведено у одјељку 4.4.1 Поступак прихватања сертификата.

4.7.6. Објављивање сертификата са новим кључем које обавља ТСП

- Као што је наведено у одјељку 4.4.2 Објављивање сертификата које обавља ТСП.

4.7.7. Обавјештавање других лица о издавању сертификата које обавља ТСП

- Као што је наведено у одјељку 4.4.3 Обавјештавање других лица о издавању сертификата које обавља ТСП.

4.8. Измјене сертификата

- Измјена сертификата је процедура која корисницима олакшава подношење захтјева за издавање сертификата са измијењеним подацима. Измјена сертификата подразумијева обнављање кључева сертификата и обрађује се као и првобитни захтјев.

4.8.1. Услови за измјене сертификата

- Корисник може тражити измјене у сертификату уколико се информације о субјекту, као што су име или е-адреса промијене.

4.8.2. Ко може тражити измјене сертификата

- Измјену сертификата може тражити корисник, носилац сертификата или субјекат који је тражио првобитно издавање сертификата.

4.8.3. Обрада захтјева за измјену сертификата

- Захтјеви за измјену сертификата обрађују се на исти начин као и првобитни захтјеви за издавање сертификата.

4.8.4. Обавјештавање корисника о издавању новог сертификата

- Као што је наведено у одјељку 4.3.2 Обавјештавање корисника о издавању сертификата које обавља ТСП.

4.8.5. Поступак прихватања измијењеног сертификата

- Као што је наведено у одјељку 4.4.1. Поступак прихватања сертификата. Објављивање измијењеног сертификата обавља ЦА.

4.8.6. Објављивање измијењеног сертификата које обавља ТСП

- Као што је наведено у одјељку 4.4.2. Објављивање сертификата које обавља ТСП.

4.8.7. Обавјештавање других лица о издавању сертификата које обавља ТСП

- Као што је наведено у одјељку 4.4.3. Обавјештавање других лица о издавању сертификата које обавља ТСП.

4.9. Опозив и суспензија сертификата

4.9.1. Услови за опозив

Опозив сертификата се може тражити:

- ако то захтијева корисник или носилац сертификата;
- ако ТСП потврди да је носилац сертификата преминуо или је изгубио способност за пословање или ако правно лице престане да постоји или ако су се околности које су у значајној мјери утицале на валидност сертификата промијениле;
- уколико је познато или се сумња да је нетачна било која информација која се налази у сертификату;
- уколико је приватни кључ који је повезан са сертификатом компромитован или се сумња да је компромитован.
- када је било који активациони податак, као што су лозинка или ПИН који се користе за заштиту приватног кључа, компромитован или се сумња да је компромитован;
- уколико ТСП утврди да сертификат није прописно издат у складу са Политиком сертификације Сертификационог тијела Агенције;
- када корисник или носилац сертификата прекрши одредбе Политике сертификације Сертификационог тијела Агенције или важећег закона (неиспуњавање обавеза корисника);
- из било ког другог разлога наведеног у Закону о електронским документима, електронској идентификацији и услугама од повјерења.
- ако Тијело за управљање политиком Сертификационог тијела Агенције сматра да је то неопходно.

4.9.2. Ко може тражити опозив

Опозив сертификата може тражити:

- Корисник (нпр. правно лице) или субјекат (носилац сертификата);
- Овлашћени представник који је поднио захтјев за издавање сертификата;
- Сертификационо тијело Агенције;
- Надлежни суд.

4.9.3. Процедура за подношење захтјева за опозив

Носилац сертификата може тражити опозив сертификата на сљедећи начин:

- Путем електронски потписаног захтјева за опозив послатог е-поштом;
- Личним контактирањем са канцеларијом регистрационог тијела Сертификационог тијела Агенције; или
- Телефонским позивом, када особа мора знати тајну ријеч/лозинку/ПИН који/а је унесен/а у образац захтјева за регистрацију дигиталног сертификата;

  Захтјев за опозив сертификата наведен је у одјељку 3.4 Идентификација и аутентикација захтјева за опозив.

Опозив због измјене података у самом сертификату

1. Захтјев за опозив:

   - Корисник шаље захтјев регистрационом тијелу Сертификационог тијела Агенције лично или путем е-поште. Важећим захтјевом се сматра онај захтјев који је потписан помоћу кључа који је издало сертификационо тијело Агенције.

- Корисник се идентификује (лично) и подноси захтјев (образац) за опозив сертификата.
- Регистрационо тијело Сертификационог тијела Агенције провјерава и одобрава опозив.

2. Регистрационо тијело Сертификационог тијела Агенције покреће опозив сертификата кроз апликацију, наводећи разлоге за опозив или шаљу захтјев за опозив оперативном тијелу Сертификационог тијела Агенције да изврши опозив наводећи и разлоге опозива.

3. За издавање нових кључева, корисници се аутентикују како је наведено у одјељку 3.2.2. Аутентикација идентитета и одјељку 3.2.3 Аутентикација идентитета појединца.

Опозив због компромитованог приватног кључа

1. Захтјев за опозив:

   - Корисник шаље захтјев регистрационом тијелу Сертификационог тијела Агенције путем е-поште или лично.
   - Телефонским позивом, када особа мора знати тајну ријеч/лозинку/ПИН који је унесен у образац захтјева за регистрацију дигиталног сертификата.
   - Корисник се идентификује (лично) и подноси захтјев (образац) за опозив сертификата.
   - Примарно регистрационо тијело Сертификационог тијела Агенције провјерава и одобрава опозив.

2. Примарно регистрационо тијело Сертификационог тијела Агенције покреће опозив сертификата кроз апликацију тако што уочи компромитујући статус или шаље захтјев за опозив оперативном тијелу Сертификационог тијела Агенције да изврши опозив уочавајући компромитујући статус.

3. У случају захтјева за издавање нових кључева, аутентикација корисника се обавља као што је наведено у одјељку 3.2.2 Аутентикација идентитета појединца.

Опозив сертификата због неиспуњавања обавеза корисника

Уколико корисник не испуни своје обавезе и дужности у складу са овом политиком и уговором закљученим са Агенцијом њен/његов сертификат ће бити опозван, при чему:

1. Регистарционо тијело провјерава статус дигиталног потписа корисника код ТСП-а
2. Запослени у оперативном тијелу Сертификационог тијела Агенције врше опозив сертификата наводећи разлоге за то.

4.9.4. Одложени опозив сертификата

- Субјекат који је сазнао за околности које захтијевају опозив сертификата дужан је да затражи опозив у најкраћем могућем року, без непотребног одлагања.

- Сертификационо тијело Агенције може извршити опозив сертификата због непоштовања обавеза корисника одмах након истека рока у којем је корисник требао да испуни своје обавезе.

4.9.5. Рок у којем ЦА мора завршити обраду захтјева за опозив

- У другим случајевима опозива сертификата, рок за опозив сертификата не би требало да буде дужи од 24 сата од пријема захтјева.

4.9.6. Захтјев за провјеру опозива за треће стране

- Треће стране прије коришћења сваког сертификата који је издало сертификационо тијело Агенције провјеравају да ли се сертификат налази на Списку опозваних сертификата Сертификационог тијела Агенције или обављају провјеру пуем Протокола

о електронској провјери сертификата. Уколико се не може извршити ваљана провјера опозива, због квара система или губитка сервиса, не треба прихватити ниједан сертификат Сертификационог тијела Агенције.

- Трећа страна провјерава одговор са Списка опозваних сертификата или путем Протокола за електронску провјеру сертификата тако што провјерава свој дигитални потпис са повезаним ТСП сертификатом и да ли је истекао.

4.9.7. Учесталост објављивања списка опозваних сертификата (ако је примјењиво)

- Сертификационо тијело Агенције редовно сваких 24 часа објављује нови списак опозваних сертификата. Рок важења списка опозваних сертификата је до 48 часова. Сертификационо тијело Агенције ажурира спискове опозваних сертификата одмах или чим је то могуће након што се обради важећи захтјев за опозив сертификата. Максималан временски период између коначног потврђивања опозива сертификата, или његове суспензије, до стварне измјене информације о статусу сертификата која је доступна трећим странама може бити до 60 минута.

4.9.8. Максимално кашњење списка опозваних сертификата (ако је примјењиво)

- Није одређено. (Види одјељак 4.9.7)

4.9.9. Доступност електронског опозива/провјере статуса

- ТСП пружа услугу Протокол за електронску провјеру сертификата. Локација услуге је назначена екстензијом authorityInfoAccess која се налази на сваком сертификату.

4.9.10. Услови за електронску провјеру опозива

- Види одјељак 4.9.6.

4.9.11. Остали начини оглашавања опозива

- Није примјењиво.

4.9.12. Посебни услови везани за компромитовање кључа

- Никакви посебни услови се не траже у случају компромитовања кључа носиоца сертификата.

