

Signing made easy – hiding complexity of eSignature solutions in a black box

Janina Mincer-Daszkiewicz¹ and Tadeusz Gąsior²

¹ University of Warsaw, Poland, jmd@mimuw.edu.pl

² OPTeam, Poland, TGasior@optem.pl

Background – who is involved?

- **MUCI** consortium develops Student Information System **USOS** for > 80 HEIs in Poland.



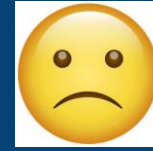
- Erasmus Without Paper (**EWP**) Network supports digitalization of the Erasmus+ programme across Europe.



- Higher Education Institutions (**HEIs**) sign many documents – for local purposes and for cross border exchange.



Supporting signing is not easy



- Many technologies, types of signatures, changing in time.
- Security and efficiency is a challenge.
- Many processes, many end users, integration is a must.
- Software should be developed, deployed, configure according to local needs, maintained – challenging for developers, admins, end users.
- HEIs (large or small) wish to have:

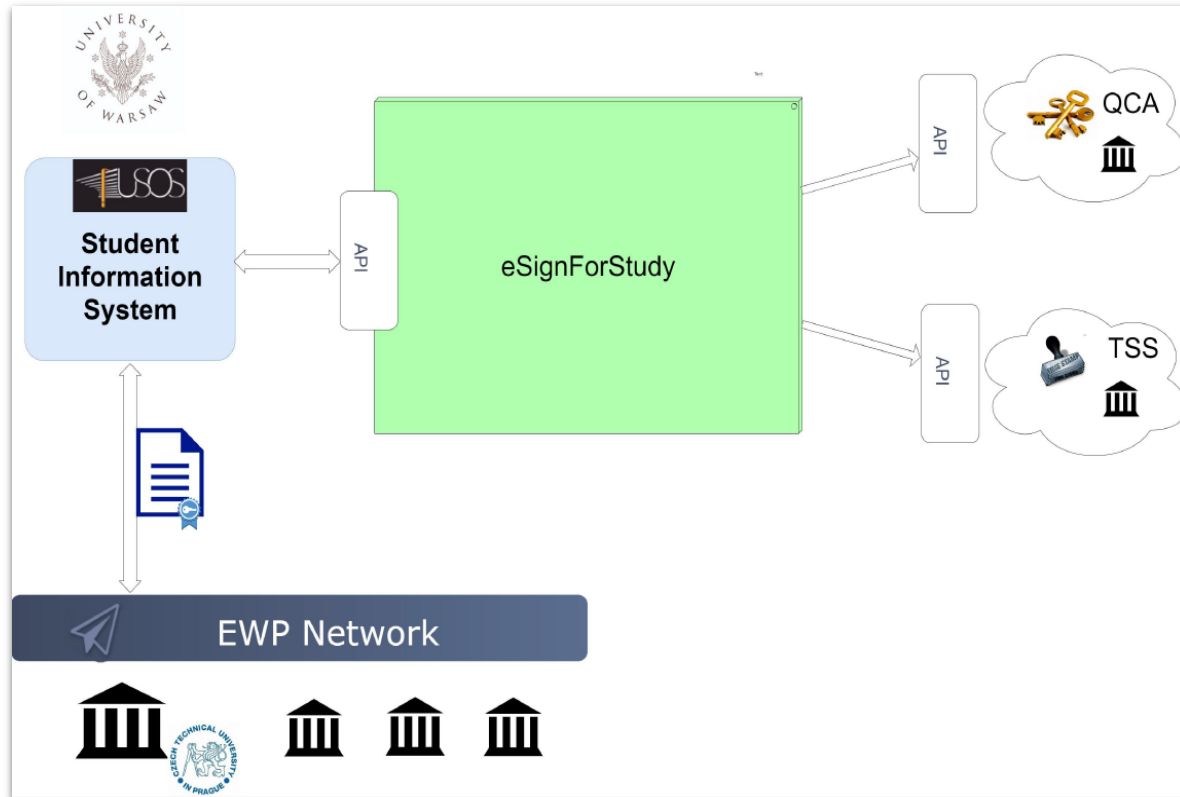
*easy-to-share, customizable, simple to install and use, low-cost
solution for*

