Co-funded by
the European Union

Micro-GEAR

Micro-credentials for Higher Education systems of Georgia and Armenia: South Caucasus lighthouse project

Grant Agreement no.: 101127144

Localized online solutions for micro-credentialing

GRENA

WP3, D3.2

Document Information

Deliverable title:	Localized online solutions for micro-credentialing
Author:	GRENA, CIMEA, GTU, UER
Confirmation:	Approved by the MICRO-GEAR Project Management Board
Deliverable number:	D3.2
Work package:	WP3
Lead partner:	GRENA
Due date of deliverable:	30/06/2026
Dissemination Level	Public
Reviewed by	GTU

Version	Date	Modified by	Modification reasons
V-1	2025-2026	GRENA, all partners	Survey conducted, Structure of the document designed
V-2	November 2025 – June 2026	GRENA, GTU, CIMEA, UC3M, NCEQE, ANCA	Workshops & webinars conducted; the survey integrated in the document; facts doublechecked
V-3	May-June 2026	GRENA, GTU, UER	CIMEA Diplome Chain ToR for partners developed. Final discussion, modification and editing of the documents

"MICRO-GEAR: MICRO-CREDENTIALS FOR HIGHER EDUCATION SYSTEMS OF GEORGIA AND ARMENIA: SOUTH CAUCASUS LIGHTHOUSE PROJECT"
Project #101127144

This project has been funded with support from the EC.
This publication reflects the views of the authors only, and the EC cannot be held responsible for any use which may be made of the information contained therein.

Abstract

This deliverable describes work performed on the technical capacity building for digital micro-credentialing in Georgia and Armenia. The deliverable is related to Task 3.2 and provides information about survey results developed by the Associazione CIMEA for measuring the level of digitalization of the piloting partners from Georgia and Armenia. A study visit and a workshop at the Universidad Carlos III de Madrid for the technical personnel on blockchain technology and infrastructure for granting digital credentials are presented. Finally, CIMEA Diplome Chain for Institutions platform, terms and condition of its usage and pilot implementation of notarization for issued by the partner's certificates are described.

Table of Contents

Table of Figures

Executive Summary

The aim of Micro-GEAR project is to enhance the institutional capacity of the higher education system in Georgia and Armenia, mainly to design, develop, promote, deliver, and evaluate micro-credentials for building the most demanded competences with the goal of solving various economic and social problems.

Work Package WP3 focuses on the following activities:

- To build the capacity of the national academic communities for the implementation of short competence-oriented educational courses leading to micro-credentials.
- To create best practice and provide bottom-up feedback to the policy level.
- To equip the academic staff with the knowledge and skills in designing, developing, and conducting micro-credentials courses at their respective universities and educational institutions.
- To support Georgian and Armenian partners in defining the processes and structures of issuing and verifying of digital micro-credentials by local stakeholders, in accordance with the national regulation in the field of education and personal data protection.

The report provides overview of performed work on the technical capacity building for digital micro-credentialing in Georgia and Armenia, which includes development and conduction of the survey by the Associazione CIMEA to understand the level of digitalization and ways of its improvement for partners from Georgia and Armenia; study visit, training and workshop for the technical personnel on blockchain technology and infrastructure; and pilot implementation of notarization using CIMEA Diplome Chain for Institutions platform for issued by the partner's certificates.

1. Introduction

The overall objective of the Micro-GEAR project is to contribute towards further modernization and improving responsiveness of the system of Higher Education HE in Georgia and Armenia by supporting structural reforms aimed at the introduction of micro-credentials into educational practice as relevant, flexible and efficient means of delivering education and skills.

In Georgia there is experience in implementing small-credit educational programs, similar to micro-credentials within the framework of non-formal education centers and various organizations. From 2019, within the framework of vocational education reform, vocational training and retraining programmes are implemented, which are excellent means of lifelong learning and can be considered micro-credentials in professional development. These programmes help interested individuals to master a new profession or upgrade their skills in a short period of time and enter the labour market. The minimum and maximum duration of programmes are not defined at the system level, although in common practice their average duration varies from one to six months[1].

The development of a national platform for digital certification falls under the responsibility of the Education Management Information System in Georgia. However, decisions concerning the development of a national digital diploma and qualification platform should be made by the Minister of Education, Science, and Youth of Georgia. The work on national legislation related to micro-credentials is still in the development stage.

During 2025 significant progress has been made in **Armenia**. The Law on Higher Education adopted in September 2025, which for the first time introduces and defines micro-qualifications. The Ministry of Education, Science, Culture and Sport is currently developing the necessary bylaws to operationalize the framework.

