

22. konferenca Dnevi slovenske informatike

Informatika – razvijamo danes za jutri

**Vseevropska
infrastruktura STORK 2.0
in čezmejne e-storitve na
podlagi e-identitet**

Tomaž Klobučar, Institut „Jožef Stefan“

14. 4. 2015

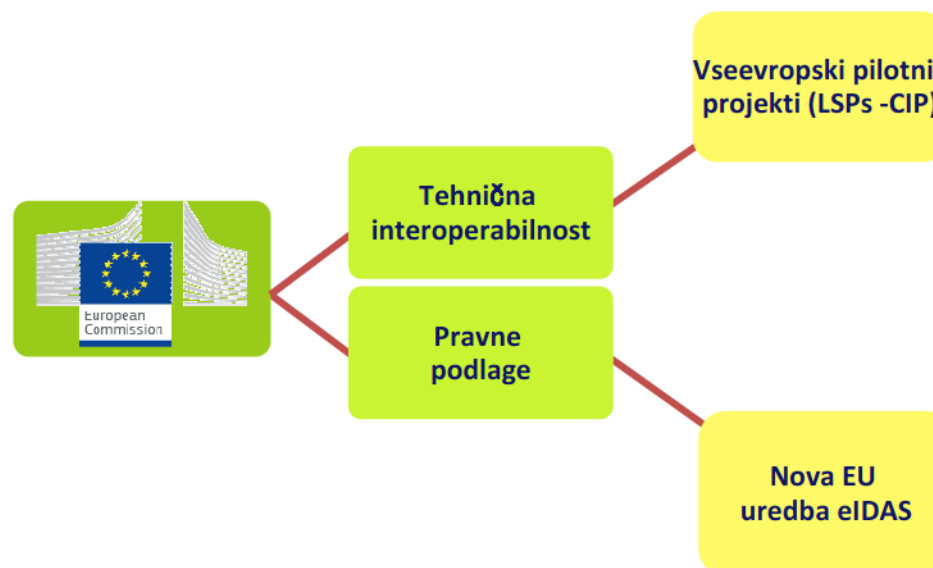
Kontekst

Varne čezmejne e-storitve in elektronske transakcije

Problemi v praksi

- Vzajemno priznavanje e-identifikacij
- Pomanjkanje interoperabilnosti sistemov za elektronski podpis
- Neenotna uporaba tehničnih standardov
- Odsotnost pravne varnosti zaradi različnih nacionalnih določb

Uredba EU o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije (eIDAS)



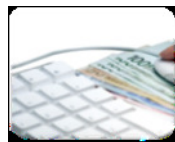
STORK 2.0

- Pilotni projekt iz programa CIP (Okvirni program za konkurenčnost in inovativnost)
- 19 evropskih držav, 58 ustanov
- Podlaga za delo so rezultati projekta STORK
- Najpomembnejši novi elementi
 - Poslovni atributi
 - Prijava v imenu druge osebe
 - Pravne osebe

