

На основу члана 23. став 1. Закона о електронском потпису („Службени гласник РС“, број 135/04), Уредбе о одређивању Министарства унутрашњих послова за издавање квалификованих електронских сертификата („Службени гласник РС“, број 111/09) и Уредбе о упису података у образац личне карте („Службени гласник РС“, бр. 4/07 и 111/09) уговорне стране:

1. Министарство унутрашњих послова Републике Србије и

2. Корисник: _____, ЈМБГ _____
(име и презиме)

Дана: _____ под бројем _____

(број личне карте)

закључују:

УГОВОР

О ИЗДАВАЊУ И КОРИШЋЕЊУ КВАЛИФИКОВАНИХ ЕЛЕКТРОНСКИХ СЕРТИФИКАТА НА ЛИЧНОЈ КАРТИ СА ЧИПОМ

Члан 1.

Министарство унутрашњих послова Републике Србије, као Сертификационо тело (у даљем тексту: Сертификационо тело), је издавач квалификованог електронског сертификата (у даљем тексту: Сертификат) у складу са Законом о електронском потпису и на основу Уредбе о одређивању Министарства унутрашњих послова за издавање квалификованих електронских сертификата и Уредбе о упису података у образац личне карте.

Члан 2.

Сертификационо тело је утврдило Општа интерна правила пружања услуге сертификације у складу са Законом која се уграђују у документа Политика сертификације (Certificate Policy – CP) и Практична правила пружања услуге сертификације (Certification Practice Statement – CPS).

Политика сертификације и Практична правила пружања услуге сертификације су јавни документи и дају се на увид приликом закључивања Уговора.

Члан 3.

Предмет овог уговора је регулисање међусобних права, обавеза и одговорности уговорних страна у вези са пружањем услуга издавања квалификованих електронских сертификата.

Сертификат се издаје на електронској личној карти са чипом.

У сертификату се Сертификационо тело означава са „MUP SA“.

Члан 4.

Кориснику се Сертификат издаје на рок од највише 5 година, односно на период важности личне карте.

Члан 5.

Издавање Сертификата за дигитални потпис на личној карти са чипом је бесплатно.

Члан 6.

Сертификати се могу користити за већину трансакција електронске управе и електронског пословања које се базирају на употреби електронских и квалификованих електронских сертификата.

Члан 7.

Сертификационо тело се обавезује на:

1. обезбеђивање услуга сертификације у складу са законом и другим прописима;
2. обезбеђивање инфраструктуре и сертификационих услуга, укључујући успоставу и одржавање репозиторијума Сертификационог тела и одговарајућег веб сајта у циљу пружања сертификационих услуга;
3. обезбеђивање сигурних механизма који укључују механизам генерисања кључева, заштите кључева, као и процедуре дељења тајни у складу са својом сопственом инфраструктуром јавних кључева;
4. обезбеђивање хитног обавештавања у случају компромитације сопственог приватног кључа;
5. издавање квалификованих електронских сертификата у складу са документима CP и CPS;
6. опозив издатих сертификата након пријема валидног захтева за опозив сертификата;
7. регуларно и периодично објављивање листе опозваних сертификата (CRL листе) која је увек доступна свим заинтересованим лицима;
8. обавештавање трећих лица о статусу сертификата путем публиковања CRL листа на online репозиторијуму Сертификационог тела;
9. достављања копије CP и CPS докумената, као и осталих докумената по захтеву заинтересованих лица.

Члан 8.

Сертификационо тело је одговорно за пружање комплетних услуга сертификације које укључују: регистрацију Корисника, формирање асиметричног пара кључева Корисника за дигитално потписивање, формирање асиметричног пара кључева за аутентикацију, формирање квалификованих електронских сертификата, дистрибуцију приватног кључа и квалификованих електронских сертификата на начин прописан Законом, управљање процедуром промене статуса квалификованих електронских сертификата и обезбеђивање статуса опозваности квалификованих електронских сертификата.

Члан 9.

Сертификационо тело није одговорно за:

1. заштиту приватних кључева Корисника намењених за креирање квалификованог електронског потписа;
2. неодговарајућу проверу валидности сертификата од лица која се поуздаје у Сертификат;
3. могућу злоупотребу Сертификата која је настала услед неиспуњавања обавеза Корисника или трећег лица које се поуздаје у сертификат који је издало Сертификационо тело;
4. неизвршавање обавеза које је последица било ког проблема органа надлежног за послове акредитације и супервизије система инфраструктуре јавних кључева у Републици Србији или неког другог органа;
5. неизвршавање обавеза које су последица ванредне ситуације или више силе.

