

**ПРАКТИЧНА ПРАВИЛА ЗА ИМПЛЕМЕНТАЦИЈУ  
КВАЛИФИКОВАНЕ УСЛУГЕ ОД ПОВЕРЕЊА: УСЛУГА  
КВАЛИФИКОВАНЕ ЕЛЕКТРОНСКЕ ДОСТАВЕ**

СРОИД:	1.3.6.1.4.1.57738.20.1.1.0.0
Важи од:	05.08.2021.
Верзија:	1.0.0
Датум верзије:	05.08.2021.
Аутор:	Јован Вистаћ
Ниво поверљивости:	Јавно
Одговорна особа:	Јован Грубер, директор

## Преглед претходних верзија

Издање	Број документа	Верзија	Датум	Опис промене	Измене припремио	Измене одобрио
1.	1.3.6.1.4.1.57738.20. 1.1.0.0	1.0.0	05.08.2021.	Прво издање	Јован Вистаћ	Јован Грубер

## Садржај

ПРАКТИЧНА ПРАВИЛА ЗА ИМПЛЕМЕНТАЦИЈУ КВАЛИФИКОВАНЕ УСЛУГЕ ОД ПОВЕРЕЊА: УСЛУГА КВАЛИФИКОВАНЕ ЕЛЕКТРОНСКЕ ДОСТАВЕ .....	1
Преглед претходних верзија.....	2
ПОЛИТИКА ИМПЛЕМЕНТАЦИЈЕ КВАЛИФИКОВАНЕ УСЛУГЕ ОД ПОВЕРЕЊА: .....	6
УСЛУГА КВАЛИФИКОВАНЕ ЕЛЕКТРОНСКЕ ДОСТАВЕ .....	6
1. УВОД.....	7
2. ОПИС КВАЛИФИКОВАНЕ УСЛУГЕ ОД ПОВЕРЕЊА .....	8
а) Претплатници (корисници).....	8
б) Трећа лица.....	8
ц) Намена и неовлашћена употреба .....	8
д) Овлашћене контакт особе .....	8
е) Приступачност за особе са инвалидитетом.....	9
ф) Објављивање информација.....	9
2.1 Квалификована електронска достава .....	9
Опис: .....	10
2.2 Регистрација корисника .....	11
2.3 Пријављивање у систем .....	12
2.4 Пријављивање – обнављање сертификата или додатни сертификат .....	13
2.5 Достава пошиљке – сервис унутар сигурног електронског сандучета.....	13
2.6 Пријем пошиљке .....	14
2.7 Интерактивно креирање пошиљке.....	17
2.8 Припрема пошиљке за сервис (B2B) .....	17
2.9 Слање електронских фактура .....	17
2.10 Слање електронске пошиљке .....	18
2.11 Електронско потписивање.....	18
2.12 Верификација идентитета .....	18
2.13 Обавештење о изменама .....	18
2.14 Докази о пруженим услугама.....	18
3. ОПШТИ ЗАХТЕВИ БЕЗАНИ ЗА ПРЕПОРУЧЕНУ ЕЛЕКТРОНСКУ ДОСТАВУ .....	20
3.1 Заштита од промене садржаја.....	20
3.2. Идентификација пошиљкоца и примаоца.....	21
3.3. Докази о извршеним трансакцијама .....	21
3.4 Временска доступност доказа.....	21
3.5. Укључивање независних пружалаца услуга поверења .....	21
4. ОДРЖАВАЊЕ И БЕЗБЕДНОСТ ИНФРАСТРУКТУРЕ .....	21
Системи контроле.....	21
4.1 Заштита од губитка, крађе, квара или неовлашћених промена .....	22

4.2 Физичка заштита.....	22
4.3 Локација и структура пружаоца услуга квалификоване електронске доставе .....	23
4.4 Физички приступ инфраструктури пружаоца услуга од поверења .....	23
4.5 Напајање и вентилација .....	23
4.6 Заштита од поплаве .....	23
4.7. Заштита од пожара.....	23
4.8 Инциденти.....	23
4.9 Складишта носилаца података.....	25
4.10 Одлагање отпада.....	25
4.11 Организациона структура пружаоца услуга од поверења .....	25
4.12. Некомпатибилност задатака .....	28
4.13 Контрола запослених.....	28
4.14 Потребне квалификације и искуство особља .....	28
4.15 Прикладност особља.....	28
4.16 Додатна обука особља .....	28
4.17 Захтеви за редовну обуку.....	28
4.18 Санкције .....	28
4.19 Захтеви за друге пружаоце услуга.....	29
4.20 Приступ особља документацији.....	29
5. Провера безбедности система.....	29
5.1 Типови логова .....	29
5.2 Учесталост прегледа логова .....	29
5.3 Време чувања записа .....	29
5.4 Резервне копије .....	29
5.5 Прикупљање података за евиденције .....	29
5.6 Процена рањивости система .....	30
6. Дуготрајно чување података .....	30
6.1 Типови дуготрајног чувања података .....	30
6.2 Рок употребе .....	30
6.3 Заштита дугорочно сачуваних података .....	30
6.4 Израда резервних копија дугорочно сачуваних података .....	30
6.5 Захтев у погледу временског жига.....	30
6.6 Методе прикупљања података .....	31
6.7 Процедура за приступ и верификацију дугорочно сачуваних података .....	31
6.8 Поступак у случају упада и злоупотребе.....	31
6.9 Процедура у случају недоступности сервиса и проблема са подацима.....	31
7. План опоравка система .....	31
8. Престанак пружања услуга од поверења .....	31

9.	Безбедносни захтеви за информациону и комуникациону опрему пружаоца услуга од поверења	31
9.1	Специфични технички захтеви за безбедност .....	31
9.2	Степен сигурности .....	32
9.3	Контрола развоја система .....	32
9.4	Менаџмент сигурности .....	32
9.5	Контрола сигурности мреже .....	32
10.	НАДЗОР .....	32
10.1	Опште .....	32
10.2	Учесталост праћења .....	32
10.3	Подручја контроле .....	32
10.4	Активности пружаоца услуга од поверења .....	33
10.5	Објављивање резултата контроле .....	33
11.	ФИНАНСИЈСКА И ДРУГА ПРАВНА ПИТАЊА.....	33
11.1	Ценовник .....	33
11.2	Финансијска одговорност .....	33
12.	Заштита пословних и личних података .....	33
12.1	Опште .....	33
12.2	Одговорност за сигурност .....	34
12.3	Пренос података .....	35
13.	Обавезе и одговорности .....	35
13.1	Обавезе и одговорности пружаоца услуга од поверења .....	35
13.2	Обавезе и одговорности клијента .....	36
13.3	Ограничење одговорности .....	36
13.4	Накнада штете .....	37
14.	Измене и допуне.....	37
14.1	Процедура за усвајање допуна .....	37
14.2	Поступак решавања спорова .....	38
14.3	Важеће законодавство .....	38
14.4	Усклађеност са важећим законом.....	38
15.	Ступање на снагу .....	38

Inception doo

**ИНТЕРНА ПРАВИЛА Inception doo**

**ПОЛИТИКА ИМПЛЕМЕНТАЦИЈЕ КВАЛИФИКОВАНЕ  
УСЛУГЕ ОД ПОВЕРЕЊА:  
УСЛУГА КВАЛИФИКОВАНЕ ЕЛЕКТРОНСКЕ  
ДОСТАВЕ**

Политика квалификоване услуге од поверења за квалификовану  
електронску доставу  
**СРОИД: 1.3.6.1.4.1.57738.20.1.1.0.0**

## 1. УВОД

1.1 INCEPTION doo представља пружаоца квалификованих услуга од поверења која користи сигурне технологије, укључујући безбедан пренос података, како би обављао услуге квалификоване електронске доставе, квалификованог електронског потписивања, коришћења квалификованог електронског печата, квалификованог временског жига, валидацију и друге сервисе.