*storing digital certificates, signing documents
and validating their signatures.*

Solution – eSignForStudy for all

- Solution *should* follow **black-box** approach with optional/interchangeable components and open interfaces to enable interoperability.
- End users *should* send requests from the system supporting their business processes **transparently** triggering digital signature procedures which should be forwarded to the black box using a **unified interface**.
- The black box *should* be **integrated** with other **external systems** needed to fully resolve the request, like Qualified Certified Authority (**QCA**) or Trusted Timestamp Services (**TSS**).
- All the **technical details**, like the types of managed certificates, media on which they are stored, security measures, software components used for validation, *should* be **hidden** to the **end user** and to **system admins**, easing the deployment in the host institution infrastructure.

eSignForStudy in the local infrastructure



Solution – summary of requirements

- Supporting legal cross-border recognition of eSignatures.
- Support for various types of eSignatures, either qualified, or issued by internal CAs.
- Easy to use for end-users.
- Simple to manage, deploy and use in an environment where there is no highly qualified IT personnel (common situation in higher education).
- Highly secure and highly efficient.
- Low cost.
- Easily exchangeable components to craft the solution to the needs of the institutions.
- Supporting set up of complex eSignature workflows and addressing the need to have documents signed more quickly.
- Supporting timestamps for long term documents.
- Supporting logging of transactions for audit purposes.

Some USOS applications which need eSignatures

- **IRK** – admission portal. Applicants for studies get the administrative decision after the admission process is finished:
 - Polish citizens – all negative decisions have to be signed.
 - Non Polish citizens – all decisions have to be signed, positive and negative.
- **USOSadm** – for administration. It contains the module for handling Erasmus+ mobility.
 - *Transcripts of Records (ToRs)* are generated for incoming students and sent to the student home university via EWP. ToR is created in the [ELMO format](#) with signed PDF.
 - *Bilateral Inter-institutional Agreements (IIAs)*, signed between partners in mobility, can carry embedded PDF, digitally signed.
- **USOSweb** – for students and academic teachers. Students apply for scholarships. All issued decisions concerning financial aid are signed and presented to students for collection.

USOS SIGN – current signing solution

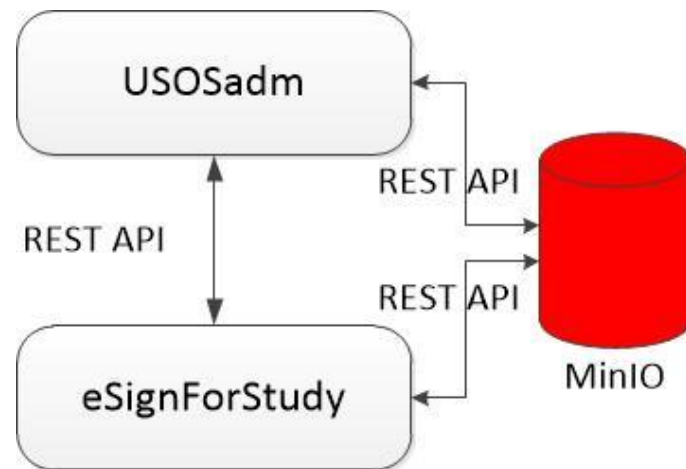
- It is a **desktop** application that must be installed on the workstation of every employee who signs documents (for largest Polish HEIs these means hundreds of installations).
- Only **one signature** can be made per **request**.
- It does not support certificates stored in the **cloud**.
- It does not support certificates stored in Hardware Security Module (**HSM**).
- It does not support university **seal**.
- It does not support **timestamps**.
- It is not possible to **verify** signatures.
- It is not possible to add **visual form** of a signature on a signed document.
- No **unified user interface** is available, so a specific one has to be developed for every application using USOS SIGN.