4.9.13. Суспензија сертификата

- Суспензија сертификата се може тражити у случају да носилац сертификата изостаје дужи временски период, нпр. породиљско одсуство. Сертификационо тијело Агенције може суспендовати сертификат носиоца сертификата за вријеме обраде захтјева за опозив сертификата.

- Суспендовани сертификати се објављују на Списку опозваних сертификата за вријеме суспензије.

4.9.14. Ко може тражити суспензију

- Суспензију сертификата може тражити:
- Корисник или субјекат (носилац сертификата)
- Овлашћени представник који је тражио издавање сертификата
- Регистрационо тијело Сертификационог тијела Агенције (РА)
- Чланови Сертификационог тијела Агенције.

4.9.15. Процедура за подношење захтјева за суспензију

- Као што је описано у одјељку 4.9.3 Процедуре за подношење захтјева за суспензију.

4.9.16. Ограничење периода суспензије

- Период суспензије није ограничен.

4.10. Сервиси провјере статуса сертификата

4.10.1. Оперативне карактеристике

- Статус сертификата се објављује коришћењем X.509 Certificate Revocation List путем протокола за електронску провјеру сертификата (ОЦСП).
- ЦРЛ списак се објављује кроз ЛДАП директорij и веб-сајт. Тачне локације LDAP i http URLs се објављују коришћењем екстензије X.509 CRL Distribution Points..
- Доступност услуге протокола за електронску провјеру сертификата је назначена као URL у сертификату.
- ЦРЛ профил и сервисни протокол за електронску провјеру сертификата (ОЦСП) описани су у одјељцима 7.2. и 7.3.

4.10.2. Доступност услуга

- Статус сертификата сертификационог тијела Агенције доступан је 24 часа дневно, 7 дана у седмици, са максималним годишњим непланираним застојима од седам (7) дана годишње.

4.10.3. Опционе карактеристике

- Није примјењиво.

4.11. Престанак важења сертификата

- Сертификат престаје да важи по истеку рока важења или након опозива сертификата. Сертификационо тијело Агенције чува документацију и податке из сертификата најмање десет (10) година по истеку или опозиву сертификата.

4.12. Депоновање и опоравак кључева

- Сертификационо тијело Агенције не подржава депоновање и опоравак кључева.

4.12.1. Политика и пракса депоновања и опоравка кључева

- Није примјењиво.

4.12.2. Политика и пракса енкапсулације и опоравка сесијског кључа

- Није примјењиво.

5. УПРАВНЕ, ОПЕРАТИВНЕ И ФИЗИЧКЕ БЕЗБЈЕДНОСНЕ КОНТРОЛЕ

5.1. Физичке контроле

5.1.1. Локација објекта и конструкција

- Техничка средства сертификационог тијела Агенције (мрежни рачунарски системи, терминали за носиоце, и информациони ресурси) се налазе у намјенским просторијама са сталним надзором у безбједној згради (објекту).
- Системске компоненте и оперативни дио Сертификационог тијела Агенције се налазе унутар физички заштићеног окружења како би се спријечила неовлаштена употреба, приступ или откривање осјетљивих информација. Контроле физичке безбједности се проводе у складу са најбољим важећим праксама физичке безбједности. Заштитне мјере подразумијевају:
- Приступ је ограничен само за запослене у сертификационом тијелу Агенције;
- Сви остали приступи су под пратњом и сваки приступ се евидентира;
- Запослени на одржавању и сервису су под видео надзором током својих посјета;
- Сигурне електронске браве и приступни систем;
- Надгледање 24 сата,7 дана у недјељи од стране чувара на лицу места, и видео надзор из центра за видео надзор у згради.

5.1.2. Физички приступ

- Само овлаштени запослени у сертификационом тијелу Агенције, у складу са њиховим дужностима, имају приступ одређеним дијеловима инфраструктуре ертификационо тијело Агенције. Сваки приступ просторијама сертификационог тијела Агенције се електронски заводи и уноси у електронски дневник приступа просторијама.

5.1.3. Електрично напајање и климатизација

- Информациони центар Агенције је опремљен са климатизацијом која регулише топлоту, влагу а све критичне компоненте су повезане на непрекидно електрично напајање.

5.1.4. Опасност од поплаве

- Унутар просторија сертификационог тијела Агенције нема водоводних инсталација. Подузете су све техничке мјере за заштиту од водоводних инсталација у окружењу.

5.1.5. Превенција и заштита од пожара

- Просторије сертификационог тијела Агенције су заштићене системом за рано откривање пожара, аутоматским пожарним алармом и системом за гашење.

5.1.6. Чување медија

- Сви рачунарски медији који садрже податке сертификационог тијела Агенције, укључујући медиј са сигурносном копијом података, чувају се у ватроотпорним ормарима, од којих се један налази унутар сертификационог тијела Агенције, а други на удаљеној безбједној локацији.

5.1.7. Одлагање отпада

- Папирна документа и електронски медији се уништавају прије одлагања на начин који осигурава да се информације не могу репродуковати. ТСП задржава све хардверске компоненте које се не могу сервисирати ради њиховог сигурног одлагања.

5.1.8. Резервне копије на другој локацији

- Сертификационо тијело Агенције чува медије података на удаљеној безбједној локацији. Медији се чувају на удаљеној безбједној локацији заштићеној од ванјских утицаја и са контролисаним приступом, који има висок ниво заштите, односно принцип банкарског сефа. Приступ сефу је ограничен на двије овлаштене особе.

5.2. Процедуралне контроле

5.2.1. Повјерљиве улоге

- Зависно од њихове улоге, запослени у сертификационом тијелу Агенције могу имати налог на хост рачунару ТСП-а, апликацији ТСП-а или на обоје. Апликација ТСП-а коју користи сертификационо тијело Агенције имплементира одређени број повјерљивих улога које су додјељене запосленима ТСП-а у складу са њиховим надлежностима. Корисничким правима налога оперативног система на хост рачунару ТСП-а се ограничава приступ запосленима сертификационог тијела Агенције само на оно што им је потребно како би извршавали своје задатке.

- Распоред улога ТСП-а је:

Одговорни запосленици	Ниво приступа у оперативном систему	Ниво приступа у апликацији ТСП-а
Главни корисник сертификационог тијела	Да	Да
Службеник за безбједност сертификационог тијела	Не	Да
Администратор сертификационог тијела	Не	Да
Администратор директорија	Не	Не
Службеници за регистрацију	Не	Да
Службеници у регистрационом тијелу	Не	Не
Правни савјетник	Не	Не

- Различити нивои физичке заштите и контроле приступа системима на основу улога у апликацији ТСП-а и корисничких права у систему се користе за раздвајање дужности.

- Повјерљиве улоге су

Улога	Дужности
Главни корисник сертификационог тијела	• Одобравати почетну ТСП апликацију и конфигурацију хардверског безбједносног модула и њихово одржавање • Покретати и заустављати услуге ТСП апликације • Одређивати прве службенике за безбједност инфраструктуре јавног кључа (PKI) • Обновитии налог PKI службеницима за безбједност када забораве шифру • Обновити ТСП административне услуге у случају да се оштети профил • Покренути процес замјене хардверско сигурносног модула • Обновити смарт картице оператора хардверско сигурносног модула • Обновити и поново шифровати ТСП базу података

Службеник за безбједност сертификационог тијела	• Управљати корисничким налозима других службеника за безбједност ПКИ и администратора ПКИ • Управљати корисничким налозима • Управаљати опоравком кључева за кориснике • Обрађивати ревизијске записе • Постављати и мијењати безбједносну политику ТСП апликације • Управљати профилима ТСП апликацијских сертификата • Вршити унакрсно сертификовање са ванјским сертификованим тијелима • Припремати извјештаје
Администратор сертификационог тијела	• Управљати корисничким налозима • Управљати сертификатима • Припремати извјештаје
Администратор директорија	• Додавати и брисати кориснике у директорију • Подешавати именик
Службеници за регистрацију	Погледати Одјељак 1.3.2
Службеници у регистрационом тијелу	Погледати Одјељак 1.3.2

5.2.2. Број особа које се захтјевају по сваком задатку

Двије (2) особе са одговарајућим повјерљивим улогама су потребне за извршавање сљедећих задатака:

- Опозивање кључа ТСП-а;
- Припремање политика кључа и сертификације;
- Креирање корисничких налога са улогом ЦА службеника за безбједност или ЦА администратора;
- Ажурирање Агенције приватног кључа сертификационог тијела;
- Ресетовање шифре на налозима главних корисника сертификационог тијела;
- Унакрсно сертификовање са ванјским сертификационим тијелима.

Једна особа може извршавати све остале задатке. Све активности које извршавају носиоци повјерљивих ТСП улога се записују и прегледају.