1.2 Компанија пружа услуге од поверења у складу са важећим правним актима Републике Србије и Европске Уније, а нарочито у складу са Уредбом (ЕУ) број 910/2014 Европског парламента која је на снази од 23. јула 2014. године, а тиче се електронске идентификације и услуга од поверења везано за електронске трансакције на интерном тржишту и укидању Директиве 1999/93 / ЕЦ (тзв. eIDAS Уредба) и у складу са техничким захтевима, смерницама и међународним стандардима, а посебно ETSI SR 019 050, EN 319 401 v2.2.1, EN 319 421 v1.1.1 ETSI TS 119 101 V1.1.1 (2016-03), ETSI EN 319 522-1 V1.1.1 (2018-09), ETSI EN 319 522-2 V1.1.1 (2018-09), ETSI EN 319 521 V1.1.1 (2019-02).

1.3 Ова политика уређује одредбе које се односе на:

- Запослене у компанији (одговорности, задаци, овлашћења и потребни услови сваког индивидуалног члана компаније) и
- Начин пружања услуге од поверења.

1.4 Снимање стања као и класификација информационог система и мрежног окружења, физичке сигурности, начина комуникације, контрола приступа информацијама и информационом систему, планирање начина рада и контроле су детаљније регулисани актима у оквиру информационе безбедности.

1.5 У складу са eIDAS Уредбом, компанија пружа услугу квалификоване електронске доставе која омогућава пренос докумената електронским путем, пружајући доказ о руковању пренетим подацима, укључујући и доказ о преносу и пријему података, као и чувању пренетих података, заштиту пренетих података од губитка, крађе, оштећења или било какве неовлашћене измене.

Услуга компаније мора да испуни следеће захтеве:

- a) Пружа је један или више пружалаца услуга квалификоване услуге од поверења;
- b) Проверава идентитет пошиљаоца са високим нивоом поверљивости;
- c) Проверава идентитет примаоца пре доставе података;
- d) Пренос и пријем података морају бити обезбеђени квалификованим електронским потписом или квалификованим електронским печатом

Inception doo

- пружаоца квалификоване услуге од поверења чиме се искључује могућност измене на начин да она прође непримеђено;
- e) Свака промена података која је потребна приликом слања или пријема мора бити јасно саопштена пошиљаоцу и примаоцу;
  - f) Датум и време преноса, пријема или било какве друге промене података означавају се квалификованим електронским временским жигом.

## 2. ОПИС КВАЛИФИКОВАНЕ УСЛУГЕ ОД ПОВЕРЕЊА

### а) Претплатници (корисници)

Корисници су правна или физичка лица која користе квалификовану услугу електронске доставе (е-достава) у улози пошиљаоца или примаоца, као и корисници додатних сервиса е-доставе за верификацију квалификованих електронских потписа и издавање и верификацију квалификованог временског жига.

### б) Трећа лица

Трећа страна су правна или физичка лица која се ослањају на информације које компанија пружа на основу пружене квалификоване услуге од поверења и у овом случају не представљају другог пружаоца квалификоване услуге од поверења, пошиљаоца или примаоца.

### ц) Намена и неовлашћена употреба

(1) Е-достава се може користити у судским и административним процесима, процесу закона о раду, арбитражи или другим поступцима који су дефинисани уговором или комуникацијом која није део уговора.

(2) Забрањено је обављање квалификоване услуге од поверења супротно одредбама, правилима и важећим прописима или ван оквира који су претходно дефинисани.

### д) Овлашћене контакт особе

Претплатници (корисници) и трећа лица могу се обратити овлашћеним лицима пружаоца услуге од поверења путем следеће адресе или телефонског броја за било каква питања у вези ових правила или законских одредби квалификоване услуге од поверења:

Јован Грубер, Inception doo, ул. Адмирала Вуковића 57, Београд, Србија



Inception doo

Тел: 011/6359620.

## е) Приступачност за особе са инвалидитетом

Услуге од поверења и сервиси за крајњег корисника треба да буду доступни за особе са инвалидитетом.

## ф) Објављивање информација

- (1) Пружалац услуга од поверења треба да објави сва обавештења у вези са начином рада и друге важне документе на веб сајту компаније <https://epismonosa.rs/>
- (2) Документа која треба да буду јавно доступна су: Општи услови, Корисничка упутства, ценовник као и друга обавештења на веб званичном веб сајту пружаоца услуге.

## 2.1 Квалификована електронска достава

### Дефиниције:

**Безбедно електронско сандуче** - представља адресу корисника за сервис квалификоване електронске доставе, која има форму@домен, адреса је ограничена на 64 карактера, а домен је из скупа подржаних домена (epismonsa.rs). (видети стандард РФЦ5322 - секције 3.2.3 и 3.4.1).

Приступ садржају безбедног електронског сандучета је заштићен. Приступ захтева потврду идентитета квалификованим електронским сертификатом, као и лозинком (за потребе администрације).

Безбедно електронско сандуче омогућава сигуран, поуздан и законски валидан начин размене електронских докумената, може бити коришћен у судским и управним поступцима као и где год је потребан висок ниво безбедности – поузданост, поверљивост и идентификација учесника.

**Власник сандучета** - особа чији се идентитет може верификовати на основу квалификованог електронског сертификата који је коришћен приликом регистрације за безбедно електронско сандуче. Власник сандучета има опцију измене подешавања и овлашћења додатних особа за приступ безбедном електронском сандучету.

**Овлашћено лице** – је особа која поседује квалификовани електронски сертификат, а није власник сандучета (особа која је извршила регистрацију) али има права приступа електронском сандучету. У случају да власник сандучета поседује више од једног квалификованог електронског сертификата за електронски потпис, додатни сертификати се сматрају као сертификати овлашћеног лица (особе од поверења). Уз потврду овлашћеног лица, могуће је отпремати и запримати електронске пошиљке, али није могућа било каква измена подешавања безбедног електронског сандучета.

Inception doo

## Опис:

**Квалификована услуга електронске доставе** омогућава размену података између корисника електронским путем, пружа доказе о руковању са пренетим подацима укључујући доказ о размени и пријему. Такође, ова услуга штити пренете податке од губитка, крађе, оштећења или неовлашћених промена и испуњава захтеве за квалификоване услуге од поверења који су у складу са EIDAS<sup>1</sup> регулативама.

Подаци који су послати или примљени путем сервиса квалификоване електронске доставе неће бити лишени правног дејства и прихватљивости као доказа у правном поступку само из разлога што су у електронској форми или не испуњавају услове за сервис квалификоване електронске доставе.

---

1 Уредба (ЕУ) број 910/2014 ЕВРОПСКОГ ПАРЛАМЕНТА И САВЕТА, 23. Јул 2014. о електронској идентификацији и услугама од поверења за електронске трансакције на локалном тржишту и укидању Директиве 1999/93 / ЕЦ

Inception doo

Што се тиче података послатих и примљених на електронски регистровану маил адресу пружаоца услуге од поверења, сматраће се да су подаци комплетни, да их је послао пошиљалац и да су установљени и тачни у погледу датума и времена испоручености и примања информација као дела сервиса за пружање квалификоване електронске доставе.

Услуга квалификоване електронске доставе се користи као електронски сервис за документа у грађанским и судским поступцима, у управном поступку и свуда где је потребан висок ниво безбедности, поузданости и валидности за испоруку докумената електронским путем.

Услуга квалификоване електронске доставе мора да испуњава следеће услове:

- ◆ Пружена је од стране Пружаоца услуге од поверења (INCEPTION doo);
- ◆ Са високим нивоом поузданости осигурава идентификацију пошиљаоца ( Користећи квалификоване електронске сертификате за електронски потпис и додатном могућношћу коришћења лозинки);
- ◆ Обезбеди идентификацију примаоца пре испоручивања података (база корисника epismonosa.rs система, аутентификација и ауторизација помоћу квалификованог електронског потписа);
- ◆ Пренос и пријем података морају бити осигурани квалификованим електронским печатом пружаоца квалификоване услуге од поверења како би се искључила могућност измене података без откривања промене;
- ◆ Било каква измена података потребних за пријем или слање података мора бити јасно саопштена пошиљаоцу и примаоцу података;
- ◆ Датум и време испоруке, пријема или било која друга промена података мора бити означена квалификованим електронским временским жигом;

Систем омогућава слање порука или прилога – докумената. Систем се разликује од обичне електронске поште из разлога што корисник мора извршити регистрацију да би користио систем и приликом регистрације мора потврдити свој идентитет квалификованим електронским сертификатом за електронски потпис. Отпремљене пошиљке могу бити додатно обележене временским жигом, чиме се осигурава јединствена идентификација времена пошиљке.