USOS Blobbox – storage for binary objects

- USOS stores **large binary objects** in a dedicated repository, **Blobbox**.
- Blobbox is supervised by **USOS API** which can become a **bottleneck** when serving as an entry point for the object storage on a massive scale.
- Regarded alternative solutions: **OpenStack Swift** and **MinIO**.
- MinIO is an easy to install solution and offers **S3 API** support.
- MinIO includes features that allow **access rights** to be transferred or delegated at single object level.
- MinIO will be used to **store documents** exchanged between USOS applications and eSignForStudy.
- MinIO will gradually **replace Blobbox** in USOS in all places.

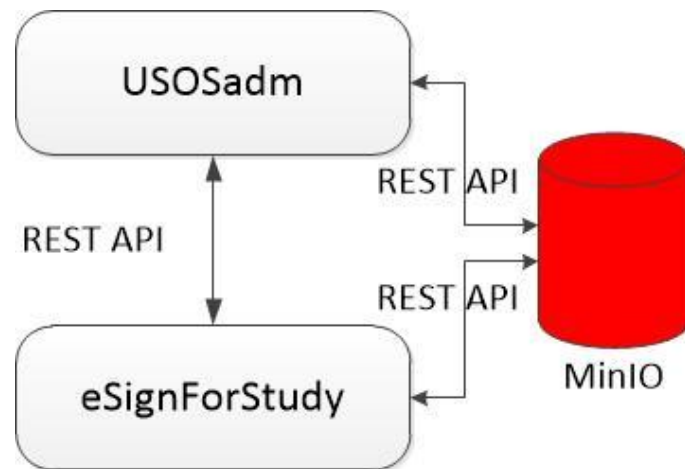
Signing process in the integrated solution

1. A user **prepares documents** for signing in the USOS application.
2. The application **stores the documents** to the **in bucket's folder** in MinIO by calling the appropriate API.
3. The application **sends a signing request** to eSignForStudy. The request includes document identifiers in MinIO, and details of the operation:
 - what type of signature is required,
 - who signs it,
 - whether a time stamp is needed,
 - whether and where a visual form of the signature should be added to the document.






Signing process in the integrated solution

- The user is **redirected** to eSignForStudy which handles the whole signing process. This includes, in a loop, for each requested document:
 - retrieving** the document from the **in folder** in MinIO,
 - signing** the document,
 - storing** the document in the **out folder** in MinIO.
- Upon signing process finalization, the user is redirected back to the USOS application. The application **collects** the documents from the **out folder** in MinIO and stores them in their final location in the USOS database.



Go to ▾ [New EWP notifications](#) [Download](#) [Get data from EWP](#) [Transcript of records ▾](#) [Transcript of records with eSignForStudy ▾](#) [? Set the filter](#) [? Reports ▾](#) [? Local reports ▾](#) [? Help](#)

Sign orders				Generate for all from the filter		Generate for selected		Sign all from the filter		Sign selected	
No	Creation date ▾	-- all values -- ▾	Type	Link to eSignForStudy page		Actions					
1	18.03.2022 13:20	Finished	TOR			→ Finish order					
2	18.03.2022 13:19	Finished	TOR			→ Finish order					
3	18.03.2022 13:17	Finished	TOR			→ Finish order					

First « « 1 2 3 4 5 » » Last 3 ▾

Arrivals filter

Choose a person by typing PESEL, student number or name [? Contact interface number](#) [Contactless interface number](#)

Choose program unit Choose program Choose stage Choose didactic cycle -- no filter -- ▾ Choose a place where program is taken [Specify filters](#)