5.2.3. Идентификација и аутентикација за сваку улогу

- Запослени у PKI са повјерљивом ПСТ улогом подлијежу безбиједносној провјери прије него што буду именовани да раде као чланови оперативног тијела сертификационог тијела Агенције.
- Оперативно тијело сертификационог тијела Агенције ће се провјерити у складу са правилима наведеним у овој Политици прије него што им се додијели било која од сљедећих привилегија:
- Додавање уноса на одговарајућу приступну листу за улазак у заштићене просторије сертификационог тијела Агенције (безбједносна и оперативна зона)

- Добијање потребног сертификата за извршавање додјељене повјерљиве улоге
- Добијање корисничког налога у оперативном систему
- Добијање смарт картице / токена
- Кориснички налози оперативног система и апликације, као и сертификати су креирани појединачно за сваку одговорну особу
- Забрањена је свакодневна употреба налога или сертификата међу запосленима сертификационог тијела Агенције. Запослени су ограничени на активности овлаштене за дату улогу кроз контролу постављену апликацијом, оперативним системом и процедурама сертификационог тијела Агенције.
- Запослени у сертификационом тијелу Агенције користе само смарт картице/токене како би испунили дужности које су им додијељене у оквиру њихових улога.

5.2.4. Улоге које захтијевају раздвајање дужности

- Администратор оперативног система има потребна права да инсталира, конфигурише и одржава хардвер и софтвер ТСП хост рачунара.
- Приликом додјеле корисничких улога и права физичког приступа строго се поштује принцип подјеле дужности, тако да једна особа не може користити криптографске материјале за извршавање безбједносно осјетљивих операција, али је увијек потребно осигурати присуство најмање двије особе.

5.3. Кадровске контроле

- Одговорне особе у сертификационом тијелу Агенције су запослене на неодређен или одређен период, ангажоване на основу уговора који утврђује њихове радне обавезе. Они требају бити адекватно квалификовани за извршавање својих радних обавеза.
- Запослени у Регистрационом тијелу су запослени на неодређен или одређен период. Они требају бити адекватно квалификовани за извршавање својих радних обавеза.
- Запослени у сертификационом тијелу Агенције и Регистрационом тијелу су уговором везани да не објављују нити откривају повјерљиве информације везане за безбједност сертификационог тијела Агенције или информације о корисницима.
- У складу са уговором, корисници су упознати са безбједносним одредбама које требају примјењивати како би заштитили своје рачунаре и уређаје за шифровање, као и са овом политиком по којој су им издати сертификати.

5.3.1. Квалификације, искуство и сигурносне провјере

- Праксе запошљавања у сертификационом тијелу Агенције подразумијевају разматрање квалификационих захтјева за сваку позицију, претходне дужности потенцијалних кандидата и број година искуства на сличним позицијама.

5.3.2. Процедуре провјере биографије

- ТСП прати провјере запослених и политику наведену у Одјељку 6.1.2 Провјера запослених и ISO/IEC 27001 захтјеви.

5.3.3. Захтјеви за обуке

- Сертификационо тијело Агенције обезбјеђује обуке за своје запослене.
- За одговорне особе у сертификационом тијелу Агенције, под обукама се подразумијевају процедуре за заштиту система и података, специфичне обуке за њихове улоге и дужности, обуке за коришћење апликације сертификационог тијела Агенције и обуке за преузимање процедура за опоравак од катастрофа и процедура континуираног пословања.

- За запослене у регистрационом тијелу, под обукама се подразумијевају процедуре за заштиту система и података и специфичне обуке за њихове улоге и дужности.

5.3.4. Фреквенција и захтјеви за поновну обуку

- Обуке за запослене у сертификационом тијелу Агенције се организују у складу са реалним потребама и технолошким измјенама.

5.3.5. Фреквенција и редослијед ротације послова

- Ротација послова се не примјењује.

5.3.6. Казне за неовлаштене радње

- У случају сумње да је извршена неовлаштена активност или је неовлаштену активност заиста извршила особа која обавља послове везане за рад сертификационог тијела Агенције или регистрационог тијела, сертификационо тијело Агенције ће му онемогућити даљи приступ техничким уређајима (хардвер и софтвер).

- Сертификационо тијело Агенције ће одузети или опозвати све сертификате издате тој особи.

- Неовлаштене активности се пријављују надлежним државним органима и институцијама, у складу са важећим законским, подзаконским и интерним актима.

5.3.7. Услови за спољне сараднике

- Сертификационо тијело Агенције нема праксу запошљавања спољних сарадника за осјетљиве послове. Али ако су такви сарадници ангажовани, проводе се одговарајуће провјере. Сви извршиоци морају потписати уговор о неоткривању података у складу са интерним процедурама сертификационог тијела Агенције.

5.3.8. Документација која се доставља запосленима

- Одговорне особе у сертификационом тијелу Агенције имају приступ документацији ТСП-а, укључујући хардвер, софтвер, приручнике за ТСП апликацију, оперативне процедуре, безбједносне и противпожарне процедуре, процедуре контроле приступа и ову Политику.

5.4. Процедуре ревизијских записа

5.4.1. Типови забиљежених догађаја

- У сертификационом тијелу Агенције се сљедећи догађаји записују аутоматски или ручно за потребе ревизије:

  - Догађаји везани за корисничке кључеве и сертификате: регистрација, издавање, опозив, суспензија;

  - Догађаји везани за ТСП кључеве;

  - Догађаји везани за администрацију, чување података и јавни директориј;

  - Догађаји оперативних система и хардверске опреме;

  - Догађаји који се односе на физички приступ ТСП-у.

- Већина електронских записа садржи датум и вријеме сваког догађаја и идентитет субјекта који га је генерисао. Сви уноси у евиденције физичке провјере идентификовани су датумом и временом.

- Записи се прикупљају и слажу у Оперативном тијелу сертификационог тијела Агенције.

5.4.2. Фреквенција процесирања записа

- Записи се провјеравају на дневном нивоу.
- Ревизија подразумијева:
  - Прикупљање свих записа од задње обраде записа,
  - Преглед уноса ревизијских записа,
  - Преглед прикупљених записа.

Потребно је анализирати и објавити све релевантне догађаје у циљу рјешавања или ограничавања ескалације проблема.
Све записе којима је истекао рок трајања треба премјестити, очистити или уништити.

5.4.3. Период чувања ревизијских записа

- У складу са важећим прописима, ревизијски записи се чувају најмање 10 година. .

5.4.4. Заштита ревизијских записа

- Приступ главном (хост) рачунарском систему који садржи датотеке ревизијских записа дозвољен је само овлаштеним лицима, уз комбинацију физичких контрола и контрола рачунарске безбједности. Рачунарски систем, резервни кертрији ревизијских записа и физички ревизијски записи чувају се у зони високе безбједности Оперативног тијела сертификационог тијела Агенције, која је опремљена физичким контролама и контролама окружења како је дефинисано у Одјељку 5.1 Физичке контроле.
- Уноси ревизијских записа које генерише ТСП хост оперативни систем су појединачно временски означени. Оперативни систем штити интегритет својих датотека ревизијских записа користећи функционалност оперативног система.
- Уноси ревизијских записа које генерише ТСП апликација су појединачно временски означени. ТСП апликација штити интегритет својих датотека ревизијских записа шифровањем јавног кључа и верификације сваког уноса при преузимању.

5.4.5. Процедуре резервних копија ревизијских записа

- Резервне копије датотека ревизијских записа се врше сваки дан као дио редовног креирања резервних копија хост система сертификационог тијела Агенције.
- Резервне копије се чувају у ватроотпорном ормару у сертификационом тијелу Оперативног тијела Агенције.
- Резервне копије које садрже консолидовану копију датотека ревизијских записа се шаљу у сигурно складиште ван локације у сврхе складиштења и архивирања ван локације.

5.4.6. Систем прикупљања ревизија (интерне или екстерне)

- Систем сакупљања ревизија сертификационог тијела Агенције је комбинација аутоматских и мануелних процеса које изводи хост оперативни систем ТСП-а, ТСП апликација, и запослени у сертификационом тијелу Агенције, као што се наводи у тебели:

Записани догађаји	Систем прикупљања	Субјект који записује
Покретање и гашење ТСП апликације	Аутоматско	ТСП хост оперативни систем
Покретање и гашење ТСП хост оперативног система	Аутоматско	ТСП хост оперативни систем
Успјешни и неуспјели покушаји креирања, модификације, уклањања, онемогућавања, омогућавања и опоравка корисника	Аутоматско	ТСП апликација