Како би приступио сервису, прималац потписује пошиљку својим квалификованим електронским потписом и тек тада ће имати приступ садржају пошиљке. Електронски потписана потврда се враћа пошиљаоцу као доказ о уручењу.

## **2.2 Регистрација корисника**

Како би користили безбедно електронско сандуче, корисници се претходно морају регистровати и потписати уговор о коришћењу услуга. Кориснику се затим додељује адреса за безбедно електронско сандуче (коју има могућност сам да одабере) и региструје се квалификовани електронски сертификат који ће користити у свом раду и везан је за адресу. Корисник се региструје тако што посећује интернет адресу [app.epismonosa.rs](http://app.epismonosa.rs) , доказује свој идентитет квалификованим електронским потписом, попуњава пријавни формулар и електронски потписује уговор за коришћење безбедног електронског сандучета

Inception doo

са квалификованим електронским потписом.

Приликом регистрације, корисник такође поставља лозинку за администрацију сандучета која мора имати минимално 8 карактера и мора садржати мала и велика слова, као и број или друге симболе (знакове интерпункције). Лозинка се у систему чува у шифрованом облику. У случају регистрације правног лица, уговор мора бити потписан од стране законског заступника правног лица.

У случају да се особа региструје за правно лице, потребно је:

- Верификовати или приступити квалификованим електронским потписом законског заступника (са приступом пословном регистру)
- Дозволити могућност допуне уговора.

Уколико закључење уговора није могуће (из горе наведених разлога), регистрација се врши писаним путем - поштом. Корисник преузима уговор у ПДФ формату, отвара се поштанско сандуче са статусом "на чекању", у којем није могуће примати и слати пошту. Поштанско електронско сандуче се активира тек након што добијемо потписану копију уговора.

По завршетку процеса регистрације, корисник путем електронске поште добија обавештење о успешном отварања безбедног електронског сандучета, систем чува корисничке податке и јавни део кључа квалификованог електронског потписа корисника.

### **2.3 Пријављивање у систем**

Корисник се пријављује у систем помоћу поступка потврде идентитета користећи квалификовани електронски потпис и верификујући кориснички налог. Сервис еПисмоноша верификује сертификат корисника на следећи начин:

1. Проверава издаваоца сертификата; издавалац сертификата мора бити на Регистру пружалаца услуга од поверења за услугу издавања квалификованих електронских потписа у складу са законом.
2. На делу за издаваоца сертификата, проверава валидност сертификата у складу са политиком верификације прописаном од стране издаваоца (потврда сертификата, валидација по датуму, ЦРЛ провера), такође се проверава да ли је издавалац на листи важећих издавалаца, на пример OU = sigen- са, O = state-institutions, C = si).
3. У сервису еПисмоноша, провера се да ли је корисник већ регистрован (идентификациони број издаваоца, идентификациони број сертификата). У случају да је корисник регистрован, сервис му даје поруку да такав корисник постоји у бази података и и може се пријавити путем форме за пријаву.

Inception doo

Ако корисник има више отворених сандучади (на пример, законски је заступник за више правних лица), даје му се могућност одабира налога ком жели да приступи.

4. Уколико корисник још увек није регистрован, систем му нуди могућност регистрације. Ако корисник не поседује квалификовани електронски потпис, систем га упућује на страницу са инструкцијама како може извадити квалификовани електронски сертификат.

## **2.4 Пријављивање – обнављање сертификата или додатни сертификат**

Сертификати за квалификовани електронски потпис имају ограничено време важења, тако да је потребно омогућити кориснику чији је сертификат истекао, да има могућност замене постојећег са новим. Такође, како би приступио сигурном електронском сандучету, корисник може користити неколико квалификованих електронских потписа од различитих издаваоца.

Уколико, приликом регистрације, систем детектује да корисник има важећи квалификовани сертификат за електронски потпис, али сертификат још увек није додат на листу корисничких сертификата, систем треба да му понуди 2 могућности, и то:

- Додавање особе од поверења (овлашћеног лица) и
- Замена сертификата

Додавање особе од поверења (овлашћеног лица) се врши тако што корисник унесе адресу сигурносног електронског сандучета, а администратор унесе приступну лозинку коју је поставио приликом регистрације.

Уколико је квалификовани електронски потпис корисника истекао и жели да приступи сервису са новим сертификатом, бира опцију за замену сертификата, уноси адресу сигурног електронског сандучета и лозинку коју је поставио приликом регистрације. Систем проверава да ли је нови сертификат издат за исту особу која је власник старог и мења податке старог сертификата са новим.

## **2.5 Достава пошиљке – сервис унутар сигурног електронског сандучета**

Сервис унутар сигурног електронског сандучета се одвија на следећи начин: Пошиљалац креира пошиљку унутар свог информационог система или на порталу за креирање пошиљке. Комуникација се врши путем безбедносних протокола и обезбеђује поуздан пренос порука.

Пошиљалац шаље пошиљку позивајући сервис за слање, која ради следеће:

- Позивалац методе је аутентификован и ауторизован са својим квалификованим електронским потписом
- Позивалац сервиса прослеђује потписану пошиљку која је намењена за сервис унутар сандучета

Inception doo

- еПисмоноша сервис проверава пошиљку
    - Исправност синтаксе: валидација према шеми
    - Исправност садржаја: провера временског жига пошиљаоца, потписа
    - Провера постојања примаоца
    - еПисмоноша обавештава пошиљаоца да је пошиљка успешно креирана у смислу исправности садржаја као и додатном поруком са Потврдом пријема у сандучету пошиљаоца која је електронски потписана.
  - еПисмоноша шаље електронски потписану Потврду о пријему пошиљке и обавештава примаоца кроз његово пријемно сандуче.
  - еПисмоноша обавештава примаоца о пријему поруке путем редовног налога електронске поште.
- Процес је графички приказан на слици 1.

## 2.6 Пријем пошиљке

Пошиљке које се налазе на листи примљених пошиљки корисника имају различите статусе. Статус пошиљке може бити "Примљено" или "На чекању". Пошиљке са статусом "На чекању" корисник преузима на начин који зависи од врсте услуге. Када кликне на пошиљку, догађа се следеће:

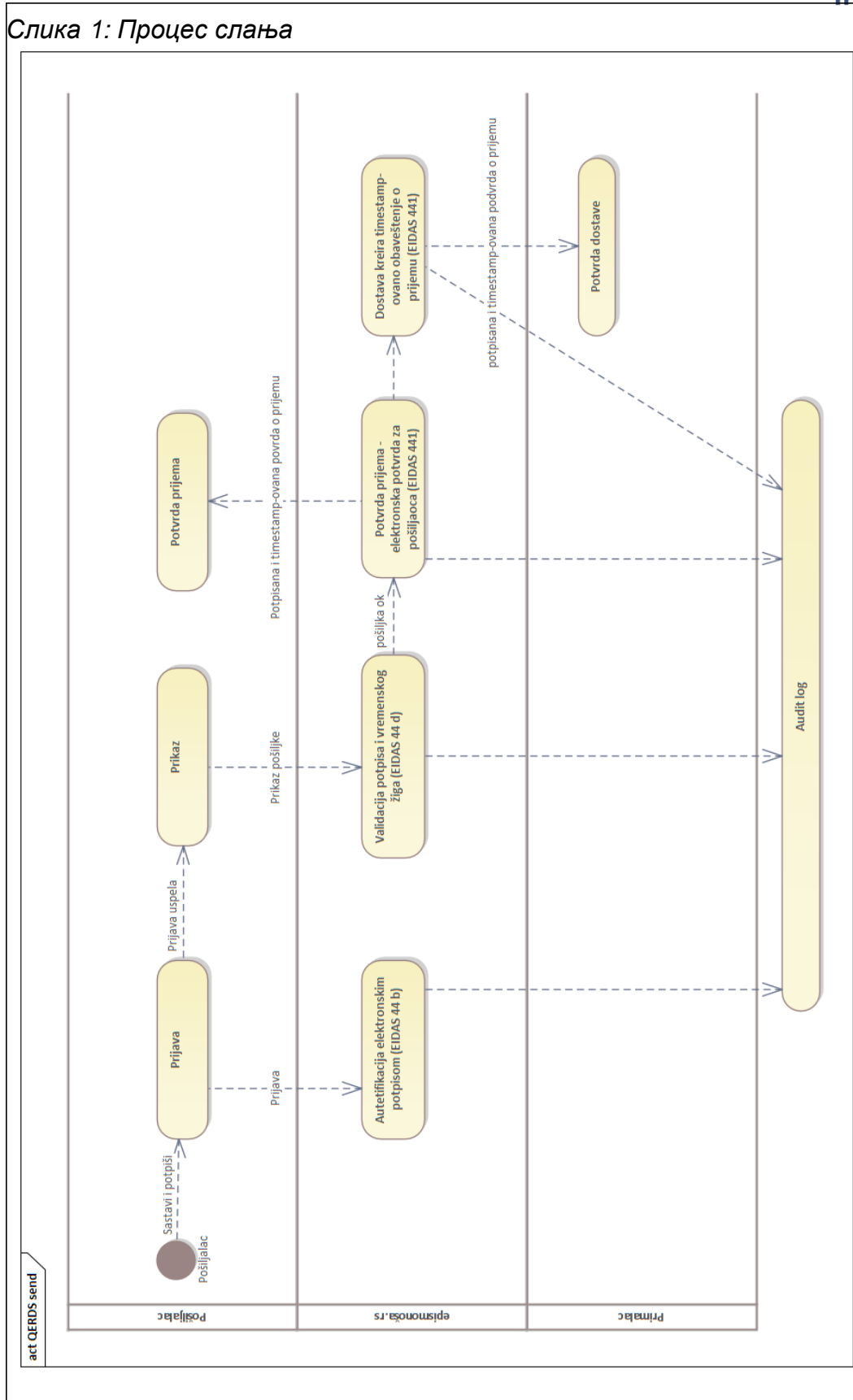
◆ Уколико је тип услуге 'нормално', приказује се садржај пошиљке и датум пријема се уписује у белешку пошиљке. Приказ пошиљке састоји се од података пошиљке (пошиљалац, датум слања, датум пријема, листа пропратних докумената и текстуални садржај).

◆ Ако тип услуге захтева Потврду пријема са повратницом – у овом случају прималац добија обавештење да му је стигла пошиљка у сандуче. Прималац ће моћи да прегледа пошиљку тек када потврди пријем својим квалификованим електронским потписом. Садржај потврде зависи од типа услуге. Када корисник електронски потпише потврду, epismonosa.rs систем доставља садржај пошиљке са статусом "Примљено" у његово сандуче и доставља потписану потврду у сандуче пошиљаоца.

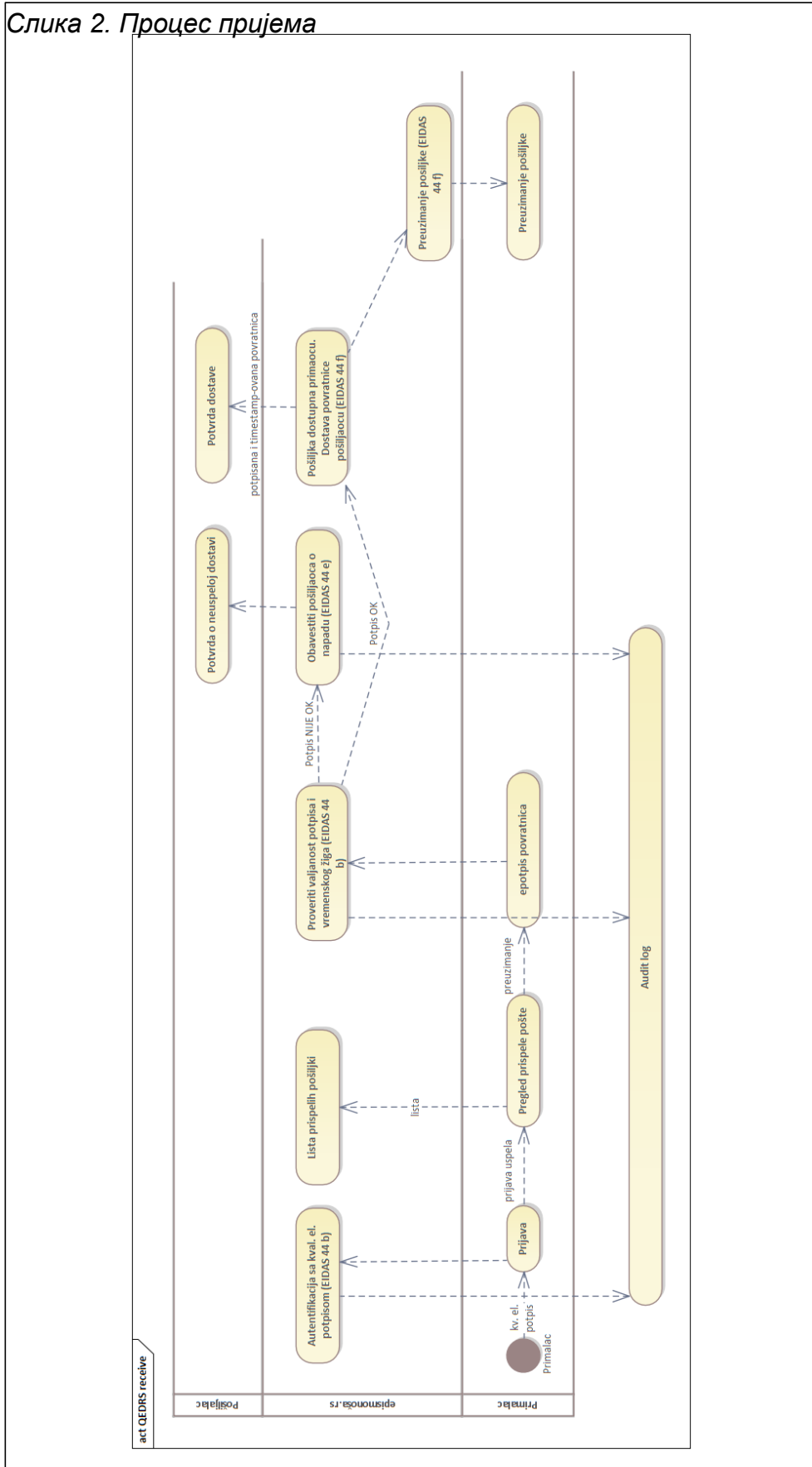
Без обзира на врсту пошиљке, систем увек проверава валидност квалификованих електронских потписа којим је пошиљка потписана.

Процес је графички приказан на слици 2.

Слика 1: Процес слања



Слика 2. Процес пријема





## 2.7 Интерактивно креирање пошилџке

Састављање пошилџке за сервис у прописаном формату је најчешће аутоматизован задатак унутар информационих система пошилџаоца који доставља документа унутар сигурног електронског сандучета путем АПИ-ја (g2b или b2b).

У случајевима када је пошилџку потребно саставити "мануелно", користи се интерактивни интерфејс за састављање безбедне електронске пошилџке.

Услов за креирање пошилџке је успешно логовање у систем и активан кориснички налог.

Функционалности интерфејса за склапање пошилџке:

- Припрема поруке (текст)
- Додавање атрибута
  - Пошилџалац поруке (аутоматски) **From**
  - Прималац поруке **To**
  - Унос предмета (теме) **Subject**
  - Избор типа услуге **Delivery type**
  - Провера идентификатора документа (**SenderId**)
  - Додавање прилога или структурираног садржаја одређивањем врсте садржаја (MIME)
  - Стављање временског жига
  - Електронско потписивање квалификованим електронским потписом
- **Визуализација пошилџке**

Порука аутоматски добија идентификатор поруке пре процеса припреме **MessageId** и осталих атрибута који се постављају на почетне вредности.

## 2.8 Припрема пошилџке за сервис (B2B)

Пошилџалац саставља пошилџку директно у информационом систему, мануелно унутар сервиса, читавањем екстерно креираних електронских докумената или B2B интеграцију и позивањем одговарајуће методе. Пошилџка се састоји од садржаја и прилога којих може бити више од једног. Садржај пошилџке и прилози могу бити у облику структурираног текста или садржај у бинарном облику. Састављена пошилџка мора имати прописани формат (валидација на основу ХМЛ шеме) како би била прихваћена од стране сигурног електронског сандучета. Након састављања, пошилџка се електронски потписује са квалификованим електронским потписом издатим од стране неког од квалификованих издавалаца електронског сертификата, заједно са квалификованим сертификатом за електронски печат од стране пружаоца услуге, фирме INCEPTION doo и опционо са временским жигом.