<input type="checkbox"/>	No	Family name	Given name	PESEL	Main student number	Main program	Person's unit
<input checked="" type="checkbox"/>	1	A	Yue	32251370300	1234271846	D-BWZ (Studenci, Obcokrajowcy, Erasmus, krótkoterminowia)	04010000
<input checked="" type="checkbox"/>	2	Abatariski	Krzysztof	25292969112	1234271486	D-BWZ (Studenci, Obcokrajowcy, Erasmus, krótkoterminowia)	04010000
<input checked="" type="checkbox"/>	3	Adam	Nele	26242499002	1234271539	D-BWZ (Studenci, Obcokrajowcy, Erasmus, krótkoterminowia)	04010000
<input type="checkbox"/>	4	Adamowicz	Anna	31262428907	1234271698	D-BWZ (Studenci, Obcokrajowcy, Erasmus, krótkoterminowia)	04010000
<input checked="" type="checkbox"/>	5	Adamowicz	Jacek	25292969716	1234271492	D-BWZ (Studenci, Obcokrajowcy, Erasmus, krótkoterminowia)	04010000
<input checked="" type="checkbox"/>	6	Adamowicz	Mateusz	39252865114	1234287129	D-BWZ (Studenci, Obcokrajowcy, Erasmus, krótkoterminowia)	04010000
<input type="checkbox"/>	7	Adaszewski	Przemysław	27231051216	1234271764	D-BWZ (Studenci, Obcokrajowcy, Erasmus, krótkoterminowia)	04010000
<input type="checkbox"/>	8	Akamiro	Austin	25322923912	1234271665	D-BWZ (Studenci, Obcokrajowcy, Erasmus, krótkoterminowia)	04010000
<input type="checkbox"/>	9	Akcagöz	Cansel	28312409306	1234271574	D-BWZ (Studenci, Obcokrajowcy, Erasmus, krótkoterminowia)	04010000
<input type="checkbox"/>	10	Akçakanat	Duygu	27231051605	1234271768	D-BWZ (Studenci, Obcokrajowcy, Erasmus, krótkoterminowia)	04010000

Number of checked: 5 Uncheck all

First « « 1 2 3 4 5 » » Last 10 ▾

2021 [2016](#) [Add](#)

Folder number:
 Foreign Higher Education Institution: Caldmore Community Garden
 Erasmus code:
 City/village: Walsall
 Country: Wielka Brytania
 Continent: Europa
 Agreement: 1002/SMP/V/18
 Type of agreement: Individual

[Programs and projects](#)

Academic year of arrival: 2021
 Academic year of funding: 2021
 Arrival type: Studies
 Duration of the intended stay:
 Planned start date: 09.02.2022
 Planned end date: 28.02.2022
 Mobility from:
 Mobility to:
 Real date of arrival:

Joint study programmes:
 Is Polonia: No
 Is Polonicum:
 Scholarships group:
 Administrative supervisor:
 E-mail:
 Phone:
 Academic supervisor:
 E-mail:

Go to ▾ New EWP notifications Download Get data from EWP Transcript of records ▾ Transcript of records with eSignForStudy ▾ ? Set the filter ? Reports ▾ ? Local reports ▾ ? Help

Sign orders

No	Creation date ▾	-- all values -- ▾	Type	Link to eSignForStudy page	Actions
1	18.03.2022 13:40	Started	TOR	https://esign.dev.usos.edu.pl/ui/signbox?order-id=e7a0fc9d-3dfa-4553-b176-8e0401245f10	→ Finish order
2	18.03.2022 13:20	Finished	TOR		→ Finish order
3	18.03.2022 13:19	Finished	TOR		→ Finish order

First « « 1 2 3 4 5 » » Last 3 ▾

Arrivals filter

Choose a person by typing PESEL, student number or name Contact interface number Contactless interface number

Choose program unit Choose program Choose state -- no filter -- ▾ Choose a place where program is taken Specify filters

