СПОДЕЛИ ДОЖИВУВАЊА

Политика за издавање на дигитални сертификати (CP) на Македонски Телеком CA

Јавен дел од правилата дефинирани од страна на Македонски Телеком АД-Скопје
како издавач на дигитални сертификати

Идентификационен бр.	POL 007
Верзија Бр.	4
Предложено од (Одговорна организациска единица)	Служба за управување со ИТ сервиси и канцелариска информатичка инфраструктура (Оперативен тим за управување на Македонски Телеком СА)

Извршен преглед

Верзија	Датум	Краток опис на промените
4	Јули 2017	Корекција во точка 9.2

Естимација на влијание на времето за реакција на пазар:

	Пополнето од Подносител	Пополнето од TQM
Нема влијание		
Мало влијание, со цел поедноставување на некои интерни процеси		
Значајно влијание	X	X

Историјат*

Верзија	Датум	Подготвено од:	Краток опис на промените
3	30.06.2017	Служба за управување со ИТ сервиси и канцелариска информатичка инфраструктура (Оперативен тим за управување на Македонски Телеком СА)	Измени согласно технички промени
2	7.09.2010	Оперативна служба на Македонски Телеком СА	Измени согласно преименувањето на МТнет ЦА во Македонски Телеком СА како и техничките измени во инфраструктурата заради надградбата на ПКИ инфраструктурата
1	30.06.2006	Оперативна служба на МТнет ЦА	Прва верзија при воспоставување на АД Македонски Телекомуникации - МТнет ЦА како регистриран издавач на дигитални сертификати

*Приказ на максимум последни 3 верзии на соодветната интерна регулатива

Содржина

1. ВОВЕД

1.1. Преглед

Овој документ е јавен дел од правилата дефинирани од страна на Македонски Телеком АД - Скопје, како издавач на сертификати. Целта на овој документ е да ги објасни техничките, процедуралните и организациските активности како и примената на инфраструктурата на јавни клучеви (PKI на Македонски Телеком CA) и имплементираните постапки за издавање сертификати кои ја демонстрираат доверливоста на Македонски Телеком АД - Скопје како издавач на сертификати за јавни клучеви.
Овој документ е во согласност со барањата од Законот за податоци во електронски облик и електронски потпис и подзаконските акти донесени врз основа на овој закон.
Правилата дефинирани во овој документ се базираат врз RFC 3647 „Интернет X.509 Политика за издавање на дигитални сертификати за инфраструктура на јавни клучеви и рамка на практиките за издавање сертификати“ (Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework) што ја содржи основата на правилата на издавачот на сертификати и усогласено со

- ETSI TS 101 456 v1.4.3 (2007-05) „Барања на политиката за издавачи на сертификати кои издаваат квалификувани сертификати (Policy requirements for Certification authorities issuing qualified certificates) и
- ETSI TS 102 042 V2.4.1 (2013-02) „Барања на политиката за издавачи на сертификати кои издаваат сертификати за јавни клучеви (Policy requirements for Certification authorities issuing public key certificates).

Политиката ги опишува јавните правила за следните категории на квалификувани сертификати:

Категорија на сертификат	**Користење/бекап на сертификатот KE –клуч за шифрирање NR – не може да се обнови)**	**Користење на токен (M - задолжително, регистрирање од корисник O - опционо, регистрирање од корисник I – издадено на токен од страна на CA C-издаден како cloud сертификат на HSM)**
Доверливост KS+	Квалификуван DS на токен	M
Доверливост KS	Квалификуван DS	O
Доверливост KS++	Квалификуван DS издаден на токен	I
Доверливост KSSC+	Квалификуван DS на токен	M
Доверливост KSSC++	Квалификуван DS на токен	I
Доверливост KSN+	Квалификуван со два пара клучеви на токен: DS (не може да се обнови); KE (може да се обнови)	M
Доверливост KSN	Квалификуван со два пара клучеви: DS (не може да се обнови); KE (може да се обнови)	O
Доверливост KSS+	Квалификуван DS, KE (не може да се обнови) на токен. Qualified DS,KE (no recovery) on token	M
Доверливост KSS	Квалификуван DS, KE (не може да се обнови)	0

Категорија на сертификат	Користење/бекап на сертификатот KE –клуч за шифрирање NR – не може да се обнови)	Користење на токен (M - задолжително, регистрирање од корисник O - опционо, регистрирање од корисник I – издадено на токен од страна на CA C-издаден како cloud сертификат на HSM)
Доверливост KSS++:	Квалификуван DS, KE (не може да се обнови) издаден на токен	I
ДоверливостKS Non-repudiation	Квалификуван NR (не може да се обнови, неотповикливост)	I
Доверливост KSCL+	Квалификуван DS во Cloud	C

И следниве категории на нормализирани сертификати:

Категорија на сертификат	Користење/бекап на сертификатот KE –клуч за шифрирање NR – не може да се обнови)	Користење на токен (M - задолжително, регистрирање од корисник O - опционо, регистрирање од корисник I – издадено на токен од страна на CA)
Доверливост NSER+	Нормализиран KE (кој може да се обнови) на токен	M
ДоверливостNSER	Нормализиран KE (кој може да се обнови)	O
Доверливост NSE+	Нормализиран KE (не може да се обнови) на токен	M
Доверливост NSE	Нормализиран KE (не може да се обнови)	O
Доверливост SSL NS	Нормализиран DS, KE (serverAuth)	O
Доверливост VPN NS	Нормализиран DS, KE (serverAuth)	O
Доверливост CS NS	Нормализиран DS (codeSign)	O
Доверливост TS NS	Нормализиран TimeStamping	I

1.2. Име и идентификација на документ

Овој документ е Политика за издавање на дигитални сертификати на Македонски Телеком како овластен издавач на дигитални сертификати, понатаму во текстот референциран како Македонски Телеком CA. Оваа политика (во понатамошниот текст референцирана како CP) е објавена на url http://www.telekom.mk/CPS и е достапна за јавноста.
Следниве Идентификациски ознаки (OIDs) се доделуваат на категории на сертификати издадени според оваа CP:
`

Категорија на сертификат	Идентификација на Политика за издавање на дигитални сертификати (OID)

Категорија на сертификат	Идентификација на Политика за издавање на дигитални сертификати (OID)
Доверливост KS+	OID 1.3.6.1.4.1.18560.1.1.1.0.1.0
Доверливост KS	OID 1.3.6.1.4.1.18560.1.1.2.0.1.0
Доверливост KS++	OID 1.3.6.1.4.1.18560.1.1.3.0.1.0
Доверливост KSSC+	OID 1.3.6.1.4.1.18560.1.1.4.0.1.0
Доверливост KSSC++	OID 1.3.6.1.4.1.18560.1.1.5.0.1.0
Доверливост KSN+	OID 1.3.6.1.4.1.18560.1.1.1.0.2.0
Доверливост KSN	OID 1.3.6.1.4.1.18560.1.1.2.0.2.0
Доверливост KSS+	OID 1.3.6.1.4.1.18560.1.1.1.0.3.0
Доверливост KSS	OID 1.3.6.1.4.1.18560.1.1.2.0.3.0
Доверливост KSS++:	OID 1.3.6.1.4.1.18560.1.1.3.0.3.0
ДоверливостKS Non-repudiation	OID 1.3.6.1.4.1.18560.1.1.3.0.4.0
Доверливост NSER+	OID 1.3.6.1.4.1.18560.1.2.1.0.1.0
ДоверливостNSER	OID 1.3.6.1.4.1.18560.1.2.2.0.1.0
Доверливост NSE+	OID 1.3.6.1.4.1.18560.1.2.1.0.2.0
Доверливост NSE	OID 1.3.6.1.4.1.18560.1.2.2.0.2.0
Доверливост SSL NS	OID 1.3.6.1.4.1.18560.1.2.2.1.1.0
Доверливост VPN NS	OID 1.3.6.1.4.1.18560.1.2.2.2.1.0
Доверливост CS NS	OID 1.3.6.1.4.1.18560.1.2.2.3.1.0
Доверливост TS NS	OID 1.3.6.1.4.1.18560.1.3.1.1.0.0
Доверливост KSCL+	OID 1.3.6.1.4.1.18560.1.4.1.1.0.0

1.3. Учесници во PKI

1.3.1. Издавачи на сертификати

Македонски Телеком CA е овластен издавач на сертификати за јавни клучеви на организации или поединци надвор од Македонски Телеком АД – Скопје, како и за нивно користење за интерни потреби.
Македонски Телеком CA функционира на база на само-потпишан коренски сертификат (self signed root) издаден сам од себе во процесот на креирање на клучеви.
Македонски Телеком CA се состои од лица кои се одговорни за целокупното функционирање на CA и лица кои работат на и го одржуваат CA серверот и CA софтверот. Овластениот Оперативен тим (OA- Operation Authority) на CA е одговорен за воспоставување и администрација на Правилата на CA и управување со приватни криптографски клучеви на CA. OA е одговорен за ревидирање на работењето на RA (Registration Authority). OA му поднесува извештаи на назначени одговорни лица за управување на CA (PMA- Primary Management Authority) за прашања во врска со работењето на CA.
Овластените лица на CA се одговорни за функционирање и администрација на CA серверот и CA софтверот.
Македонски Телеком CA е одговорен за:

- генерирање на парови на клучеви на CA, безбедносно управување со приватни клучеви на CA и дистрибуирање на јавни клучеви на CA;
- воспоставување на средина и регулирање постапка за барателите на сертификат да можат да ги доставуваат нивните барања за сертификат;
- идентификација и автентикација на поединци или субјекти кои аплицираат за сертификат;

- одобрување или одбивање на барањата за сертификат;
- потпишување и издавање на X.509 сертификати обврзувајќи ги претплатниците со нивните јавни клучеви како одговор на одобрените барања за сертификати;
- распределување на X.509 сертификати преку директориуми;
- иницирање на поништување на сертификати, било на барање на претплатникот или на иницијатива на субјектот;
- поништување на сертификати, вклучувајќи и издавање и објавување на регистар на поништени сертификати (CRL);
- утврдување и автентикација на идентитетот на поединците или субјектите кои поднесуваат барања за обновување на сертификати или издавање на нов сертификат по процесот за обновување на клучот и процесите утврдени погоре за издадени сертификати како одговор на одобрените барањата за обновување на сертификати и за обновување на клучеви;
- работење на CA во согласност со македонските закони и овие CPS правила;
- одобрување и назначување на поединци за пополнување на позициите за PKI службеник;
- прегледување и ревидирање на работењето на RA и LRA во рамките на нивниот домен;
- решавање на спорови помеѓу крајните корисници и CA , RA или LRA;
- барање за поништување на сертификатите до службеникот за CA и овластен тим за регистрација.

Кога е неопходно, овие CPS правила разликуваат различни корисници и улоги кои имаат пристап до функциите на CA. Кога оваа дистинкција не е потребна, терминот CA се користи за целокупниот CA субјект, вклучувајќи го и софтверот и неговите операции.

1.3.2. Овластен тим за регистрација на Македонски Телеком CA (RA)

Овластен тим за регистрација на Македонски Телеком CA (RA- Registration Authority) користи две генерални категории за регистрација. Првата категорија (Овластен локален тим за регистрација -LRA) вклучува назначени лица за регистрација кои се одговорни за извршување на “face-to-face” докажување на идентитетот и за собирање на информации за корисниците со цел поддршка на регистрирање на корисниците и рутинско обновување на клучевите. Втората категорија за регистрација (Овластен Примарен тим за регистрација или PRA) вклучува назначени лица, кој ги ревидира информациите на корисниците и одобрува барања за регистрација.
Функциите на LRA за јавни сертификати ги извршуваат назначени вработени за продажба од Македонски Телеком АД – Скопје.
Функциите на PRA ги извршуваат назначени вработени од Македонски Телеком АД – Скопје.
Назначените лица од LRA се одговорни за:

- идентификација и автентикација на поединци или субјекти кои аплицираат за сертификат;
- идентификација и автентикација на поединците или субјектите кои поднесуваат барања за обновување на сертификати или за издавање на нов сертификат по процесот за обновување на клучот и процесите утврдени погоре за издадени сертификати како одговор на одобрените барањата за обновување на сертификати или за обновување на клучеви;
- одобрување или одбивање на барањата за сертификат;
- потврдување на идентитетот на претплатниците;
- потврдување на податоците содржани во барањата на претплатниците и поднесување на барања за сертификат, барања за обновување на клучеви, барања за суспензија на сертификатот и барања за поништување на сертификатот до Овластениот оперативен тим на Македонски Телеком CA.

Назначените лица од PRA се одговорни за следново:

- одобрување на издавањето на сертификат;

- добивање на авторизациски кодови на претплатникот од Овластениот оперативен тим на Македонски Телеком СА и нивно дистрибуирање и помагање при активацијата на претплатникот во рамките на пропишаниот временски период за активација, во случај кога автоматското праќање на кодови нема да биде извршено:
- следење на статусот на информациите за претплатникот.

1.3.3. Претплатници

Претплатници на Македонски Телеком СА се лица, физички лица (поединци) и/или правни лица (компании) кои ги користат PKI услугите на Македонски Телеком СА.
Претплатник е страна која бара од Македонски Телеком СА сертификат во име на еден или повеќе субјекти. На пример, компанија која бара сертификат за своите вработени.
Субјект е лице идентификувано во сертификатот како носител на приватен клуч поврзан со јавниот клуч даден во сертификатот.
Претплатникот ја сноси крајната одговорност за користењето на приватниот клуч поврзан со сертификатот за јавен клуч, но субјектот е поединец на кој се врши автентикација со приватниот клуч.
Во случај на сертификати издадени на поединци за нивна сопствена употреба, претплатникот и субјектот се едно исто лице.
Термините претплатник и субјект (носител на сертификат) со оваа експлицитна разлика се користат во овој документ секаде каде што имаат разлика во значењето.

1.3.4. Трети лица (Relaying Parties)

Трети лица се субјекти, вклучувајќи физички лица (поединци) и/или правни лица (компании) кои се потпираат на сертификатот и/или електронскиот потпис поврзан со јавниот клуч наведен во сертификатот на субјектот.
За проверка на валидноста на сертификатот што го добиваат, третите лица мораат секогаш да се повикаат првенствено на регистарот на поништени сертификати на Македонски Телеком СА пред да се потпрат на информациите во сертификатот.

1.3.5. Други учесници

Не е применливо.

1.4. Употреба на сертификатот

1.4.1. Соодветни употреби на сертификатот

Сертификатите на Македонски Телеком СА можат да се користат за следниве цели:

- Апликации кои бараат користење на квалификуван сертификат во согласност со Законот за податоци во електронски облик и електронски потпис на Република Македонија.
- Шифрирање и дешифрирање на документи во електронски облик
- Потврда на електронски потпишани документи
- Идентификација на носителот на сертификатот
- Безбедна комуникација по e-mail
- Други цели на барање на корисниците и во согласност со Законот за податоци во електронски облик и електронски потпис и други релевантни закони во РМ.

1.4.2. Забранети употреби на сертификатот

Сите сертификати издадени од Македонски Телеком СА треба да се користат во согласност со законодавството на Република Македонија.

1.5. Администрација на политиката

1.5.1. Организација која управува со документот

Со Македонски Телеком СА управува Македонски Телеком АД – Скопје.

1.5.2. Лице за контакт

Адреса: Македонски Телеком АД - Скопје
Кеј 13-ти Ноември“ бр. 6,
1000 Skopje

E-mail: cainfo@telekom.mk
Интернет: http://www.telekom.mk/CPS

1.5.3. Лице кое ја утврдува соодветноста на CPS за политиката

Не е применливо.

