СУФ

Систем за управљање фактурама

* Основни појмови и подручје примене квалификованог електронског сертификата

Упутство:

[Основни појмови и подручје примене квалификованог електронског сертификата 2](#_Toc58594007)

[Коришћење приватног кључа и сертификата корисника 2](#_Toc58594008)

[Недозвољене примене 2](#_Toc58594009)

[Услови за издавање сертификата 2](#_Toc58594010)

[Поступак преузимања квалификованог сертификата 3](#_Toc58594011)

[Накнада за издавање и коришћење квалификованог електронског сертификата 3](#_Toc58594012)

[Право корисника на опозив, суспензију, прекид суспензије, обнављање сертификата и деблокаду личне карте 3](#_Toc58594013)

[Технологија за безбедно електронско потписивање и проверавање квалификованог електронског потписа 3](#_Toc58594014)

[Пријава квалификованим електронским сертификатом 4](#_Toc58594015)

[Заборавили сте или блокирали ПИН? 4](#_Toc58594016)

[Пријава двофакторском аутентикацијом (еИД) 5](#_Toc58594017)

[Пријава корисничким именом и лозинком 5](#_Toc58594018)

[Потврда адресе електронске поште 6](#_Toc58594019)

[ЗАХТЕВ ЗА ПРУЖАЊЕ УСЛУГЕ ИЗДАВАЊА И ОБНАВЉАЊА КВАЛИФИКОВАНОГ ЕЛЕКТРОНСКОГ СЕРТИФИКАТА 7](#_Toc58594020)

# Основни појмови и подручје примене квалификованог електронског сертификата

Квалификовани електронски сертификат је електронски сертификат који је издат од стране сертификационог тела за издавање квалификованих електронских сертификата и који садржи податке предвиђене законом. Квалификовани електронски сертификати потврђују везу између јавног криптографског кључа корисника и идентитета корисника који је извршио потписивање електронског документа. Квалификовани електронски сертификати и припадајући приватни криптографски кључеви користе се за квалификовано електронско потписивање датотека или порука и аутентикацију корисника. Квалификовани електронски потпис је електронски потпис који испуњава услове утврђене законом и којим се поуздано гарантује идентитет потписника, интегритет електронских докумената и онемогућава накнадно порицање одговорности за њихов садржај.

## Коришћење приватног кључа и сертификата корисника

 Приватни криптографски кључ корисника се користи за креирање квалификованог електронског потписа, а квалификовани сертификат за верификовање потписа.

## Недозвољене примене

 Корисник је дужан да се упозна са условима коришћења и издавања квалификованих електронских сертификата који су садржани у документу „ПРАКТИЧНА ПРАВИЛА РАДА СЕРТИФИКАЦИОНОГ ТЕЛА МУП РС“, који је објављен на Web сајту http://ca.mup.gov.rs. Свака употреба квалификованог електронског сертификата која није у сагласности са одредбама наведеног документа као и одредбама Закона о електронском потпису, није дозвољена.

##  Услови за издавање сертификата

За издавање квалификованог електронског сертификата, корисник је дужан да:

- поднесе Захтев за издавање квалификованог електронског сертификата. Својим потписом на обрасцу Захтева, подносилац Захтева је сагласан да МУП РС обрађује личне податке подносиоца Захтева који су садржани у Захтеву у сврху издавања, опозива, суспензије, прекида суспензије сертификата за електронски потпис и деблокаде личне карте.

- испуни захтеве за идентификацију,

- поседује електронски идентификациони документ (електронску личну карту) са чипом,

- **у присуству службеника потпише Захтев и Уговор о издавању и коришћењу квалификованих**

електронских сертификата на електронској личној карти.

Услов за издавање квалификованог електронског сертификата је провера идентитета корисника, који подразумева физичко присуство корисника приликом подношења Захтева. Корисник је у обавези да поседује важећи електронски идентификациони документ. ЈМБГ је саставни део имена корисника сертификата и може бити видљив за примаоца потписаног документа.

Само сертификат у који је уписан ЈМБГ може да се користи у електронским сервисима државних органа.

## Поступак преузимања квалификованог сертификата

Кориснику се сертификат уручује лично, при чему је у поступку генерисања квалификованог електронског сертификата за електронско потписивање неопходно омогућити кориснику да сам укуца своју лозинку за приступ идентификационом документу. Корисник је дужан да се приликом преузимања квалификованог електронског сертификата за електронски потписупозна са условима издавања и коришћења квалификованог електронског сертификата, односно са овим обавештењем.

## Накнада за издавање и коришћење квалификованог електронског сертификата

Издавање квалификованог електронског сертификата је бесплатно.

## Право корисника на опозив, суспензију, прекид суспензије, обнављање сертификата и деблокаду личне карте

Корисник има право да захтева опозив, суспензију, прекид суспензије, обнављање сертификата и деблокаду личне карте.

