NAČRT ZA OKREVANJE IN ODPORNOST

Univerza v Mariboru

REPUBLIKA SLOVENIJA
MINISTRSTVO ZA VISOKO ŠOLSTVO, ZNANOST IN INOVACIJE

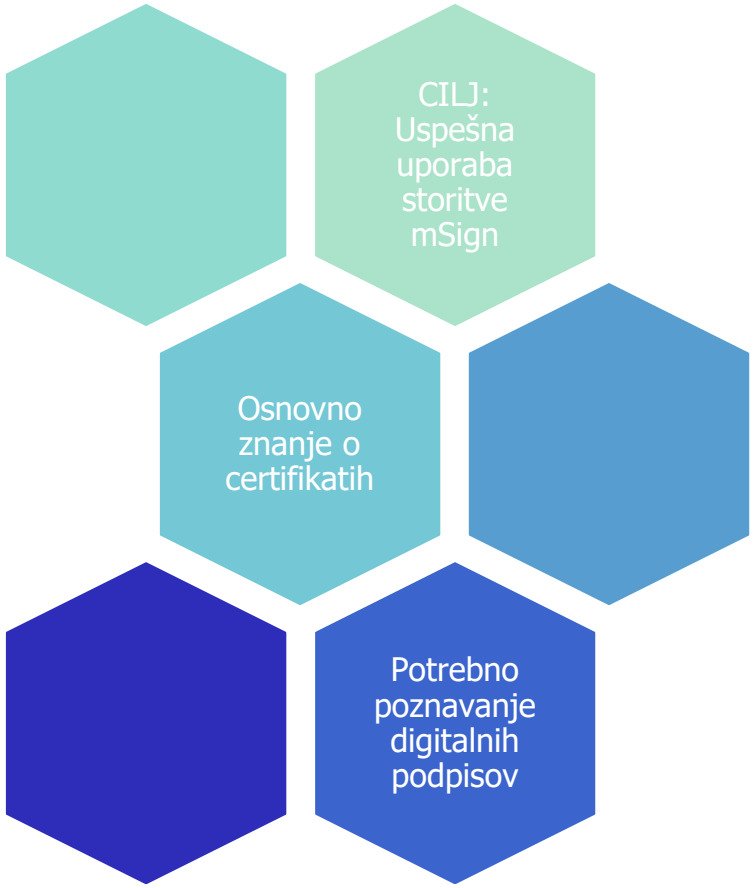
Financira Evropska unija
NextGenerationEU

Elektronsko podpisovanje v praksi: nivoji podpisov in uporaba storitve mSign

Izvajalec: dr. Marko Kežmah
Datum in ura: 4.4.2025 ob 10:00
Lokacija: MS Teams

Projekt sofinancirata Republika Slovenija, Ministrstvo za visoko šolstvo, znanost in inovacije, in Evropska unija – NextGenerationEU. Projekt se izvaja skladno z načrtom v okviru razvojnega področja Pametna, trajnostna in vključujoča rast, komponente Krepitev kompetenc, zlasti digitalnih in tistih, ki jih zahtevajo novi poklici in zeleni prehod (C3 K5), za ukrep investicija F. Izvajanje pilotnih projektov, katerih rezultati bodo podlaga za pripravo izhodišč za reformo visokega šolstva za zelen in odporen prehod v družbo 5.0: projekt Pilotni projekti za prenovo visokega šolstva za zelen in odporen prehod.

Načrt predavanja



Kako boste uporabili orodje?

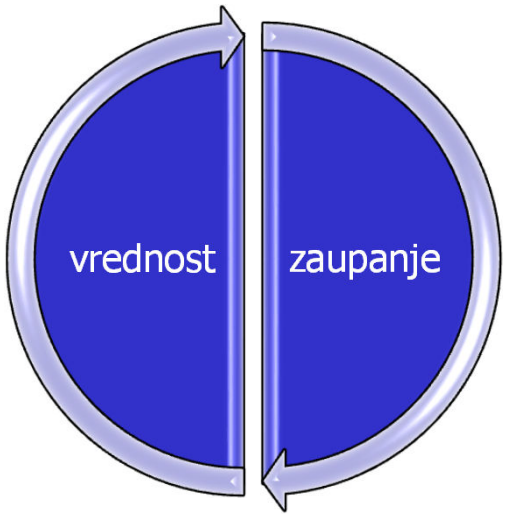
NAČRT ZA OKREVANJE IN ODPORNOST
Univerza v Mariboru
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA VISOKO ŠOLSTVO, ZNANOST IN INOVACIJE
Financira Evropska unija
NextGenerationEU

digitalno potrdilo – digitalni certifikati - certifikat

Certifikat → datoteka

Bankovec → kos papirja

Osebni dokument → kos plastike



Sistemi delujejo le, če se zanašamo na verodostojnost izdajatelja.