E-izobraževanje



E-bančništvo



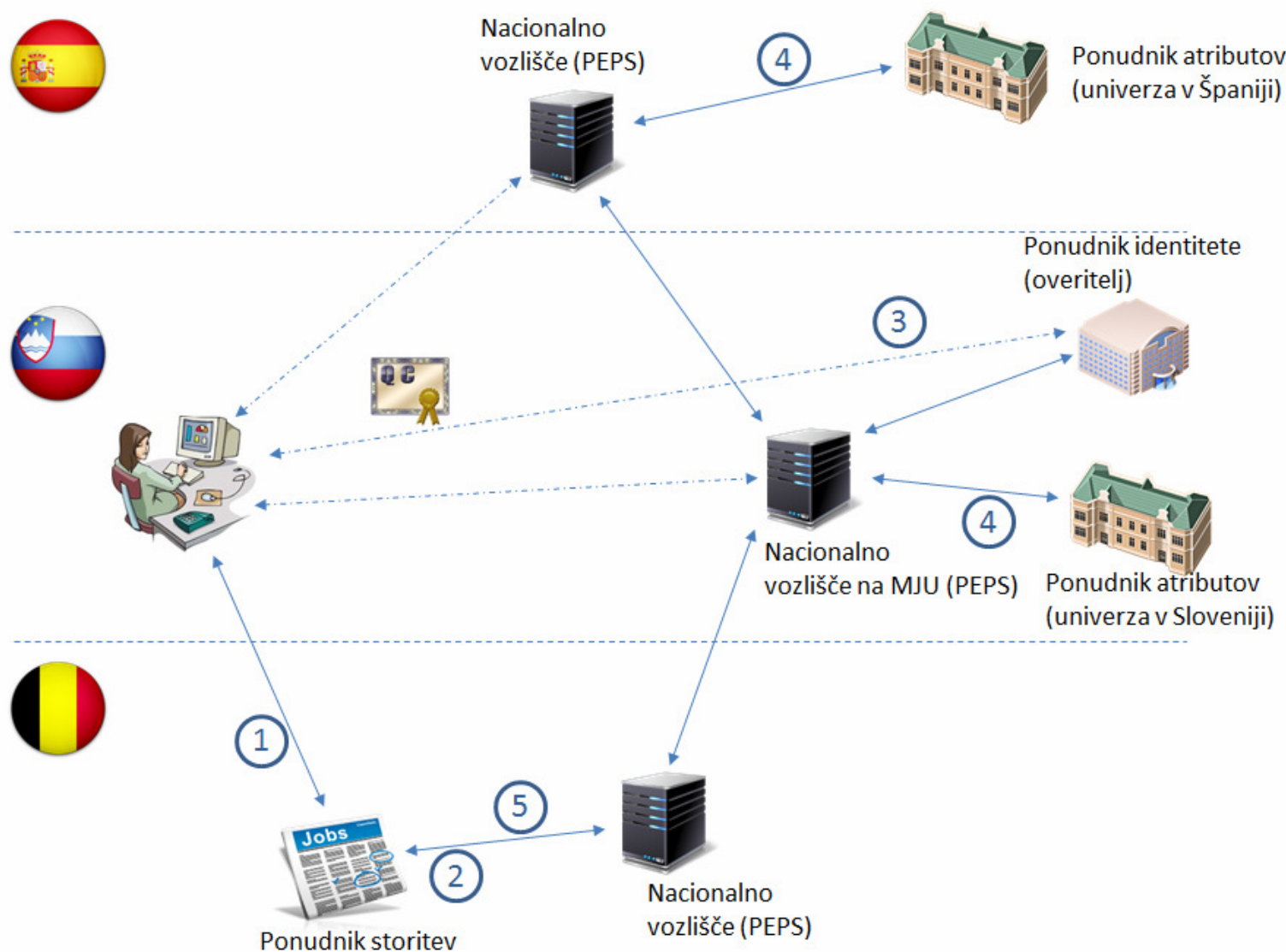
Javne e-storitve za podjetja



E-zdravje



Infrastruktura STORK 2.0



Ponudniki identitete in akademskih atributov

Ponudniki identitete

- SIGOV-CA
- SIGEN-CA
- Pošta Slovenije
- NLB
- Halcom

Ponudniki akademskih atributov

- Slovenske visokošolske organizacije

Fakulteta za računalništvo in informatiko, Univerza v Ljubljani

- Centralni evidenčni sistem eVŠ

Attributes	Jozef Stefan Institute, SI-IJS		
	eLearning	eSurvey	job selection
Diploma Supplement Attributes			
surnameOfHolder	R	R	R
givenNameOfHolder	R	R	R
dateOfBirthOfHolder	R	R	O
studentIdentificationCode	R	R	R
nameOfQualification	N	R	O
nameOfTitle	N	R	O
mainFieldsOfStudy	N	R	O
nameOfAwardingInstitution	N	R	O
statusOfAwardingInstitution	N	N	O
nameOfInstitutionAdministeringStudies	N	N	O
statusOfInstitutionAdministeringStudies	N	N	O
languageOfInstruction	N	N	O
languageOfAssessment	N	N	O
levelOfQualification	N	R	O
officialLengthOfProgramme	N	N	O
accessRequirement	N	N	O
modeOfStudy	N	R	O
programmeRequirements	N	N	O
programmeDetails	N	N	O
gradingScheme	N	N	O
gradingDistributionGuidance	N	N	O
overallClassification	N	N	O
accessToFurtherStudy	N	N	O
professionalStatus	N	N	O
additionalInformation	N	N	O
additionalInformationSources	N	N	O
higherEducationSystemInformation	N	N	O
Attributes about current Studies			
studyYear	O	R	O
grade	O	R	O
courses	O	R	O
recommendation	N	N	O
isEligibleForInternship	N	N	O
languages	O	O	O
Attributes indicating Roles			
isStudent	R	R	R
isAcademicStaff	R	R	O
isTeacherOf	O	R	O
isCourseCoordinator	R	N	N
isAdminStaff	O	N	R
Other Attributes			
habilitation (eid[, knowledge_area])	N	R	O
email (eid)	R	O	O