Записани догађаји	Систем прикупљања	Субјект који записује
Успјешни и неуспјели покушаји креирања, модификације, уклањања, онемогућавања, омогућавања и опоравка налога ТСП хост оперативног система	Аутоматско	ТСП хост оперативни систем
Успјешни и неуспјели покушаји креирања, модификације, уклањања, онемогућавања, омогућавања и опоравка налога ТСП апликације	Аутоматско	ТСП апликација
Успјешни и неуспјели покушаји логовања на ТСП апликацију	Аутоматско	ТСП апликација
Успјешни и неуспјели покушаји логовања на хост рачунар	Аутоматско	ТСП хост оперативни систем
Неовлаштени покушаји приступа системским датотекама	Аутоматско	ТСП хост оперативни систем
Неовлаштени покушаји приступа PKI мрежи	Аутоматско	Рутери и ТСП хост оперативни систем
Успјешни и неуспјели покушаји генерисања, ажурирања и опоравка кључева	Аутоматско	ТСП апликација
Успјешни и неуспјели покушаји креирања, ажурирања, обуставе, опозива и опоравка сертификата	Аутоматско	ТСП апликација
Промјене политика креирања сертификата (нпр. период важења)	Аутоматско	ТСП апликација
Успјешни и неуспјели покушаји ТСП-а да се повеже, прочита и упише у директориј	Аутоматско	ТСП апликација
Значајне промјене имена	Аутоматско	ТСП апликација
ТСП резервне копије базе података и опоравак	Аутоматско	ТСП апликација и ТСП хост оперативни систем
Резервна копија, опоравак и брисање ревизијских записа	Аутоматско	ТСП хост оперативни систем и ТСП запосленици
Физички приступ просторијама ТСП-а	Мануелно	ТСП запосленици
Промјене конфигурације система	Мануелно	ТСП запосленици
Ажурирање софтвера и хардвера	Мануелно	ТСП запосленици
Планирано и непланирано одржавање система и сајта	Мануелно	ТСП запосленици
Неслагања и прилагођавања	Мануелно	ТСП запосленици
Кадровске промјене	Мануелно	ТСП запосленици
Уништавање одређених информација	Мануелно	ТСП запосленици

5.4.7. Обавјештавање субјекта који је проузроковао догађај

- Субјекат који је проузроковао одређени ревизијски догађај се не обавјештава.

5.4.8. Оцјена рањивости система

- Сертификационо тијело Агенције реализује оцјену рањивости система као дио процедуре обраде ревизијских записа.

5.5. Архивирање записа

5.5.1. Типови архивираних записа

- Сертификационо тијело Агенције чува сљедеће записе:

  - Информације о ревизијама наведеним у Одјељку 5.4 Процедуре ревизијских записа;

  - Уговори корисника и све форме које припадају захтјеву;

- Сертификати, статус опозива сертификата;

- Неслагање и прилагођавање и кореспонденција.

5.5.2. Период чувања архиве

- У складу са релевантним законима, архива се чува најмање 10 година.

5.5.3. Заштита архиве

- Приступ подацима из архиве сертификационог тијела Агенције је дозвољен само запосленима у ТСП-у на принципу нужног знања.

5.5.4. Процедуре резервних копија архиве

- Архивирани подаци се чувају на намјенском архивском медију или као копија на папиру. Најмање једном мјесечно се премештају на безбједно мјесто на удаљену локацију предвиђену за њихово складиштење.

- Архивски материјал се складишти ван локације у безбједном објекту где су физичке и безбједносне контроле исте онима које се примјењују на примарној локацији ТСП-а.

5.5.5. Захтјеви за временску ознаку записа

- Архивски записи су временски означени у тренутку њиховог креирања, користећи вријеме система на којем је догађај снимљен.

- Сви системи су временски синхронизовани који се могу пратити према универзалном времену.

5.5.6. Систем прикупљања архива (интерни или екстерни)

- Сертификационо тијело Агенције користи интерну резервну копију и архивски систем у сертификационом тијелу Агенције.

5.5.7. Процедуре за добијање и верификацију информација из архиве

- Приступ сачуваним подацима је дозвољен само представницима сертификационог тијела Агенције који морају да знају информације или у складу са важећим законом.

5.6. Замјена кључева

- Замјена кључа приватног кључа ТСП-а ће се извршити благовремено прије истека ТСП сертификата. Приликом промјене кључа приватног кључа ТСП-а, нови ТСП јавни кључ ће бити доступан власницима сертификата прекоТСП јавног репозиторија.

5.7. Компромитација и опоравак у случају катастрофе

5.7.1. Процедуре за поступање у инцидентним и компромитујућим ситуацијама

- Сертификационо тијело Агенције спроводи процедуру усклађену са ISO/IEC 27001 за поступање у случају безбједносног инцидента и квара.

5.7.2. Рачунарски ресурси, софтвер и/или подаци који су оштећени

- Сертификационо тијело Агенције је донијело план за непредвиђене ситуације и опоравак од катастрофе, а који се односи на опоравак операција након оштећења рачунских ресурса, софтвера и података.

5.7.3. Процедуре које се спроводе код компромитације приватног кључа корисника

- У случају компромитације ТСП приватног кључа за потписивање, ТСП ће опозвати и поново издати све сертификате сертификационог тијела Агенције који се тренутно користе.

5.7.4. Управљање капацитетом пословања након катастрофе

- Након природне или друге врсте катастрофе, рад ТСП операција и информационог центра ће бити поново успостављен на независној локацији за опоравак од катастрофе користећи резервне податке. Сертификационо тијело Агенције ће предузети све разумне мјере за поновно успостављање услуга у најкраћем могућем року, али не дужем од пет (5) радних дана.

5.8. Завршетак рада ТСП-а или Регистрационог тијела

У случају да Агенција добровољно прекине своје активности, ТСП ће:

- Обавјестити Уред за надзор и акредитацију овјерилаца и све актуелне кориснике најмање деведесет (90) дана прије намјере престанка рада;
- У договору са Уредом за надзор и акредитацију овјерилаца пребацити своје активности на другог пружаоца услуга од повјерења или опозвати све важеће сертификате на дан или након истека отказног рока;
- У случају да пребацивање услуга другом пружаоцу услуга није могуће, сертификационо тијело Агенције ће доставити сву документацију, податке и опрему Министарству транспорта и комуникација Босне и Херцеговине у складу са Законом о дигиталном потпису;
- Обезбиједити да се сва документација и архива пребаци на другог пружаоца услуга од повјерења или на Министарство транспорта и комуникација Босне и Херцеговине или да се чува најмање десет (10) година од посљедњег дана рада;
- Обезбиједити доступност и приступ релевантним списковима опозваних сертификата и ОЦСП-у у периоду од 6 мјесеци након опозива свих сертификата.
- Прије престанка пружања услуга, Агенција ће уништити приватне кључеве сертификационог тијела, укључујући и резервне копије или их повући из употребе, на начин да се приватни кључеви не могу поново преузети.
- Обавијестити веб-сајту Агенције о прекиду пружања услуга.

6. ТЕХНИЧКЕ БЕЗБЈЕДНОСНЕ КОНТРОЛЕ ТСП-А

6.1. Генерисање и инсталација пара кључева

6.1.1. Генерисање пара кључева

- Пар кључева за потпис сертификационог тијела Агенције се креира на хардверски безбједносноом модулу (ХСМ) током почетне процедуре генерисања кључа ТСП-а и заштићен је мастер кључем. У току генерисања пара криптографских кључева сертификационог тијела користи се вишеструка аутентификација овлаштених особа и заштита која вриједи за просторије сертификационог тијела Агенције.

- Пар кључева за потпис носиоца сертификата ТСП-а се увијек генерише путем ПКИ корисничке апликације или на смарт картици/токену).

- Приватни кључеви који се користе за квалификовани електронски потпис или квалификовани електронски печат се генеришу у хардверском токену који је у складу са спецификацијом смарт картице/ токена. Приватни кључеви који се користе за друге типове сертификата се генеришу у софтверском крипто токену код корисника или на хардверском токену (уређај за креирање потписа).

6.1.2. Испорука приватног кључа кориснику

- ТСП генерише приватне кључеве на смарт картици/токену и доставља кориснику.

- Приватне кључеве за друге сертификате (који се не издају на смарт картици/токену) генерише сам корисник на својој апликацији ПКИ тако да се не достављају носиоцу сертификата.

6.1.3. Достава јавног кључа до издаваоца сертификата

- Јавни кључеви ТСП-а се достављају до ТСП апликације у PKCS#10 формату. PKCS#10 захтјев мора бити потписан приватним кључем који одговара јавном кључу садржаном у PKCS#10 захтјеву.

6.1.4. Достава јавног кључа ТСП-а трећим странама

- ТСП доставља јавне кључеве за верификацију потписа сертификационог тијела Агенције корисницима у облику X.509 сертификата, као дио процедуре уписа.

- Јавни кључ сертификационог тијела Агенције је доступан у форми сертификата на сљедећим локацијама:

  - У јавном ЛДАП директорију;

  - На веб-сајту.

- Сертификат ТСП-а се такође може добити контактирањем Сертификационог тијела Агенције (погледати Одјељак 1.5.2 Контакт особа).

- У сваком случају, субјекат који користи сертификате сертификационог тијела Агенције мора провјерити аутентичност и интегритет сертификата ТСП-а.

6.1.5. Дужине кључева

- ТСП генерише своје асиметричне кључеве за потпис са дужином најмање 3072бита RSA.

- Носилац сертификата генерише своје асиметричне привате кључеве за потпис са дужином најмање 2048 бита RSA.