The law establishes micro-qualifications as documented proof of specific skills and knowledge acquired through short, non-degree or non-formal learning. It enables higher education institutions to offer such programs, issue certificates upon completion, and integrate recognized micro-credentials into bachelor's and master's degree programs where appropriate. It also foresees the inclusion of micro-qualifications in the national qualifications register, ensures accreditation requirements for programs awarding ECTS credits, and introduces a centralized system for recording qualifications and learning outcomes.

Despite this emerging legal basis, the system is still in an early stage of implementation. Armenian universities already provide various short courses, some of which align with micro-credential principles in terms of learning outcomes and structure. In 2022, the Government introduced a 30 ECTS teacher training program to address teacher shortages in high-mountainous and border regions, implemented by licensed higher education institutions and training providers, which is closely aligned with the concept of micro-credentials. Since then, four Armenian universities, as well as a few private training organizations, have received a license from the Ministry of Education, Science, Culture and Sports of the Republic of Armenia to provide the teacher training course, which is well-fitted to the definition of micro-credentials.

[1] https://microgear.org/files/Analysis-of-Existing-Micro-Cedential-System-Practices-in-Higher-Education-System-of-Georgia.pdf

In addition, universities, research institutes, NGOs, and private providers offer a range of short courses that issue certificates indicating learning hours and content. However, these offerings are not yet uniformly regulated or systematically integrated into a national micro-credential framework.

The Higher Education and Science Committee is actively working on the development of a national digital diploma and qualification platform. This state-level system is intended to cover all types of qualifications awarded by higher education institutions in Armenia, including future developments related to micro-credentials.[2]

Until the establishment of fully functioning National platforms, Project Management Board asked Associazione CIMEA to use CIMEA Diplome Chain platform for Institutions for the notarization of the micro-credentials, for the courses developed and conducted in the framework of the Micro-GEAR project. This will allow project participants to gain experience and expertise in notarizing the issued certificates.

Task 3.2 was focused on the technical capacity building for digital micro-credentialing in Georgia and Armenia. The following activities were performed:

- Launch of a survey developed by the Associazione CIMEA to measure the level of digitalization for the piloting partners in Georgia: Georgian Technical University (GTU), University of Georgia (UG), Georgian Research and Educational Networking Association (GRENA) and Armenia: Yerevan State University (YSU), Eurasia International University (EIU), Center for Ecological-Noosphere Studies (CENS).
- Contribution from the partners from Georgia and Armenia and analyses of the obtained results.
- Study visit of the group of professionals from Georgia and Armenia to the Universidad Carlos III de Madrid (UC3M) to get acquainted with the infrastructure and available solutions for micro-credentialing.
- Online preparatory meeting (13 November 2025) and face-to-face training workshop (15 December 2025) for the technical personnel on blockchain technology and infrastructure for granting digital credentials developed and delivered by Associazione CIMEA representatives.
- Pilot implementation of notarization of the project courses based on the CIMEA Diplome Chain for Institutions platform.

The deliverable describes work performed in frame of Micro-GEAR project on technical capacity building for digital micro-credentialing in Georgia and Armenia. It consists of: Introduction, Section 1, presents results of survey developed by the Associazione CIMEA on digital micro-credentialing readiness of piloting partners Section 2. Workshop on blockchain technology and infrastructure for granting digital credentials is described in Section 3. The CIMEA Diplome Chain for Institutions platform functionalities are presented in Section 4. The main parts of the Micro-GEAR Terms and Conditions for the use of CIMEA Diplome Chain for Institutions is described in Section 5. Pilot use of CIMEA Diplome Chain for Institutions platform for notarization of certificates is presented in Section 6. The final Section 7 draws some conclusions.

[2] https://microgear.org/files/Analysis_of_Existing_Micro_Credential_Practices_in_HE_of_GEO_and_Armenia.pdf.

2. Survey results on digital micro-credentialing readiness

The survey was developed by the Associazione CIMEA and focused on institutions participating in piloting the digital issuing of micro-credentials within the Micro-GEAR project. The objective was to identify the current level of digitalization, technical preparedness and institutional needs in order to support the implementation of micro-credentialing systems in Georgia and Armenia.

Survey Methodology

The survey methodology combined both close-ended and open-ended questions. The questionnaire was structured around several thematic areas, including the current state of credential awarding, technical skills related to blockchain technology, infrastructure development, and future implementation steps. Respondents were asked to provide information regarding existing institutional practices, digital systems, knowledge of blockchain technology, training needs and future plans for digital credentialing.