1.5.4. Процедури за одобрување на CPS

Политиката за издавање сертификати на Македонски Телеком CA ја подготвува и одржува Овластениот оперативен тим на Македонски Телеком CA, а ја одобрува Главниот директор за Техника и ИТ.

1.6. Дефиниции и кратенки

Дефиниции:
Електронски потпис (electronic signature) подразбира низа на податоци во електронски облик, кои се содржани или се логично поврзани со други податоци во електронски облик и е наменет за утврдување на автентичноста на податоците и за утврдување на идентитетот на потписникот.
Општо прифатен електронски потпис (advanced electronic signature) се смета за електронски потпис ако:

- исклучиво и единствено е поврзан со потписникот;
- може од него со сигурност да се утврди потписникот;
- е креиран со употреба на податоци и средства за општо прифатено електронско потпишување кои се во целосна контрола на потпишувачот, и
- е поврзан со податоците на кои се однесува, на начин што овозможува утврдување на секоја подоцнежна промена на тие податоци на кои се однесува потписот или промена на логичната поврзаност на самите податоци.

Временски жиг (time-stamp) е електронски потпишана потврда од страна на издавачот на сертификати, за одредена содржина на податоци во точно одредено време и датум.
Потписник (signer) е лице кое, во свое име или во име на друго правно или физичко лице кое го застапува, стави електронски потпис односно се потпише во електронски облик.
Информатички систем е систем кој се користи за составување, праќање, примање, чување или друга обработка на електронски податоци.
Податоци за електронско потпишување (signature-creation data) се единствени податоци користени при креирање на електронскиот потпис како, на пример, кодови или приватни криптографски клучеви.
Уред за електронско потпишување (signature-creation device) е конфигурирана програмска или машинска опрема која се користи за оформување на електронски потпис.
Уред за општо прифатено електронско потпишување (secure-signature -creation device - SSCD) е: уред со кој се обезбедува единствени, сигурни и доверливи податоци за електронско потпишување, да не може во разумно време и со разумни средства од податоците за проверка на електронскиот потпис да се добијат податоци за електронско потпишување; електронскиот потпис да биде заштитен од фалсификување со употреба на моментално достапната технологија и потписникот да може сигурно да ги зачува податоците за електронско потпишување од неовластен пристап.
Податоци за проверка на електронски потпис (signature-validation data) се единствени податоци користени при проверка на електронскиот потпис како, на пример, кодови или јавни криптографски клучеви.
Уред за проверка на електронски потпис (signature-validation device) е конфигурирана програмска или машинска опрема која се користи за проверка на електронски потпис.
Сертификат (certificate) е потврда во електронски облик со кој се потврдува врската меѓу податоците за проверка на електронски потпис со одредено лице, носителот на сертификатот и идентитетот на тоа лице.

Квалификуван сертификат (Qualified Certificate) е сертификат кој содржи име или назив и држава на живеалиштето, односно седиштето на издавачот; име или назив односно псевдоним на носителот или назив односно псевдоним на информатичкиот систем со назнака на носителот; податоци за проверка на електронскиот потпис кои се поврзани со податоците за електронско потпишување; почеток и крај на важењето на сертификатот; идентификационен број на сертификатот; општо прифатениот електронски потпис на издавачот и евентуалните ограничувања за употреба на сертификатот.
Нормализиран сертификат (Normalized Certificate) е сертификат кој има исти технички својства и нуди исто ниво на доверливост како и квалификуваниот сертификат, но е без законски ограничувања во неговата наменета употреба.
Издавач на сертификати (Certification Authority) е физичко или правно лице кое издава сертификати или обезбедува други услуги поврзани со сертификати, односно електронски потписи.
Субјект (Subject) е субјектот идентификуван во сертификатот како закупник на приватен клуч поврзан со јавен клуч даден во сертификатот.
Претплатник (Subscriber) е странка која бара сертификат од издавач во име на еден или повеќе носители. Претплатникот во исто време може да биде и носител во случај кога сертификатите се издадени на поединец за лична употреба.
Трето лице (Relying party) е субјект кој има разумна доверба во сертификатот.
Компјутерска корисничка сметка (computer user account) - Компјутерска корисничка сметка претставува збир на атрибути кои овозможуваат пристап до компјутерски систем за одредено лице. Секоја корисничка сметка е уникатна на секој компјутерски систем, што е реализирано преку интерни функции на компјутерскиот систем. Основа за пристап до корисничката сметка претставува пар од корисничко име и лозинка. Корисничкото име е низа од алфанумерички карактери која претставува идентификациско име на корисник во еден компјутерски систем. Ваквото идентификациско име мора да биде уникатно на ниво на компјутерски систем. Лозинката е исто така низа од алфанумерички карактери, која му е позната само на сопственикот на корисничката сметка. Во компјутерски системи во кои е потребна високо ниво на безбедност, корисничката лозинка може да биде дополнета или заменета со чип картичка.
Енкрипциски пар на клучеви (Encryption key pair) подразбира пар на симетрични клучеви составен од јавен екрипциски клуч и пропратен приватен декрипциски клуч. Исто така познат и како доверлив пар на клучеви (confidentiality key pair).
Приватен декрипциски клуч (Private decryption key) Види Енкрипциски пар на клучеви.
Приватен клуч за потпишување (Private sighning key) Види Енкрипциски пар на клучеви.
Јавен енкрипциски клуч (Public encryption key) Види Енкрипциски пар на клучеви.
Сертификат со клуч со двојна намена (Public dual-usage key certificate) е сертификат кој содржи јавен клуч кој се користи во исто време и за енкрипција и за верификација.
Сертификат со јавен енкрипциски клуч (Public encryption key certificate) е сертификат кој содржи јавен енкрипциски клуч.
Јавен клуч за верификација на потпис (Public signature verification key) Види Енкрипциски пар на клучеви.
Сертификат со јавен клуч за верификација на потпис (Public signature verification key certificate) е сертификат кој содржи јавен клуч за потпишување.
Пар на клучеви за потпишување (Signature key pair) е пар на асиметрични клучеви сочинети од приватен клуч за потпишување и пропратен јавен клуч за верификација на потписот.
SSCD (Smart Card) Smart картичка/токен во која можат да се чуваат сите парови на клучеви.
HSM (Hardware Security Module) – физички уред за безбедно складирање на дигитални клучеви
Кратенки:
Список на кратенки, кои се споменуваат во овој документ и во Политиката, е даден во следнава табела:

Кратенка	**Објаснување**
ARL	(Authority Revocation List) Регистар на поништени сертификати од издавачи
CA	(Ceritifie Authority) - Овластен издавач на сертификати
CN	(Common Name) - Име X.500
CPS	(Cerification Practice Statement) Правилата на издавачот на сертификати (ПИС)

CRL	(Certificate Revocation List) Регистар на поништени сертификати (РПС)
DN	(Distinguish Name) - Единствено име X.500
EAL	(Evaluation Assurance Level) стандард за означување на нивото на сигурност на компјутерските системи
RA	(Registration Authority) Овластен тим за регистрација
LRA	(Local Registration Authority) - Овластен локален тим за регистрација – назначени вработени за продажба од Македонски Телеком АД – Скопје
PRA	(Primary Registration Authority) - Овластен примарен тим за регистрација – одговорни вработени од Македонски Телеком АД – Скопје
PMA	Primary Management Autority – Овластен тим за управување
OA	Овластен оперативен тим на МКТ
FIPS 140-1	(Federal Information Processing Standards) Стандард за означување на нивото на сигурност од аспект на обработка на информациите http://csrc.nist.gov/publications/fips/fips140-1/fips1401.pdf
PKCS #10	(Public-Key Cryptography Standard #10) Стандард за форматот на барањето за сертификат
PKI	(Public Key Infrastructure) Инфраструктура на јавните криптографски клучеви
PKIX	(X.509 based PKI) PKI базиран на X.509 стандардот
PKIX-CMP	(PKIX-Certificate Management Protocols) Стандарден протокол за управување со сертификати, опишан во RFC 4510
X.509	Стандард за електронски сертификати опишан во RFC 3280

2. ОДГОВОРНОСТИ ЗА ОБЈАВУВАЊЕ И СКЛАДИРАЊЕ

2.1. Складишта

Македонскии Телеком СА објавува информации поврзани со услугите за сертификација во складиштата на следниве адреси:
Јавна веб страна: http://www.telekom.mk/CPS
LDAPv3 ldap://ldap-ca.ca.telekom.mk
Директориум:

2.2. Објавување на информации за сертификација

Македонски Телеком СА објавува:

- Издадени сертификати за енкрипција (Јавен дел)
- Посебни и комбинирани регистри на поништени сертификати (CRL)
- Сертификат на СА
- Политика за издавање на дигитални сертификати
- Македонски Телеком СА известува за и објавува јавни информации поврзани и со други услуги за сертификација.

2.3. Време или фреквенција на објавување

Сертификатите се објавуваат веднаш по нивното издавање како што е утврдено во Делот 4.4. Регистарите на поништени сертификати се објавуваат веднаш по нивното издавање како што е утврдено во Делот 4.9.7. Сите информации се објавуваат веднаш откако ќе бидат изменети или откако ќе станат достапни за СА.

2.4. Контроли на пристап до складиштата

Сите јавни информации се достапни само во формат којшто може само да се чита, но не и да се менува, без ограничувања. Складиштата се дополнително заштитени од неовластени измени.

3. ИДЕНТИФИКАЦИЈА И АВТЕНТИКАЦИЈА

3.1. Именување

3.1.1. Видови на имиња

Атрибутот на името на субјектот во сертификатите издадени од страна на Македонски Телеком CA го содржи автентицираното име на претплатникот како што е дефинирано за Името (CN) во табелата во Делот 3.1.4 Правила за толкување на различни форми на имиња. Атрибутот на субјектот на сертификатот во CA сертификатот и во сертификатите издадени на претплатниците е во форма на X.501 Единствено име (DN). Единственото име е во форма на X.501 UTF8String и мора да биде присутно во сите издадени сертификати.

3.1.2. Потреба од осмислени имиња

Збирот на атрибути на Единственото име на субјектот на сертификатот на уникатен начин го идентификува секој носител на сертификат и има осмислено значење. Атрибутот на серискиот број, кога го има, се користи за да се разликуваат имињата каде инаку полето на субјектот би било идентично.

3.1.3. Анонимност или псевдонимност на претплатниците

Не е применливо.

3.1.4. Правила за толкување на различни форми на имиња

Полето на името на субјектот се дефинира како X.501 вид на Име (x.500 Единствено име) во согласност со RFC 3280.
Атрибутот на „субјектот“ Македонски Телеком CA и атрибутот на „Издавачот на сертификати“ во CA сертификатот е:

Компонента на Единственото име	Вредност
Држава (C)	MK
Организација (O)	Makedonski Telekom
Име (CN)	Makedonski Telekom CA

x.500 Единственото име во сертификатите издадени од Македонски Телеком CA може да биде во еден од следниве формати:

Компонента на Единственото име	Вредност
Држава (C)	MK
Организација (O)	Makedonski Telekom
Име (CN)	Makedonski Telekom CA
Организациска единица (OU)	Опционо кратко име и даночен број на правното лице;
Организациска единица (OU)	Опционен сектор/ниво на организациска единица (во сертификатите издадени на правни лица)
Име (CN)	• Име и презиме на носителот на сертификатот кога сертификатот е издаден на физичко лице • Целосно квалификувано име на домен или IP адреса кога сертификатот е издаден за сервери, услуги или уреди, и
Сериски број (serialNumber)	Опционен единствен сериски број

Компонента на Единственото име	Вредност
Држава (C)	MK
Организација (O)	Краток назив на правното лице
Организациска единица (OU)	Опционен сектор/ниво на организациска единица (во сертификатите издадени на правни лица)
Име (CN)	• Име и презиме на носителот на сертификатот кога сертификатот е издаден на физичко лице • Целосно квалификувано име на домен или IP адреса кога сертификатот е издаден за сервери, услуги или уреди, и
Сериски број (serialNumber)	Опционен единствен сериски број

Се објавува следниов вид на комбиниран регистар на поништени сертификати CRL:

Компонента на Единственото име	Вредност
Држава (C)	MK
Организација (O)	Makedonski Telekom
Име (CN)	Makedonski Telekom CA: Регистар на поништени сертификати

Се објавува следниов вид на дистрибуиран регистар на поништени сертификати (CRL):

Компонента на Единственото име	Вредност
Држава (C)	MK
Организација (O)	Makedonski Telekom
Име (CN)	Makedonski Telekom CA
Име (CN)	CRLn (n = реден број во Регистарот)

Серискиот број (serialNumber), ако се користи, е вклучен во Единственото име како дел од RDN со повеќе вредности (RDN = CN + serialNumber).

3.1.5. Уникатност на имињата

Македонски Телеком CA назначува во предметот на сертификатот комбинација од атрибути на Единственото име, како што е дефинирано во делот 3.1.2 и 3.1.4, за да се обезбеди недвосмисленост и уникатност на имињата.

3.1.6. Препознавање, автентикација и улога на заштитните знаци

Македонски Телеком CA строго ќе се придржува кон правилата за доделување имиња дадени во точките Видови на имиња и осмислени имиња. На претплатниците им се забранува да бараат име за субјектите со кое би се повредиле интелектуалните и сопственичките права на другите претплатници.
Македонски Телеком CA прави разумни напори за да ги реши споровите кои можат да произлезат од доделувањето на имиња, на пример CA може да контактира со барателот и да се согласи атрибутот на Името (CN) во субјектот да се промени, за да се разликува Единственото име од постојното Единствено име.
Македонски Телеком CA може, по сопствено наоѓање, да го одбие, промени, повторно да го издаде или поништи сертификатот во врска со било кое Единствено име.

3.2. Првично потврдување на идентитетот

3.2.1. Метод за докажување на поседувањето на приватен клуч

Доказ за поседување на приватен клуч од страна на претплатникот се обезбедува преку безбедна размена помеѓу CA апликацијата и PKI клиент апликацијата со користење на Протоколи за управување со сертификати во согласност со PKIX-CMP или PKCS#10 во согласност со RSA PKCS#10 Certification Request Syntax стандардот.

3.2.2. Автентикација на идентитетот на организацијата

Секоја организација (правно лице), што сака да стане претплатник на Македонски Телеком CA, мора да обезбеди доволен доказ дека организацијата го има идентитетот за кој тврди дека го поседува.
Прилогот кон договорот - Формуларот за добивање на квалификуван дигитален сертификат за правни и физички лица, регистрирани за извршување на дејност го пополнува одговорното лице (законски застапник на правниото лице) запишано во централен регистар или од него овластено лице. Одговорното лице или лицето овластено од него го доставува пополнетиот формулар заедно со документите за идентификација и Полномошното на правното лице до овластенатиот тим за регистрација.
Македонски Телеком CA ќе го потврди идентитетот на одговорното лице, како што е дефинирано во Делот 3.2.3 Автентикација на идентитетот на корисникот, и неговото овластување да постапува во име на организацијата како што е дефинирано во Делот 3.2.5 Потврдување на издавачот.
Македонски Телеком CA води евиденција на начините со кои се потврдува идентитетот на организацијата и поединецот кој е овластен да постапува во име на организацијата.