Država

Centralna banka

CA: Certification Authority

NAČRT ZA OKREVANJE IN ODPORNOST
Univerza v Mariboru
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA VISOKO ŠOLSTVO, ZNANOST IN INOVACIJE
Financira Evropska unija
NextGenerationEU

Digitalno potrdilo: za kaj se uporablja?

Avtentikacija (preverjanje identitete)

- Namen: Potrditi identiteto uporabnika ali sistema v digitalnih interakcijah.

Celovitost podatkov

- Namen: Zagotoviti, da podatki niso bili spremenjeni ali ponarejeni.

Digitalni podpis

- Namen: Zagotoviti, da je podpisnik pristna oseba in da dokument ni bil spremenjen po podpisu.
- Torej združuje avtentikacijo in celovitost podatkov

Šifriranje

- Namen: Zaščititi vsebino sporočila pred nepooblaščenim dostopom.

Časovno žigosanje

- Namen: Dokazati, da je bil dokument ali transakcija podpisan v določenem trenutku.

Avtorizacija (dovoljenje za dostop)

- Namen: Dovoliti dostop do določenih virov ali podatkov na podlagi identitete.
- Izhaja iz avtentikacije

NAČRT ZA OKREVANJE IN ODPORNOST
50 let Univerza v Mariboru
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA VISOKO ŠOLSTVO, ZNANOST IN INOVACIJE
Financira Evropska unija NextGenerationEU

Digitalno potrdilo: kako ga pridobimo?

DIGITALNO POTRDILO

- Lahko ga izda katerikoli overitelj (tudi ne-kvalificirani).
- Lahko ga izdelamo sami z ustrezno programsko opremo
- **Primer:** Podjetje izda digitalni certifikat za svoje zaposlene za podpisovanje internih dokumentov ali varno komunikacijo preko e-pošte.

KVALIFICIRANO DIGITALNO POTRDILO

- Izda ga lahko **samo kvalificirani overitelj**, ki je certificiran po eIDAS uredbi.
- Zahteva **strogo identifikacijo podpisnika** (osebna identifikacija).
- Priznan kot zanesljiv dokaz identitete pri pravno pomembnih transakcijah.