6.1.6. Генерисање јавних кључева и провјера квалитета

- Сертификационо тијело Агенције тренутно не издаје) кључеве са алгоритмом дигиталног потписа.

6.1.7. Намјене екстензије "Key usage" (дефинисано у X.509 v3 пољу употребе кључа)

- Сертификационо тијело Агенције користи поља екстензије „Key usage" у сертификатима за означавање намјене јавних кључева у сертификатима, као што је дефинисано у RFC 5280 "Интернет X.509 Сертификат инфраструктуре јавног кључа и у профилима списка опозваних сертификата".

- Поред те екстензије, сертификационо тијело Агенције такође користи проширену намјену кључа (extKeyUsage) за додатно означавање намјене или ограничавања употребе јавних кључева у сертификатима као што је дефинисано RFC 5280 "Интернет X.509 Сертификат инфраструктуре јавног кључа и у профилима списка опозваних сертификата":

- serverAuth: TLS WWW server authentication
- clientAuth: TLS WWW client authentication
- codesigning: Signing of downloadable executable code
- email Protection: E-mail protection
- timestamping: Binding the hash of an object to a time
- EKU Ossining: Signing OCSP responses

- За сертификате за потписивање и списак опозваних сертификата ТСП-а користе се само приватни криптографски кључеви сертификованог тијела.

- Криптографски кључеви и сертификати одговорних особа у сертификационом тијелу Агенције се користе само за рад са техничким средствима у власништву сертификационог тијела Агенције (хардвер и софтвер).

- Преостали сертификати сертификационог тијела Агенције се могу користити за намјене поља „Key usage", као што је приказано у доле наведеној табели.

- Употреба кључа се наводи у сертификатима које издаје сертификационо тијело Агенције у пољима екстензија „Key usage" и „extKeyUsage", зависно од врсте сертификата и врсте јавног кључа у сертификату, као што је приказано у доле наведеној табели.

Врста сертификата	**Употреба у пољу „Key usage"**
Сертификациона тијела(Регистрационо тијело, организација)	keyCertSign, cRLSign
Квалификовани дигитални потпис за квалификовани електронски потпис	digitalSignature, nonrepudiation, keyEncipherment
Нормализовани ДС - ОЦСП	digitalSignature extKeyUsage: OCSPSigning

6.2. Заштита приватног кључа и контрола криптографског хардверског модула

6.2.1. Стандарди и контроле криптографског модула

- Генерисање свих ТСП-ових кључева за дигитално потисивање и активности везане за потписивање сертификата се врше у оквиру криптографског хардверског модула која испуњава стандард FIPS 140-2 Ниво 3. Све друге криптографске активности се врше у криптографском модулу који испуњава стандард FIPS 140-2 Ниво 3.

- Приватни кључеви које се користе за квалификовани дигитални потпис и квалификовани дигитални печат се генеришу и користе у криптографском хардверком модулу сертификованом у складу са спецификацијама.

- Приватни кључеви носиоца сертификата ослањају се на физичке и логичке контроле које штите рачунарски систем носиоца сертификата. Одговорност носиоца сертификата је да осигура да се приватни кључ чува у окружењу са довољним нивоом физичке заштите. Међутим, препоручује се да носилац сертификата има QSCD оцјену која задовољава најмање стандард FIPS 140-2 ниво 2 или други стандард верификован на једнак ниво безбједности.

6.2.2. Контрола приватних кључева од стране више особа (н од м)

- Као што је дефинисано у Одјељку 5.2.2 Број особа које се захтјевају по сваком задатку.

6.2.3. Чување (енгл. Escrow) приватног кључа код трећих лица

- Сертификационо тијело Агенције не подржава чување приватног кључа код трећих лица.

6.2.4. Сигурносне копије приватног кључа

- ТСП задржава копију приватног кључа сертификационог тијела.

- Копије корисничких приватних кључева ТСП-а се не чувају код сертификационог тијела Агенције.

6.2.5. Архивирање приватног кључа

- Приватни кључеви се не архивирају.

6.2.6. Пренос приватних кључева са и на криптографски модул

- Приватни кључеви за потписивање сертификационог тијела Агенције се генеришу у хардверски безбједносном модулу (ХСМ). Пренос приватних кључева ТСП-а на или са ХСМ-а се оганичава само за сврхе креирања сигурносних копија или опоравка. Приватни кључеви ТСП-а су заштићени шифровањем када се преносе са једног на други ХСМ, тако да приватни кључ за потписивање ТСП-а никада није без заштите уколико је изван ХСМ-а.

- Кључеви који се чувају на смарт картици/токену се не преносе.

6.2.7. Чување приватног кључа у криптографском модулу

- Приватни кључ за потписивање сертификационог тијела Агенције се користи само у хардверски безбједном модулу. Приватни кључ за потписивање сертификационог тијела се чува на копираном токену хардверски безбједносног модула за сврхе сигурносних копија и опоравка.

6.2.8. Поступак активације приватног кључа

- Приватни криптографски кључ за потписивање сертификационог тијела Агенције се активира након покретања апликације сертификационог тијела. За активацију је потребна смарт картица или токен за приступ криптографском хардверском модулу као и корисничка шифра са улогом мастер корисника сертификационог тијела.

- Кориснички приватни криптографски кључеви који су генерисани на смарт картици/токену се активирају након успјешне аутентификације PIN бројем.

6.2.9. Поступак деактивирања приватног кључа

- Криптографски кључ за потписивање сертификационог тијела Агенције се деактивира прекидом рада апликације ТСП.

- Корисничке апликације деактивирају приватни криптографски кључ када се корисник излогује из система, тј. апликације.

6.2.10. Поступак уништавања приватног кључа

- Приватни кључеви ТСП-а се бришу када сертификат ТСП-а престане да важи, на начин да се брише приватни кључ на ХСМ-у и брисањем резервих копија у резервнем ХСМ-у.

- Сервисни кључеви који се чувају на смарт картици се бришу уништавањем картице.

- Корисничке апликације морају избрисати приватне криптографске кључеве из оперативне меморије прије него што их поновно додијеле. Такође морају избрисати цијели простор на диску који се користи за приватне криптографске кључеве прије него што се тај простор додијели оперативном систему.

6.2.11. Оцјењивање криптограског модула

- Погледати Одјељак 6.2.1 Стандарди и контроле криптографског модула.

6.3. Други аспекти управљања паром кључева

6.3.1. Архивирање јавног кључа

- Сертификационо тијело Агенције архивира јавне кључеве сертификационог тијела и корисничке јавне кључеве као што је дефинисано у Одјељку 5.5.4 Процедуре резервних копија архиве.

6.3.2. Периоди валидности сертификата и парова кључева

Период важења јавних и приватних криптографских кључева у серификатима које издаје сертификационо тијело Агенције је:

- „Root“ јавни верификацијски кључ и сертификат ТСП-а: 20 година.
- „Root“ приватни кључ за потписивање ТСП-а: 20 година.
- Јавни верификацијски кључ и сертификат издаваоца ТСП-а: 10 година.
- Приватни кључ издаваоца ТСП-а: 10 година.
- Јавни верификацијски кључ и сертификат корисника: до 10 година.
- Приватни кључ корисника: до 10 година.
- ОЦСП јавни верификацијски кључ и сертификат: до 3 године.
- ОЦСП приватни кључ за потписивање: до 3 године.

- Сертификационо тијело Агенције може прилагодити период важења неких криптографских кључева корисника на основу посебних захтјева и захтјева јавне набавке у складу са прописима и врстом сертификата.

6.4. Активациони подаци

6.4.1. Генерисање и инсталација активационих података

- Референтне бројеве и ауторизационе кодове генерише ТСП апликација и чувају се шифровани у бази података ТСП-а до испоруке корисницима. Бројеви и кодови су јединствени и генеришу се на непредвидив начин.

- ТСП генерише ПИН код за кључ који је генерисан на смарт картици/токену шаље се односно уручује кориснику као дио процедуре дефинисане у Одјељку 4.1.2. Процес достављања захтјева за издавање сертификата и одговорност.

6.4.2. Заштита активационих података

- Активациони кодови се генеришу безбједно у ТСП апликацији и чувају се шифровани у бази података ТСП-а.

6.4.3. Други аспекти који се односе на активационе податке

- Није наведено.

6.5. Безбједносне контроле рачунара

6.5.1. Специфични технички захтјеви за безбједност рачунара

- Сертификационо тијело Агенције врши низ техничких безбједносних контрола на рачунарима, које проводе хост оперативни систем ТСП-а и ТСП апликација, укључујући:
- Контрола приступа услугама ТСП-а;
- Строго раздвајање дужности и улога оперативним лицима ТСП-а;
- Кориштење смарт картица за чување профила службеника за безбједност сертификционог тијела и администратора за сертификате;
- Шифроване сесије између апликације ТСП-а и корисничких апликација корисника;
- Шифровање осјетљивих података у бази података ТСП-а;
- Архива историје сертификата и ревизијских података ТСП-а и корисника;
- Ревизија догађаја који се односе на безбједност;
- Механизми опоравка за кључеве и ТСП апликацију.