3.2.3. Автентикација на идентитетот на поединецот

Сите поединци (физички лица) кои сакаат да станат претплатник на Македонски Телеком CA ќе бидат предмет на "face to face" верификација. Физичкото лице го идентификува лицето кое е одговорно за прашања поврзани со регистрацијата со увид во важечка лична карта или пасош и копија од личната карта или од пасошот на лицето кое бара сертификат или услуга.
Македонски Телеком CA води евиденција на начините со кои се потврдува идентитетот на корисникот.

3.2.4. Непотврдени информации за претплатникот

Не е применливо.

3.2.5. Потврдување на издавачот

Поединецот кој бара сертификат во име на една организација (правно лице), мора да обезбеди важечка документација за името (корпоративно) на организацијата кое треба да биде внесено во сертификатот во согласност со одредбите од Делот 3.2.2 Автентикација на идентитетот на организацијата. Организациското или корпоративното име, кое треба да биде внесено во сертификатот, мора да биде идентично со целосното или скратеното име на организацијата како што е утврдено во обезбедената документација.
Претплатниците кои доставуваат барања за јавни сертификати за сопствена употреба мора да бидат предмет на автентикација како лицето идентификувано во сертификатот.

3.2.6. Критериуми за меѓусебна соработка

Македонски Телеком CA ќе биде признаен заедно со другите регистрирани издавачи на сертификати од страна на соодветно овластениот државен орган со заеднички договор и во согласност со Законот за податоци во електронски облик и електронски потпис и сите релеватни подзаконски акти во Република Македонија.
Процедурите и практиките на сите меѓусебно поврзани издавачи на сертификати ќе бидат материјално идентични со процедурите и практиките на Македонски Телеком CA дефинирани во оваа Политика за издавање на сертификати. Македонски Телеком CA ги дефинира деталните барања на база на поединечен случај.

3.3. Идентификација и автентикација за барања за обновување на клучеви

3.3.1. Идентификација и автентикација за рутинско обновување на клучеви

Рутинското обновување на клучеви се врши кога ќе истече важноста на сертификатот или периодот на користење на приватниот клуч.
За сертификатите издадени и управувани во согласност со PKIX-CMP, автоматски ќе се генерира нов клуч и соодветен сертификат. Претплатниците се предмет на автентикација со користење на нивните важечки парови на клучеви за електронски потпис.
Претплатниците кои користат сертификати издадени и управувани во согласност со PKIX#10, се предмет на автентикација како што е утврдено во деловите 3.2.2 Автентикација на идентитетот на организацијата и 3.2.3 Автентикација на идентитетот на корисникот по истекот на договорот. За времетраењето на Договорот може да се генерира нов клуч и соодветни сертификати како што е утврдено во Делот 4.1.2 без аплицирање за и автентикација на сертификатот на претплатникот.

3.3.2. Идентификација и автентикација за рутинско обновување на клучеви по поништување

Претплатниците кои бараат обновување на клучеви по поништување се предмет на автентикација како што е утврдено во деловите 3.2.2 Автентикација на идентитетот на организацијата и 3.2.3 Автентикација на идентитетот на корисникот. Ова потврдување се врши пред издавањето на обновениот клуч за сертификатот.

3.4. Идентификација и автентикација на барање за поништување

Барањата за поништување од страна на претплатникот или носителот на сертификатот се доставуваат со испраќање на потпишана апликација за поништување по пошта или факс, лично во канцеларијата на овластен тим за регистрација на CA или со дигитално потпишано барање кое се потпишува со приватен клуч за потпишување на субјектот кој бара поништување.
Овластените поединци, кои бараат поништување преку потпишана електронска комуникација, се предмет на автентикација врз основа на нивниот електронски потпис, дури и кога постои сомневање дека користениот приватен клуч за потпишување е компромитиран.
Во спротивно, овластените поединци се предмет на автентикација врз основа на информациите содржани во досието на претплатникот или како што е предвидено во деловите 3.2.2 Автентикација на идентитетот на организацијата и 3.2.3 Автентикација на идентитетот на корисникот.

4. ОПЕРАТИВНИ ПОСТАПКИ ПОВРЗАНИ СО ПЕРИОДОТ НА ВАЛИДНОСТ НА СЕРТИФИКАТОТ

4.1. Постапки за издавање на сертификат

4.1.1. Кој може да поднесе барање за сертификат

Барање за јавен сертификат може да поднесе:

- секој поединец (физичко лице) кој ги исполнува условите утврдени во: Формуларот за добивање на дигитален сертификат, Политиката за издавање на сертификати на Македонски Телеком CA и релевантниот договор помеѓу CA и крајниот корисник;
- секоја организација (правно лице) која ги исполнува условите утврдени во: Формуларот за добивање на дигитален сертификат, Политиката за издавање на сертификати на Македонски Телеком CA и релевантниот договор помеѓу CA и фирмата на клиентот.

4.1.2. Процес на регистрација и одговорности

Македонски Телеком CA издава сертификати само по потврдување на идентитетот на претплатникот и успешното завршување на процесот на регистрација. Главни чекори на процесот на регистрација на сертификатот се:

- Претплатникот поднесува потпишан формулар за добивање на дигитален сертификати обезбедува важечки документ за идентификација
- Претплатникот ја прифаќа Политиката за издавање на сертификати на Македонски Телеком CA и неговите обврски со потпишувањето на договор за краен корисник
- Формуларот за сертификат го одобрува Овластениот тим за регистрација на Македонски Телеком CA
- Овластен тим за регистрација го доставува формулаотрт за сертификат преку соодветна апликација за регистрација или директно до Овластениот оперативен тим на Македонски Телеком CA
- Овластениот оперативен тим на Македонски Телеком CA креира корисник со соодветен профил на сертификат и генерира кодови за активација кои се состојат од референтен број и авторизациски код. Доколку барањето е испратено преку апликацијата за регистрација, генерирањето на кодовите е автоматски или мануелно. На крајниот корисник му се потребни двата кода за активација за да побара сертификат од CA.
- Кодовите за активација на регистрирањето на сертификат се испраќаат до носителот на сертификатот:
- Референтниот број се испраќа по e-mail до претплатникот на e-mail адресата наведена во формуларот за добивање на дигитален сертификат..
- Авторизацискиот код се испраќа до претплатникот преку пошта; СМС или се дава лично во службите за регистрација во CA испечатен во заштитено плико.

Корисникот користи кодови за активација за да го побара својот сертификат од CA, со користење на клиент апликација обезбедена од страна на Македонски Телеком CA или од интернет пребарувачот. Листата на поддржани клиент апликации и интернет пребарувачи е објавена заедно со упатство на веб страната на Македонски Телеком CA наведена во Делот 2.1 Складишта.

4.2. Обработка на барањето за сертификат

4.2.1. Вршење на функции за идентификација и автентикација

Македонски Телеком CA врши идентификација и автентикација како што е дефинирано во деловите 3.2.2 Автентикација на идентитетот на организацијата и 3.2.3 Автентикација на идентитетот на корисникот.

4.2.2. Одобрување или одбивање на апликацијата за сертификат

Побарувањето на сертификат до Македонски Телеком СА ќе биде одобрено ако се исполнети сите услови како што следува:

- Претплатникот (физичко или правно лице) поднел Формулар за добивање на дигитален сертификат и е извршена успешна идентификација и автентикација согласно член 3.2;
- Барателот има соодветно овластување ако постапува во име на организација (правно лице);
- Формуларот за добивање на дигитален сертификат, документот за идентификација и овластувањата се успешно верификувани;
- Претплатникот има потпишано релевантен договор со Македонски Телеком СА

Во случај некој од горенаведените критериуми да не е исполнет, или ако постои разумно сомневање дека барателот ги прекршува одредбите од овој документ, Договорот за краен корисник или применливото законодавство, тогаш овластен тим за регистрација на Македонски Телеком СА ќе го одбие барањето за сертификација. Македонски Телеком СА го задржува правото да го одбие барањето за сертификација без да ги наведе причините за тоа.

4.2.3. Потребно време за обработка на барањата за сертификат

Формуларот за добивање на дигитален сертификат и документот за идентификација се потврдуваат и обработуваат за време на присуството на барателот од страна на овластен тим за регистрација на Македонски Телеком СА.

4.3. Издавање на сертификатот

4.3.1. Постапки на СА во текот на издавањето на сертификатот

Системот за издавање на сертификати на Македонски Телеком СА по приемот на податоците за сертификација ќе го изврши следното:

- ќе ја потврди важноста на кодовите за активација содржани вопримените податоци;
- ќе потврди дека претплатникот поседува приватен клуч поврзан со јавниот клуч испратен за сертификација, како што е предвидено во Делот 3.2.1 Метод за докажување на поседувањето на приватен клуч;
- ќе потврди дека барањето за сертификат е во согласност со протоколот (PKIX-CMP или PKCS#10) од техничката спецификација.
- ќе го издаде бараниот сертификат ако сите горенаведени услови се исполнети.

4.3.2. Известување до претплатникот од страна на СА за издавање на сертификат

Апликацијата на Македонски Телеком СА веднаш ќе му го презентира издадениот сертификат на барателот така што нема да има потреба од дополнително известување.

4.4. Преземање на сертификатот

4.4.1. Постапка која претставува преземање на сертификатот

Процедурата за регистрација на сертификатот зависи од видот на сертификатот.

- SSCD (smart картичка / Токен) се доставува лично до претплатникот или со препорачана пошта на адресата на претплатникот, ако се работи за физичко лице, додека за правни лица се доставува до адресата на правното лице или се подига лично;
- Сертификатите Доверливост KSN и Доверливост KSN+ се регистрираат со користење на PKIX-CMP протокол и соодветна апликација;
- Сертификатите Доверливост KS, Доверливост KS+, Доверливост CS NS, Доверливост SSL NS, Доверливост VPN NS, Доверливост TS и Доверливост KSCL+, се регистрираат со користење на апликација на интернет пребарувач.

Упатствата за регистрирање на сертификатот можат да се најдат на веб страната на Македонски Телеком CA http://www.telekom.mk/CPS. Претплатникот ќе добие упатства и по e-mail кога ќе го добие референтниот број. Самите упатства се подложни на промена во согласност со моменталните промени во рамките на PKI и не се составен дел од оваа Политика. За успешно регистрирање на сертификатот меродавни се последните објавени упатства.
Претплатникот може да го регистрира сертификатот (ова не се однесува на SSCD сертификатите) само со важечки податоци за активација: референтен број и авторизациски код. Периодот на важност на податоците за активација е ограничен на 30 дена. По истекот на податоците за активација, постапката за регистрација треба да се повтори.
Во случај на неуспешно регистрирање, носителот на сертификатот ќе го пријави проблемот до овластен тим за регистрација на Македонски Телеком CA (види информации за контакт на овластен тим за регистрација во Делот 1.5.2. Лице за контакт).

4.4.2. Објавување на сертификатот од страна на CA

Македонски Телеком CA ги објавува сертификатите во јавен LDAP директориум утврден во Делот 2.1. Складишта. ldap://ldap-ca.ca.telekom.mk. Сертификати кои се користат само за дигитални потписи (само електронски потпис на неотповиклив бит сет) нема да се објавуваат.

4.4.3. Известување за издавање сертификат од страна на CA до другите субјекти

Македонски Телеком CA нема да известува други субјекти.

4.5. Употреба на пар на клучеви и сертификат

4.5.1. Употреба на приватниот клуч и сертификатот на претплатникот

Македонски Телеком CA издава сертификати кои можат да поддржат повеќе употреби на клучеви. Оваа поддршка се обезбедува со вклучување на соодветни продолжувања на користењето на клучевите.
Претплатниците ќе ги користат сертификатите во согласност со keyUsage и extKeyUsage X.509 екстензиите на сертификатите и за целите дефинирани во Делот 1.4.1. Соодветни употреби на сертификатот. Претплатниците мора да ги чуваат нивните приватни клучеви на безбедно место и да преземат заштитни мерки за да спречат компромитирање и неовластено користење на клучевите.

4.5.2. Употреба на јавниот клуч и сертификатот од страна на трето лице

Трето лице ќе го ограничи потпирањето на јавните клучеви содржани во сертификтите издадени од страна на Македонски Телеком CA на соодветна употреба како што е детално наведено во Делот 1.4.1. Соодветни употреби на сертификатот. Третото лице е исто така одговорно за следново:

- Да внимава на ограничувањата на сертификатот и одговорноста на CA како што е детално наведено во оваа Политика.
- Да обезбеди дека сертификатот не е повиштен со пристапување онлајн на кој било и на сите применливи регистри на повиштени сертификати (CRL).
- Веднаш да го извести CA за евентуалното сомневање за злоупотреба или за потврдената злоупотреба на кој било сертификат издаден од CA.

4.6. Обновување на сертификат (без генерирање на нов клуч)

Обновувањето на сертификатот е процес во кој CA издава нов сертификат за истиот субјект. Македонски Телеком CA не дозволува и не поддржува обновување на квалификуван дигитален сертификат чија намена е за дигитално потпишување.

4.6.1. Околности за обновување на сертификати

Не е поддржано, како што е наведено во Делот 4.6. Обновување на сертификат (без генерирање на нов клуч).

4.6.2. Кој може да бара обновување

Не е поддржано, како што е наведено во Делот 4.6. Обновување на сертификат (без генерирање на нов клуч).

4.6.3. Обработка на барањата за обновување на клучот на сертификатот

Не е поддржано, како што е наведено во Делот 4.6. Обновување на сертификат (без генерирање на нов клуч).

4.6.4. Известување до претплатникот за издавање на нов сертификат

Не е поддржано, како што е наведено во Делот 4.6. Обновување на сертификат (без генерирање на нов клуч).

4.6.5. Постапка која претставува преземање на сертификатот со обновен клуч

Не е поддржано, како што е наведено во Делот 4.6. Обновување на сертификат (без генерирање на нов клуч).

4.6.6. Објавување на обновениот сертификат од страна на CA

Не е поддржано, како што е наведено во Делот 4.6. Обновување на сертификат (без генерирање на нов клуч).

4.6.7. Известување за издавање на сертификати од страна на CA до други субјекти

Не е поддржано, како што е наведено во Делот 4.6. Обновување на сертификат (без генерирање на нов клуч).

4.7. Обновување re-key на сертификат (обновување со генерирање на нов клуч)

Обновување re-key на сертификатот е процес во кој на претплатникот му се издава нов сертификат од страна на CA. Новиот сертификат ги содржи истите информации на субјектот како и во стариот сертификат и нови клучеви.

4.7.1. Околности за обновување на клучот на сертификатот

Обновување на кучот на сертификатот се врши:

- по поништување на сертификатот;
- откако истекла важноста на сертификатот или периодот на употреба на клучот;

4.7.2. Кој може да бара сертификат со нов јавен клуч

Обновување на клучот на сертификатот може да побара претплатникот, носителот на сертификатот или овластен претставник кој побарал првично издавање на сертификатот.

4.7.3. Обработка на барањата за обновување на клучот на сертификатот

Обновување на клучот на сертификатите управувани со користење на PKIX-CMP се врши автоматски пред да истече приватниот клуч за потпишување на носителите на сертификатот. Доколку приватниот клуч истече пред да се изврши обновување на клучот на сертификатот, процесот е ист како и за барање за првичен сертификат.
Обновување на клучот на сертификатите управувани со користење на PKCS#10 се врши на истиот начин како и барањето за првичен сертификат по истекот на договорот. За времетраењето на Договорот ќе се генерира нов клуч и соодветни сертификати како што е утврдено во Делот 4.1.2 без аплицирање за и автентикација на сертификатот на претплатникот.