Pridobitev spletnega potrdila SIGEN-CA za fizične osebe

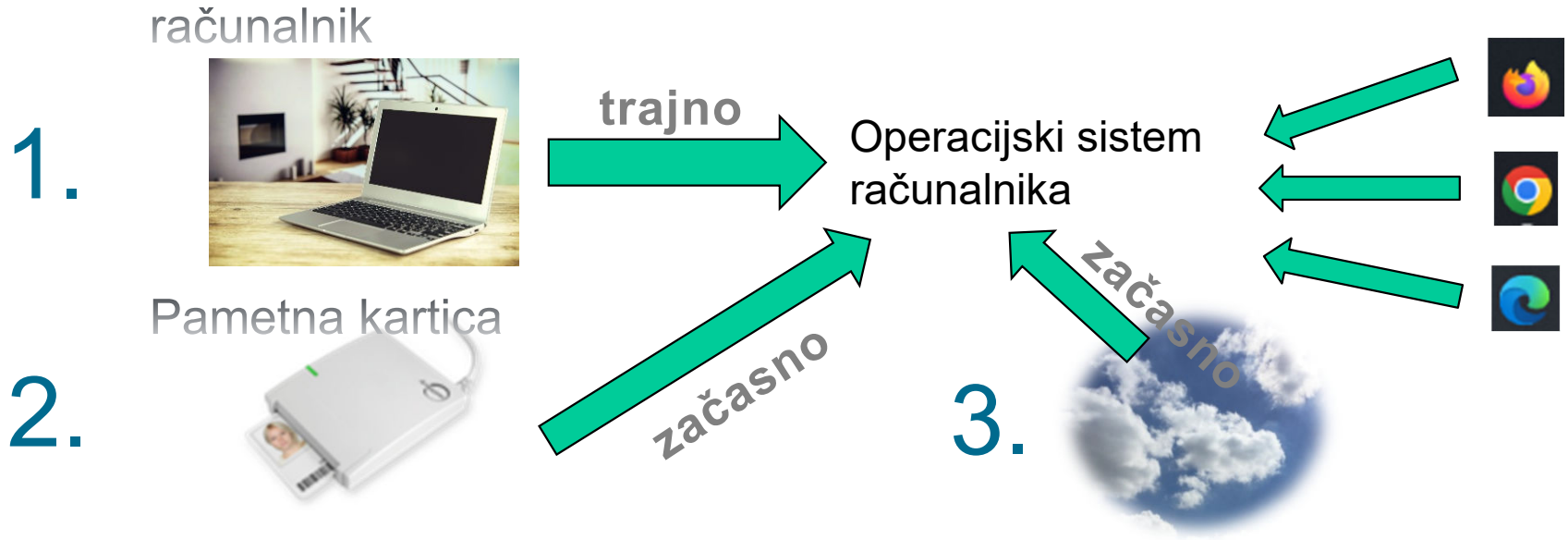
Zahtevek je potrebno oddati **osebno** na **prijavni službi na upravni enoti.**

Za to potrebujete **osebni dokument** (osebna izkaznica, potni list, vozniško dovoljenje ali drug uradno veljaven osebni dokument) in **izpolnjen zahtevek**, ki ga najdete spodaj. Zahtevki so na voljo v treh jezikih: slovenskem, italijanskem in madžarskem.

NAČRT ZA OKREVANJE IN ODPORNOST
50 let Univerza v Mariboru
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA VISOKO ŠOLSTVO, ZNANOST IN INOVACIJE
Financira Evropska unija
NextGenerationEU

Digitalno potrdilo: kam ga hranimo?

Osebni certifikat



Kaj pa korenski certifikati? (root certificate)

- Hranimo jih „na računalniku“
  - So predhodno naloženi (npr. s strani Microsoft)
  - Omogočajo preverjanje ostalih certifikatov (tudi, ko nismo povezani na splet)
    - preko verige zaupanja
  - Neveljavni certifikat:
    - Lahko da je neveljaven (potekel, preklican, neustrezen)
    - Lahko, da nimamo nameščenega ustreznega korenskega certifikata (na kar nas opozori sistem)

NOO | NAČRT ZA OKREVANJE IN ODPORNOST
50 let Univerza v Mariboru
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA VISOKO ŠOLSTVO, ZNANOST IN INOVACIJE
Financira Evropska unija
NextGenerationEU

Podpisi: Fizični podpis

OPRAVIČILO

Spoštovani,

sporočam vam, da je bil moj sin, Jaka, odsoten od pouka

od 3. 3. 2025

do 6. 3. 2025

zaradi bolezni. Prosimo za razumevanje glede njegovega izostanka in za morebitne napotke glede snovi, ki jo je v tem času zamudil.

Hvala za vaše razumevanje in prijaznost.

Lep pozdrav,

YK

OPRAVIČILO

Spoštovani,

sporočam vam, da je bil moj sin, Jaka, odsoten od pouka

od 3. 3. 2025

do 6. 3. 2025

zaradi bolezni. Prosimo za razumevanje glede njegovega izostanka in za morebitne napotke glede snovi, ki jo je v tem času zamudil.

Hvala za vaše razumevanje in prijaznost.

Lep pozdrav,

YK

NAČRT ZA OKREVANJE IN ODPORNOST

50 let Univerza v Mariboru

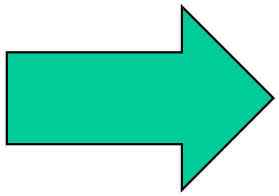
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA VISOKO ŠOLSTVO, ZNANOST IN INOVACIJE

Financira Evropska unija
NextGenerationEU

Podpisi: digitalni podpisi

Digitalni podpis omogoča preverjanje:

1. avtentičnosti (kdo je podpisal)
2. integritete (ali se dokument ni spremenil po podpisu) in
3. nepovračljivosti (podpisnik ne more zanikati, da je podpisal).