Pilotne akademske e-storitve

Porazdeljeno e-izobraževalno okolje za
skupni študijski program

Anonimne e-ankete

TADS (ang. trusted attribute display
service)

Prijava na prosto delovno mesto ali razpis
za štipendijo

Preverjanje kvalifikacij za zaposlitev



<https://www.eid-stork2.eu/pilots/elearning/index.php/en/>

Virtualno učno okolje

Study Slovenščina (sl) ▼ Niste prijavljeni. (Prijava)

Study room - Laboratory for Open Systems and Networks

GLAVNI MENI

- Contact
- Feedback

NAVIGACIJA

- Domov
- Contact
- Feedback
- Predmeti

Predmeti na voljo

STORK 2.0 Joint course

Izvajalec: [ANTON HAUGHEY](#)
Izvajalec: [ANDRIUS JANUTA](#)
Izvajalec: [Tomaž Klobučar](#)

This is a joint pilot course among European higher educational institutions on identity management and security. The content of the course (seven modules) is distributed among several learning systems in different countries. Here, you can find a module on digital signatures and public key cryptography.

You can access the course using your national public-key credentials. Students must select isStudent and email from the list of optional attributes.

Welcome to the Laboratory for Open Systems and Networks e-learning environment at Jozef Stefan Institute.

KOLENDAR

March 2015

ned	pon	tor	sre	čet	pet	sob
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Niste prijavljeni. (Prijava)



Virtualno učno okolje (II)

STORK 2.0 Joint course

Home ► STORK101

NAVIGATION

Home

- My home
- Site pages
- My profile
- ▼ Current course
 - ▼ STORK101
 - Participants
 - Badges
- My courses

ADMINISTRATION

- ▼ SCORM package administration
 - Edit settings
 - Locally assigned roles
 - Permissions
 - Check permissions
 - Filters
 - Logs
 - Backup
 - Restore
- Course administration
- Switch role to...
- My profile settings

Module 3

Review mode

Public Key Infrastructure

- ☒ Public Key Infrastructure
- ☒ Electronic signature
- ☒ Advanced electronic signature
- ☐ Electronic seal and advanced ele...
- ☐ Digital signature
- ☐ Digital signature creation and ver...
- ☐ Process of digital signing and sig...
- ☐ Digital signature formats
- ☐ CMS
- ☐ XML signature
- ☐ CAdES
- ☐ XAdES
- ☐ XAdES example
- ☐ PAdES
- ☐ Security properties of digital sign...
- ☐ Digital certificate
- ☐ Certification authority
- ☐ Public key certificate
- ☐ X.509 public key certificate
- ☐ X.509 public key certificate form...
- ☐ X.509 public key certificate exa...
- ☐ Qualified certificates
- ☐ Qualified certificates for electron...
- ☐ Public key infrastructure
- ☐ Registration authority
- ☐ Digital certificate issuance
- ☐ How to select an appropriate cert...
- ☐ Qualified certification service pr...
- ☐ Secure handling of private keys ...
- ☐ Public key validation
- ☐ Trust anchor
- ☐ Trusted list

Public Key Infrastructure > XML signature

XML signature

XML Signatures provide integrity, message authentication, and/or signer authentication services for data of any type, whether located within the XML that includes the signature or elsewhere. They are represented by the **Signature element** which has the following structure:

```

<Signature ID?>
  <SignedInfo>
    <CanonicalizationMethod/>
    <SignatureMethod/>
    (<Reference URI?>
      (<Transforms?>?
        <DigestMethod>
        <DigestValue>
      </Reference>)+
    </SignedInfo>
    <SignatureValue>
    (<KeyInfo>)?
    (<Object ID?>)*
  </Signature>