<input type="checkbox"/>	No	Family name ▾	Given name ▾	PESEL		Person's unit ▾
<input checked="" type="checkbox"/>	1	A	Yue	32251370300		cy, Erasmus, krótkoterminowia) 04010000
<input checked="" type="checkbox"/>	2	Abratański	Krzysztof	25292969112		cy, Erasmus, krótkoterminowia) 04010000
<input checked="" type="checkbox"/>	3	Adam	Nele	26242499002		cy, Erasmus, krótkoterminowia) 04010000
<input type="checkbox"/>	4	Adamowicz	Anna	31262428907		cy, Erasmus, krótkoterminowia) 04010000
<input checked="" type="checkbox"/>	5	Adamowicz	Jacek	25292969716	1234271492	D-BWZ (Studenci, Obcokrajowcy, Erasmus, krótkoterminowia) 04010000
<input checked="" type="checkbox"/>	6	Adamowicz	Mateusz	39252865114	1234287129	D-BWZ (Studenci, Obcokrajowcy, Erasmus, krótkoterminowia) 04010000
<input type="checkbox"/>	7	Adaszewski	Przemysław	27231051216	1234271764	D-BWZ (Studenci, Obcokrajowcy, Erasmus, krótkoterminowia) 04010000
<input type="checkbox"/>	8	Akamiro	Austin	25322923912	1234271665	D-BWZ (Studenci, Obcokrajowcy, Erasmus, krótkoterminowia) 04010000
<input type="checkbox"/>	9	Akcagöz	Cansel	28312409306	1234271574	D-BWZ (Studenci, Obcokrajowcy, Erasmus, krótkoterminowia) 04010000
<input type="checkbox"/>	10	Akçakanat	Duygu	27231051605	1234271768	D-BWZ (Studenci, Obcokrajowcy, Erasmus, krótkoterminowia) 04010000

Warning

You will be now redirected to eSignForStudy page.

Continue
Cancel

Number of checked: 5 Uncheck all First « « 1 2 3 4 5 » » Last 10 ▾

2021 2016 Add

<p>Folder number:</p> <p>Foreign Higher Education Institution: Caldmore Community Garden</p> <p>Erasmus code:</p> <p>City/village: Walsall</p> <p>Country: Wielka Brytania</p> <p>Continent: Europa</p> <p>Agreement: 1002/SMP/V/18</p> <p>Type of agreement: Individual</p>	<p>Academic year of arrival: 2021</p> <p>Academic year of funding: 2021</p> <p>Arrival type: Studies</p> <p>Duration of the intended stay:</p> <p>Planned start date: 09.02.2022</p> <p>Planned end date: 28.02.2022</p> <p>Mobility from:</p> <p>Mobility to:</p> <p>Real date of arrival:</p>	<p>Joint study programmes:</p> <p>Is Polonia: No</p> <p>Is Polonicum:</p> <p>Scholarships group:</p> <p>Administrative supervisor:</p> <p>E-mail:</p> <p>Phone:</p> <p>Academic supervisor:</p> <p>E-mail:</p>
--	--	---

Programs and projects

Signing

Home > Actions > Signing

Stop

- ✓ Accepting documents for signature
- ✓ Authentication of the signer
- ✓ Signing and Delivery
- 4 End

Information

Successful signing and sending


Download UPO

Finish

Document preview

Basic view

81c6ff40-81ef-48fb-8fa5-e06988...
1 / 2
100%
+
+
+



UNIWERSYTET WARSZAWSKI

Stamp of the organizational unit

Warsaw, 18.03.2022

TRANSCRIPT OF RECORDS HIGHER EDUCATION INSTITUTION

INFORMATION ON THE STUDENT

Surname: *Adamczyk*
 First name(s): *Piotr*
 Date of birth (day, month, year): *30.09.2048*
 Student identification number or code: *1234334148*

INFORMATION ON THE STUDIES

Name of the programme: *Short-term International Students*
 Form of study: *International exchange*
 Period of Studies: *12.02.2020 - 01.07.2020*
 ISCED code: *0312 - Political sciences and civics*