NE PRI VSEH PODPISIH!

Pravna podlaga

- Nivoji digitalnih podpisov so definirani v evropski uredbi **eIDAS (Electronic Identification, Authentication and Trust Services)**. Ta uredba določa standarde za elektronsko identifikacijo in storitve zaupanja za elektronske transakcije v Evropski uniji.
- V Sloveniji je pravna podlaga določena tudi v **Zakonu o elektronskem poslovanju in elektronskem podpisu (ZEPEP)** ter **Zakonu o splošnem upravnem postopku (ZUP)**, ki priznavata kvalificirani digitalni podpis kot pravno enakovreden fizičnemu podpisu.

! kvalificirani digitalni podpis ≠ Podpis s kvalificiranim digitalnim potrdilom

NAČRT ZA OKREVANJE IN ODPORNOST
Univerza v Mariboru
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA VISOKO ŠOLSTVO, ZNANOST IN INOVACIJE
Financira Evropska unija
NextGenerationEU

Podpisi: Nivoji digitalnih podpisov

Elektronski podpis (ES - Electronic Signature):

- Najnižji nivo, ki vključuje vse podatke v elektronski obliki, ki jih podpisnik uporabi za podpisovanje.

Napreden elektronski podpis (AdES - Advanced Electronic Signature):

- Izpolnjuje naslednje zahteve:
  - Enolično je povezan s podpisnikom.
  - Omogoča identifikacijo podpisnika.
  - Povezan je s podatki tako, da se vsaka sprememba po podpisu lahko zazna.
- Kadar uporablja ne-kvalificirana digitalna potrdila.

Kvalificiran elektronski podpis (QES - Qualified Electronic Signature):

- Je **napreden elektronski podpis s kvalificiranim potrdilom**, ki je **ustvarjen na kvalificirani napravi za ustvarjanje podpisov (QSCD)**.
- Po eIDAS uredbi je **pravno enakovreden lastnoročnemu podpisu** v vseh državah članicah EU.

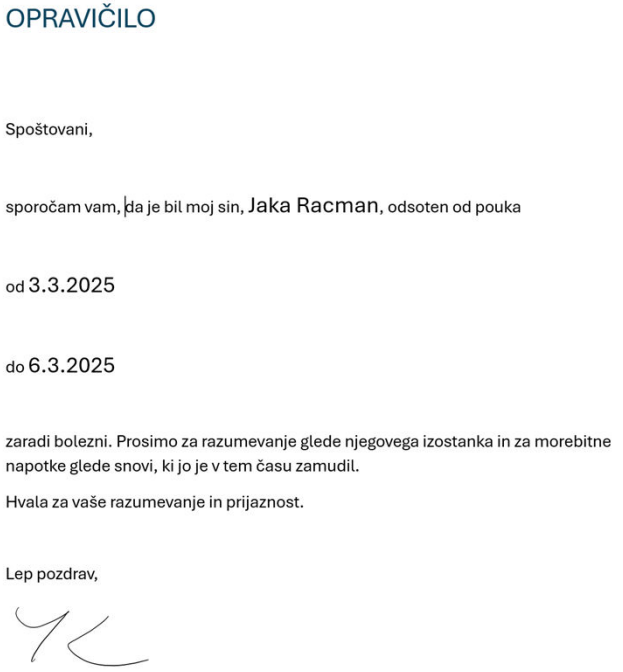
Napreden elektronski podpis s kvalificiranim potrdilom (AdES-QC - Advanced Electronic Signature with Qualified Certificate):

- Je napreden elektronski podpis, podprt s **kvalificiranim potrdilom**.
- **V SLO ni pravno enakovreden lastnoročnemu podpisu**.

NAČRT ZA OKREVANJE IN ODPORNOST
Univerza v Mariboru
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA VISOKO ŠOLSTVO, ZNANOST IN INOVACIJE
Financira Evropska unija
NextGenerationEU

Podpisi: Navaden elektronski podpis

Dokument je enostavno spremenljiv, identifikacija podpisnika ni zanesljiva



OPRAVIČILO

Spoštovani,

sporočam vam, da je bil moj sin, Jaka Racman, odsoten od pouka

od 3.3.2025

do 6.3.2025

zaradi bolezni. Prosimo za razumevanje glede njegovega izostanka in za morebitne napotke glede snovi, ki jo je v tem času zamudil.