## 2.9 Слање електронских фактура

Корисници платформе epimonosa.rs могу слати електронске фактуре креиране унутар финансијског софтвера кроз систем директно или путем интерфејса на epimonosa.rs

Електронске фактуре морају бити у формату УБЛ 2.1 e-Slog version 1.6 or higher, и морају бити електронски потписане.

Корисник надгледа статус послатих електронских фактура кроз "управљење рачуница", могући статуси су "послато", "примљено" и "грешка". У случају статуса "грешка", корисник може мануелно иницирати поновно слање.

### **2.10 Слање електронске пошиљке**

Слање већ креиране електронске пошиљке се ради на следећи начин:

- Информације се корисник оцени услуге
- Проверава форма пошиљке према XML шеми
- Верификација временског жига и електронског потписа
- Верификација примаоца: систем проверава постојање примаоца;

### **2.11 Електронско потписивање**

Пошиљке послате преко еПисмоноша система су електронски потписане (печатиране) са квалификованим електронским печатом пружаоца услуге у складу са захтевима EIDAS Уредбе. Систем такође дозвољава потписивање прилога у ПДФ формату.

### **2.12 Верификација идентитета**

Аутентификација се спроводи путем квалификованог електронског сертификата за електронски потпис у складу са EIDAS Уредбом. Уколико је власник сертификата за електронско потписивање регистровани корисник еПисмоноша платформе или има овлашћење, дозвољен му је приступ платформи.

### **2.13 Обавештење о изменама**

Систем обавештава примаоца и пошиљаоца пошиљке о променама које су се десиле у току испоруке (REQ-ERDS-4.1.1-06). Промене на пошиљци могу настати из техничких разлога (пример је Конверзија формата записа), грешка или неовлашћена интервенција трећег лица. У сваком случају, систем обавештава пошиљаоца, примаоца и администратора система путем е-маила о било каквој промени. Провера да ли се промена десила се врши путем верификације електронског потписа поруче где се врши верификација електронског потписа и временског жига.

### **2.14 Докази о пруженим услугама**

Систем пружа доказе о пруженим услугама у зависности од карактеристика сваке врсте испоруке која се нуди.

Доказ о појединачном догађају врши се у облику електронски потписаног документа који корисник прима у своје сигурно електронско сандуче. Доказ је електронски потписан и обележен временским жигом.<sup>3</sup> Докази се чувају у складу са политиком управљања комуникацијама. У случају да корисник обрише своју копију доказа, пружалац услуге може наплатити накнаду за издавање новог.<sup>4</sup>

Inception doo



---

2 ETSI EN 319 521 V1.1.1, REQ-ERDS-4.1.1-10  
3 ETSI EN 319 521 V1.1.1, REQ-ERDS-4.1.1-11.  
4 ETSI EN 319 521 V1.1.1, REQ-ERDS-4.1.1-12

### **3. ОПШТИ ЗАХТЕВИ ВЕЗАНИ ЗА ПРЕПОРУЧЕНУ ЕЛЕКТРОНСКУ ДОСТАВУ**

#### **3.1 Заштита од промене садржаја**

Систем све послате поруке обележава електронским печатом на основу квалификованог сертификата за електронски печат пружаоца услуге и квалификованог електронског временског жига. У случају да систем у било ком тренутку открије да је дошло до промене садржаја, порука о грешци са свим релевантним информацијама аутоматски се шаље пошиљаоцу, примаоцу и администратору система.

## **. Идентификација пошиљаоца и примаоца**

Идентификација пошиљаоца врши се на основу средстава за идентификацију или електронског идентитета са високим нивоом поверења према EIDAS (високој) регулативи. Квалификовани сертификати смештени на листи сертификата унутар сервиса могу се користити за идентификацију.

Идентификација примаоца врши се на основу средстава за идентификацију или електронског идентитета са високим нивоом поверења према EIDAS (високој) регулативи.

### **3.3. Докази о извршеним трансакцијама**

Пошиљалац добија доказе (потврде) о пошиљци и току испоруке, које електронски потписују давалац и прималац. Примање сертификата аутоматски зависи од изабране услуге. У случају да корисник жели додатне потврде из евиденције, може их добити на захтев и уз плаћање накнаде по подношењу информација битних за њихову претрагу (Id пошиљке, време испоруке, прималац ...).

Докази о приступу сигурном поштанском сандучету, испоруци пошиљке, прихватању пошиљке, верификацији потписа и печата, брисању пошиљки, грешкама у приступу и неуспелим покушајима приступа, као и грешкама због промена у садржају.

### **3.4 Временска доступност доказа**

Пружалац услуге пружа аутоматске доказе у облику сертификата најмање три месеца, спискове примљених и послатих пошиљки током 7 година, док се евиденција контролних дневника (AUDIT LOG) чува трајно.

### **3.5. Укључивање независних пружалаца услуга поверења**

Поред услуга од поверења у пружању квалификоване регистроване услуге електронске доставе, пружалац услуге укључује и друге квалификоване пружаоце услуга:

- ЈП Пошта Србије
- Привредна комора Србије
- Halcom а.д.

## **4. ОДРЖАВАЊЕ И БЕЗБЕДНОСТ ИНФРАСТРУКТУРЕ**

### **Системи контроле**

- (1) Компанија планира и спроводи све мере безбедности у складу са ИСО / ИЕЦ 27001 стандардом и техничким захтевима ETSI SR 019 050 - Електронски потписи и инфраструктура (ЕПИ);

Inception doo

Рационализовани оквир стандарда за електронске регистроване услуге испоруке применом електронског потписа.

- (2) Опрема компаније смештена је у посебне, одвојене просторије и обезбеђена је вишестепеним системом физичке и противпровалне заштите. Опрема је заштићена од неовлашћеног приступа. Такође је осигурана и заштићена противпожарним системом, системом против изливања, вентилационим системом и системом непрекидног напајања на више нивоа.
- (3) Компанија складишти резервне и дистрибутивне медије на такав начин да се у највећој могућој мери спречава губитак, упад или неовлашћена употреба или промена ускладиштених података. И за опоравак података и за архивирање важних информација, обезбеђују се резервне копије које се чувају на месту које није ускладиштени софтвер како би се осигурало поновни рад у случајевима када би подаци на основној локацији били уништени.
- (4) Детаљан опис инфраструктуре предузећа, оперативног пословања, поступака управљања инфраструктуром и контроле над безбедносном политиком њеног пословања утврђује се актима из области информационе безбедности.

## 4.1 Заштита од губитка, крађе, квара или неовлашћених промена

(1) Понуђач ће спровести доле наведене опште безбедносне поступке и додатно обезбедити:

- Поновну проверу интегритета и валидности електронских потписа при испоруци поруке примаоцу,
- Сви приступи се чувају у евиденцијама, што додатно штити од нежељених промена,
- Све примљене поруке чувају се у бази података пружаоца услуге, која гарантује репликацију на удаљеном месту,
- приступ подацима је могућ само овлашћеним лицима на начин који осигурава праћење и спречава неовлашћени приступ или промене података.

## 4.2 Физичка заштита

(1) Опрема пружаоца услуга од поверења заштићена је вишестепеним системом физичке и електронске заштите.

(2) Заштита инфраструктуре пружаоца услуга поверења врши се у складу са препорукама струке за највиши ниво заштите.

(3) Комплетни опис инфраструктуре пружаоца услуга поверења и поступци управљања и њихова заштита утврђени су актима из области информационе безбедности.

### **4.3 Локација и структура пружаоца услуга квалификоване електронске доставе**

- (1) Опрема пружаоца услуга од поверења смештена је у посебне, сигурне, одвојене просторије.
- (2) Опрема је осигурана системом физичке и електронске заштите на више нивоа.
- (3) Детаљне одредбе су у актима из области информационе безбедности.