The survey was designed not only to gather statistical information but also to better understand institutional concerns, recommendations, and expectations related to the implementation of blockchain-supported digital micro-credentials. The collected data contributed to identifying the main challenges and opportunities for developing sustainable and interoperable micro-credential systems across the partner countries.

Current State of Credential Issuing

The survey results demonstrated that the majority of participating institutions continue to rely primarily on paper-based qualifications and credentials. Institutional procedures for issuing qualifications were found to be relatively similar among higher education institutions, although some differences existed for non-higher education partners. Most institutions still use traditional administrative procedures and have not yet fully transitioned to born-digital credentials.

Only one participating institution indicated that it currently issues additional digital documents such as enrolment certificates, academic transcripts, student status confirmations, internship letters, and fee receipts. The majority of institutions confirmed that digital credential issuance remains limited and that significant institutional and legal developments are still required before large-scale implementation can take place.

The survey also explored institutional data collection and storage practices. Participating organizations reported storing data using different systems, including Excel spreadsheets, internal institutional platforms, and national-level systems. While some institutions have already started discussions on further digitalization of their processes, respondents emphasized that national legal regulations and policy frameworks are essential prerequisites for moving toward fully digital credentialing systems.

Micro-Credentials and Digitalization

The findings revealed that only one institution currently issues micro-credentials in selected educational programmes. The institution reported using procedures that differ from standard diploma issuance processes. For the remaining partners, micro-credentialing is still considered a developing area that requires further institutional preparation, policy support and technological infrastructure.

Despite the limited implementation of micro-credentials at the institutional level, the survey demonstrated strong interest among all participating organizations in further exploring and adopting digital credentialing systems. Institutions acknowledged the growing importance of short competence-oriented educational units and recognized the need to modernize qualification issuance in line with international trends and best European practices.

Blockchain Technology and Technical Skills

A major section of the survey focused on institutional knowledge and technical skills related to blockchain technology. The results showed that awareness and practical use of blockchain technology for issuing, verifying, and managing digital credentials are still very limited among the participating institutions.

Several institutions indicated that before participating in the Micro-GEAR project, there had been little or no awareness of blockchain technology in relation to digital credentials. As a result, respondents expressed the need for both introductory and advanced technical training to strengthen institutional capacity.

The requested areas for capacity building included basic training on blockchain technology for digital credentials, blockchain architecture, interoperability standards, cybersecurity, management of digital signatures and cryptographic keys, and integration of blockchain credentialing systems with existing student information systems. Institutions also highlighted the need for legal guidance related to governance, personal data protection and compliance with international standards.

Recommendations and Capacity Building Needs

Participants suggested several methods for effective knowledge sharing and institutional capacity building. These included workshops, practical training sessions, webinars with international experts, study visits, peer-to-peer exchange activities, mentorship opportunities, and joint pilot projects. Respondents emphasized that sustainable capacity building should combine both theoretical and practical learning approaches.

Institutions also recommended the development of technical documentation and follow-up support mechanisms to ensure long-term sustainability of digital micro-credentialing systems. Collaboration between Georgian and Armenian institutions was considered particularly important for sharing experiences, harmonizing approaches and establishing interoperable regional practices.

Infrastructure Development

The survey further examined the availability of infrastructure, equipment, hardware, and software necessary for implementing blockchain technology and digital credentialing systems. Most institutions indicated that future investments in infrastructure would depend on national legislation, institutional priorities and financial justification.

Participants proposed several strategic recommendations for infrastructure development. These included the creation of centralized platform in the country for secure digital credentialing, upgrading server and network capacities, establishing secure testing environments and developing national registries of micro-credentials to ensure recognition and portability.

Additionally, respondents suggested exploring the possibility of creating a shared regional blockchain node or consortium-based infrastructure between Georgian and Armenian institutions. Such cooperation was viewed as an important step toward ensuring interoperability, sustainability and cross-border recognition of digital credentials.

Conclusions

Overall, the survey results highlighted both the opportunities and challenges associated with the implementation of digital micro-credentialing systems in Georgia and Armenia. While the majority of participating institutions are still in the early stages of digital transformation and blockchain adoption, there is clear institutional interest and commitment to further development in this area.

The findings demonstrated the need for continued technical training, institutional support, infrastructure development, and policy alignment in order to establish secure, reliable, and interoperable digital credentialing systems. The survey also provided valuable insights that will support future project activities, pilot implementations and cooperation among project partners working toward the advancement of micro-credentials in higher and vocational education.