4.7.4. Известување до претплатникот за издавање на нов сертификат

Како што е опишано во Делот 4.3.2 Известување до претплатникот од страна на CA за издавање на сертификат.

4.7.5. Постапка која претставува преземање на сертификатот со обновен клуч

Како што е опишано во Делот 4.4.1 Постапка што претставува преземање на сертификатот.

4.7.6. Објавување на сертификат со обновен клуч од страна на CA

Како што е опишано во Делот 4.4.2 Објавување на сертификатот од страна на CA.

4.7.7. Известување за издавање на сертификати од страна на CA до други субјекти

Како што е опишано во Делот 4.4.3 Известување за издавање сертификат од страна на CA до другите субјекти.

4.8. Измени во сертификатот

Измените во сертификатот е постапка која им олеснува на претплатниците да бараат сертификат со изменети информации. Измените во сертификатот овозможуваат обновување на клучот на сертификатот и се обработуваат како барање за првична сертификација.

4.8.1. Околности за измени во сертификатот

Претплатникот може да побара измени во сертификатот кога информациите за субјектот, како што се името или e-mailot се изменети.

4.8.2. Кој може да побара измени во сертификатот

Измени во сертификатот може да побара претплатникот, носителот на сертификатот или субјектот кој побарал првично издавање на сертификат.

4.8.3. Обработка на барањата за измени во сертификатот

Барањето за измени во сертификатот се обработува како барање за првична сертификација.

4.8.4. Известување до претплатникот за издавање на нов сертификат

Како што е опишано во Делот 4.3.2 Известување до претплатникот од страна на CA за издавање на сертификат.

4.8.5. Постапка која претставува преземање на изменетиот сертификат

Како што е опишано во Делот 4.4.1 Постапка што претставува преземање на сертификатот. Објавување на изменетиот сертификат од страна на CA

4.8.6. Објавување на изменетиот сертификат од страна на CA

Како што е опишано во Делот 4.4.2 Објавување на сертификатот од страна на CA.

4.8.7. Известување за издавањето на сертификат од страна на CA на други субјекти

Како што е опишано во Делот 4.4.3 Известување за издавање сертификат од страна на CA до другите субјекти.

4.9. Поништување и суспензија на сертификатот

4.9.1. Околности за поништување

Поништување на сертификацијата се бара:

- ако е побарано од претплатникот или од носителот на сертификатот;
- ако CA потврди дека носителот на сертификатот починал или ги изгубил своите деловни способности или правното лице престанало да постои или ако околностите, кои имаат значително влијание на целокупната важност на сертификатот, се променети;
- кога која било информација содржана во сертификатот се смета за неточна или за која постои сомневање дека е неточна;
- кога приватниот клуч поврзан со сертификатот е компромитиран или постои сомневање дека е компромитиран;
- кога кои било податоци за активација, како што се лозинка или ЕМБГ, кои се користат за заштита на приватниот клуч, се компромитирани или за кои постои сомневање дека се компромитирани;

- ако CA утврди дека сертификатот не бил соодветно издаден во согласност со Политиката за издавање на сертификати на Македонски Телеком CA;
- претплатникот или носителот на сертификатот ги прекршува одредбите од Политиката за издавање на сертификати на Македонски Телеком CA или применливиот закон (неисполнување на обврските на претплатникот);
- сите останати причини утврдени во Законот за податоци во електронски облик и електронски потпис.

Органот за управување со политиката на Македонски Телеком CA може да го поништи сертификатот на Македонски Телеком CA кога ќе смета дека поништувањето е неопходно.

4.9.2. Кој може да бара поништување

Поништување на сертификатот може да побара:

- Претплатникот (односно правното лице) или субјектот (носителот на сертификат)
- Овластениот претставник кој побарал издавање на сертификат
- Македонски Телеком CA
- Надлежниот суд.

4.9.3. Постапка за барање на поништување

Претплатникот или носителот на сертификатот може да побара поништување на сертификатот на следниве начини:

- со потпишано барање за поништување испратено по пошта или по факс;
- лично во преку контакт на овластените лица за регистрација од Македонски Телеком овластен тим за регистрацијаCA;
- Со телефонски повик при што мора да го знае тајниот збор/лозинка внесен во формуларот за издавање на дигитален сертификат.
- Барањето за поништување на сертификатот се идентификува како што е дефинирано во Делот 3.4. Идентификација и автентикација на барање за поништување.

Поништување заради измени на податоците во самиот сертификат

1. Барање за поништување:

   - Претплатникот го испраќа барањето до овластен тим за регистрација на Македонски Телеком АД по e-mail или лично во канцелариите на локалната служба за регистрација (LRA). За важечко барање се смета она што е потпишано со клучот издаден од Македонски Телеком АД – Скопје.
   - Претплатникот треба да биде идентификуван (лично) доколку се работи за физичко лице или преку одговорното лице на правниот субјект и да го предаде барањето (формуларот) за поништување на сертификатот.
   - Овластен примарен тим за регистрација на Македонски Телеком CA го проверува и го одобрува поништувањето.

2. Овластен примарен тим за регистрација на Македонски Телеком CA го иницира поништувањето на сертификатот преку апликација во која се наведуваат причините за поништување или го испраќа барањето за поништување до Овластениот оперативен тим на Македонски Телеком CA за извршување на поништувањето со наведување на причините за истото.

3. За издавање на нови клучеви претплатниците се предмет на автентикација како што е утврдено во деловите 3.2.2 Автентикација на идентитетот на организацијата и 3.2.3 Автентикација на идентитетот на корисникот.

Поништување заради компромитирање на приватниот клуч

1. Барање за поништување:

   - Претплатникот го испраќа барањето до овластен тим за регистрација на Македонски Телеком СА по e-mail или лично.
   - Со телефонски повик при што мора да го знае тајниот збор/лозинка внесен во иницијалното барање за регистрација
   - Претплатникот треба да биде идентификуван (лично) доколку се работи за физичко лице или преку одговорното лице на правниот субјект и да го предаде барањето (формуларот) за поништување на сертификатот.
   - Овластен примарен тим за регистрација на Македонски Телеком СА го проверува барањето и го одобрува поништувањето.

2. Овластен примарен тим за регистрација на Македонски Телеком СА го иницира поништувањето на сертификатот преку апликација со наведување на причината „компромитиран“ или го испраќа барањето за поништување до Овластениот оперативен тимна Македонски Телеком СА за извршување на поништувањето со наведување на причината „компромитиран“.

3. Во случај на барање за издавање на нови клучеви, претплатниците се предмет на автентикација како што е утврдено во деловите 3.2.2 Автентикација на идентитетот на организацијата и 3.2.3 Автентикација на идентитетот на корисникот.

Поништување на сертификатот заради неисполнување на обврските од страна на претплатникот

Доколку претплатникот не ги исполнува своите обврски и должности кон и во согласност со оваа политика и договорот склучен со Македонски Телеком АД - Скопје, може да дојде до поништување на неговиот сертификат, при што:

1. Овластен тим за регистрација го проверува дигиталниот потпис на претплатникот во СА
2. Овластениот оперативен тим на Македонски Телеком СА го поништува сертификатот наведувајќи ги причините за истото
3. Овластениот оперативен тим на Македонски Телеком СА дополнително го деактивира претплатникот од СА и ги брише неговите податоци од базата на податоци.

4.9.4. Дозволено време од барањето за поништување до поништувањето на сертификатот

Субјектот, кој станал свесен за околностите според кои е потребно поништување на сертификатот, треба да побара поништување во најкус можен рок и без непотребно одложување.
Македонски Телеком СА може да го изврши поништувањето на сертификатот како резултат на неисполнување на обврските од страна на претплатникот веднаш по истекот на временскиот период во рамките на кој претплатникот требало да ги исполни своите обврски.

4.9.5. Временски период во рамките на кој СА мора да го обработи барањето за поништување

Во други случаи на поништување на сертификати, временскиот период помеѓу приемот на барањето и поништувањето на сертификатот не треба да биде подолг од 24 часа.

4.9.6. Поништување со проверка на барањето за трети лица

Трето лице треба да го провери регистарот на поништени сертификати на Македонски Телеком СА пред да користи некој сертификат издаден од Македонски Телеком СА. Доколку не може да

се изврши валидна проверка на поништување поради грешка во системот или губење на услугата, не треба да се прифаќа ниту еден сертификат од Македонски Телеком CA.
Трето лице кое ќе добие пристап до CRL треба да го верификува CRL со проверка на својот дигитален сертификат со соодветниот сертификат од Македонски Телеком CA и треба да провери дали истиот е истечен.

4.9.7. Зачестенот на објавување на регистар на поништени сертификати CRL (ако е применливо)

Македонски Телеком CA го објавува новиот регистар на поништени сертификати редовно на секои 24 часа. Периодот на важност на CRL изнесува најмногу 48 часа. Македонски Телеком CA го ажурира CRL веднаш или што е можно поскоро по обработката на валидното барање за поништување.

4.9.8. Максимална латентност за CRL (ако е применливо)

Не е утврдено. (Види Дел 4.9.7)

4.9.9. Можност за онлајн проверка на поништувањето/статусот

Не е поддржано.

4.9.10. Барања за онлајн проверка на поништувањето

Не е применливо.

4.9.11. Други достапни форми на објавување на поништувањето

Не е применливо.

4.9.12. Посебни барања во врска со компромитирањето на клучот

Не се потребни посебни барања во случај на компромитирање на клучот на Носителот на сертификатот.

4.9.13. Околности за суспензија

Суспенција на сертификатот може да се побара кога носителот на сертификатот ќе замине на подолг временски период, на пример, на породилно отсуство. Македонски Телеком CA може исто така да ги суспендира сертификатите на претплатникот при верификација на барањето за поништување на сертификатот.
Суспендираните сертификати се објавуваат во регистарот на поништени сертификати (CRL) за време на периодот на суспензија.

4.9.14. Кој може да побара суспензија

Суспензија и укинување на суспензијата на сертификат може да се побара од страна на:

- Претплатник или субјект (носител на сертификат)
- Овластен претставник којшто побарал издавање на сертификат
- Овластен тим за регистрација на Македонски Телеком CA
- Членовите на Македонски Телеком CA

4.9.15. Процедура за барање на суспензија

Како што е опишано во Делот 4.9.3 Постапка за барање на поништување

4.9.16. Ограничувања на периодот на суспензија

Периодот на суспензија не е ограничен.

4.10. Услуги во однос на статусот на сертификатот

4.10.1. Оперативни карактеристики

Статусот на сертификатот се објавува со помош на X.509 Регистар на поништени сертификати (CRL). CRL се објавува преку LDAP директориумот и веб страницата. Точните локации (LDAP и http URLs) се објавуваат со помош на X.509 CRL екстензија за дистрибуциски точки.

4.10.2. Достапност на услуга

Македонски Телеком CA гарантира достапност на статус на сертификатот само во текот на работното време, со максимално годишно непланирано нефункционирање од 7 (седум) дена годишно.

4.10.3. Опциони карактеристики

Не е применливо.

4.11. Крај на претплатата

Услугата завршува по истекот или поништувањето на сертификат. . Македонски Телеком CA ја чува документацијата, и податоците за сертификатите најмалку 5 години по истекот на услугата.

4.12. Чување на копии на клучеви кај овластени трети страни и нивно обновување

Македонски Телеком CA не поддржува чување на копии на клучеви кај овластени трети страни.

4.12.1. Политики и практики за чување на копии на клучеви кај овластени трети страни и нивно обновување

Обновувањето се поддржува само за сертификати за доверливост со обновување на клуч (NSER и NSER+) коишто се управуваат со користење на PKIX-CMP и соодветна клиент апликација обезбедена од Македонски Телеком CA.
Обновувањето на клуч може да се побара од некој претплатник, носител на сертификат или овластен претставник којшто побарал првично издавање на сертификат. Идентитетот на барателот се потврдува како што е утврдено во Делот 3.2 Првично потврдување на идентитетот.
Обновувањето на клучот и пријавувањето за сертификат се вршат на ист начин како и првичното пријавување за сертификат.
Обновувањето на клучот мора секогаш да биде одобрено со две операции на администраторите на Македонски Телеком CA, со соодветни дозволи.

4.12.2. Политика и практики за енкапсулација на клучот за сесијата и обновување

Не е применливо.

5. КАПАЦИТЕТ, УПРАВУВАЊЕ И ОПЕРАТИВНИ КОНТРОЛИ

5.1. Физички контроли

5.1.1. Мапа на локација и конструкција

Техничките средства на Македонски Телеком СА (мрежни компјутерски системи, операторски терминали и ИТ ресурси) се наоѓаат во посебни, континуирано набљудувани простории (локации) во обезбедена зграда (објект).
Компонентите на системот и работењето на Македонски Телеком СА се наоѓаат во физички заштитено опкружување со цел да се спречи неовластена употреба, пристап, или откривање на чувствителни информации. Контролите на физичката безбедност се имплементирани во согласност со важечките најдобри практики за физичка безбедност. Заштитните мерки вклучуваат:

- Пристапот е ограничен на вработените на Македонски Телеком СА
- Сите други пристапи се вршат под придружба, а секој пристап се евидентира
- На вработените за одржување и услуги се врши видео мониторинг во текот на нивните посети
- Безбедни електронски брави и систем за пристап
- Непрекинат надзор, чување од страна на чувари на лице место и видео мониторинг од мониторинг центарот на зградата

5.1.2. Физички пристап

Само овластените вработени на Македонски Телеком СА, во согласност со нивната функција, имаат пристап до одредени делови на инфраструктурата на Македонски Телеком СА. Секој пристап до локациите на Македонски Телеком СА се снима електронски и се внесува во електронскиот дневник за пристап до локациите.

5.1.3. Напојување и климатизација

ИТ центарот на Македонски Телеком СА е опремен со климатизер за контрола на топлината и влажноста, при што сите критични компоненти се поврзани со непрекинато напојување (UPS) единици, коишто исто така го регулираат напојувањето.

5.1.4. Изложеност на вода

Во просториите на Македонски Телеком СА нема водоводни инсталации. Преземени се сите технички мерки за заштита од водоводните инсталации во опкружувањето.

5.1.5. Превенција и заштита од пожари

Просториите на Македонски Телеком СА се заштитени со систем за рано откривање на пожари, автоматски аларм за пожар и систем за гасење на пожари.

5.1.6. Складирање на носители на податоци

Сите компјутерски носители на податоци што содржат податоци на Македонски Телеком СА, вклучувајќи ги и носителите на бекап на податоци, се чуваат во огноотпорни контејнери, од кои едниот се наоѓа во рамките на Македонски Телеком СА а другиот се наоѓа на оддалечена безбедна локација.

5.1.7. Отстранување на отпадот

Пред да се фрлат, документите во печатена форма и магнетните носители на податоци се уништуваат на начин на кој што информацијата неможе да се репродуцира. СА ги задржува сите нефункционални хардверските компоненти за цели на безбедно ослободување од истите.

5.1.8. Складирање на резервни копии на оддалечена локација

Македонски Телеком СА користи безбедна оддалечена локација за складирање на податоци на носители на податоци. Носителите на податоци се чуваат на оддалечена безбедна локација

заштитена од надворешни влијанија и со контролиран пристап, којашто има високо ниво на заштита, односно сеф. Пристапот до сефот е ограничен само на две овластени лица.