```

Algorithm used for signature generation and validation

Identification of the data to be signed

One-way hash of the data

Signed element SignedInfo

Information about the key needed to validate the signature

Position of the Signature element depends on the type of the XML signature:

- **Enveloping signature** - the object being signed is to be included in the Signature element
- **Enveloped signature** - the signature is over the XML content that contains the signature as an element
- **Detached signature** - signature over external network resources or local data objects that reside within the same XML document as sibling elements

Interesting

[XML Signature Syntax and Processing Version 1.1](#)

Objava prostih delovnih mest in študentskih praks

Welcome to the STORK 2.0 Job Selection pilot service

This service enables you to post or apply to a job position or student internship opportunity. What makes the service different from other job portals is that you are authenticated by your national eID credential and that proofs of required qualifications are provided in an electronic way.

Institutions can specify in your job or internship position descriptions which proofs of qualifications the applicants need to submit in an electronic way when applying for the position. You can post a new position by clicking the "Submit a Job" button on the right side of this page.

Applicants can use your national eID credentials to authenticate to the service and automatically collect proofs of qualifications from your higher educational institutions. Click on the filters below to single out the positions available for a particular country or type or use the search bar at the top of the page. In order to apply for the position you will need to provide the required valid student credentials.

STORK 2.0 is an EU co-funded project INFOS-ICT-PSP-297263.

User privacy disclaimer

In order to identify your eligibility to apply to a particular position advert, the system will need to access some of your personal information. This information will be displayed to you in full disclosure, BEFORE it is sent to our server, giving you the option to cancel the process of authentication at any time. The infrastructure ensures that your rights are safeguarded, as your personal data is protected and disclosed only with your consent.

Latest Jobs

Contract	Freelance	Full-time	Internship	Part-time	Scholarship	Student Exchange	Temporary	Filter
Germany	Italy	Slovenia						

Internship	Student internship Jožef Stefan Institute – Posted by Tomaž Klopučar	Ljubljana Ljubljana, Slovenia	25 Feb 2015
Temporary	Software development Jožef Stefan Institute – Posted by Tomaž Klopučar	Ljubljana Ljubljana, Slovenia	25 Feb 2015
Full-time	Researcher Jožef Stefan Institute – Posted by Tomaž Klopučar	Ljubljana Ljubljana, Slovenia	25 Feb 2015

Submit a Job

Browse by... Tags

Job Type

Job Salary

Job Category

Date posted

Facebook

Najdi nas na Facebooku

Stork eID

Všeč mi je

583 ljudem je všeč Stork eID.

Facebookov socialni vrčnik

Twitter

Open Data: national company register data now freely accessible <http://t.co/EnJNYFzH4y>
19 hours ago

RT @IEUws: Pre-#EURO insights - #EnergyUnion will empower EU as one of biggest energy Importers | VIDEO: <http://t.co/AQEDQOFOz> <http://t.co/...>
22 hours ago

RT @eSENS_EU: #cebit15 continues! We've just been

Anonimne e-ankete

General Anonymity options **Stork attributes** Presentation & navigation Publication & access control
Notification & data management Tokens Import Copy

Choose which STORK attributes and their values must be used to restrict participation on this survey.
A citizen will only be able to participate if all selected attributes are provided and their values match
the restrictions. With complex attributes, it is not mandatory to fill all the fields.

eIdentifier: One alternative option per line

Country code of birth: One alternative option per line

Gender: Female
Male
Select multiple alternative options

Age: between and

Is age over:

Nationality code: One alternative option per line

e-mail: One alternative option per line

Marital status: Single
Married
Separated
Divorced
Select multiple alternative options

Is student:

Institution: One alternative option per line

line

Programme of study:

Druge pilotne storitve

E-bančništvo

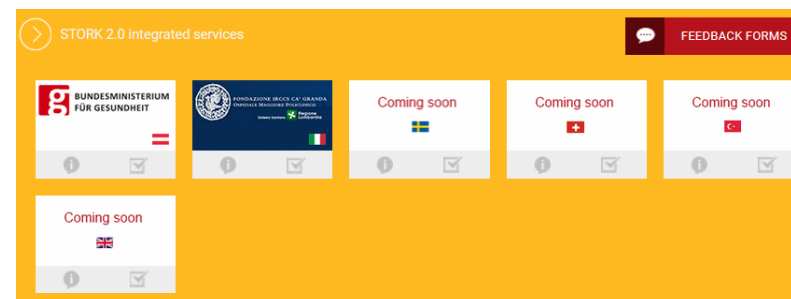
- Odprtje bančnega računa v drugi državi prek interneta
- Prijava v e-bančni sistem z nacionalnim digitalnim potrdilom
- Čezmejni e-računi (preverjanje)