### **4.4 Физички приступ инфраструктури пружаоца услуга од поверења**

- (1) Приступ инфраструктури пружаоца услуга од поверења одобрава се само овлашћеним лицима пружаоца услуга од поверења у складу са њиховим задацима и овлашћењима.
- (2) Сви приступи заштићени су у складу са законодавством и препорукама.
- (3) Детаљне одредбе су у актима из области информационе безбедности.

### **4.5 Напајање и вентилација**

- (1) Инфраструктура пружаоца услуга од поверења има загарантовано непрекидно напајање и одговарајуће системе климатизације.
- (2) Детаљне одредбе су у актима из области информационе безбедности.

### **4.6 Заштита од поплаве**

- (1) Инфраструктура пружаоца услуга од поверења неће бити изложена опасностима од поплаве, осим у случајевима више силе.
- (2) Детаљне одредбе су у актима из области информационе безбедности.

### **4.7. Заштита од пожара**

- (1) Просторије пружаоца услуга од поверења су заштићене од могућег пожара.
- (2) Детаљне одредбе су у актима из области информационе безбедности.

### **4.8 Инциденти**

- (1) Безбедносни догађај је сваки догађај који се односи на безбедност. Примери безбедносних инцидената су овлашћени или неовлашћени улазак у објекат, промена података од стране овлашћеног или неовлашћеног лица.
- (2) Безбедносни инцидент је сваки безбедносни догађај који се догоди другачије од предвиђеног

Inception doo

важећим прописима или интерним актима, крши га или је резултат више силе.

(3) Безбедносни инциденти су класификовани у две различите категорије, и то:

- 1.) безбедносни инциденти који угрожавају интегритет услуга поверења (нпр. упад или крађа пошиљки, грешке у одржавању које угрожавају интегритет система/сервера, физички приступ неовлашћене особе и сл.);
- 2.) сигурносни инциденти који не угрожавају интегритет услуга од поверења (нпр. нестанци струје, кварови на комуникационој линији, злоупотреба овлашћења, покушаји упада, ДДОС напади...).

(4) Ако постоји било каква сумња у коју категорију спада безбедносни инцидент, сматраће се да инцидент спада у прву категорију.

(5) Свако лице које открије или посумња на безбедносни инцидент дужно је да га одмах пријави. Пријављивање безбедносних инцидената одвија се на било који начин (лично, телефоном, е-поштом, путем веб интерфејса ...), што омогућава обавештавање релевантних лица у најкраћем могућем року.

(6) За безбедносне инциденте у вези са заштитом живота и здравља лица или за безбедносне инциденте у вези са заштитом предузећа обавештава се директор или прокуриса, а у случају неопходног деловања државни органи, односно надлежне службе (полиција, ватрогасци, спасиоци).

(7) За безбедносне инциденте који угрожавају интегритет услуге поверења обавештавају се директор или прокуриса за информациону безбедност.

(8) За безбедносне инциденте који не угрожавају интегритет услуге поверења обавештавају се директор или прокуриса за информациону безбедност.

(9) За све безбедносне инциденте који угрожавају услугу поверења, примаоци обавештења о безбедносном инциденту обавестиће директора.

(10) Примаоци обавештења о безбедносном инциденту дужни су да истраже пријављене безбедносне инциденте и да предузму или предложи одговарајуће мере за спречавање поновне појаве безбедносног инцидента.

(11) Сваки сигурносни инцидент евидентиран је у евиденцији сигурносних инцидената. Основне информације о сваком безбедносном инциденту су:

- назив или кратак опис инцидента или догађаја,
- датум и време догађаја,
- опис последица догађаја,
- категорија инцидента са објашњењем критеријума за одређивање категорије,
- мере предузете за санирање инцидента и његових последица.

(12) Евиденција безбедносних инцидената служи као база знања за брзу акцију у случају понављања истих или сличних безбедносних инцидената.

(13) Обавештавање о сигурносним инцидентима и инцидентима не замењује поступке и обавештења по појединим радним областима (нпр. Обавештење о



Inception doo

отклањању штете и друге поступке које одговорна лица треба да изврше по појединим областима).

Извештавање о инцидентима врши се у складу са актима компаније.



#### 4.9 Складишта носилаца података

(1) Носиоци података, било у папирном или електронском облику, морају се сигурно чувати у заштићеним објектима.

(2) Резервне копије софтвера и шифрованих база података пружаоца услуга од поверења редовно се обнављају и чувају у два одвојена и физички заштићена простора, на различитим локацијама.

#### 4.10 Одлагање отпада

(1) Компанија обезбеђује сигурно уклањање и уништавање докумената у физичком и електронском облику.

(2) Одлагање отпада врши посебна комисија у складу са актима из области информационе сигурности.

#### 4.11 Организациона структура пружаоца услуга од поверења

(1) Оперативним, организационим и професионално коректним радом пружаоца услуга од поверења руководи директор компаније Inception doo Јован Грубер.

(2) Запослени код пружаоца услуга од поверења подељени су у организационе групе које покривају следећа подручја:

Организациона група	Улога	Кључни задаци	Бр. извршилаца
Менаџмент услуга и информационог система	Менаџер за имплементацију	<ul style="list-style-type: none"><li>• Пружање услуга поверења</li><li>• Именовање инжењера безбедности</li><li>• Оперативно руководство</li></ul>	1
Менаџмент база података	Инжењер базе података	<ul style="list-style-type: none"><li>• Управљање базом података (инсталација, одржавање, структурне промене),</li><li>• Планирање тренутне и будуће доступности,</li><li>• Надгледање и побољшања (оптимизација)</li></ul>	1

Менаџмент система и мрежне инфраструктуре	Систем инжењер (екстерно, уговор о техничкој сарадњи)	<ul style="list-style-type: none"> <li>• Управљање хардвером</li> <li>• Управљање оперативним системом</li> <li>• Брига о редовном одржавању (надоградње, додаци)</li> <li>• Одржавање резервних копија</li> </ul>	Више
Безбедност и сигурност информација	Инжењер за безбедност	<ul style="list-style-type: none"> <li>• Учешће у имплементацији безбедног рада система</li> <li>• Примена унутрашњих контрола</li> <li>• Сарадња у управљачким инцидентима</li> <li>• Саветовање у вези са сигурношћу информација</li> </ul>	1
Одељење за подршку клијената и тестирање	Корисничка подршка	<ul style="list-style-type: none"> <li>• Брига о корисницима</li> <li>• Комуникација са купцима у писаној форми и телефоном</li> <li>• Сарадња у решавању инцидента</li> <li>• Апликативна опрема за операцију валидације</li> </ul>	3
Правна служба	Административни радник	<ul style="list-style-type: none"> <li>• Пријем, подношење и евидентирање пословне документације</li> <li>• Чување документације у складу са планом класификације</li> </ul>	1
Усклађеност са регулативом	Адвокат	<ul style="list-style-type: none"> <li>• Праћење важећих европских и српских прописа, међународних стандарда и препорука</li> <li>• Припрема предлога неопходних измена и допуна због законских, технолошких или организационих промена и налаза у пракси</li> <li>• Савети о доследној примени задатака</li> </ul>	1

Заштита личних података	Лице задужено за заштиту личних података	<ul style="list-style-type: none"> <li>• Праћење важећих европских и словеначких прописа, међународних стандарда и препорука у области заштите података</li> <li>• Саветовање о процени утицаја на заштиту података и праћење његове примене</li> <li>• Савети о обезбеђивању приватности и друге релевантне анализе или активности на пољу заштите података;</li> <li>• Праћење поштовања Општих уредби о заштити података</li> </ul>	1
Интерна контрола	Службеник за унутрашњу контролу	<ul style="list-style-type: none"> <li>• преглед, оцењивање, процена и верификација адекватности и ефикасности контрола, система и поступака;</li> <li>• предлози за унапређење система управљања;</li> <li>• савети о припреми интерних аката, смерница, образовних програма,</li> <li>• вођење потребне евиденције и извештаја за активност.</li> </ul>	1

## **4.12. Некомпатибилност задатака**

За сваку радну позицију тачно је одређено са којим позицијама може или не мора и не сме бити компатибилна. У случају непредвиђеног одсуства појединих запослених, њихове улоге преузимају други запослени, ако то није неспојиво у складу са актима из области информационе безбедности.