INFORMATION ON THE RESULTS GAINED

Courses by didactic cycles	Language of instruction	Type/No. of hrs	Grade	Distribution %	ECTS
<i>Summer semester 2019/20</i>					
<i>(4003-CEE-ERASMUS-OG) Central and Eastern Europe in International Relations - regional and global perspectives</i>	<i>EN</i>	<i>kon 15</i>	<i>4</i>	<i>38 (54) 8</i>	<i>6</i>
<i>(2102-ERASMUS-FOEU) Football in Europe – political and social aspects</i>	<i>EN</i>	<i>wyk 30</i>	<i>3,5</i>	<i>11 (8) 81</i>	<i>5</i>
<i>(1900-ERASMUS-GTT) Global tourism trends</i>	<i>EN</i>	<i>kon 15</i>	<i>5</i>	<i>n/a</i>	<i>3</i>
<i>(2100-ERASMUS-HIME) History of the Middle East</i>	<i>EN</i>	<i>kon 20</i>	<i>5</i>	<i>10 (90) 0</i>	<i>4</i>
<i>(2102-ANG-L-D4POPS) Political Philosophy</i>	<i>EN</i>	<i>wyk 15 / kon 15</i>	<i>[WYK] 4 [KON] ZAL</i>	<i>0 (27) 73 0 (100) 0</i>	<i>6</i>
<i>(2102-ANG-L-D4POGL) Processes of Globalization</i>	<i>EN</i>	<i>kon 30</i>	<i>5</i>	<i>50 (50) 0</i>	<i>4</i>
<i>(4023-O-PLYW2) Swimming – intermediate level</i>	<i>PL</i>	<i>wf 30</i>	<i>NZAL</i>	<i>0 (14) 86</i>	
ECTS in total:					28

Go to [New EWP notifications](#) [Download](#) [Get data from EWP](#) [Transcript of records](#) [Transcript of records with eSignForStudy](#) [Set the filter](#) [Reports](#) [Local reports](#) [Help](#)

Sign orders

No	Creation date	-- all values --	Type	Link to eSignForStudy page	Actions
1	18.03.2022 15:51	Signed	TOR		→ Finish order
2	18.03.2022 15:47	Finished	TOR		→ Finish order
3	18.03.2022 15:42	Finished	TOR		→ Finish order

First [1](#) [2](#) [3](#) [4](#) [5](#) [List](#) 3

Arrivals filter

Folder number:

Sex:

City/village: [Choose](#)

Include projects and agreements: [Choose](#)

Joint study programmes:

ISCED code: [Choose](#)

Type of mobility:

Academic year of funding: [Choose](#)

Status of the person:

Is Polonicum:

Planned date from: until:

Organizational unit: [Choose](#)

Foreign Institution: [Choose](#)

Country: [Choose](#)

Agreement: [Choose](#)

Exchange project: [Choose](#)

Purpose of mobility:

Academic year: [Choose](#)

Duration of the intended stay:

Needs accommodation:

Place of accommodation:

Form of mobility: Physical Virtual Mixed

[Filter](#) [Clear the filter](#)

Choose a person by typing PESEL, student number or name

[Contact interface number](#)[Contactless interface number](#)[Specify filters](#)

<input type="checkbox"/>	No	Family name	Given name	PESEL	Main student number	Main program	Person's unit
<input type="checkbox"/>	1	A	Yue	32251370300	1234271846	D-BWZ (Studenci, Obcokrajowcy, Erasmus, krótkoterminowi)	04010000
<input type="checkbox"/>	2	Abad Ayuso	Rafael	42270768411			12000000
<input type="checkbox"/>	3	Abad Serra	Stanislaw	40292497810	1234304909	S2-HS (Historia sztuki, stacjonarne, drugiego stopnia)	31050000