Javne e-storitve za podjetja

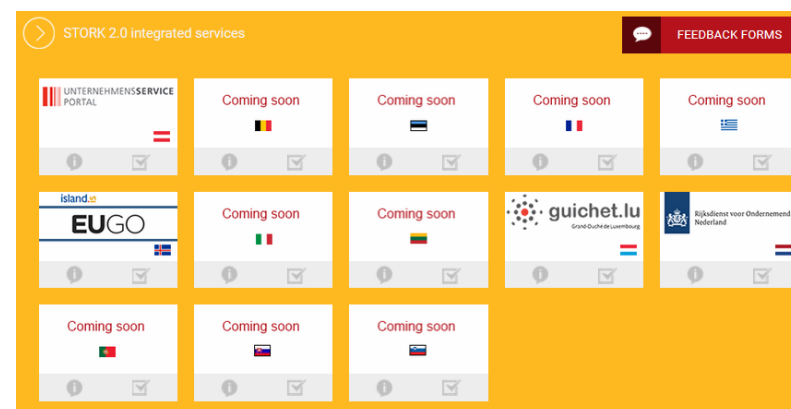
- Preverjanje pooblastil za zastopanje v primeru uporabe e-storitev v imenu podjetja
- Dodeljevanje pooblastil

E-zdravje

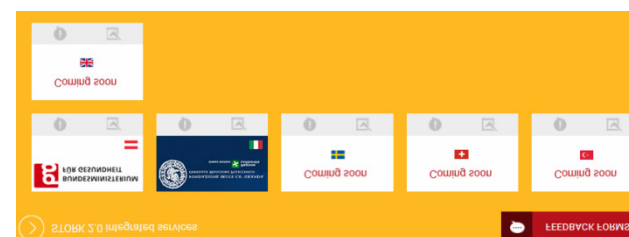
- Dostop pacienta do elektronske kartoteke
- Dostop pooblaščenca do elektronske kartoteke
- Overjanje zdravstvenih delavcev



<https://www.eid-stork2.eu/pilots/ebanking/index.php/en/>



https://www.eid-stork2.eu/pilots/public_services/index.php/en/



<https://www.eid-stork2.eu/pilots/ehealth/index.php/en/>

Koristi za deležnike

Ponudnik storitev

Višja raven varnosti in zanesljivosti preverjanja identitete, preverjeni elektronski podatki o kvalifikacijah, večje število potencialnih uporabnikov

Izobraževalna ustanova

Dodatne učne priložnosti za študente in skupne izobraževalne aktivnosti z drugimi ustanovami, poenostavljena administrativna opravila, standardizacija (npr. elektronska različica priloge k diplomi)

Posameznik

Dostop do storitev kjerkoli in kadarkoli na podlagih nacionalnih poverilnic

Podjetja in druge organizacije

Preverjeni elektronski podatki o kvalifikacijah, manjša administrativna bremena s preverjanjem papirantih dokazil

Prikaz pilotne storitve

Prijava na razpis

Welcome to the STORK 2.0 Job Selection pilot service

This service enables you to post or apply to a job position or student internship opportunity. What makes the service different from other job portals is that you are authenticated by your national eID credential and that proofs of required qualifications are provided in an electronic way.

Institutions can specify in your job or internship position descriptions which proofs of qualifications the applicants need to submit in an electronic way when applying for the position. You can post a new position by clicking the "Submit a Job" button on the right side of this page.

Applicants can use your national eID credentials to authenticate to the service and automatically collect proofs of qualifications from your higher educational institutions. Click on the filters below to single out the positions available for a particular country or type or use the search bar at the top of the page. In order to apply for the position you will need to provide the required valid student credentials.

STORK 2.0 is an EU co-funded project INFOS-ICT-PSP-297263.