6.5.2. Оцјењивање безбједности рачунара

- Хост оперативни системи ТСП-а су комерцијални готови производи.

6.6. Животни циклус и безбједносне контроле

6.6.1. Контроле развоја система

- Све апликације и производи које користи сертификационо тијело Агенције су комерцијални готови производи.

6.6.2. Провјере управљања безбједношћу

- Сертификационо тијело Агенције спроводи процедуре управљања проблемима, промјенама и конфигурацијом за све ПКИ софтверске и хардверске компоненте у складу са захтјевима ISO/IEC 27001.

6.6.3. Провјера безбједности животног циклуса

- ТСП тестира све софтвере и процедуре у контролисаном окружењу.

6.7. Контроле мрежне безбједности

- Рачунарска мрежа сертификационог тијела Агенције састоји се од повезаних мрежних сегмената, гдје су смјештени сервери и оперативне станице. Ти сегменти су међусобно повезани заштитним зидовима (енгл. Firewalls). Рачунарска мрежа сертификационог тијело Агенције повезана је на Интернет преко неколико нивоа заштите. Безбједносна правила тих заштитних зидова дозвољавају промет само за протоколе који су неопходни за приступ услугама сертификационог тијела Агенције.

6.8. Временски печат

- Датум и вријеме се додају у све ревизијске записе на нивоу система и апликације. Системско вријеме је синхронизовано с више ваљских референци које се могу пратити према универзалном времену. За синхронизацију се користи NTP протокол.

7. ПРОФИЛИ СЕРТИФИКАТА, СПИСКА ОПОЗВАНИХ СЕРТИФИКАТА И ОЦСП

7.1. Профили сертификата

7.1.1. Број верзије сертификата

- Сертификационо тијело Агенције издаје сертификате у X.509v3 формату и у складу са RFC 5280, EN 319 412-2, EN 319 412-3 и EN 319 412-5. Сљедећа основна поља X.509 се користе:

Екстензија X.509	Опис
Потпис	ТСП потпис за аутентификацију сертификата
Издавалац	ТСП назив
Период важења	Датум активације и истека важења сертификата
Субјекат	Препознатљиво име корисника
Информације о јавном кључу корисника	Алгоритам ID, кључ
Верзија	Верзија сертификата X.509, верзија 3 (2)
Серијски број	Јединствени серијски број сертификата

7.1.2. Екстензије сертификата

- Сљедећа поља основне екстензије X.509 се користе

Екстензија X.509	Опис
Потпис	ТСП потпис за аутентификацију сертификата
Издавалац	ТСП назив
Период важења	Датум активације и истека важења сертификата
Субјекат	Одређено име корисника
Информације о јавном кључу корисника	Алгоритам ID, кључ
Верзија	Верзија сертификата X.509, верзија 3 (2)
Серијски број	Јединствени серијски број сертификата

- Сертификати ТСП-а садрже сљедеће критичне екстензије:

Екстензија X.509	Опис
keyUsage	keyCertSign, cRLSign
basicConstraints	CA=TRUE, pathLenConstraint

- Кориснички и сертификати услуга могу садржавати сљедеће екстензије:

Екстензија X.509	Опис
authorityKeyIdentifier	Хаш кључа издаваоца
subjectKeyIdentifier	Хаш кључа носиоца
keyUsage	Као што је дефинисано у одјељку 6.1.7 Намјена екстензије “keyUsage” Екстензије су увијек означене као критичне.
extendedKeyUsage	Као што је дефинисано у одјељку 6.1.7 Намјена екстензије “keyUsage”
privateKeyUsagePeriod	Као што је дефинисано у одјељку 6.3.2. Периоди важења сертификата и парова кључева
certificatePolicies:	Политика сертификације OID = OID као што је дефинисано у 1.2 Назив документа и идентификација
CertPolicyID	
CPS URI	

CRLDistributionPoints	Локације спискова опозваних сертификата
subjectAlternativeName	Алтернативно име корисника
basicConstraints	CA=false
Authority Information Access	accessMethod=caIssuers; and accessMethod=OCSP
qcStatement	According to ETSI EN 319 412-5

7.1.2.1. Екстензије приватних сертификата

X.509	OID
Key Usage: digitalSignature,nonRepudiation,keyEncipherment	2.5.29.15
extendedKeyUsage: Document Signing,	1.3.6.1.4.1.311.10.3.12
extendedKeyUsage: PDF Signing	1.2.840.113583.1.1.5

7.1.3. Идентификатор објекта алгоритама

Алгоритам	Идентификациони број
RSA	1.2.840.113549.1.1.1
SHA512 with RSA	1.2.840.113549.1.1.13

7.1.4. Облици назива

- У све сертификате које издаје сертификационо тијело Агенције се уписује пуно јединствено име сертификационог тијела и субјекта сертификата у поља име издаваоца односно име корисника. Кодирање тих имена се врши у UTF8 string или PrintableString формату.

7.1.5. Ограничења имена

- Није примјењиво.

7.1.6. Идентификатор објекта политике сертификације

- Сви сертификати које издаје ТСП садрже OID политике сертификације по којој се издаје сертификат. OID за сваки сертификат је дефинисан у Одјељку 1.2 Назив документа и идентификација.

7.1.7. Употреба „Policy Constraints" екстензија

- Није примјењиво.

7.1.8. Синтакса и семантика квалификатора политике

- Квалификатори политике се користе у складу са RFC5280.

7.1.9. Семантика процесирања критичне екстензије „Certificate Policies"

- Корисничке апликације PKI-а морају обрадити екстензију сертификата као критичну у складу са RFC5280.

7.2. Профил списка опозваних сертификата

7.2.1. Број верзије сертификата

- ТСП издаје спискове опозваних сертификата у X.509 v2 формату користећи низ дистрибуционих тачака у оквиру LDAP директорија и „http web" сервера.

- Сљедећа основна поља екстензије X.509 се користе:

Екстензија X.509	Опис
Верзија	Set to v2
Потпис	Алгоритам идентификатора који се користи за потписивање списка опозваних сертификата
Издавалац	Одређено име сертификационог тијела
thisUpdate	Датум издавања списка опозваних сертификата
nextUpdate	Датум наредног издавања списка опозваних сертификата
revokedCertificate	Серијски бројеви опозваних сертификата

7.2.2. Списак опозваних сертификата и „entry" екстензије списка опозваних сертификата

Екстензија X.509	Опис
CRLNumber	Редни број списка опозваних сертификата
authorityKeyIdentifier	"Хаш" кључа издаваоца
reasonCode	ТСП може садржавати вриједности у складу са RFC5280
invalidityDate	Попуњава ТСП апликација како је оператер одредио
expiredCertsOnCRL	Списак опозваних сертификата који садржи ову екстензију укључује информације о статусу опозива за сертификате који су већ истекли.

7.3. ОЦСП профил

- Профил ОЦСП који се користи дефинисан је у RFC 6960.

7.3.1. Број верзије сертификата

- Верзија ОЦСП в1 у складу са RFC 6960 се користи.

7.3.2. Екстензије ОЦСП

- Екстензије ОЦСП захтјева су:

Екстензија	Опис
nonce	Вриједност "nonce" повезује захтјев и одговор како би се спријечили напади понављања. Вриједност ће бити у складу са RFC6280

- Екстензије ОЦСП одговора су :

Екстензија	Опис
nonce	Иста вриједност као у захтјеву уколико се тражи тако у захтјеву.
ArchiveCutoff	Временски период који ОЦСП чува информације о опозиву након истека сертификата.

8. РЕВИЗИЈА УСКЛАЂЕНОСТИ И ДРУГА ОЦЈЕЊИВАЊА

8.1. Учесталост или услови оцјењивања

- Ревизију усклађености сертификационог тијела Агенције са релевантним законима се врши у складу са Законом о електронском потпису и другим важећим законским прописима Босне и Херцеговине.
- Сертификационо тијело Агенције спроводи обавезне интерне ревизије најмање једном годишње.

8.2. Идентитет/квалификације процјењивача (интерна ревизија)

- Интерни ревизор је запослен у сертификационом тијелу Агенције, са одговарајућим информационим знањем и искуством у ревизији.
- Независног екстерног ревизора ангажује надлежна независна компанија која испуњава одговарајуће домаће и међународне стандарде и правила праксе.
- Интерни и екстерни ревизор треба да испуњавају сљедеће услове:
- Значајно искуство у примјени ПКИ и криптографске технологије;
- Искуство у раду са апликацијом ТСП-а;
- Искуство у обављању активности сертификације или ревизије система информационих технологија.

8.3. Однос ревизора с предметом ревизије

- Интерни или екстерни ревизор не смије бити у сукобу интереса, односно треба бити независан од ТСП-а.