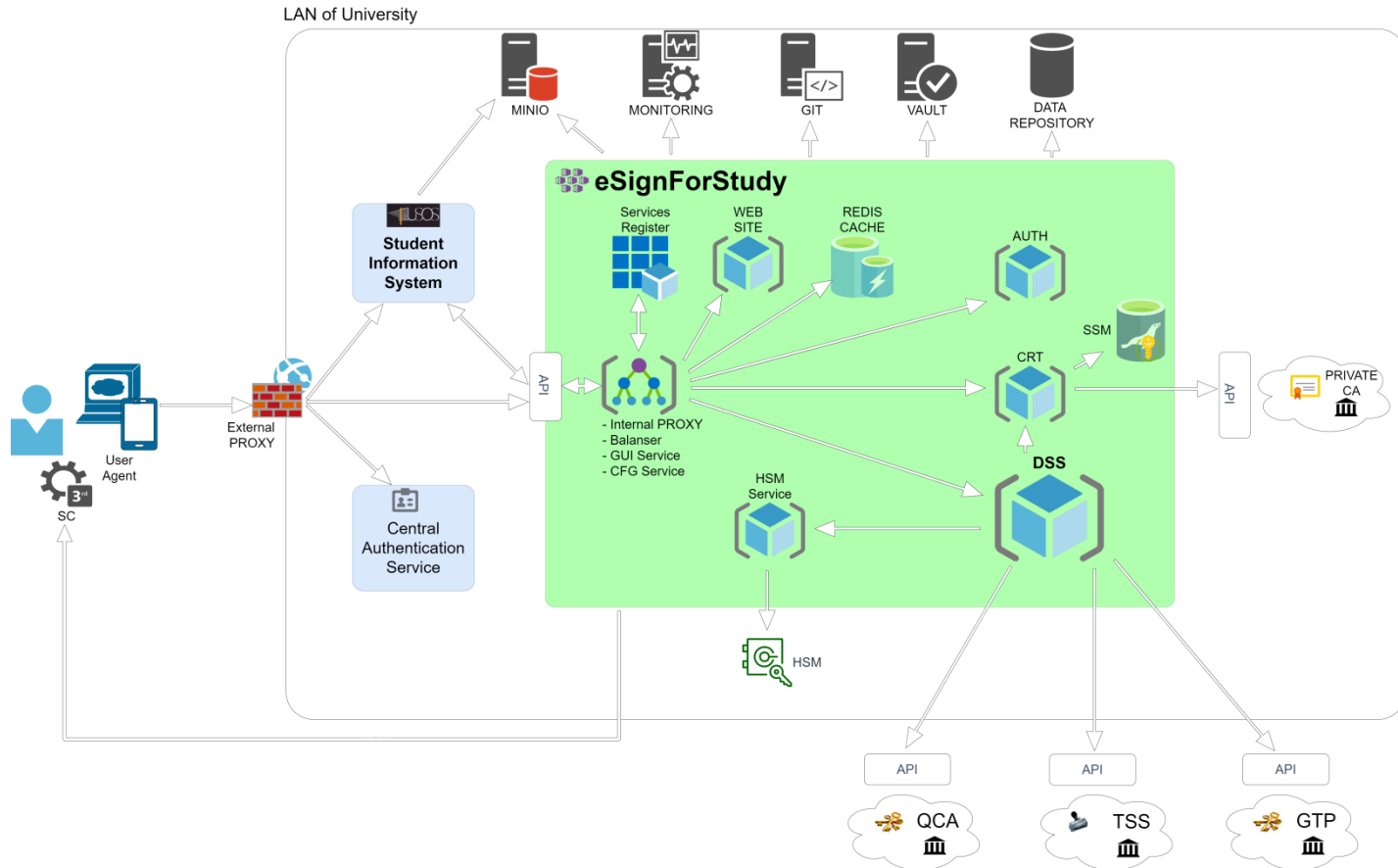
Number of checked: 0 [Uncheck all](#)First [1](#) [2](#) [3](#) [4](#) [5](#) [List](#)