User privacy disclaimer

In order to identify your eligibility to apply to a particular position advert, the system will need to access some of your personal information. This information will be displayed to you in full disclosure, BEFORE it is sent to our server, giving you the option to cancel the process of authentication at any time. The infrastructure ensures that your rights are safeguarded, as your personal data is protected and disclosed only with your consent.

Latest Jobs

Contract	Freelance	Full-time	Internship	Part-time	Scholarship	Student Exchange	Temporary	Filter
Germany	Italy	Slovenia						

Temporary	Flemish Speaker Warranty Assessor (M/F) MSX International – Posted by Marco Mezzalama	Candiolo Piedmont, Italy	15 Sep 2014
Temporary	Evaluation of web services Jožef Stefan Institute – Posted by Tomaž Klobučar	Anywhere	15 Sep 2014
Internship	Student internship Jožef Stefan Institute – Posted by Tomaž Klobučar	Ljubljana Ljubljana, Slovenia	5 Sep 2014

Submit a Job

Browse by...

Tags

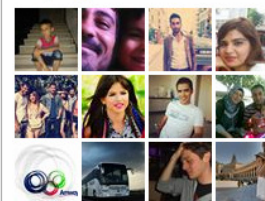
Job Type	>
Job Salary	>
Job Category	>
Date posted	>

Facebook

Najdi nas na Facebooku



519 ljudem je všeč Stork eID.



Facebookov socialni vtičnik

Twitter

Final report on electronic communications and information society in Enlargement countries
<http://it.co/D7mDx2deiy>

22 hours ago

Video: Commissioner Kroes to her successors: "It's about a different mindset" <http://t.co/80onPn7Y6L>

23 hours ago

Izbira države

Job Description

Laboratory of Open Systems and Networks at Jožef Stefan Institute is offering 1-month student internship during the 2014 autumn period. You should be a student on information and communication technologies who already has a degree in this field equivalent to 1st Bologna level (3 years of studies).

You are eligible for this position if your credentials fulfil the requirements displayed below. Select your country and click on the "European ID Login" button below in order to apply for the position and start the authentication and requirements validation process.

Is Student: Y

Name of study institution: Any

Study programme: 061

Study course: Any

Has Degree: Y

Degree level: S (Bachelor's Degree)

Name of institution issuing the degree: Any

Degree obtained on or after: Any

Degree study programme: 061

Job Categories: Science, Technology. Job Types: Internship.

34 total views, 1 today

Please click the button below to log in with your EID
Select your country:

 Slovenia - Slovenija



 Apply Online

 Print Job

 View Map

Zahtevani podatki

CENTRALNIVERIFIKACIJSKI SISTEMJAVNE UPRAVE

Strinjanje za pridobitev podatkov

Ponudnik storitev DEMO-SP z nivojem QAA 3 povprašuje po naslednjih podatkih:

Podatki

Obvezni podatki

- ☒ E-identifikator
- ☒ Ime
- ☒ isStudent
- ☒ Datum rojstva
- ☒ Stopnja
- ☒ Priimek

PošljiOpusti

Overjanje



CENTRALNI

VERIFIKACIJSKI

JAVNI

Strinjanje za pridobitev podatkov

Ponudnik storitev DEMO-SP z nivojem QAA 3 povprašuje za pridobitev vaših podatkov.

Podatki

Obvezni podatki

- ☒ E-identifikator
- ☒ Ime
- ☒ isStudent
- ☒ Datum rojstva
- ☒ Stopnja
- ☒ Priimek

Pošlji **Opusti**

Zahteva po identifikaciji uporabnika

Ta stran zahteva, da se predstavite z digitalnim potrdilom:

peps-test.mju.gov.si:443
Organizacija: "state-institutions"
Izdano pod: "state-institutions"

Izberite digitalno potrdilo, ki vas predstavlja:

1744f1ef919722676d52f69dc4def48a_20dbf8a6-c977-4053-bf5b-171eb9f5d519 [40:B2:B6:2D]

Podrobnosti o izbranem digitalnem potrdilu:

Izdano komu: CN=Ana Vzorec+serialNumber=2302201000002,OU=certificates-web,OU=SITEST-CA,O=state-institutions,C=si
Serijska številka: 40:B2:B6:2D
Veljavno od 23.2.2010 12:42:19 do 23.2.2015 13:12:19
Uporaba ključa digitalnih potrdil: Podpisuje,Šifriranje ključa
e-pošta: ana.vzorec@test.si
Izdajatelj: OU=sitest-ca,O=state-institutions,C=si