5.2. Процедурални контроли

5.2.1. Доверливи улоги

Во зависност од нивната улога, вработените на Македонски Телеком СА може да има корисничка сметка на главниот СА компјутер, на СА апликацијата, или и на главниот СА компјутер и на СА апликацијата. СА апликацијата што ја користи Македонски Телеком СА содржи голем број на доверливи улоги коишто му се доделуваат на вработените на СА во согласност со надлежностите на истиот. Привилегиите доделени на сметката на оперативниот систем на главниот СА компјутер го ограничуваат пристапот на вработените на Македонски Телеком СА до оној степен што им е потребен за извршување на должностите.
Распоредот на доверливите улоги е даден во табелата подолу:

Одговорни лица на Македонски Телеком СА	Ниво на пристап на оперативниот систем	Ниво на пристап на СА апликацијата
Главен корисник на СА (CA Master User)	Не	Да
Службеник за безбедност на СА (CA Security Officer)	Да	Да
Администратор на СА	Не	Да
Вработени на Овластен тим за регистрација	Не	Да
Правен советник	Не	Не

За да се обезбеди поделба на должностите се користат различни нивоа на физичка контрола и контрола на пристап до системите базирани на улогите доделени во СА апликацијата и привилегиите на сметката на системот.
Доверливите улоги се:

Улога во Македонски Телеком СА	Одговорности
Главен корисник на СА	• Ја одобрува првичната СА апликација и конфигурацијата на хардверскиот криптографски модул (HSM) и неговото тековно одржување • Ги иницира и ги стопира сервисите на СА апликацијата • Ги креира почетните PKI Службеници за безбедност • Ги обновува PKI Службениците за безбедност кога ќе ја заборават својата лозинка • Ја обновува услугата за СА администрација во случај нејзиниот профил да биде оштетен • Иницира замена на HSM • Ги обновува smart картичките на операторот на HSM • Врши обнова и повторно шифрирање на базата на податоци на СА

Службеник за безбедност на CA	• Управува со корисничките сметки на останатите PKI Службеници за безбедност и PKI администратори • Управува со корисничките сметки на претплатниците • Управува со обновувањето на клучевите на претплатниците • Ги обработува записите од ревизиите • Ја утврдува и ја изменува безбедносната политика на CA апликацијата • Управува со профилите на сертификатот на CA апликацијата • Непосредно го поврзува Македонски Телеком CA со надворешни CA-и • Составува извештаи
Администратор на CA	• Управува со корисничките сметки на претплатниците • Управува со сертификати • Составува извештаи
Администратор на директориум	• Додава и брише корисници во/од директориумот • Го конфигурира директориумот

5.2.2. Потребен број на лица по задача

Потребни се две (2) лица со соодветна доверлива улога коишто ќе ги вршат следниве задачи:

- Обновување на декрипцискиот клуч на крајниот корисник
- Поништување на клуч издаден од CA
- Утврдување на политики за клучевите и сертификатите
- Креирање на кориснички сметки со улога на CA службеник за безбедност или CA администратор
- Ажурирање на приватните клучеви издадени од страна на Македонски Телеком CA
- Промена на лозинки на корисничките сметки на главните корисници на CA
- Непосредно поврзување со надворешни CA

Една личност може да ги извршува сите останати задачи. Сите активности што се вршат од носителите на доверливи CA улоги се евидентираат и се ревидираат.

5.2.3. Идентификација и автентикација за секоја улога

PKI вработените со доверлива CA улога се подложуваат на безбедносна проверка пред да бидат назначени да работат како членови на Оперативниот тим на Македонски Телеком CA. Оперативнииот тим на Македонски Телеком CA ќе биде проверен во согласност со правилата дефинирани во оваа политика, пред да им биде доделена некоја од следниве привилегии:

- Додавање на запис на соодветната листа за пристап за влез во заштитените простории на Македонски Телеком CA (безбедносна и оперативна зона)
- Добивање на сертификат потребен за вршење на доделената доверлива улога
- Добивање на корисничка сметка на оперативниот систем
- Добивање на smart картичка / токен
- Корисничките сметки на оперативниот систем и на апликациите и сертификатите се креираат за секое одговорно лице поединечно.

Заедничкото користење на налози или сертификати меѓу вработените на Македонски Телеком СА е забрането. Вработените се ограничени на активности кои се авторизирани за дадената улога преку контролата која ја поставува апликацијата, оперативниот систем и процедурите на Македонски Телеком СА.
Вработените на Македонски Телеком СА ги користат smart картичките/токените само за извршување на должностите кои му се доделени во рамките на неговите улоги.

5.2.4. Улоги кои бараат поделба на должностите

Со цел да се задржи поделбата на должностите, мора да постои усогласеност со следнава матрица како што е прикажано во табелата:

Улога на Македонски Телеком СА	Корисничка сметка на оперативниот систем	Корисничка сметка на апликацијата	Улога на СА апликацијата
Главен корисник на СА	Да	Не	Главен корисник
Службеник за безбедност на СА	Не	Да	Службеник за безбедност
Администратор на СА	Не	Да	Администратор
Службеник на СА	Не	Да	Краен корисник
Администратор на директориум	Да	Не	Не е применливо
Администратор на оперативниот систем	Да	Не	Не е применливо

Администраторот на оперативниот систем ги има потребните права за инсталација, конфигурирање и одржување на главниот компјутерски хардвер и софтвер на СА.

5.3. Контрола на вработените

Одговорните лица на Македонски Телеком СА се вработени на неопределено или определено време, ангажирани врз основа на договор со кој се одредуваат нивните работни должности. Тие треба да се соодветно квалификувани за извршување на работните должности.
Овластен тим за регистрација се вработени на неопределено или определено време. Тие треба да се соодветно квалификувани за извршување на работните должности.
Вработените на Македонски Телеком СА и вработените во овластен тим за регистрација се обврзуваат со договор дека не смеат да објавуваат или соопштуваат доверливи информации поврзани со безбедноста на Македонски Телеком СА или информации за претплатниците.
Врз основа на договорот, претплатниците се запознаени со безбедносните правила кои е потребно да ги применуваат со цел да ги заштитат нивните компјутери и уредите за енкрипција, како и со оваа Политика според која се издадени нивните сертификати.

5.3.1. Барања за квалификации, искуство и безбедносна проверка

Во практиките за вработување во Македонски Телеком се земаат предвид барањата за потребни квалификации за секоја позиција, претходните назначувања на потенцијалните кандидати и бројот на години поминати на слични позиции.

5.3.2. Процедури за проверка на биографските податоци

СА ја реализира проверката и политиката во однос на вработените како што е утврдено во Делот 6.1.2 Проверка на вработените и барањата на ISO/IEC 27001.

5.3.3. Потребна обука

Македонски Телеком СА обезбедува обука за сите свои вработени.
За одговорните лица на Македонски Телеком СА, обуката вклучува постапки за заштита на системот и податоците, обука специфична за нивните улоги и одговорности, обука за користење на апликацијата на Македонски Телеком СА и обука за преземање на постапки за опоравување на системот од катастрофи и процедура за континуитет на деловното работење.
За вработените на овластен тим за регистрација, обуката вклучува постапки за заштита на системот и податоците и обука специфична за нивните улоги и одговорности.

5.3.4. Зачестеност и барања за повторна обука

Согласно актуелните потреби се организираат потребни обуки за вработените на Македонски Телеком СА.

5.3.5. Зачестеност и редослед на ротациите на работните места

Ротација на работни места не се спроведува.

5.3.6. Санкции за неовластени активности

Во случај да биде извршена или пак да постои сомневање дека била извршена неовластена активност од страна на лице кое извршува обврски во врска со работата на Македонски Телеком СА или Овластен тим за регистрација, Македонски Телеком СА ќе го оневозможи неговиот/нејзиниот понатамошен пристап до техничките средства (хардвер и софтвер), Македонски Телеком СА ќе ги суспендира или поништи сите сертификати издадени на тоа лице.
Извршените неовластени активности се пријавуваат на надлежните државни органи и институции во согласност со постоечките закони, подзаконски акти и интерни правила.

5.3.7. Барања во однос на независните изведувачи

Македонски Телеком СА обично не ангажира надворешни лица на која било чувствителна активност. Онаму каде што се ангажираат такви вработени, се спроведуваат соодветни проверки. Сите изведувачи се обврзани да потпишат договор за доверливост во согласност со внатрешните прописи на Македонски Телеком АД - Скопје.

5.3.8. Документација што се доставува на вработените

Овластените лица на Македонски Телеком СА имаат пристап до документацијата на СА, вклучително и хардверот, софтверот и прирачниците, процедурите за работа, процедурите за безбедност и противпожарна заштита, процедурите за контрола на пристап и оваа Политика за издавање на сертификати.

5.4. Процедури за ревизија на записите

5.4.1. Видови на настани што се евидентираат

Следниве видови на настани се евидентираат автоматски или рачно од страна на Македонски Телеком СА за цели на ревизија:

- Настани поврзани со клучеви и сертификати на претплатници, издавање, преземање, поништување, суспендирање
- Настани поврзани со клучеви на СА
- Настани поврзани со администрацијата, чувањето на податоците и јавниот именик
- Настани на оперативните системи и хардверската опрема
- Настани кои се поврзани со физичкиот пристап до СА

Најголемиот дел од електронските записи го содржат датумот и времето на секој настан и идентитетот на субјектот што го креирал. Сите записи на физичките записи од ревизии се идентификуваат според датум и време.
Записите се собираат и се консолидираат во Овластениот оперативен тим на Македонски Телеком СА.

5.4.2. Зачестеност на обработка на записите

Записите ќе се прегледуваат еднаш дневно.
Прегледот вклучува:

- Собирање на сите записи од последниот преглед
- Преглед на собраните записи
- Анализа и известување во врска со сите релевантни случувања со цел да се разреши или да се ограничи ескалацијата на проблемите.

5.4.3. Период на складирање на записите

Најмалку 5 години, согласно релевантните закони.

5.4.4. Заштита на записите

Пристап до главниот компјутерски систем што содржи записи имаат само овластени лица, со комбинација од физички контроли и компјутерски безбедносни контроли. Компјутерскиот систем, картриџите за бекап на записите и физичките записи се чуваат во зоната со висок степен на безбедност на Овластениот оперативен тимна Македонски Телеком АД којашто е опремена со физички и окружувачки контроли како што е дефинирано во Делот 5.1. Физички контроли.
На вносовите за записите што се креирани од главниот оперативен систем на CA им се става поединечна ознака за време. Оперативниот систем го заштитува интегритетот на своите записи со користење на функционалност на оперативниот систем.
На вносовите за записите што се креирани од апликацијата на CA им се става поединечна ознака за време. Апликацијата на CA го заштитува интегритетот на своите записи со користење на енкрипција на јавен клуч и со верификација на секој внос при враќање.

5.4.5. Процедури за креирање на резервни копии од записите

Резервни копии од записите се прават секојдневно, во рамките на редовниот бекап на главниот систем на Македонски Телеком CA. Back up лентите со резервни копии се чуваат во сеф кај Овластениот оперативен тим на Македонски Телеком CA.
Секои две недели, лентите со бекапот направен на тој ден, коишто содржат консолидирана копија на фајловите со записите, се испраќаат на безбедна надворешна локација за складирање за цели на надворешно складирање и архивирање.

5.4.6. Систем за собирање на записи од ревизии (внатрешен наспроти надворешен)

Системот за собирање на записи за ревизија на Македонски Телеком CA е комбинација од автоматски и рачни процеси што се спроведуваат од страна на главниот оперативен систем на CA, апликацијата на CA и вработените на Македонски Телеком CA, како што е наведено во табелата подолу:

Евидентирани настани	Систем за собирање	Субјект што го врши евидентирањето
Стартување и исклучување на апликацијата на CA	Автоматски	Главен оперативен систем на CA
Стартување и исклучување на главниот оперативен систем на CA	Автоматски	Главен оперативен систем на CA
Успешни и неуспешни обиди да се креираат, менуваат, отстрануваат, оневозможуваат, овозможуваат и да се враќаат претплатници	Автоматски	Апликација на CA
Успешни и неуспешни обиди да се креираат, менуваат, отстрануваат, оневозможуваат, овозможуваат и да се враќаат сметки на главниот оперативен систем на CA	Автоматски	Главен оперативен систем на CA
Успешни и неуспешни обиди да се креираат, менуваат, отстрануваат, оневозможуваат, овозможуваат и да се враќаат сметки на апликацијата на CA	Автоматски	Апликација на CA
Успешни и неуспешни обиди за најавување и одјавување од апликацијата на CA	Автоматски	Апликација на CA
Успешни и неуспешни обиди за најавување и одјавување од главниот компјутер	Автоматски	Главен оперативен систем на CA
Неовластени обиди за пристап до системските фајлови	Автоматски	Главен оперативен систем на CA

Евидентирани настани	Систем за собирање	Субјект што го врши евидентирањето
Неовластени обиди за пристап до PKI мрежата	Автоматски	Рутери и главен оперативен систем на CA
Успешни и неуспешни обиди за генерирање, ажурирање и враќање на клучеви	Автоматски	Апликација на CA
Успешни и неуспешни обиди за креирање, ажурирање, суспендирање, поништување и враќање на сертификати	Автоматски	Апликација на CA
Промени во политиките за креирање на сертификати (на пример, периодот на важност)	Автоматски	Апликација на CA
Успешни и неуспешни обиди од страна на CA да се поврзе, да чита и да пишува во директориумот	Автоматски	Апликација на CA
Промени во единственото име	Автоматски	Апликација на CA
Резервна копија и враќање на база на податоци на CA	Автоматски	Апликација на CA и главен оперативен систем на CA
Креирање резервна копија, враќање и прочистување на записите	Автоматски	Главен оперативен систем на CA и вработени на CA
Физички пристап до CA локации	Рачно	Вработени на CA
Промени на конфигурацијата на системот	Рачно	Вработени на CA
Ажурирање на софтвер и хардвер	Рачно	Вработени на CA
Планирано и непланирано одржување на системот и локацијата	Рачно	Вработени на CA
Разлики и компромитирања	Рачно	Вработени на CA
Промени кај вработените	Рачно	Вработени на CA
Уништување на одредени информации	Рачно	Вработени на CA

5.4.7. Известување на субјектот што предизвикал настан

Субјектот што предизвикал настан на ревизија не се известува.

5.4.8. Проценка на ранливост

Македонски Телеком CA спроведува проценки на ранливост како дел од процедурите за обработка на записи.

5.5. Архивирање на евиденција

5.5.1. Видови на архивирана евиденција

Македонски Телеком CA ја чува следнава евиденција:

- Информациите за ревизија утврдени во Делот 5.4 Процедури за ревизија на записите.
- Претплатничките договори и сите формулари што му припаѓаат на барањето
- Сертификати, статус за поништување на сертификат
- Приватни декрипциски клучеви на претплатникот (доколку е применливо)

5.5.2. Период на чување на архивата

Најмалку 5 години, согласно релевантните закони.

5.5.3. Заштита на архивата

Пристап до архивските информации на Македонски Телеком CA им се дава на вработените на CA во согласност со потребата.

5.5.4. Процедури за креирање на резервни копии од архивата

Архивираните податоци се чуваат на посебен медиум за архивирање или како копија во печатена форма. Еднаш неделно, овие архиви се преместуваат на безбедно место на оддалечена локација наменета за нивно складирање.

5.5.5. Барања за ставање на временски жиг на записите

Архивските записи се означуваат за време во моментот на нивното создавање, со употреба на системското време на системот на кој е снимен настанот.