8.4. Теме које су обухваћене ревизијом

- Интерна ревизија утврђује да ли:
- Политика довољно испуњава техничке, процедуралне и организационе активности ТСП-а, у складу са условима Закона о електронском потпису и другим важећим прописима Босне и Херцеговине.
- Систем ТСП-а је усклађен и са техничким, процедуралним и организационим праксама и политикама.

8.5. Активности предузете као резултат утврђених недостатака

- Сертификационо тијело Агенције ће предузети одговарајуће активности за рјешавање свих недостатака или неусклађености идентификованих као резултат ревизије унутар договореног временског оквира који зависи од озбиљности укљученог ризика.

8.6. Саопштавање резултата

- Информације о ревизији које се односе на усклађеност сертификационог тијела Агенције са релевантним законима сматрају се изузетно осјетљивим и не смију се открити никоме нити из било којег разлога, осим за потребе ревизије или у случајевима наметнутим законом.

9. ДРУГИ ПОСЛОВНИ И ПРАВНИ АСПЕКТИ

9.1. Накнаде

9.1.1. Накнаде за издавање или обнову сертификата

- Сертификационо тијело Агенције ће наплаћивати своје услуге сертификације ПКИ. Цјеновник ће бити објављен на веб-сајту ТСП-а.

9.1.2. Накнаде за приступ сертификату

- Погледати одјељак 9.1.1 Накнаде за издавање или обнову сертификата.

9.1.3. Накнаде за опозив и приступ информацијама о статусу сертификата

- Погледати одјељак 9.1.1 Накнаде за издавање или обнову сертификата.

9.1.4. Накнаде за остале услуге

- Погледати одјељак 9.1.1 Накнаде за издавање или обнову сертификата.

9.1.5. Повратак накнаде

- Подносиоци захтјева за сертификате могу бесплатно отказати захтјев за сертификат прије издавања активационих кодова. Никакве накнаде неће бити враћене након што се испоруче активациони кодови, издају сертификати или софтвер буде испоручен или инсталиран.

9.2. Финансијска одговорност

9.2.1. Покривање осигурања

- Сертификационо тијело Агенције има осигурање у оквиру осигурања опште одговорности и одговорности за производе, укључујући покриће чистог финансијског губитка, што је уобичајено за основну дјелатност. Ограничења покрића су у складу са законодавством Босне и Херцеговине.

9.2.2. Остала средства

- Нема одредби.

9.2.3. Осигурање или гаранције за крајње кориснике

- Корисници и треће стране су искључиво одговорни да обезбиједе адекватно осигурање или покриће гаранције у односу на употребу или услугу њиховог сертификата.

9.3. Заштита личних података

- Сви лични подаци достављени сертификационом тијелу Агенције или њеним овлаштеним представницима чуваће се у складу са захтјевима прописаним Законом о заштити личних података Босне и Херцеговине. Објављивање наведених информација треба бити само у складу са Законом о заштити личних података, Политиком заштите личних података сертификационог тијела Агенције или у складу са другим важећим прописом.

9.3.1. Опсег повјерљивих информација

- Све информације које прикупља, генерише, преноси или чува сертификационо тијело Агенције сматрају се повјерљивим, осим информација наведених у Одјељку 9.3.2, које се сматрају неповјерљивим.

9.3.2. Информације које нису у опсегу повјерљивих информација

- Информације које се објављују као дио сертификата сертификационог тијела Агенције, списка опозваних сертификата, Политике сертификације и друге информације објављене у јавном репозиторију сертификационог тијела се не сматрају повјерљивим информацијама.

9.3.3. Одговорност за заштиту повјерљивих информација

- Сертификационо тијело Агенције је одговорно за заштиту повјерљивих информација у складу са Политиком заштите личних података сертификационог тијела Агенције и Законом о заштити личних података и другом важећим прописима.

9.4. Приватност личних информација

9.4.1. План приватности

- Као што је наведено у Одјељку 9.3 и 9.4.

9.4.2. Опсег приватних информација

- Све информације везане за носиоца сертификата или корисника, а које нису објављене у сертификату који издаје сертификационо тијело Агенције, списку опозваних сертификата или јавном ЛДАП директорију се сматрају повјерљивим.

9.4.3. Информације које се не сматрају приватним

- Све информације које су садржане у сертификату који издаје сертификационо тијело Агенције, списку опозваних сертификата или јавном ЛДАП директорију се не сматрају повјерљивим.

9.4.4. Одговорност за заштиту повјерљивих информација

- Као што је наведено у Одјељку 9.3.3.

9.4.5. Обавјештење и сагласност за употребу приватних информација

- Сертификационо тијело Агенције ће користити привате информације само за потребе за које је корисник дао сагласност у процесу регистрације.

9.4.6. Откривање информација у складу са правним и административним процесима

- Сертификационо тијело Агенције ће открити повјерљиве информације само представницима институција надлежним за примјену закона у складу са важећим прописима.

9.4.7. Друге околности за откривање информација

- Сертификационо тијело Агенције ће открити приватне информације само у околностима утврђеним Политиком заштите личних података сертификационог тијела Агенције, Законом о заштити личних података Босне и Херцеговине и другим релевантним законима, на захтјев суда или другог легитимног органа, а под условом да захтјев има правни основ.

9.5. Права интелектуалног власништва

- Није примјењиво.

9.6. Обавезе и одговорности

9.6.1. Обавезе и одговорности ТСП-а

- Сертификационо тијело Агенције ће издавати сертификате, проводити остале процедуре управљања сертификатима и управљати инфраструктуром сертификационог тијела у складу са Политиком сертификације и важећим законима. ТСП је одговоран за усклађивање са процедурама наведеним у овој политици, чак и када функционалност ТСП-а преузима регистрационо тијело или подизвођачи.

- Укратко, неекслузивна листа обавеза сертификационог тијела Агенције је:
  - Издавање Политике сертификације
  - обезбиједити процедуре корисницима сертификата за подношење захтјева за добијање сертификата;
  - Издавање кључева и сертификата у складу да активностима дефинисаним у овој Политици, безбједно управљање приватним кључевима сертификационих тијела сертификационо тијело Агенције ЦА и дистрибуција јавних кључева сертификационо тијело Агенције ЦА
  - одобравање или одбијање захтјева корисника сертификата;
  - потписивање и издавање сертификата у формату X.509 са јавним кључевима носиоца као одговор на одобрене захтјеве за сертификате;
  - објављивање X.509 сертификата у директоријима;
  - опозив сертификата, укључујући објављивање списка опозваних сертификата;
  - утврђивање идентитета корисника апликације који подносе захтјев за издавање сертификата, за обнову сертификата или захтјеве за нови сертификат у случају опозива сертификата;
  - обезбиједити да су особе задужене за регистрацију одговарајуће обучене и да дјелују у складу са правилима која се на њих примјењују у овој политици;
  - осигурати да су крајњи корисници упознати и сагласни да прихвате одредбе и услове за добијање кључева и сертификата;
  - потврдити рад у складу са активностима описаним у овој Политици путем периодичних ревизија пословања (најмање свака 24 мјесеца);
  - запошљавање лица која, поред општих услова за запошљавање, испуњавају и посебне услове прописане Законом о електронском документу, електронској идентификацији и повјерљивим услугама
  - осигурати да су информације о кориснику и ТСП-у које су садржане у сертификатима тачне;
  - доказивање идентитета подносиоца захтјева прије издавања сертификата;
  - обезбиједити тачност и интегритрет информација објављених у LDAP директорију или другом репозиторију;
  - омогућити приступ електронском јавном директорију;
  - издавање сертификата одобреним подносиоцима захтјева у складу са овом Политиком сертификације;
  - опозив сертификата које је издало сертификационо тијело, по пријему ваљаног захтјева за то, или у складу са овом Политиком сертификације;
  - издавање и објављивање списка опозваних сертификата;
  - Одржавање ООЦСП услуге;
  - Обезбиједити да су регистрациона тијела упозната са одредбама које се на њих односе у овој Политици сертификације.

9.6.2. Одговорности и обавезе регистрационог тијела

- Регистрационо тијело је одговорно за тачност и потпуност информација корисника о одобреним обрасцима за пријаву. Детаљне обавезе Регистрационог тијела су наведене у релевантним одјељцима ове Политике сертификације.