☒ Zapomni si to odločitev

V redu **Prekliči**

Izbira ponudnika atributov

CENTRALNIVERIFIKACIJSKI SISTEM
JAVNE UPRAVE

Prosim, izberite ponudnike atributov za naslednje podatke:

Obvezni podatki

☒ isStudent
IJS-AP ▼ SI-PEPS ▼

☒ Stopnja
IJS-AP ▼ SI-PEPS ▼

Neobvezni podatki

Soglasje za zbiranje atributov

STORK 2.0:: (Secure Identity Across Borders
Linked 2.0)

CitizenConsentAction.title

attribute.mandatory

- ☒ eIdentifier
- ☒ isStudent
- ☒ givenName
- ☒ dateOfBirth
- ☒ hasDegree
- ☒ surname

attribute.optional

Zbrani podatki



CENTRALNI
VERIFIKACIJSKI SISTEM
JAVNE UPRAVE



SECURE
IDENTITY
ACROSS
BORDERS
LINKED

Spodaj boste našli zbrane podatke. Če potrebujete dodatne podatke, uporabite gumb Dodaj in priskrbite potrebne informacije. Če ne, uporabite gumb Pošlji, da zaključite postopek.

Zbrani podatki

eIdentifier:
9990601505001;Q87/wZG+af18fwwZ+R2zJSU8nkHaNUhtAoJE2zE1yJWPv0oZ4l4m+jZRaaE=

givenName: Ana

isStudent: course:STORK101, study:061, AQAA:3, nameOfInstitution:Univerza v Ljubljani

dateOfBirth: 19990101

hasDegree: level:S, yearObtained:2013, nameOfInstituion:Univerza v Ljubljani, study:061, AQAA:3

surname: Vzorec

Več podatkov

Soglasje za razkritje podatkov



CENTRALNI
VERIFIKACIJSKI SISTEM
JAVNE UPRAVE



Strinjanje za posredovanje vrednosti podatkov

Pošlji naslednje podatke ponudniku DEMO-SP z nivojem dostopa 3?

☐ Enostavni podatki ☒ Sestavljeni podatki ☐ Dekodiran odgovor SAML

Obvezni podatki

E-identifikator	SI/SI/Q87 /wZG+af18fwwZ+R2zJSU8nkHaNUhtAoJE2zE1yJWPv0oZ4l4m+jZRaaE=
Ime	Ana
Datum rojstva	19990601
Priimek	Vzorec

Dodatni podatki

Job Description

Laboratory of Open Systems and Networks at Jožef Stefan Institute is offering 1-month student internship during the 2014 autumn period. You should be a student on information and communication technologies who already has a degree in this field equivalent to 1st Bologna level (3 years of studies).

If you are eligible for this position, please use below submission form to apply for the job. Otherwise consult the reasons below why you cannot apply.

Is Student: Y
Name of study institution: Any
Study programme: 061
Study course: Any
Has Degree: Y
Degree level: S (Bachelor's Degree)
Name of institution issuing the degree: Any
Degree obtained on or after: Any
Degree study programme: 061

Job Categories: Science, Technology; Job Types: Internship.

35 total views, 2 today

Ana Vzorec	Name *
ana.vzorec@e5.ijs.si	Email *
Prijava na razpis	Message (4000 characters max.) *
Prebrskaj ... Datoteka ni izbrana.	Upload resumé (zip, pdf, doc, txt, rtf)
Prebrskaj ... Datoteka ni izbrana.	Upload cover letter (zip, pdf, doc, txt, rtf)
Apply for Job	

Uspešno oddana prijava

[Contact](#) [Terms & Conditions](#) [Submit a Job](#) [Browse Resumes](#) [My Dashboard](#) [Logout](#)

Job Selection



Student internship - Internship 13 Jun
Jozef Stefan Institute – Ljubljana, Ljubljana, Slovenia 2014

 Your application has been sent successfully!

Submit a Job

Browse by... **Tags**

Job Type >

Job Salary >

Hvala za vašo pozornost!

Vprašanja?

Pripombe?

Predlogi?