Члан 10.

Обавезе Корисника су:

1. поштовање Политике сертификације (CP) и Практичних правила рада (CPS);

2. упознавање, разумевање и сагласност са свим ставовима и условима у CP и CPS, као и другим документима који су објављени на репозиторијуму Сертификационог тела;

3. коришћење Сертификата само за легалне и ауторизоване сврхе у складу са CP, CPS и законом;

4. обавештавање Сертификационог тела о свим променама информација које су раније достављене;

5. прекид коришћења Сертификата уколико је било која информација у Сертификату постала невалидна;

6. прекид коришћења Сертификата уколико сам Сертификат постане невалидан;

7. коришћење само једног квалификованог сертификата, издатог из једног сертификационог тела за квалификовани електронски потпис у датом тренутку;

8. спречавање компромитације, губљења, објављивања, модификације или било ког другог неауторизованог коришћења свог приватног кључа;

9. коришћење безбедних уређаја и производа који обезбеђују одговарајућу заштиту приватних кључева;

10. захтевање опозива Сертификата у случају догађаја који материјално утиче на интегритет Сертификата;

11. пријављивање сваке могуће злоупотребе свог приватног кључа и захтевање да се Сертификат опозове у том случају.

Члан 11.

Сертификационо тело се придржава правила заштите приватности персоналних података и правила поверљивости.

Сертификационо тело сматра приватним све информације које се односе на Корисника.

Сертификационо тело не сматра приватним само оне информације о Кориснику за које је сам Корисник дао сагласност да се могу публиковати.

Члан 12.

Сертификационо тело поседује и задржава сва права интелектуалног

КОРИСНИК:

власништва придружена његовим базама података, Веб сајтовима, електронским сертификатима које издаје, као и било којим другим публикацијама које на било који начин припадају или потичу од Сертификационог тела, укључујући CP и CPS.

Члан 13.

Након одговарајућег захтева Сертификационо тело врши опозив Сертификата у случају:

1. губитка, крађе, модификације, неауторизованог објављивања или неке друге компромитације приватног кључа Корисника;
2. да је Корисник нарушио материјалне обавезе које су дефинисане у CP или у CPS документу;
3. да извршење одговарајућих обавеза лица која су наведена у CP и CPS касни или је спречено услед природне катастрофе, рачунарског или комуникационог отказа, или услед другог узрока који излази ван контроле датог лица и да су информације о другом лицу материјално угрожене или компромитоване;
4. да се десила промена одређених информација у Сертификату.

Члан 14.

Сертификат се суспендује ако суспензију захтева:

1. Корисник или овлашћени службеник Сертификационог тела;
2. надлежни орган за заштиту података или други надлежни орган;
3. суд, тужилац или институције које врше кривичну истрагу да би спречили даље вршење кривичних дела.

Члан 15.

Захтев за суспензију сертификата се доставља дигиталном поруком коју је потписао Корисник или овлашћени службеник Сертификационог тела.

Члан 16.

Суспензија сертификата траје док трају и услови због којих је захтевана.

Члан 17.

Реактивацију сертификата може захтевати:

1. Корисник или овлашћени службеник Сертификационог тела;
2. надлежни орган за заштиту података или други надлежни орган на основу чијег захтева је извршена суспензија;
3. суд, тужилац или институција на основу чијег захтева је извршена суспензија.

Члан 18.

Уговор се закључује на време трајања сертификата, или до опозива сертификата.

Уговор ступа на снагу кад га потпише Корисник и његовим прихватањем Сертификата.

Члан 19.

Сертификационо тело не прихвата било какву другу одговорност осим оне која је изрчито одређена Уговором, законом, као и CP и CPS документима.

Члан 20.

У случају промене прописа који на другачији начин регулишу издавање и коришћење електронских сертификата, закључиће се анекс Уговора.

Члан 21.

Спорове настале применом Уговора, уговорене стране ће решавати споразумно, а уколико споразум није могућ, спор ће решавати надлежни суд у Београду.

Члан 22.

Уговор ступа на снагу потписивањем обе уговорене стране.

Члан 23.

Уговор је сачињен у два примерка, по један за сваку уговорену страну.

ОВЛАШЋЕНО ЛИЦЕ :