3

Architecture of eSignForStudy

- It supports the handling of certificates stored in local secure repositories – *Hardware Security Module (HSM)* or its software equivalent (**SSM**).
- If qualified signatures are needed and cannot be downloaded to the local infrastructure, they can be stored in a remote cloud managed by the *Qualified Certified Authority (QCA)* and handled from inside the institution's infrastructure by means of an API.
- It enables the use of *Trusted Timestamp Services (TSS)* delivered by certified providers.
- It is based on **DSS** open-source library, which provides the means to create and validate electronic signatures and electronic seals compliant with eIDAS and related standards.
- It offers two deployment alternatives:
 - as a modular **monolith solution** using WildFly Java server (dedicated for small HEIs),
 - as **containerized microservices** dynamically managed according to a current system load handled by Kubernetes (for systems using multiple servers).

eSignForStudy – overview of internal structure



Co-systems – external and shared

Software System	Description
Monitoring	Shared. Monitoring system of the institution network. (e.g. Sentry, Prometheus, Grafana, Telegraf).
GIT	Shared. Versioning system for configuration files.
VAULT	Shared. Management of tokens, passwords, certificates, encryption keys for protecting secrets and other sensitive data.
Data Repository	Shared. Relational database system (MariaDb MySQL Postgres MS SQL Oracle)
Private Certification Authority	Shared. Certification authority of the institution PKI infrastructure (EJBCA).
Hardware Security Module (HSM)	Shared. Users' private key store based on a hardware cryptographic module, in a dedicated partition. Other partitions may be used by other applications.
QCA	External. Qualified Certified Authority.
TSS	External. Trusted Timestamp Services.
GTP	External. Governmental Trusted Profile .
SC	External. Smart Card System on user workstation.

Modules in separate Docker containers

eSignForStudy Module	Description of provided functionality	Technology
Software Security Module (SSM)	An encrypted storage of user's private keys based on a database engine.	Java, MariaDb and PKCS#12
Hardware Security Module (HSM) Service	Service used by DSS to access HSM. It is needed for licensing reasons.	Java, PKCS#11
DSS	Online signing and signature verification via JSON/ HTTPS API. The main module of eSignForStudy, many instances of it will operate under high loads.	Java and Spring MVC
CRT	Online certificates managing and remote encryption.	Java and Spring MVC
AUTH	OpenId Connect, JWT tokens, OAUTH2 and OTP.	KeyCloak Application and extensions in JAVA
Application registry	Registration of microservices.	CONSUL
WEB SITE	Web pages.	Java and Spring MVC
Single-Page application	eSignForStudy functionality for end users via web browser.	JavaScript and Angular
Proxy and balance	Balances servers load.	NGINX
CFG	Online configuration for other modules.	Java and Spring MVC
AUDIT	Audit log.	Java and Spring MVC

Summary

- Signing process, due to its **complexity** and **diversity of solutions**, usually puts an extra burden on end users.
- eSignForStudy, which is **well integrated** with systems supporting student management and which allows the **avoidance of hardware components** at the user end, is a strongly appreciated benefit.
- Well designed and configured signature services which can be crafted to the requirements of the institution not only ensure **convenience** but also **efficiency**.
- The eSignForStudy solution is aligned with the strategies and activities at **Polish national level**, by supporting digitalization of the Higher Education Area, and also on a **European level**, by supporting cross-border exchange and validation of signed documents, thus increasing interoperability and mutual recognition of electronic signatures across the EU.

eSignForStudy project is co-funded by the CEF-TC-2020-1:elidentification (eID) & eSignature programme under the grant 2020-EU-IA-0056.

University of Warsaw is also co-financed by the program of the Minister of Science and Higher Education entitled "PMW" in the years 2021-2022; contract No. 5183/CEF/2021/2.