## **4.13 Контрола запослених**

- (1) Компанију надгледа Службеник за унутрашњу контролу.
- (2) У случају откривених недостатака, службеник за унутрашњу контролу наложиће одговарајуће мере за отклањање тих недостатака, које је предузеће дужно да примени, и надгледа спровођење њихово спровођење.

## **4.14 Потребне квалификације и искуство особља**

- (1) Особље пружаоца услуга од поверења мора имати одговарајуће квалификације и искуство у складу са захтевима важећих прописа и техничким стандардима и препорукама.
- (2) Сво особље се редовно обучава и стиче додатна знања из своје стручности и из области информационе безбедности и заштите података о личности и користи административне и управљачке поступке који су у складу са европским или међународним стандардима.

## **4.15 Прикладност особља**

Компанија запошљава довољан број поузданог и професионално обученог особља за које је утврђено да није кажњавано.

## **4.16 Додатна обука особља**

Лица која обављају задатке горе поменутих организационих група редовно добијају сву потребну обуку у складу са интерним актима и годишњим планом.

## **4.17 Захтеви за редовну обуку**

Особље је обучено према потребама или сходно иновацијама које су повезане са радом инфраструктуре пружаоца услуга од поверења.

## **4.18 Санкције**

Санкције у случају неовлашћеног или несавесног обављања послова извршавају се за овлашћена лица пружаоца услуга поверења у складу са важећим прописима и интерним правилима о одговорности запослених за кршење уговорних и других обавеза које проистичу из радног односа.

#### **4.19 Захтеви за друге пружаоце услуга**

Потенцијални екстерни запослени подлежу истим захтевима као и овлашћена лица пружаоца услуга поверења.

#### **4.20 Приступ особља документацији**

Сва потребна документација доступна је овлашћеним лицима пружаоца услуга поверења у складу са њиховим дужностима и задацима.

### **5. Провера безбедности система**

#### **5.1 Типови логова**

(1) Пружалац услуга од поверења редовно проверава и евидентира све што значајно утиче на:

- сигурност инфраструктуре,
- несметан рад свих сигурносних система и
- да ли је у међувремену дошло до упада или покушаја неовлашћених особа везано за опрему или податке.

(2) Детаљне информације о томе утврђују се актима из области информационе сигурности.

#### **5.2 Учесталост прегледа логова**

Пружалац услуга поверења свакодневно врши безбедносне провере своје инфраструктуре.

#### **5.3 Време чувања записа**

Најважнији записи се чувају трајно, а сви остали се чувају 6 година од настанка записа.

#### **5.4 Резервне копије**

Резервне копије се креирају на дневном нивоу.

#### **5.5 Прикупљање података за евиденције**

Подаци се прикупљају аутоматски или ручно, у зависности од врсте података.

- (1) Анализу евиденција и контролу над спровођењем свих поступака редовно врше овлашћена лица даваоца услуга поверења или аутоматски други безбедносни механизми на свим информационам и комуникационим уређајима пружаоца услуга од поверења.
- (2) Процена рањивости врши се на основу анализе евиденција, безбедносних догађаја и других релевантних података.

## **6. Дуготрајно чување података**

### **6.1 Типови дуготрајног чувања података**

Пружалац услуга од поверења чува следећи материјал у складу са одредбама важећих прописа:

- дневници,
- оперативне политике или други акти у области информационе сигурности,
- публикације и обавештења пружаоца услуга од поверења; и
- остала документа у складу са важећим прописима.

### **6.2 Рок употребе**

Најважнији подаци се чувају трајно, а сви остали се чувају 7 година од настанка.

### **6.3 Заштита дугорочно сачуваних података**

(1) Дугорочно ускладиштени подаци су осигурани.

(2) Детаљнија регулатива утврђена је актима из области информационе сигурности у складу са важећим прописима, стандардима и препорукама.

### **6.4 Израда резервних копија дугорочно сачуваних података**

(1) Копија дугорочно сачуваних података је осигурана.

(2) Детаљнија регулатива утврђена је актима из области информационе сигурности у складу са важећим прописима, стандардима и препорукама.

### **6.5 Захтев у погледу временског жига**

Подаци се означавају временским жигом једном годишње.

## **6.6 Методе прикупљања података**

(1) Подаци се прикупљају на начин који је у складу са врстом документа.

(2) Детаљнија регулатива утврђена је актима из области информационе сигурности у складу са важећим прописима, стандардима и препорукама.

## **6.7 Процедура за приступ и верификацију дугорочно сачуваних података**

(1) Приступ дугорочно сачуваним подацима могућ је само овлашћеним лицима.

(2) Детаљнија регулатива утврђена је актима из области информационе сигурности у складу са важећим прописима, стандардима и препорукама.

## **6.8 Поступак у случају упада и злоупотребе**

Детаљнија регулатива утврђена је актима из области информационе безбедности у складу са важећим прописима, стандардима и препорукама.

## **6.9 Процедура у случају недоступности сервиса и проблема са подацима**

Детаљнија регулатива утврђена је актима из области информационе безбедности у складу са важећим прописима, стандардима и препорукама.

# **7. План опоравка система**

Обезбеђено је дуплирање критичних делова система и чување података на географски удаљеним локацијама. Детаљнија регулатива утврђена је актима из области информационе безбедности у складу са важећим прописима, стандардима и препорукама.

## **8. Престанак пружања услуга од поверења**

Детаљнија регулатива утврђена је актима из области информационе безбедности у складу са важећим прописима, стандардима и препорукама.

## **9. Безбедносни захтеви за информациону и**

### **комуникациону опрему пружаоца услуга од поверења**

#### **9.1 Специфични технички захтеви за безбедност**

Детаљнија регулатива утврђена је актима из области информационе безбедности у

Inception doo

складу са важећим прописима, стандардима и препорукама.

## 9.2 Степен сигурности

Детаљнија регулатива утврђена је актима из области информационе безбедности у складу са важећим прописима, стандардима и препорукама.

## 9.3 Контрола развоја система

Компанија користи софтвер реномираних и светски познатих произвођача или водећих компанија, као и сопствено развијен софтвер.

## 9.4 Менаџмент сигурности

Детаљнија регулатива утврђена је актима из области информационе безбедности у складу са важећим прописима, стандардима и препорукама.

## 9.5 Контрола сигурности мреже

Детаљнија регулатива утврђена је актима из области информационе безбедности у складу са важећим прописима, стандардима и препорукама.

# 10. НАДЗОР

## 10.1 Опште

- (1) Пружалац услуге од поверења мора имати Службеника за унутрашњу контролу који је стручњак са релевантним технолошким и правним знањем и који не обавља оперативне задатке у вези са услугама од поверења.
- (2) Службеник за унутрашњу контролу надгледа рад компаније у пружању услуга од поверења. У случају откривања недостатака, организациона група наложиће одговарајуће мере за отклањање тих недостатака, које је компанија дужна да примени, и надгледа њихово спровођење.

## 10.2 Учесталост праћења

Службеник за унутрашњу контролу и кохерентност врши инспекција најмање једном годишње.

## 10.3 Подручја контроле

Области контроле дефинисане су актима из области информационе безбедности.



## **10.4 Активности пружаоца услуга од поверења**

У случају утврђених недостатака или грешака, Службеник за унутрашњу контролу наложиће одговарајуће мере за отклањање тих недостатака, које је предузеће дужно да примени, и надгледа њихово спровођење. Примена мера детаљно је утврђена актима из области информационе безбедности.

## **10.5 Објављивање резултата контроле**

Резултате контроле чува пружалац услуга од поверења.

# **11. ФИНАНСИЈСКА И ДРУГА ПРАВНА ПИТАЊА**

## **11.1 Ценовник**

Компанија одређује ценовник за коришћење својих услуга, потребне опреме и инфраструктуре и објављује га на сопственој веб страници.

## **11.2 Финансијска одговорност**

Компанија преузима одговорност за покривање потраживања која произилазе из финансијске обавезе властитим средствима.