5.5.6. Систем за собирање на архива (внатрешен или надворешен)

Македонски Телеком СА користи интерен систем за бекап и архивирање на Македонски Телеком СА.

5.5.7. Процедури за добивање и верифицирање на архивски информации

Пристап до задржаните податоци му се дозволува на претставник на Македонски Телеком СА онолку колку што е потребно или во согласност со применливиот закон.

5.6. Промена на клучеви

Промената на клуч на приватниот клуч на СА ќе се изврши при истекот на 70% од векот на траење на сертификатот на СА или порано. При промената на клуч на приватниот клуч на СА, на носителите на сертификат ќе им биде ставен на располагање нов СА јавен клуч преку веб и онлајн складиштето за директориуми на СА.

5.7. Компромитирање и опоравување од катастрофи

5.7.1. Процедури за постапување со инциденти и компромитирања

Македонски Телеком СА спроведува процедура во согласност со ISO / IEC 27001 за одговарање на безбедносни инциденти и дефекти.

5.7.2. Оштетени компјутерски ресурси, софтвер, и / или податоци

Македонски Телеком СА има имплементирано план за непредвидени ситуации и за опоравување од катастрофи кој предвидува решенија за враќање на работењето по оштетување на компјутерските ресурси, софтверот и податоците.

5.7.3. Процедури кои се применуваат во случај на компромитирање на приватен клуч на субјект

Кога приватниот СА клуч за потпис е компромитиран, СА ќе ги поништи и повторно ќе ги објави сите сертификати на Македонски Телеком СА што се користат во моментот.

5.7.4. Капацитет за континуитет на деловното работење по катастрофа

Поради природни катастрофи или друг вид на вонредни состојби,ако има потреба работењето на СА операции и ИТ центарот ќе биде повторно воспоставен на друга локација, со помош на бекап податоците. Македонски Телеком СА ќе ги преземе сите разумни мерки со цел услугите да бидат повторно воспоставени во најкус можен рок, но не подоцна од пет (5) работни дена.

5.8. Престанок на работата на СА или RA

Во случај на доброволен престанок на работата на Македонски Телеком СА, СА:

- ќе ги извести сите постојни претплатници, корпорации-клиенти и сите непосредно поврзани СА-и најмалку деведесет (90) дена пред својата намера да престане со работењето.
- ќе ги објавуви информациите за престанокот на услугите на јавните веб страни на Македонски Телеком АД.
- ќе ги поништи сите валидни сертификати на или по истекот на отказниот рок.

- ќе обезбеди достапност и пристап до релевантните CRL-и за период од 6 месеци по поништувањето на сите сертификати.
- ќе се увери дека архивите ќе се задржат најмалку пет (5) години од последниот ден на работењето.

6. КОНТРОЛИ НА ТЕХНИЧКА ЗАШТИТА

6.1. Генерирање и инсталирање на парот клучеви

6.1.1. Генерирање на парот клучеви

Парот на клучеви за потпишување на Македонски Телеком CA се креира на хардверски криптографски модул (Hardware Security Module - HSM) во текот на почетната постапка за генерирање на CA клучеви и е заштитен со главен (master) клуч. Во текот на генерирање на CA парот криптографски клучеви се користи повеќекратна автентикација на овластените лица и заштита која важи за просториите на Македонски Телеком CA.
Претплатничкиот енкрипциски пар на клучеви со дигитална идентификација и со обновување на клучевите (key recovery) го генерира CA апликацијата. Претплатничкиот енкрипциски пар на клучеви со дигитална идентификација без обновување на клучевите (key recovery) го генерира PKI корисничката апликација.
Парот на клучеви за потпишување на носителот на сертификатот секогаш ги генерира PKI корисничката апликација.

6.1.2. Доставување на приватниот клуч до претплатникот

Приватниот декрипциски клуч којшто го генерира CA апликацијата се доставува до PKI корисничката апликација на претплатникот со користење на PKIX-CMP протоколот.
Приватните клучеви за потпишување и декрипциските клучеви со дигитална идентификација без обновување на клучевите (key recovery) ги генерира PKI корисничката апликација така што не е потребно тие да се доставуваат до носителот на сертификатот.

6.1.3. Доставување на јавниот клуч до издавачот на сертификатот

Парот на клучеви за потпишување и парот на клучеви со дигитална идентификација коишто се управуваат со користење на PKCS#10 ги генерира PKI корисничката апликација, што значи дека јавните клучеви треба да се достават до CA апликацијата на сигурен начин со цел да се генерираат сертификати со јавен клуч. Јавните клучеви се доставуваат до CA апликацијата со користење на PKIX-CMP протоколот, или во PKCS#10 формат.
Доверливиот пар на клучеви со дигитална идентификација со обновување на клучевите (key recovery), управувани со користење на PKIX-CMP, ги генерира CA апликацијата, па оттука нема потреба од доставување на јавни екрипциски клучеви.

6.1.4. Доставување на CA јавен клуч до трети лица

Јавниот клуч за верификација на потпис на Македонски Телеком CA се доставува во CA вид на сертификат до претплатникот со користење на PKIX-CMP протоколот или во PKCS#7 формат како дел од постапката за регистрација.
Јавниот клуч на Македонски Телеком CA е достапен во вид на сертификат на следните локации:
Во јавниот LDAP директориум: ldap://ldap-ca.ca.telekom.mk
На веб страната: http://ca.telekom.mk
CA сертификатот можете да го добиете и доколку се обратите во Македонски Телеком CA (види 1.5.2. Лице за контакт).
Во секој случај, субјектот кој ги користи сертификатите на Македонски Телеком CA мора да ја потврди автентичноста и интегритетот на CA сертификатот.

6.1.5. Должини на клучевите

CA го генерира својот асиметричен приватен клуч за потпишување со RSA должина од минимум од 3072 битови.
Носителот на сертификатот го генерира својот асиметричен приватен клуч за потпишување со RSA должина од минимум 2048 битови. Носителите на сертификатот коишто користат smart картички можат да користат и клучеви со RSA должина од 1536 битови.

6.1.6. Генерирање и проверка на квалитетот на параметрите на јавниот клуч

Македонски Телеком CA во моментов не издава DSA (Digital Signature Algorithm) клучеви.

6.1.7. Намена за користење на клучевите (дефинирана во X.509 вер. 3 поле Key Usage)

Македонски Телеком го користи keyUsage полето во сертификатите за означување на намената на јавните клучеви во сертификатите, како што е дефинирано во RFC 3280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”:

a) **електронски потпис - digitalSignature:** за верификација на дигиталниот потпис кој има задачи поинакви од оние назначени под б), ѓ) или е) подолу.
b) **неотповикливост - nonRepudiation**: за верификација на дигиталниот потпис што е користен во обезбедување на неотповикливост, кој штити од потпишување и непризнавање на истата акција. (исклучок: потпишување на сертификат или потпишување на регистар на поништени сертификати како во ѓ) или е) подолу);
c) **криптирање на клуч - keyEncipherment**: за енкрипција на клучеви или други доверливи информации. На пр. транспорт на клучеви.
d) **криптирање на информации - dataEncipherment**: за енкрипција на претплатничките информации, но не и енкрипција на клучеви или други доверливи информации како во в) погоре.;
e) **keyAgreement**: се користи како јавен клуч;
f) **keyCertSign** за верификација на потписот на издавачот на сертификатите;
g) **cRLSign**: за верификација на потписот на издавачот на сертификати на регистарот на поништени сертификати;
h) **enchiperOnly**: јавен keyAgreement со функција dataEncipherment (криптирање на информациите) и се користи со подесен keyAgreement бит. (значењето на другите битови за сетирањето не е дефинирано);
i) **decipherOnly:** јавен keyAgreement со функција dataDecipherment (декрипција на информациите) и се користи со подесен keyAgreement бит. (значењето на другите битови за сетирање не е дефинирано);

Македонски Телеком покрај keyUsage користи и Extended Key Usage (extKeyUsage) за дополнително означување или ограничување на намената на јавните клучеви во сертификатите, како што е дефинирано во RFC 3280 “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”:

serverAuth: TLS WWW server authentication
clientAuth: TLS WWW client authentication
codeSigning: Signing of downloadable executable code
emailProtection: E-mail protection
timeStamping: Binding the hash of an object to a time
OCSPSigning: Signing OCSP responses

Намената е наведено во сертификатите што ги издава Македонски Телеком CA во keyUsage и extKeyUsage полето во зависност од видот на сертификатот и видот на јавниот клуч во сертификатот, како што се прикажано во табелата подолу.
За потпишување на сертификатот и регистарот на поништени сертификати се употребува исклучиво приватниот криптографски клуч на Македонски Телеком CA.
Криптографските клучеви и сертификати на одговорните лица за Македонски Телеком CA се користат само за работа со техничките средства кои ги поседува Македонски Телеком (хардвер и софтвер).
Останатите сертификати на Македонски Телеком CA можат да се употребуваат за намени прикажани во полето Key Usage како што е прикажано во табелата подолу.

Намена за различни видови на сертификати и различните видови на јавни клучеви во сертификатите

Вид на сертификат		Намена во keyUsage полето
Македонски Телеком CA	сертификат со јавен клуч за верификација (public verification key cerificate)	keyCertSign, cRLSign

Вид на сертификат		Намена во keyUsage полето
Доверливост KS+	сертификат со јавен клуч за верификација (public verification key cerificate)	digitalSignature, keyEncipherment
Доверливост KS	сертификат со јавен клуч за верификација (public verification key cerificate)	digitalSignature, keyEncipherment
Доверливост KS++	сертификат со јавен клуч за верификација (public verification key cerificate)	digitalSignature, keyEncipherment
Доверливост KSSC+	сертификат со јавен клуч за верификација (public verification key cerificate)	digitalSignature, keyEncipherment (Smart Card Logon (1.3.6.1.4.1.311.20.2.2) Encrypting File System (1.3.6.1.4.1.311.10.3.4) Secure Email (1.3.6.1.5.5.7.3.4) Client Authentication (1.3.6.1.5.5.7.3.2) in enhanced key usage)
Доверливост KSSC++	сертификат со јавен клуч за верификација (public verification key cerificate)	digitalSignature, keyEncipherment (Smart Card Logon (1.3.6.1.4.1.311.20.2.2) Encrypting File System (1.3.6.1.4.1.311.10.3.4) Secure Email (1.3.6.1.5.5.7.3.4) Client Authentication (1.3.6.1.5.5.7.3.2) in enhanced key usage)
Доверливост KSN+	сертификат со јавен клуч со двојна намена (public dual-usage key certificate)	digitalSignature, keyEncipherment
Доверливост KSN	сертификат со јавен клуч со двојна намена (public dual-usage key certificate)	digitalSignature, keyEncipherment
Доверливост KSS+	сертификат со јавен клуч со двојна намена (public dual-usage key certificate)	digitalSignature, keyEncipherment
Доверливост KSS	сертификат со јавен клуч со двојна намена (public dual-usage key certificate)	digitalSignature, keyEncipherment
Доверливост KSS++:	сертификат со јавен клуч со двојна намена (public dual-usage key certificate)	digitalSignature, keyEncipherment
Доверливост KS Non-repudiation	неотповикливост	nonRepudiation
Доверливост KSCL+	сертификат со јавен клуч за верификација (public verification key cerificate)	digitalSignature, keyEncipherment
Доверливост NSER+	сертификат со јавен енкрипциски клуч (public encryption key certificate)	keyEncipherment
ДоверливостNSER	сертификат со јавен енкрипциски клуч (public encryption key certificate)	keyEncipherment
Доверливост NSE+	сертификат со јавен енкрипциски клуч (public encryption key certificate)	keyEncipherment

Вид на сертификат		Намена во keyUsage полето
Доверливост NSE	сертификат со јавен енкрипциски клуч (public encryption key certificate)	keyEncipherment
Доверливост SSL NS	сертификат со јавен клуч со двојна намена (public dual-usage key certificate)	digitalSignature, keyEncipherment
Доверливост VPN NS	сертификат со јавен клуч со двојна намена (public dual-usage key certificate)	digitalSignature, keyEncipherment
Доверливост CS NS	сертификат со јавен клуч со двојна намена (public dual-usage key certificate)	digitalSignature, keyEncipherment
Доверливост TS NS	Сертификат за временски жиг	Digital Signature Enhanced Key Usage (Critical): Time Stamping (1.3.6.1.5.5.7.3.8)

6.2. Заштита на приватниот клуч и контроли за управување со криптографскиот модул

6.2.1. Стандарди и контроли за криптографскиот модул

Сите операции за генерирање на клуч за електронски потпис и за потпишување на сертификатот се вршат во хардверски криптографски модул кој го задоволува стандардот FIPS 140-2 ниво 3. Сите останати CA криптографски операции се вршат во криптографски модул кој го задоволува стандардот FIPS 140-2 ниво 2.
Приватниот клуч на носителот на сертификатот се потпира на физичките и логичките контроли кои го штитат компјутерскиот систем на носителот на сертификатот. Носителот на сертификатот е должен да осигури дека приватниот клуч се чува во средина со доволно ниво на физичка заштита. Сепак, се препорачува носителот на сертификатот да користи smart картичка која го задоволува барем стандардот FIPS 140-2 ниво 2 или друг стандард со еднакво ниво на осигурување.

6.2.2. Контрола на приватниот клуч од страна на повеќе лица (n од m)

Како што е дефинирано во Делот 5.2.2. Потребен број на лица по задача.

6.2.3. Чување на копија на приватниот клуч кај овластени трети страни

Македонски Телеком CA не поддржува чување на копија на клучот кај овластени трети страни.

6.2.4. Копија на приватниот клуч

Македонски Телеком CA апликацијата чува историјат на приватните декципциски клучеви на носителот на сертификатот во неговата база на податоци за цели на обновување на клучевите. Исто така, CA апликацијата чува копија од приватниот клуч за потпишување на CA.
CA апликацијата прави копија од базата на податоци најмалку три пати на ден, и од неа се прави копија секој ден како дел од редовното правење копии на CA главниот систем.
Македонски Телеком CA не прави копии од приватните клучеви за потпишување и од доверливите (декрипциски) клучеви без копија на претплатникот.

6.2.5. Архивирање на приватните клучеви

Приватните клучеви се архивираат како што е дефинирано во Делот 5.5.4 Процедури за бекап на архивирани податоци.

6.2.6. Префрлање на приватните клучеви во или од криптографски модул

Приватниот клуч за потпишување на Македонски Телеком CA се генерира во рамки на хардверскиот криптографски модул (HSM). CA приватниот клуч за потпишување никогаш не се појавува во јасна форма надвор од HSM.

Претплатничкиот приватен декрипциски клуч којшто го генерира софтверскиот криптографски модул на CA апликацијата се доставува до криптографскиот модул на претплатникот со користење на PKIX-CMP протоколот.
Нема потреба од претплатнички приватни клучеви за потпишување бидејќи тие се генерираат во рамки на криптографскиот модул на корисникот.

6.2.7. Складирање на приватните клучеви на криптографски модул

Приватниот клуч за потпишување на Македонски Телеком CA се користи само на хардверскиот криптографски модул (HSM). CA приватниот клуч за потпишување се складира на клониран Хардверски безбедносен модул токен за цели на правење на резервна копија и обновување на клучевите.

6.2.8. Постапка за активирање на приватниот клуч

Приватниот криптографски клуч за потпишување на Македонски Телеком CA се активира по стартувањето на апликацијата на органот за сертификација. За активирање е потребна smart картичка / токен за пристап до хардверскиот криптографски модул, како и лозинка на претплатникот со CA Master User улога.
Корисничките приватни криптографски клучеви се активираат по успешната автентикација на претплатникот со лозинка во претплатничката апликација.