9.6.3. Корисничке одговорности и обавезе

- Корисник преузима пуну одговорност за употребу приватног кључа повезаног са јавним кључем у сертификату при чему је власник физичко лице идентификовано приватним кључем.
- Када се сертификати издају лицу за личну употребу, корисник и власник чине једно те исто лице.
- Прије издавања кључева и сертификата, корисници закључују уговор са сертификационим тијелом Агенције, узимајући у обзир правила и услове кориштења.
- Корисници су одговорни да:
  - Буду потпуно свјесни својих дужности и одговорности као што је наведено у релевантној документацији која је горе наведена, као и правила по којима се сертификати издају;
  - У року од пет радних дана од дана пријема покрену иницијални код који им шаље сертификационо тијело Агенције – употреба приватних кључева за предвиђену сврху;
  - Контролишу приступ рачунару, уређају или специјалном хардверском уређају који садржи приватни кључ за који су одговорни;
  - Чувају шифре које се користе за приступ приватним кључевима;
  - Хитно обавијесте сертификационо тијело Агенције о свакој сумњи за компромитацију њиховог приватног кључа.
- Прихватањем сертификата који издаје сертификационо тијело Агенције, корисник треба да:
  - чува у тајности свој приватни кључ за потписивање;
  - чува у тајности своју шифру;
  - одмах обавијести сертификационо тијело о свим нетачностима или промјенама у информацијама садржаним у сертификату;
  - искључиво користи свој сертификат у законите сврхе и овлаштене сврхе детаљно описане у одјељку 1.4 Употреба сертификата;
  - одмах обавијести сертификационо тијело о сумњивој или откривеној компромитацији приватног кључа;
  - одмах обавијести сертификационо тијело Агенције о свакој сумњи или познатој злоупотреби било којег сертификата изданог од стране сертификационог тијела.

9.6.4. Обавезе и одговорности трећих страна

- За провјеру валидности сертификата који добијају, трећа лица се увијек морају прво позвати на списак опозваних сертификата сертификационог тијела Агенције.
- Трећа страна,којој је повјерен сертификат који издаје сертификационо тијело Агенције је дужна да:
  - Ограничи валидност сертификата само у сврху дефинисану у овом документу;
  - Провјери валидност сертификата;
  - Прочита овај доцумент и научи дужности, одговорноси и ограничења ТСП-а;
  - Затражи опозив сертификата ако:
    - Има сазнања да је приватни кључ компромитован тако да утиче на правилну употребу,
    - Постоји опасност од злоупотребе,
    - Постоје промјене у подацима наведеним у сертификату.

- Прије преузимања сертификата, одговорности трећих страна су:
    - Упознати са ограничењима сертификата и одговорностима ТСП-а као што је детаљно описано у овој Политици;
    - ограничити ослањање на сертификате које издаје ТСП на одговарајућу употребу као што је детаљно описано у одјељку 1.4 Употреба сертификата;
    - обезбиједити да сертификат није опозван приступом важећим, било којим и свим, примјењивим списковима опозваних сертификата или ОЦСП;
    - одмах обавијестити сертификационо тијело Агенције о свакој сумњи или познатој злоупотреби било којег сертификата издатог од стране ТСП-а.

9.6.5. Одговорности и обавезе других учесника

- Сви други учесници су обавезни да користе сертификате и дјелују у складу да овом Политиком и важећим прописима.

9.7. Непризнавање гаранција

- Осим гаранција наведених у овој Политици сертификације и сродним уговорима, и у највећој мјери дозвољеној законом, сертификационо тијело Агенције искључује било које друге могуће гаранције, услове или изјаве (изричите, подразумијеване, усмене или писмене), укључујући било коју гаранцију могућности за продају или прикладности за одређену употребу. ТСП посебно искључује:
- сваку одговорност за могућу штету која може настати од тренутка када ТСП прими важећи захтјев за опозив, до тренутка објављивања информација о опозиву на списку опозваних сертификата-у у складу са Одељком 4.9.6;
- сваку гаранцију у погледу тачности или поузданости било које информације садржане у сертификатима коју не даје сертификационо тијело Агенције;
- одговорност за представљање информација садржаних у сертификату;
- сваку гаранцију у погледу овлаштења или статуса било које особе која користи сертификат сертификационог тијела Агенције
- сваку одговорност везано за питања које су ван властите контроле, укључујући доступност или рад Интернета, или телекомуникационе или друге инфраструктуре или система РА, укључујући хардвер и софтвер;
- сваку одговорност за штету као резултат више силе као што је детаљно описано у Одјељку 9.16.5 Виша сила.

9.8. Ограничења одговорности

Сертификационо тијело Агенције одриче се одговорности било које врсте за било какву врсту накнаде, штете или друге захтјеве или обавезе било које врсте по основу одштетног права, уговора или било којег другог разлога у вези с било којом услугом повезаном са издавањем, кориштењем или ослањањем на сертификат издат од сертификационог тијела Агенције.

9.9. Накнада штете

- Свака страна сноси искључиву одговорност за обештећење сертификационог тијела Агенције или других страна за губитке или штету који су резултат лажне употребе сертификата или непоступања у складу са овом Политиком сертификата и важећим законима.

9.10. Трајање и престанак важења

9.10.1. Трајање

- Политика сертификације сертификационог тијела Агенције и других докумената постају важећа потврдом од стране ОРГАНИЗАЦИЈЕ, и објављивања на веб-сајту сертификационог тијела Агенције као што је дефинисано у Одјељку 2.1. Репозиторији.

9.10.2. Престанак важења

- Престанак важења Политике сертификације сертификационог тијела Агенције није временски одређено. Тренутна верзија престаје да важи када се објави нова верзија.

9.10.3. Посљедице престанка важења и наставак дјеловања

- Након престанка важења ове Политике сертификације, као резултат објављивања нове верзије, сертификат ће се користити у складу са оном верзијом Политике сертификације која је била важећа на дан издавања сертификата. У случају да се околности промијене у мјери у којој то није могуће, сертификационо тијело Агенције ће обавијестити кориснике како је дефинисано у одјељку 9.12.2 Механизам и период обавјештавања и треће стране путем веб-сајта као што је дефинисано у одјељку 2.1 Репозиторији.

9.11. Појединачна обавјештења и комуникација са учесницима

- Сертификационо тијело Агенције дистрибуише тренутну верзију ове Политике сертификације и тренутну верзију свих других јавних докумената путем своје интернет странице дефинисане у одјељку 2.1 Репозиторији.

- Такође погледати 9.12.2 Механизам и период обавештавања.

9.12. Измјене и допуне

9.12.1. Поступак измјена и допуна

- Запослени у сертификационом тијелу Агенције и други субјекти могу послати своје коментаре директно Тијелу за управљање политиком у писаној форми, путем е-поште или на адресе наведене у одјељку 1.5.2 Контакт особа.

9.12.2. Механизам и период обавјештавања

- Сертификационо тијело Агенције може одлучити да ли ће обавијестити кориснике и треће стране у случају измјена са малим или без утицаја. Сертификационо тијело Агенције одлучује да ли измјене имају утицај на кориснике и треће стране према властитом нахођењу.

- Све промјене Политике сертификације ће бити објављене као што је описано у одјељку 2. Одговорности објављивања и репозиторија. Сертификационо тијело Агенције ће обавијестити кориснике о промјенама које утичу на кориснике или треће стране путем е-поште.

9.12.3. Околности под којима се мора мијењати идентификатор објекта OID

- ОИД Политике сертификације ће се измијенити у случају када измјене утичу на кориснике или треће стране.

9.13. Поступак рјешавања спорова

- Сви спорови везани за пословање са сертификатима упућују се писаним путем сертификационом тијелу Агенције на адресу дефинисану у Одјељку 1.5.2 Контакт особа. Ако је могуће, спор треба ријешити споразумом. Спор који се не ријеши преговорима рјешава надлежни суд.

9.14. Важећи прописи

- Ова Политика сертификације и однос између ТСП-а, Регистрационог тијела, корисници, субјекти (носиоци сертификата) и остале треће стране подлијежу и тумачиће се у складу са законима Босне и Херцеговине.

9.15. Усклађеност са важећим прописима

- Закон о заштити личних података
- Закон о електронским документима, електронској идентификацији и повјерљивим услугама и подзаконски акти усвојени на основу поменутог Закона.
- Други релевантни прописи

9.16. Остале одредбе

9.16.1. Комплетан уговор

- Политика сертификације сертификационо тијела Агенције и уговор сертификационог тијела Агенције са крајњим корисником наводе све релевантне одредбе о односу између сертификационог тијела Агенције и носиоца сертификата сертификационог тијела Агенције јавних сертификата.

9.16.2. Додјељивање

- Корисницима и носиоцима сертификата није дозвољено да уступају права и обавезе које произилазе из овог уговора ни у цјелини ни дјелимично трећој страни по било ком основу.

9.16.3. Случајеви непримјењивости одредби (раздвојеност)

- Непримјењивост једног или више дијелова овог документа, неће утицати на примјењивост осталих одредби, под условом да то не утиче на материјалне одредбе (поузданост сертификата и коришћење сертификата).

9.16.4. Извршење (адвокатске накнаде и одрицање од права)

- Није примјењиво

9.16.5. Виша сила

- Виша сила означава хитне и непредвидиве ситуације попут природних катастрофа, тероризма, нестанка електричне енергије или телекомуникација, пожара, непредвидивих инцидената као што су вируси или блокада услуга због хакерских напада, владиних мјера и нарушавања јачине криптографских алгоритама.
- Сертификационо тијело Агенције или друге стране неће бити одговорни за било какву штету узроковану догађајима више силе.

9.17. Остале одредбе

Није примјењиво