# **12. Заштита пословних и личних података**

## **12.1 Опште**

Компанија поверљиво поступа са:

- свим подацима о раду и пословном процесу клијената и њихових пословних партнера, који су неопходни за пружање услуга од поверења;
- свим поверљивим подацима, под условом да „поверљиви подаци“ укључују све податке (без обзира на то да ли су означени као поверљиви) комерцијалне, финансијске и техничке природе и све остале податке које клијент сматра поверљивим и који се припремају и преносе у било ком облику (материјалном или нематеријалном), укључујући софтвер, анализе, табеле, податке, студије и друге документе, или усмено;

Поверљиве информације из претходног члана сматрају се нарочито информације које се односе на:

финансијске обавезе, цене, купце / наручиоце, друге уговорне стране наручиоца, запослене наручиоца, економско и финансијско стање наручиоца и његове пословне и

Inception doo

развојне политике, сврхе и циљеви, као и остале информације (нпр. непријатности, губитак времена итд.) ако би неовлашћене треће стране сазнале за њих.

(1) Компанија обавештава своје запослене:

- са дужношћу да дају предност интересима компаније или у вези са њом и да избегавају, најбоље што могу, наношење штете наручиоцима;
  - са одредбама Закона о заштити личних података, другим српским и европским законодавством у области заштите података о личности и са мерама и поступцима за заштиту личних података на снази у компанији;
  - да сви подаци и подаци који су класификовани као пословна тајна морају бити пажљиво заштићени и не смеју се откривати, објављивати или стављати на располагање трећим лицима без изричитог одобрења компаније, при чему су трећа лица у смислу ове тачке и други запослени компаније, купци, клијенти и други уговорни сарадници, осим у мери која је строго неопходна за испуњење уговорних обавеза;
  - да су дужни да пажљиво штите личне податке, без обзира на појединца на којег се односе, и без обзира на њихов облик и локацију, и да дају све од себе да не дође до намерног или случајног неоправданог уништавања, брисања, преноса трећих лица или других обрада ових података;
  - да је обрада личних података (прикупљање, чување, измена, пренос, брисање и било која друга обрада) дозвољена само ако постоји правни основ за обраду у складу са законодавством којим се уређује заштита личних података;
  - да је неовлашћено откривање поверљивих информација основа за прекид пословне сарадње;
- да издаја и неоправдано стицање пословне тајне представљају кривично дело;  
-да злоупотреба личних података представља кривично дело.

## 12.2 Одговорност за сигурност

(1) Компанија не преузима никакву одговорност за садржај података које клијент електронски шифрира, потписује или доставља, чак и ако је клијент испоштовао све важеће прописе, све одредбе ових правила и друга правила компаније.

(2) Компанија не преузима никакву одговорност за последице које настају зато што клијент није поштовао сигурносне захтеве ових правила.

## 12.3 Пренос података

(1) Компанија не пружа друге податке о клијентима који нису наведени у општим условима или овим правилима, осим ако су одређене информације посебно потребне за пружање одређених услуга и ако је клијент за то овлашћен или на захтев надлежног суда, прекршајног или управног органа.

(2) Подаци се пружају и без писмене сагласности, ако је то одређено законом или важећим прописима.

## 13. Обавезе и одговорности

### 13.1 Обавезе и одговорности пружаоца услуга од поверења

(1) Пружалац услуга од поверења дужан је да:

- поступа у складу са својим интерним актима и осталим важећим прописима и законима,
- поступа у складу са међународним препорукама,
- објави све релевантне документе који одређују његов рад;
- објави на својој веб страници све информације о оним променама у вези са активностима пружаоца услуга од поверења које на било који начин утичу на претплатника,
- придржава се одредби које се односе на безбедно руковање личним, пословним и поверљивим информацијама у вези са претплатником.

(2) Пружалац услуга од поверења дужан је да:

- осигура одговарајућу физичку сигурност просторија и приступ просторијама пружаоца услуга од поверења;
- као добар менаџер брине о несметаном раду и максималној доступности услуге,
- као добар менаџер брине о што већој доступности услуга,
- као добар менаџер брине за несметан рад свих осталих пратећих услуга,
- покушава да реши проблеме најбоље што може и у најкраћем могућем року,
- стара се о оптимизацији хардвера и софтвера,
- информиса претплатнике о важним питањима, и
- испуњава све остале захтеве у складу са овом уредбом.

(3) Пружалац услуга од поверења мора осигурати максималну могућу доступност својих услуга, свих дана у години, не узимајући у обзир следеће случајеве:

- унапред планиране техничке, али сервисне интервенције на инфраструктури,
- непланиране техничке или сервисне интервенције на инфраструктури као резултат неподвижених кварова,
- техничке или сервисне интервенције због квара на инфраструктури изван надлежности пружаоца услуга од поверења; и
- неприступачност као резултат више силе или ванредних догађаја.

(4) Радове на одржавању или надоградњи инфраструктуре добављач услуга мора најавити најмање три дана пре почетка рада.

(5) Пружалац услуга од поверења одговоран је за све изјаве у овом документу и за спровођење свих одредби ових правила.

## 13.2 Обавезе и одговорности клијента

Корисник услуга - пошиљалац, прималац или треће лице или пословни субјект одговоран је за:

- било какву штету која је директно или индиректно проузрокована неовлашћеним лицима због употребе или злоупотребе услуга од поверења,
- било које друге штете настале услед непридржавања одредби ових правила и других обавештења компаније и важећих прописа.

## 13.3 Ограничење одговорности

Пружалац услуга од поверења неће бити одговоран за штету насталу услед:

- коришћење услуга од поверења у сврху и на начин који није изричито предвиђен овим правилима,
- нетачне или недовољне заштите лозинки, откривање поверљивих података и неодговорно понашање претплатника,
- злоупотребу или упад у клијентов информациони систем,

Inception doo

- неисправност или неадекватност информационе инфраструктуре претплатника или трећих лица,
- понашање наручиоца супротно обавештењима компаније, овим правилима и другим прописима,
- квар инфраструктуре који није у домену провајдера,
- понашање претплатника током коришћења услуге, чак и ако се претплатник придржавао свих одредби ових правила, обавештења компаније или других важећих прописа,
- употребу и поузданост клијентовог хардвера и софтвера.

### **13.4 Накнада штете**

За штету ће одговарати странка која је проузроковала штету због непоштовања одредби ових правила и важећег закона.

## **14. Измене и допуне**

### **14.1 Процедура за усвајање допуна**

- (1) Измене или допуне ових правила компанија може објавити у виду допуна.
- (2) Свака предложена измена подлеже технолошком и правном прегледу пре одобрења директора компаније како би се осигурали законитост, сигурност и квалитет.
- (3) Пружалац услуга од поверења утврђује почетак и крај важења измена.
- (4) Измене и допуне објављују се на [www.epismonosa.rs](http://www.epismonosa.rs)
- (5) У случају да се промене законске одредбе или одредбе других прописа на основу којих се усвајају ова правила, одговарајуће промене узимаће се у обзир до усаглашавања правила.
- (6) Пружалац услуга од поверења обавестиће надзорни орган о свакој промени пружања својих квалификованих услуга од поверења и о намери да престане са обављањем ових активности у року од 45 дана.

Inception doo

## 14.2 Поступак решавања спорова

- (1) Све жалбе купаца решава интерна служба за корисничку подршку.
- (2) Све спорове између предузећа и клијента решава надлежни суд у Београду.

## 14.3 Важеће законодавство

За одлучивање о свим спорним и другим правним питањима у вези са пружањем услуга или уговорним односима са клијентима примењиваће се закон Републике Србије.

## 14.4 Усклађеност са важећим законом

- (1) Надзор над усаглашеношћу рада пружаоца услуга од поверења са важећим законима и прописима врши Министарство државне управе, а с времена на време (најмање сваке две године) изабрано тело за оцењивање усаглашености.
- (2) Интерне провере усаглашености врше овлашћена лица у оквиру пружаоца услуга од поверења.

## 15. Ступање на снагу

- (1) Ова правила ступају на снагу када их потпише директор предузећа, а примењиваће се у року од 3 дана након упознавања запослених са њима, али не пре 05.08.2021.
- (2) На почетку рада, сваки запослени мора бити упознат са садржајем ових правила и потписати изјаву да је свестан тога. Писана изјава чува се у личном досијеу запосленог. Ове изјаве такође потписују сви спољни сарадници (ученици и студенти, предузетници и други).

Београд, 05.08.2021.  
директор

Јован Грубер,