6.2.9. Постапка за деактивирање на приватниот клуч

Криптографскиот клуч за потпишување на Македонски Телеком CA се деактивира со стопирање на апликацијата на органот за сертификација.
Корисничките апликации мораат да го деактивираат приватниот криптографски клуч кога претплатникот ќе се одјави од системот, односно апликацијата.

6.2.10. Постапка за уништување на приватниот клуч

При стопирање на Македонски Телеком CA апликацијата се уништуваат сите криптографски клучеви кои се наоѓаат во системската меморија.
Корисничките апликации мораат да ги исчистат приватните криптографски клучеви од работната меморија пред таа повторно да ја доделат. Исто така, мора да го пребришат целиот простор на дискот кој се користи за приватните криптографски клучеви, пред тој простор да му се додели на оперативниот систем.

6.2.11. Ниво на криптографкиот модул

Види Дел 6.2.1. Стандарди и контроли за криптографскиот модул

6.3. Останати аспекти на управување со парот клучеви

6.3.1. Архивирање на јавниот клуч

Македонски Телеком АД ги архивира CA јавниот клуч за верификација на потпис и претплатничкиот јавен екрипциски клуч на начин утврден во Делот 5.5.4 Процедури за креирање на резервни копии од архивата.

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

Периодот на користење на јавните и приватните криптографски клучеви во сертификатите кои ги издава Македонски Телеком CA изнесува:

- CA јавен клуч за верификација и сертификат: 20 години.
- CA приватен клуч за потпишување: 20 години.
- Претплатнички јавен клуч за верификација и сертификат: до 5 години.
- Претплатнички приватен клуч за потпишување: до 5 години.
- Претплатнички јавен енкрипциски клуч и сертификат до 5 години.
- Претплатнички приватен декрипциски клуч: Периодот на користење не е ограничен

Македонски Телеком СА може да го прилагоди рокот на важност на одредени претплатнички криптографски клучеви врз основа на специфични барања од корисниците и барањата од јавните набавки во согласност со прописите и видот на сертификатот.
Лицето, кое ги чува електронски потпишаните податоци, најдоцна во рок од еден месец пред истекот на важноста на потписот потребно е да обезбеди повторно електронско потпишување од страна на сите лица кои ги потпишале податоците првиот пат или заверка од страна на нотар, како и да бара потврдување на овие податоци со општо прифатен временски жиг на Македонски Телеком АД.

6.4. Податоци за активација

6.4.1. Генерирање и инсталирање на податоците за активација

Референтните броеви и авторизациските кодови се генерираат во софтвер во СА апликацијата и се чуваат во СА енкриптираната база на податоци до доделувањето на претплатниците. Броевите и кодовите се единствени и се генерираат на непредвидлив начин.
Претплатнците користат лозинки за активирање на нивниот криптографски модул. Секој претплатник избира своја лозина врз основа на строга политика за лозинки што ја спроведува корисничката апликација. Лозиниките не треба да се чуваат во PKI корисничките апликации.

6.4.2. Заштита на податоците за активација

Кодовите за активација се генерираат на безбеден начин во СА апликацијата и се внесуваат во СА енкриптираната база на податоци. Кодовите за активација се доставуваат како што се утврдено во Делот 4.1.2.**Error! Reference source not found.** Процес на регистрација и о дговорности.

6.4.3. Останати аспекти на податоците за активација

Нема одредби.

6.5. Контрола на безбедноста на компјутерите

6.5.1. Конкретни технички барања за безбедноста на компјутерите

Македонски Телеком СА имплементираше голем број на технички контроли за безбедноста на компјутерите коишто ги вршат главниот оперативен систем на СА и СА апликацијата, вклучувајќи:

- Контрола на пристап до СА сервисите
- Строга поделба на задолженијата и улогите на оперативните лица на СА
- Користење на smart картички за складирање на профилот на службениците за безбедност на СА и администраторите на сертификати
- Екриптирани сесии меѓу СА апликацијата и PKI корисничките апликации на претплатникот
- Енкриптирање на чувствителни податоци во базата на податоци на СА
- Архивирање на историјатот на клучеви и податоци за ревизијата на СА и на претплатникот
- Ревизија на настани поврзани со безбедноста
- Механизми за обновување на клучевите и на СА апликацијата

6.5.2. Ниво на безбедност на компјутерите

СА апликацијта што ја користи Македонски Телеком АД – Скопје е рангирана на EAL 4+ зголемено ниво на осигурување.
Главните оперативни системи и останатите користени производи се комерцијални готови производи.

6.6. Технички контроли за управување со векот на траење

6.6.1. Контроли на развојот

Сите апликации и производи што ги користи Македонски Телеком CA се комерцијални готови производи.

6.6.2. Контроли за управување со безбедноста

Македонски Телеком CA има имплементирано постапки за управување со проблеми, промени и конфигурации за сите софтверски и хардверски компоненти на PKI кои се во согласност со барањата ISO/IEC 27001.

6.6.3. Контрола на безбедноста во текот на животниот циклус

CA го тестира целокупниот софтвер и постапки во контролирана средина.

6.7. Контрола на безбедноста на мрежата

Компјутерската мрежа на Македонски Телеком CA е составена од поврзани мрежни сегменти на кои се наоѓаат серверите и работните станици. Сегментите се меѓусебно поврзани со *firewall*-и. Компјутерската мрежа на Македонски Телеком CA е поврзана на Интернет преку повеќе нивоа на *firewall*-и. Безбедносните правила на *firewall*-ите дозволуваат сообраќај само за протоколите кои се неопходно потребни за пристап до сервисите на Македонски Телеком CA.

6.8. Временски жиг

Не е поддржано.

7. ПРОФИЛИ НА СЕРТИФИКАТОТ, РЕГИСТАРОТ НА ПОНИШТЕНИ СЕРТИФИКАТИ И НА OCSP

7.1. Профил на сертификатот

7.1.1. Број на верзија на сертификатот:

Македонски Телеком CA издава X.509 сертификати верзија 3 во согласност со RFC 3280. Се користат следните основните полиња на X.509:

X.509 екстензија	Опис
signature (потпис)	CA потпис за автентикација на сертификатот
issuer (издавач)	Назив на CA
validity (важност)	Датум на активирање и истекување на важноста на сертификатот
subject (субјект)	Единствено име на претплатникот
subjectPublicKeyInformation	Идентификација на алгоритам, клуч
version (верзија)	Верзија на X.509 сертификатот, верзија 3 (2)
serialNumber (сериски број)	Единствен сериски број на сертификатот

7.1.2. Екстензии на сертификатот

Користени екстензии на сертификатот:

X.509 екстензија	Опис
authorityKeyIdentifier	Го дава CA апликацијата
subjectKeyIdentifier	Го дава CA апликацијата
keyUsage	Како што е дефинирано во Делот6.1.7 Намена за користење на клучевите (дефинирана во X.509 вер. 3 поле key usage).
extendedKeyUsage	Како што е дефинирано во Делот 6.1.7 Намена за користење на клучевите (дефинирана во X.509 вер. 3 поле key usage).
privateKeyUsagePeriod	Како што е дефинирано во Делот 6.3.2 Оперативени периоди на сертификатите и периоди на користење на парот клучеви.
certificatePolicies:	Идентификациска ознака на политиката на сертификати (OID) = OID како што е дефинирано во Делот 1.2. Име и идентификација на документ.
CertPolicyID	
CPS URI	
CRLDistributionPoints	CRL локации
subjectAlternativeName	GeneralName=SMIME e-mail address
basicConstraints	CA=true во CA сертификат, CA=false во сите останати сертификати

7.1.2.1. Екстензии на приватни сертификати на Македонски Телеком CA

X.509 екстензија	Опис и OID
EMB	Број за идентификација OID: 1.3.6.1.4.1.18560.2.1

7.1.3. Идентификациски ознаки на алгоритмите

Алгоритам	Број за идентификација
RSA encryption	1.2.840.113549. 1.1.1
SHA-1 with RSA Encryption	1.2.840.113549.1.1.5
SHA256 with RSA Encryption	1.2.840.113549.1.1.11

7.1.4. Облици на имиња

Сертификатите коишто ги издава Македонски Телеком CA во полињата име на издавачот и име на субјектот го содржат целосното единствено име на издавачот на сертификатот и на субјектот на сертификатот. Единствените имиња се во X.501 UTF8 *string* формат.

7.1.5. Ограничување на имињата

Македонски Телеком CA ја користи екстензијата *nameConstraints* само во меѓусебна сертификација, доколку е применливо.

7.1.6. Идентификациска ознака на политиката за сертификати

Сите сертификати издадени од страна на CA содржат идентификациската ознака (OID) на политиката за сертификати според којашто бил издаден сертификатот. Идентификациската ознака (OID) за секоја политика за сертификати е дефинирана во Делот 1.2. Име и идентификација на документ.

7.1.7. Употреба на екстензиите за ограничување на политиката

Македонски Телеком CA ја користи екстензијата *policyConstraints* само во меѓусебна сертификација, доколку е применливо.

7.1.8. Објавување на битни веб страници во сертификатите

Не се користи.

7.1.9. Обработка на информации за битни екстензии од политиката за сертификати

PKI корисничките апликации мораат да ги обработуваат екстензиите на сертификатите кои се означени како критични, во согласност со RFC 3280.

7.2. Профил на регистарот на поништени сертификати (CRL)

7.2.1. Број(-еви) на верзија на сертификатот:

CA ги издава регистрите на поништени сертификати (CRL) во согласност со стандардот X.509 верзија 2 со користење на повеќе дистрибутивни точки во рамки на својот LDAP директориум и http web сервер.
Се користат следниве основни полиња во согласност со X.509 стандардот:

X.509 екстензија	Опис
Version (верзија)	Утврдена на верзија 2
Signature (потпис)	Ознака на алгоритмот што се користи за потпишување на CRL
Issuer (издавач)	Единствено име на CA
thisUpdate	Време на издавање на CRL
nextUpdate	Време на следно издавање на CRL
revokedCertificate	Сериски броеви на поништени сертификати

7.2.2. Регистар на поништени сертификати и екстензии на регистарот на поништени сертификати

X.509 екстензија	Опис
CRLNumber	Го дава CA апликацијата
reasonCode	Го дава CA апликацијата како што го утврдил операторот. Може да содржи (0) Не е наведено, (1) Компромитација на клуч, (3) Промена на припадност, (4) Заменет, (5) Престанок со работа
invalidityDate	Го дава CA апликацијата како што го утврдил операторот.

7.3. OCSP профил

7.3.1. Број на верзија на сертификатот:

Не е поддржано.

7.3.2. OCSP екстензии

Не е поддржано.

8. ПРОВЕРКА НА УСОГЛАСЕНОСТА И ДРУГИ КОНТРОЛИ

8.1. Зачестеност или околности во кои се врши контола

Проверката на усогласеноста на Македонски Телеком СА со релевантните закони се врши со согласност со Законот за податоци во електронски облик и електронски потпис и други важечки законски прописи во Република Македонија, како и интерните регулативи.
Македонски Телеком АД спроведува задолжителни интерни проверки најмалку еднаш годишно.

8.2. Идентитет/квалификации на контролорот (интерна проверка)

Интерниот проверувач е вработен во Македонски Телеком со соодветно ИТ знаење и искуство за проверки.
Независниот надворешен проверувачр е вработен од надлежна независна стручна компанија којашто се придржува кон соодветните национални и меѓународни стандарди и деловници за работа.
Внатрешниот или надворешниот проверувач ги исполнуваат следните критериуми:

- Значително искуство во примената на и криптографска технологија
- Искуство во користење и работа со СА апликацијата
- Искуство во вршење на активности за сертификација или ревизии на системи од областа на информатичката технологија

8.3. Однос на контролорот со субјектот предмет на контрола (интерна проверка)

Внатрешниот или надворешниот проверувач немаат конфликт на интереси и се независни од СА.

8.4. Прашања опфатени со оценувањето

Интерната проверка утврдува дали:

- Политиката, во доволно детали, ги исполнува техничките, процедуралните и организациските активности на СА, согласно барањата на Законот за податоци во електронски облик и електронски потпис и други важечки законски прописи во Република Македонија.
- СА системот функционираво согласност со техничките, процедуралните и организациските практики и политики

8.5. Активности што се преземаат како резултат на најдените пропусти

Македонски Телеком СА презема соодветни активности за отстранување на недостатоците или неусогласностите што биле идентификувани во текот на проверката во рамки на договорениот рок во зависност од големината на ризикот поврзан со нив.

8.6. Соопштување на резултатите

Информациите од проверката коишто се однесуваат на усогласеноста на Македонски Телеком СА со релевантните закони се сметаат за исклучително осетливи (доверливи) и не треба да се откриваат на било кое трето лице или од било која причина, освен за потребите на проверката или во случаи утврдени со закон.

9. ДРУГИ ДЕЛОВНИ И ПРАВНИ ПРАШАЊА

9.1. Надоместоци

9.1.1. Надоместоци за издавање или обновување на сертификатите

Македонски Телеком СА наплаќа за своите услуги за сертифицирање на PKI. Ценовникот е објавен на јавните веб страни на СА.

9.1.2. Надоместоци за пристап до сертификатите

Видете го Делот 9.1.1 Надоместоци за издавање или обновување на сертификатите.

9.1.3. Надоместоци за поништување или пристап до информации за состојбата

Видете го Делот 9.1.1. Надоместоци за издавање или обновување на сертификатите.

9.1.4. Надоместоци за други услуги

Видете го Делот 9.1.1. Надоместоци за издавање или обновување на сертификатите.

9.1.5. Политика за рефундирање

Барателите на сертификати можат да откажат барање за сертификат пред издавањето на кодовите за активирање, без надомест. Откако ќе се достават кодовите за активирање, откако ќе се издаде сертификатот или откако ќе се достави или инсталира софтверот, ниту еден надомест нема да се рефундира.

9.2. Финансиска одговорност

9.2.1. Покритие на осигурувањето

Македонски Телеком АД – Скопје поседува осигурително покритие за Општа одговорност и одговорност од производ, вклучувајќи и Чиста финасиска загуба, вообичаени за основната дејност. Лимитите на покритие се во согласност со законодавство на Република Македонија.

9.2.2. Други средства

Не е применливо.

9.2.3. Покритие на осигурување или гаранција за крајни корисници

Претплатниците и третите лица се единствено одговорни да обезбедат соодветно покритие на осигурување или гаранција во согласност со намената на сертификатот или услугата.

9.3. Заштита на лични податоци

Сите лични податоци доставени до Македонски Телеком СА или неговите овластени застапници се чуваат во согласност со барањата утврдени во Законот за заштита на личните податоци на Република Македонија. Објавувањето на наведените информации може да се врши само во согласност со Законот за заштита на личните податоци, Политиката за заштита на личните податоци на Македонски Телеком АД – Скопје или како што се бара од кое било друго применливо законодавство.

9.3.1. Делокруг на доверливите информации

Сите информации, собрани, генерирани, пренесени или чувани од страна на Македонски Телеком СА се сметаат за доверливи, освен информациите утврдени во дел 9.3.2, коишто не се сметаат за доверливи.

9.3.2. Информации коишто не влегуваат во делокругот на доверливи информации

Информациите коишто се објавени како дел од сертификат на Македонски Телеком СА, CRL, Политика за издавање на дигитални сертификати или други информации објавени во јавното складиште на СА, не се сметаат за доверливи.