## Технологија за безбедно електронско потписивање и проверавање квалификованог електронског потписа

Приватни криптографски кључ се користи за формирање квалификованог електронског потписа, генерише се у средству за формирање квалификованог електронског потписа (на електронском идентификационом документу, односно личној карти) и никада га не напушта, а квалификовани електронски потпис формира се такође на електронској личној карти. Електронска лична карта има придружену лозинку/ПИН, за активирање приватног кључа.

Три пута погрешно унета лозинка блокира личну карту.

# Пријава квалификованим електронским сертификатом

- Висок ниво поузданости -

Пријава квалификованим електронским сертификатом представља висок ниво поузданости и корисницима који се пријављују на овај начин доступне су све електронске услуге. Корисници који се пријављују на овај начин могу самостално да генеришу остала два начина пријаве (ниже нивое поверења: основни и средњи ниво поузданости) као и да електронски потписују документа и захтеве.

**ВАЖНО:**

За правилно коришћење квалификованих електронских сертификата неопходно је да на свом рачунару инсталирате софтвер сертификацоног тела које Вам је издало сертификат, јер без тога није могуће користити квалификоване електронске сертификате.

Софтвер је доступан на интернет страници сертификационог тела.

## Заборавили сте или блокирали ПИН?

Уколико сте више од четири пута унели погрешан ПИН или сте заборавили ПИН Вашег сертификата, обратите се сертификационом телу које Вам је издало сертификат.

# Пријава двофакторском аутентикацијом (еИД)

Пријава двофакторском аутентикацијом представља средњи ниво поузданости и корисницима који се пријављују на овај начин доступно је 98% услуга. Предност овог начина пријављивања јесте у томе што корисницима нису потребни квалификовани електронски сертификати, већ инсталирана апликација на њиховим паметним уређајима (мобилни телефон или таблет). Овај начин пријаве омогућава корисницима да услуге могу да користе и путем мобилног телефона.

За овај начин пријаве на систем, неопходно је да корисник поседује параметре за подешавање апликације коју треба да инсталира на мобилни телефон.

Уколико изаберете овај начин пријаве, потребно је да преузмете апликацију „ConsentID”:

За Android кориснике, апликацију можете да преузмете на линку:

 [ConsentID - Apps on Google Play](https://play.google.com/store/apps/details?id=nl.aeteurope.mpki.gui&hl=en)

За iOS кориснике, апликацију можете да преузмете на линку:

[‎ConsentID on the App Store (apple.com)](https://apps.apple.com/us/app/consentid/id883224643)

**Напомена:**

У зависности од избора језика на телефону (српски или енглески), апликација ће се исписивати на том језику приликом коришћења.

Корисници iOS оперативног система српски језик могу подесити тако што ће у својим подешавањима да изаберу апликацију ConsentID и ту одаберу жељени језик (Settings>ConsentID>Preferred Language).

# Пријава корисничким именом и лозинком

- Основни ниво поузданости -

Пријава корисничким именом и лозинком представља основни ниво поузданости и овим корисницима доступан је ограничен број електронских услуга.

**ВАЖНО:**

Сви корисници који већ имају креиран кориснички налог на Порталу еУправа могу се пријавити са истим креденцијалима (корисничким именом и лозинком) и на нови Портал еУправа. Неопходно је додавање очитаног, скенираног или фотографисаног\*или личног документа са сликом (лична карта или пасош), како бисте прошли верификацију за основни ниво поузданости.

\*уколико прилажете скенирану или фотографисану личну карту обавезно је да приложите обе стране документа.

Овај начин креирања корисничког налога захтева да приложите очитан, фотографисан или скениран лични документ са сликом (лична карта или пасош), а највише 2 документа, максималне величине 3 MБ (3 MB) по приложеном документу.

Достављањем документа, потврђујете да сте лице за које сте се изјаснили да јесте и којем је омогућено даље коришћење различитих портала и извршавање електронских услуга. Бићете обавештени електронском поштом када овлашћено лице потврди/активира Ваш кориснички налог.

**ВАЖНО:** документа која могу бити прихваћена су искључиво лична карта (обе стране) или путна исправа.

## Потврда адресе електронске поште

Након регистрације, на адресу електронске поште коју сте навели добићете поруку и линк који је потребно да потврдите.

**ВАЖНО:** Могуће је да верификациони маил стигне кориснику у фолдер са непожељном поштом.

Провера документа у року до 24 сата.

Кориснички налог постаје активан када се Ваша документа провере од стране овлашћеног лица најкасније у року до 24 часа.

# ЗАХТЕВ ЗА ПРУЖАЊЕ УСЛУГЕ ИЗДАВАЊА И ОБНАВЉАЊА КВАЛИФИКОВАНОГ ЕЛЕКТРОНСКОГ СЕРТИФИКАТА