Hvala za vaše razumevanje in prijaznost.

Lep pozdrav,

V kombinaciji z ustreznim informacijskim sistemom se lahko zanesljivost močno poveča

-> zaupanje/kontrola
-> Revizijska sled

NAČRT ZA OKREVANJE IN ODPORNOST
50 let Univerza v Mariboru
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA VISOKO ŠOLSTVO, ZNANOST IN INOVACIJE
Financira Evropska unija
NextGenerationEU

Podpisi: Napreden elektronski podpis

Word → PDF → PDF-nevidno

OPRAVIČILO

Spoštovani,

sporočam vam, da je bil moj sin, Jaka Racman, odsoten od pouka

od 3.3.2025

do 6.3.2025

zaradi bolezni. Prosimo za razumevanje glede njegovega izostanka in za morebitne napotke glede snovi, ki jo je v tem času zamudil.

Hvala za vaše razumevanje in prijaznost.

Lep pozdrav,

OPRAVIČILO

Spoštovani,

sporočam vam, da je bil moj sin, Jaka, odsoten od pouka

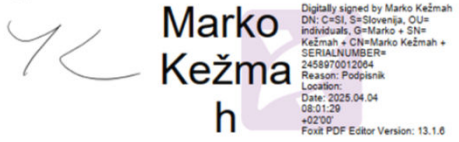
od 3. 3. 2025

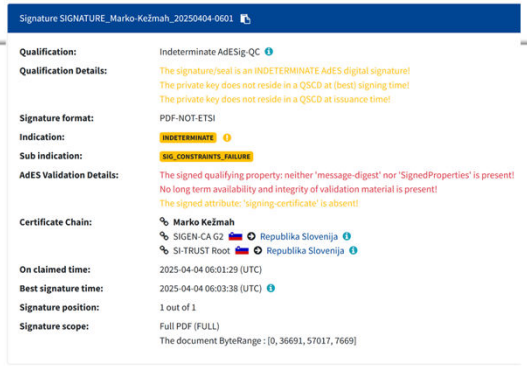
do 6. 3. 2025

zaradi bolezni. Prosimo za razumevanje glede njegovega izostanka in za morebitne napotke glede snovi, ki jo je v tem času zamudil.

Hvala za vaše razumevanje in prijaznost.

Lep pozdrav,





OPRAVIČILO

Spoštovani,

sporočam vam, da je bil moj sin, Jaka Racman, odsoten od pouka

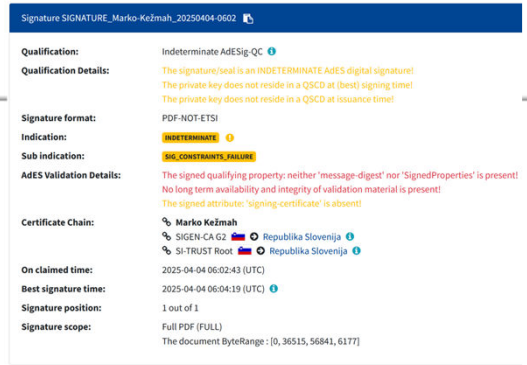
od 3.3.2025

do 6.3.2025

zaradi bolezni. Prosimo za razumevanje glede njegovega izostanka in za morebitne napotke glede snovi, ki jo je v tem času zamudil.

Hvala za vaše razumevanje in prijaznost.

Lep pozdrav,



NAČRT ZA OKREVANJE IN ODPORNOST
50 let Univerza v Mariboru
REPUBLIKA SLOVENIJA MINISTRSTVO ZA VISOKO ŠOLSTVO, ZNANOST IN INOVACIJE
Financira Evropska unija NextGenerationEU

Podpisi: Kvalificiran elektronski podpis

Digital Signatures

- **Rev.1:Signed by Marko Kezmah**
  - Signature is valid:
    - Source of Trust obtained from European Union Trusted Lists (EUTL).
    - This is a Qualified Electronic Signature according to EU Regulation 910/2014
      - The document has not been modified since this signature was applied.
      - The signer's identity is valid.
      - Signing time is from the clock on the signer's computer.
      - Signature is not LTV enabled and will expire after 2026/03/19 10:53:31 +02'00'
  - Signature Details
    - Certificate Details...
  - Last Checked: 2025.04.04 07:56:05+02'00'
  - Field: Signature1 on page 1
  - Click to view this version