9.3.3. Одговорност за заштита на доверливите информации

Македонски Телеком CA е одговорен за заштита на доверливите податоци во согласност со Политиката за заштита на личните податоци на Македонски Телеком и Законот за заштита на личните податоци на Република Македонија и друго важечко законодавство.

9.4. Приватност на личните информации

9.4.1. План за приватност

Како што е утврдено во деловите 9.3 и 9.4.

9.4.2. Информации коишто се третираат како приватни

Сите информации за некој носител на сертификат или претплатник коишто не се веќе објавени во сертификат издаден од страна на Македонски Телеком CA, CRL или јавниот LDAP директориум се сметаат за приватни.

9.4.3. Информации коишто не се сметаат за приватни

Сите информации коишто се содржани во сертификат издаден од страна на Македонски Телеком CA, CRL, Политика за издавање на дигитални сертификати или други информации објавени во јавното складиште на CA, не се сметаат за приватни.

9.4.4. Одговорност за заштита на приватните информации

Како што е предвидено во Делот 9.3.3.

9.4.5. Известување и одобрување за користење на приватни информации

Македонски Телеком CA ќе ги користи приватните информации единствено за целите коишто претплатникот дал согласност во текот на процесот на регистрација.

9.4.6. Откривање во согласност со судски или административен процес

CA може да доставува доверливи информации само на претставници на институциите задолжени за спроведување на законите во согласност со применливото законодавство.

9.4.7. Други околности на откривање на информации

Македонски Телеком CA ќе открие приватни информации само во околностите утврдени во Политиката за заштита на личните податоци на Македонски Телеком АД, Законот за заштита на личните податоци на Република Македонија и друго важечко законодавство, на барање од судовите или друг легитимен орган, под услов барањето да е издадено на правна основа.

9.5. Право на интелектуална сопственост

Не е применливо.

9.6. Изјави и гаранции

9.6.1. Изјави и гаранции на CA

Македонски Телеком CA треба да издава сертификати, да спроведува процедури за управување со сертификати и да управува со CA инфраструктурата во согласност со Политиката за издавање на сертификати и применливите закони. CA е одговорен за усогласеноста со процедурите пропишани во оваа политика, дури и кога функционалноста на CA е преземена од RA или подизведувачи.
На кратко, обврските на Македонски Телеком CA се:

- јавно да објави Политика - Правила на издавачот на сертификати и редовно да ги ажурира
- да обезбеди процедура (процедури) за корисникот на сертификатот за поднесување на барање за добивање сертификат

- да издава клучеви и сертификати во согласност со активностите објаснети во оваа Политика, безбедно управување со приватниот клуч на Македонски Телеком АД и дистрибуција на јавниот клуч на Македонски Телеком АД
- одобрување или одбивање на барањата на претплатниците на сертификати;
- потпишување и издавање на X.509 сертификати обврзувајќи ги потписниците со нивните јавни клучеви како одговор на одобрените барања за сертификати;
- објавување на X.509 сертификати во директориуми;
- поништување на сертификати, вклучувајќи и објавување на Регистар на поништени сертификати;
- утврдување на идентитетот на корисниците на апликацијата кои поднесуваат барање за добивање на сертификат, кои бараат обновување на сертификат или издавање на нов сертификат во случај на поништување на сертификатот
- да се осигури дека лицата одговорни за регистрација се соодветно обучени и постапуваат во согласност со правилата кои се однесуваат на нив во оваа Политика;
- да осигури дека крајните корисници се свесни и се согласуваат да ги прифатат условите под кои ќе ги добиваат клучевите и сертификатите;
- да го потврди работењето во согласност со активностите опишани во оваа Политика со периодични ревизии во работата
- да вработува лица коишто покрај општите услови за вработување ги задоволуваат и посебните услови предвидени во Законот за податоците во електронски облик и електронски потпис
- да осигури дека информациите за претплатникот и издавачот CA содржани во сертификатите се точни
- да го потврди идентитетот на подносителот на барањето пред издавање на сертификат
- да осигури точност и интегритет на информациите објавени во LDAP директориумот или друго складиште
- да обезбеди пристап до онлајн јавен директориум
- да издаде сертификати на одобрени подносители на барања во согласност со оваа Политика за издавање на дигитални сертификати
- да обезбеди пристап до онлајн јавен директориум
- да ги поништи сертификатите коишто се издадени од страна на CA, по приемот на важечкото барање за тоа, или во согласност со оваа Политика за издавање на дигитални сертификати
- да издава и објавува Регистри на поништени сертификати (CRL)
- да осигури дека неговите RA се свесни за одредбите од оваа Политика за издавање на дигитални сертификати коишто се однесуваат на нив.

9.6.2. Изјави и гаранции на RA

RA е одговорен за точноста и целосноста на информациите за претплатниците дадени во одобрените формулари за поднесување на барање. Деталните обврски на RA се утврдени во соодветните делови од оваа Политика за издавање на сертификати.

9.6.3. Изјави и гаранции на претплатникот

Претплатникот презема целосна одговорност за користењето на приватниот клуч поврзан со јавниот клуч во сертификатот, со тоа што носителот е поединец кој е идентификуван со приватниот клуч.
Во случај кога сертификатите се издадени на поединец за лична употреба, претплатникот и носителот се ист ентитет.

Пред да се издадат клучевите и сертификатите, претплатниците склучуваат договор со Македонски Телеком АД-Скопје, земајќи ги предвид правилата и условите за употреба. Претплатниците се одговорни за:

- Да бидат целосно свесни за нивните задачи и обврски како што е предвидено во соодветната документација, како што е наведено погоре и правилата според кои се издадени сертификатите.
- иницијализација во рок од пет работни дена од моментот на добивање на Иницијализирачкиот код испратен од страна на Македонски Телеком АД – Скопје - употреба на приватните клучеви согласно нивната намена;
- контролирање на пристапот до компјутер, уред или специјален хардверски уред кој содржи приватен клуч за кој тие се одговорни;
- заштита на лозинките кои што се употребуваат за пристап до приватните клучеви;
- итно известување до Македонски Телеком АД - Скопје за какво било сомнение за компромитирање на нивниот приватен клуч.

Со прифаќање на сертификат издаден од страна на Македонски Телеком СА, претплатникот треба:

- да го чува во тајност својот приватен клуч за потпишување
- да ја чува во тајност својата лозинка
- веднаш да го извести СА за сите неправилности или промени на информациите содржани во сертификатот
- да го користи својот сертификат исклучиво за законски цели и за дозволената намена коишто се детално опишани во дел 1.4 Употреба на сертификатот
- веднаш да го извести СА во случај на сомнеж или откривање на компромитирање на приватниот клуч
- веднаш да го извести Македонски Телеком СА за секој сомнеж или позната злоупотреба на кој било сертификат издаден од страна на СА

9.6.4. Изјави и гаранции на трети лица

За проверка на важноста на сертификатот коишто го добиваат, третите лица треба секогаш прво да ја земат предвид листата на поништени сертификати на Македонски Телеком СА. Третото лице, на коешто му е доверен сертификат издаден од страна на Македонски Телеком СА, е должно:

- да ја ограничи важноста на сертификатот само на целите дефинирани во овој документ
- да ја провери важноста на сертификатот
- да го прочита овој документ и да ги научи задачите, одговорностите и ограничувањата на СА
- да побара поништување на сертификатот доколку:
    - дознае дека приватниот клуч е компромитиран на начин којшто влијае на неговата соодветна употреба, или
    - доколку постои опасност од злоупотреба, или
    - доколку има промени во податоците наведени во сертификатот.

Пред да се стекне со сертификат од Македонски Телеком, третото лице има обврска:

- да е запознат со ограничувањата на сертификатот и обврската на СА како што е детално опишано во оваа Политика за издавање на сертификати.
- да го ограничи потпирањето на сертификатите издадени од страна на СА на соодветно користење како што е детално опишано во делот 1.4 Употреба на сертификатот.
- Да осигури дека сертификатот не е поништен со пристапување до важечките, кои било и сите, применливи Регистри на поништени сертификати (CRL)

- веднаш да го извести Македонски Телеком СА за секој сомнеж или позната злоупотреба на кој било сертификат издаден од страна на СА

9.6.5. Изјави и гаранции на други учесници

Сите други учесници се обврзани да ги користат сертификатите и да постапуваат во согласност со оваа Политика за издавање на дигитални сертификати и важечките закони.

9.7. Оградување од гаранции

Освен гаранциите наведени во оваа Политика за издавање на дигитални сертификати и поврзаните договори и до целосен степен дозволен со закон, Македонски Телеком СА ги исклучува сите други можни гаранции, услови или изјави (изјавени, сугерирани, во усна или писмена форма), вклучувајќи ја секоја гаранција за продажба и соодветност за одредена употреба. СА особено го исклучува следново:

- секоја одговорност за можна штета којашто може да настане од моментот кога СА го добива важечкото барање за поништување, до моментот на објавување на информациите за поништување во CRL во согласност со Делот 4.9.6.
- сите гаранции во однос на точноста или сигурноста на информациите содржани во сертификатите коишто не се утврдени од Македонски Телеком СА,
- обврска за објавување на информации содржани во сертификатот,
- секоја гаранција во однос на овластувањата или статусот на кое било лице што користи сертификат издаден од страна на Македонски Телеком СА,
- било каква одговорност, во однос на прашањата надвор од негова контрола, вклучувајќи ја достапноста или работењето на интернет, или телекомуникациска или друга инфраструктура или системи на РА, вклучувајќи хардвер и софтвер.
- било каква одговорност за штети коишто се резултат на настани на виша сила како што е детално опишано во Делот 9.16.5 Виша сила

9.8. Ограничувања на одговорност

Македонски Телеком СА се оградува од која било одговорност за која било компензација, оштета или друго побарување или каква било обврска којашто произлегува од некој прекршок, договор или друга причина во однос на која било услуга поврзана со издавањето, користењето или потпирањето на сертификат издаден од страна на Македонски Телеком СА во износ од над 12.300.000,00 денари за случај на користење од страна на претплатникот или трети лица.

9.9. Оштета

Секоја страна е единствено одговорна да му плати оштета на Македонски Телеком СА или други страни за загуба или штета коишто се резултат на незаконско користење на сертификатите или доколку не постапува во согласност со оваа Политика за издавање на дигитални сертификати и применливите закони.

9.10. Времетраење и престанок

9.10.1. Времетраење

Политиката за издавање на сертификати на Македонски Телеком СА и другите документи стапуваат на сила по одобрувањето од страна на Македонски Телеком АД – Скопје и објавувањето на веб страната на Македонски Телеком СА дефинирана во Делот 2.1. Складишта.

9.10.2. Престанок

Важноста на Политиката за издавање на сертификати на Македонски Телеком СА не е временски ограничена. Постојната верзија е во сила до објавување на нова верзија.

9.10.3. Престанок и продолжување на применливоста на одредбите

По престанокот на важноста на Политиката за издавање на сертификати како резултат на објавување на нова верзија, сертификатот се користи во согласност со верзијата на Политиката за издавање на сертификати која што важи на датумот на издавање на сертификатот. Во случај околностите да се сменат до степен којшто тоа не е возможно, Македонски Телеком СА ќе ги извести претплатниците како што е утврдено во дел 9.12.2 Механизам и период на известување, и третите страни преку јавната веб страна утврдена во Делот 2.1.Складишта.

9.11. Индивидуални известувања и комуникација со учесниците

Македонски Телеком СА ја дистрибуира постојната верзија на оваа Политика за издавање на дигитални сертификати и постојните верзии на сите други јавни документи преку неговата веб страна утврдена во Делот 2.1. Складишта.
Видете го исто така Делот 9.12.2. Механизам и период на известување.

9.12. Измени

9.12.1. Процедура за измени

Вработените на Македонски Телеком СА и другите субјекти можат да ги испратат своите коментари директно до одговорните лица за управување со политики на Македонски Телеком СА во писмена форма или по електронска пошта, на адресите наведени во Делот 1.5.2. Лице за контакт.

9.12.2. Механизам и период на известување

Македонски Телеком СА може да одлучи да не ги извести претплатниците и третите лица во случај на промени со мало или никакво влијание. Македонски Телеком СА одлучува дали промените имаат некакво влијание на претплатниците или третите страни, по сопствено убедување.
Сите промени во Политиката за издавање на сертификати ќе бидат објавени како што е опишано во Дел 2. ОДГОВОРНОСТИ ЗА ОБЈАВУВАЊЕ И СКЛАДИРАЊЕ. Македонски Телеком СА ќе ги извести претплатниците за измените коишто имаат влијание на претплатниците или третите лица по електронска пошта .

9.12.3. Околности во кои OID треба да се промени

OID на Политиката за издавање на сертификати ќе се промени во случај кога промените влијаат на претплатниците или третите лица.

9.13. Одредби за решавање на спорови

Сите спорови поврзани со корпоративните сертификати се поднесуваат во писмена форма до Македонски Телеком СА на адресата утврдена во Делот 1.5.2. Лице за контакт. Спорот треба да се реши спогодбено, доколку е тоа можно. За спорот којшто не може да се реши по пат на преговори, одлучува надлежниот суд.

9.14. Важечко право

Оваа Политика за издавање на дигитални сертификати и односите помеѓу СА и RA, претплатниците, субјектите (носителите на сертификат) и кои било трети лица подлежат на и се толкуваат во согласност со законите на Република Македонија.

9.15. Усогласеност со применливото законодавство

- Закон за заштита на личните податоци
- Законот за податоци во електронски облик и електронски потпис и подзаконските акти донесени врз основа на овој закон
- друго важечко законодавство

9.16. Разни одредби

9.16.1. Целосен договор

Оваа Политика за издавање на дигитални сертификати на Македонски Телеком СА и договорот за крајни корисници на Македонски Телеком СА ги содржат сите релевантни одредби за односот помеѓу Македонски Телеком СА и носителите на јавни сертификати издадени од страна на Македонски Телеком СА.

9.16.2. Пренесување

Претплатниците или носителите на сертификати не смеат да ги пренесуваат, во целост или делумно, правата и обврските од овој договор на трето лице на која било основа.

9.16.3. Случаи на неприменливост на одредби (отстранување)

Невалидноста на еден или повеќе делови од овој документ нема да влијае на валидноста на другите одредби, под услов да не се влијае на материјалните одредби (доверба во сертификатот и користење на сертификатот).

9.16.4. Спроведување (надоместоци за адвокат и одрекување од правата)

Нема.

9.16.5. Виша сила

Под виша сила се подразбираат итни и непредвидени ситуации како што се природни катастрофи, тероризам, испади во снабдување со електрична енергија или телекомуникациски услуги, пожар, непредвидени инциденти како што се вируси или блокирање на услугите како резултат на хакерски напади, владини мерки, намалување на јачината на криптографските алгоритами.
Македонски Телеком СА или другите страни нема да бидат одговорни за штетите предизвикани од настаните на виша сила.

9.17. Други одредби

Нема.

9.18. Завршен дел

Оваа Политика влегува во сила на денот на нејзиното одобрување и објавување на корпоративниот портал на Македонски Телеком АД – Скопје. По објавувањето на оваа Политика, Политиката за издавање на сертификати (CP) на Македонски Телеком СА , од 7.09.2010 престанува да важи.

9.19. Додаток

Овие правила се сметаат за важечки со следниве дополненија: Доверлив дел од правилата на Македонски Телеком СА.

Датум:

Овластено лице за управување:
Мирослав Јовановиќ