Signature SIGNATURE_Marko-Kezmah_20250404-0555

Qualification:	QESig
Signature format:	PAdES-BASELINE-B
Indication:	TOTAL_PASSED
Certificate Chain:	**Marko Kezmah** Halcom CA FO e-signature 2 → HALCOM D.D. Halcom Root Certificate Authority → HALCOM D.D.
On claimed time:	2025-04-04 05:55:22 (UTC)
Best signature time:	2025-04-04 05:57:10 (UTC)
Signature position:	1 out of 1
Signature scope:	Full PDF (FULL) The document ByteRange : [0, 47801, 66747, 131233]

OPRAVIČILO

Spoštovani,

sporočam vam, da je bil moj sin, Jaka, odsoten od pouka

od 3. 3. 2025

do 6. 3. 2025

zaradi bolezni. Prosimo za razumevanje glede njegovega izostanka in za morebitne napotke glede snovi, ki jo je v tem času zamudil.

Hvala za vaše razumevanje in prijaznost.

Lep pozdrav,

Marko Kezmah
Serijska št. potrdila / Datum podpisa
150A74 / 04.04.2025, 07:55

Podpisi: Pravni učinki elektronskih podpisov

eIDAS

Člen 25

Pravni učinki elektronskih podpisov

1. Elektronskemu podpisu se ne odvzameta pravni učinek in dopustnost kot dokaz v pravnih postopkih le zato, ker je v elektronski obliki ali ker ne izpolnjuje zahtev za kvalificirani elektronski podpis.

2. Kvalificirani elektronski podpis ima enakovreden pravni učinek kot lastnoročni podpis.

3. Kvalificirani elektronski podpis, ki temelji na kvalificiranem potrdilu, izdanem v eni državi članici, se prizna kot kvalificirani elektronski podpis v vseh drugih državah članicah.

Preverjanje nivoja podpisa

PREKO BRSKALNIKA
1. Evropska komisija:
- https://ec.europa.eu/digital-building-blocks/DSS/webapp-demo/validation
2. SI-PASS (zahteva predhodno prijavo):
- https://sicas.gov.si/shibboleth-sp/about.html
3. VerifySignature.eu:
- https://verifysignature.eu/?utm_source=chatgpt.com

NAMEŠČENA PROGRAMSKA OPREMA
1. Adobe Acrobat Reader

2. Foxit reader

NAČRT ZA OKREVANJE IN ODPORNOST
Univerza v Mariboru
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA VISOKO ŠOLSTVO, ZNANOST IN INOVACIJE
Financira Evropska unija
NextGenerationEU

mSign

- Dostopno vsem zaposlenim na UM
- Omogoča elektronsko podpisovanje dokumentov z digitalnim potrdilom, zajemom ročnega podpisa in drugimi možnostmi – vse iz spletnega brskalnika na osebnih računalnikih ali mobilnih napravah.
- Nudi revizijsko sled za vse dokumente.
- Omogoča večkratno podpisovanje v uporabniško nastavljivi verigi podpisnikov.
- Dokument lahko pošljemo v podpis tudi zunanjim podpisnikom, ki niso uporabniki storitve mSign.
- E-hramba dokumentov je certificirana pri Arhivu Republike Slovenije preko brezšivne integracije s storitvijo mSef.

ZA POTREBE TESTIRANJA PUSTITE ZADNJI PODPIS NEPODPISAN
(tako je mogoč izbris dokumenta)

NAČRT ZA OKREVANJE IN ODPORNOST
50 let Univerza v Mariboru
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA VISOKO ŠOLSTVO, ZNANOST IN INOVACIJE
Financira Evropska unija
NextGenerationEU

Hvala za pozornost!

NAČRT ZA OKREVANJE IN ODPORNOST
Univerza v Mariboru
REPUBLIKA SLOVENIJA
MINISTRSTVO ZA VISOKO ŠOLSTVO, ZNANOST IN INOVACIJE
Financira Evropska unija
NextGenerationEU