Below are presented some key results obtained from the conducted survey.

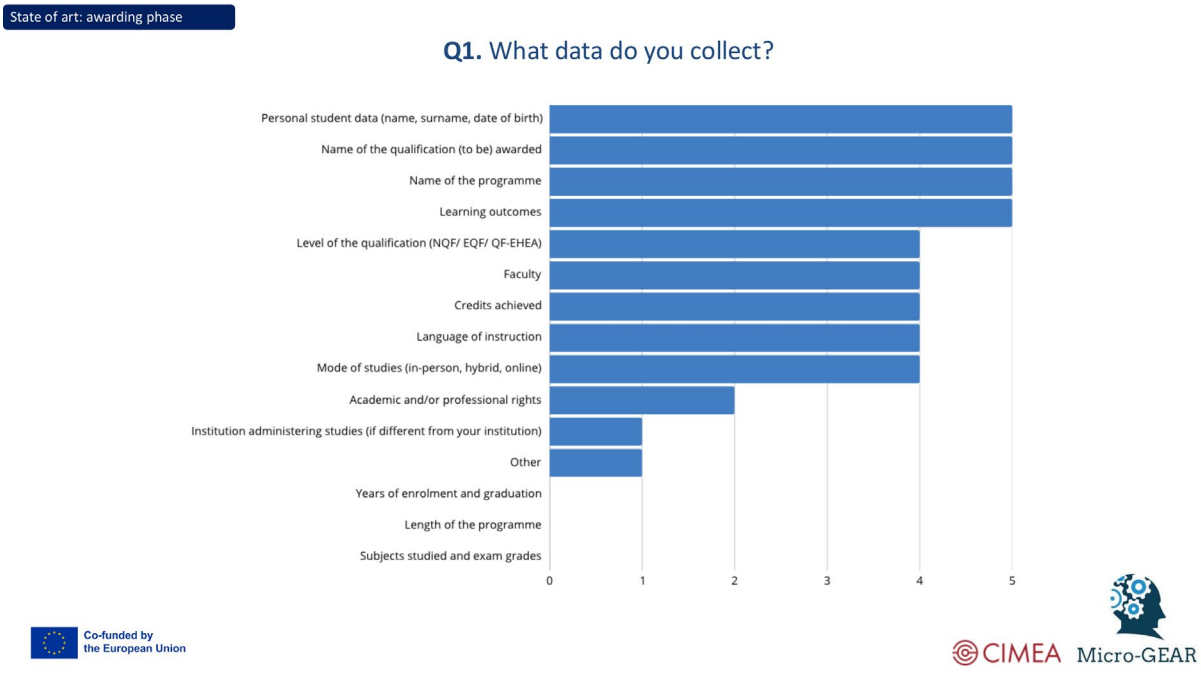


Figure 1. Data collected by the institutions

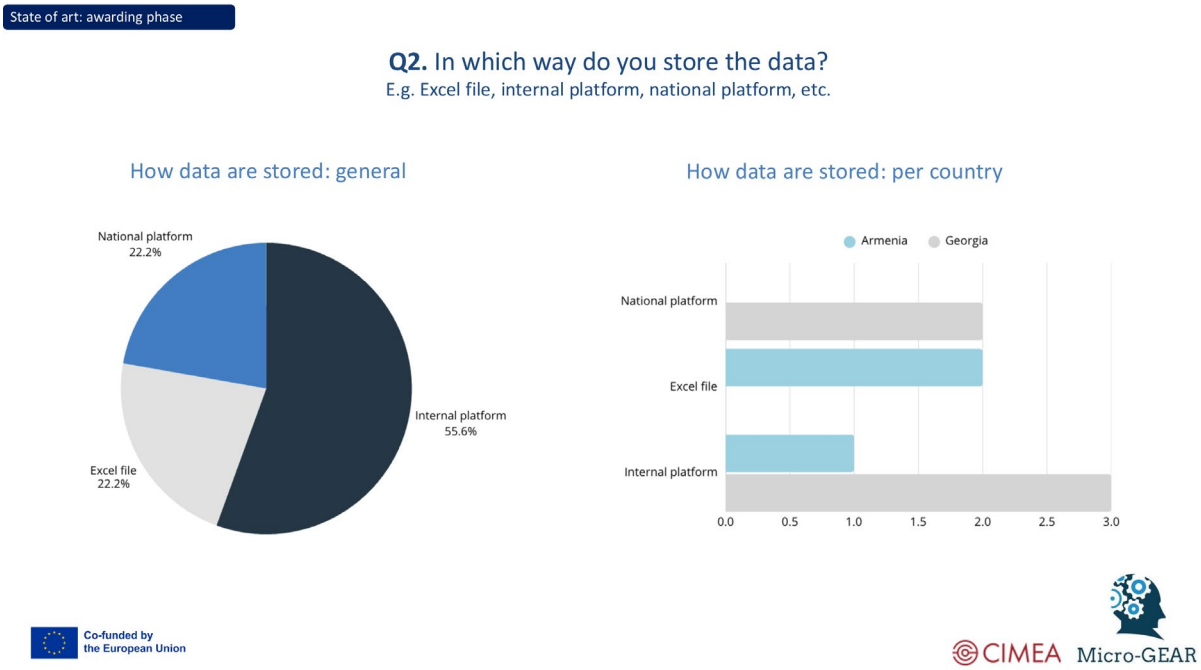


Figure 2 Used storage methods

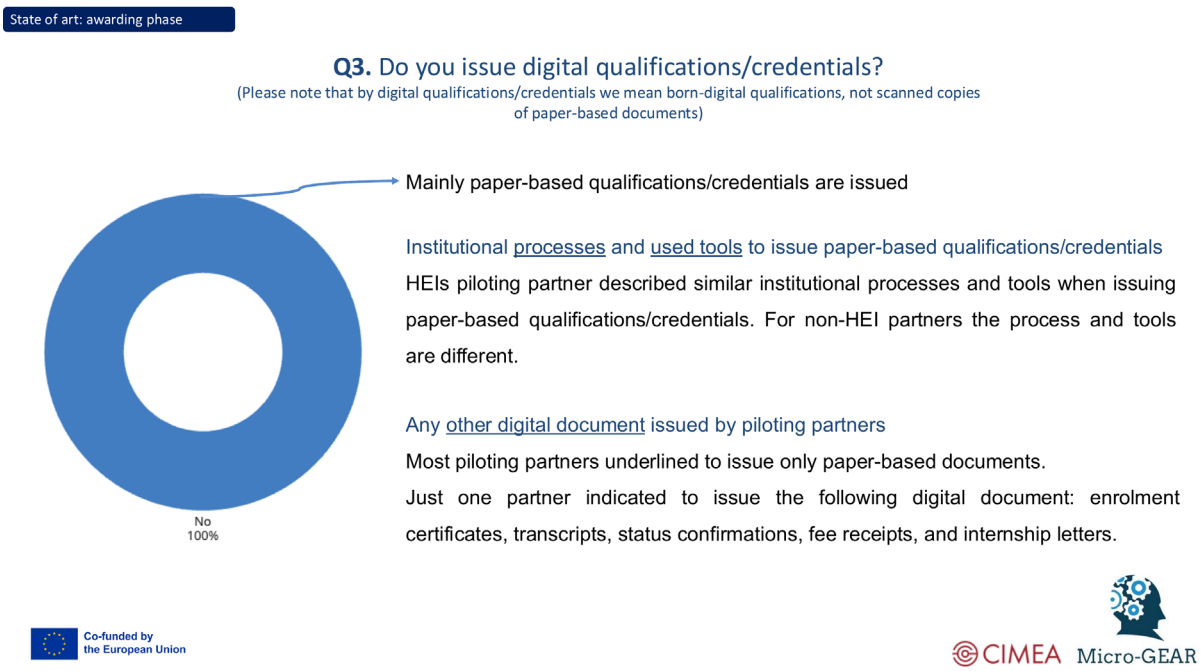
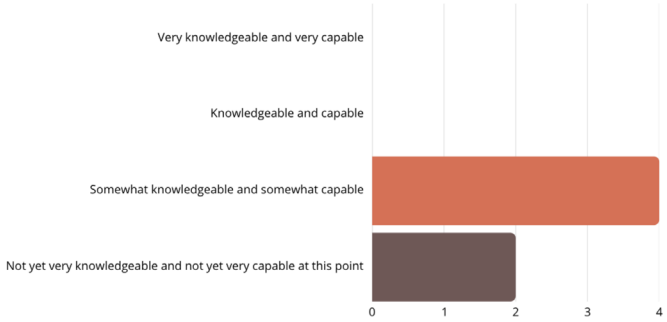


Figure 3 Digital qualifications/credentials

Technical skills and blockchain technology

Q6. To what extent is your institution currently knowledgeable about blockchain technology, and currently capable of (in terms of skills) implementing blockchain technology for issuing, verifying, and managing digital credentials?



- Knowledge on blockchain technology is mainly concentrated into programme courses. When it comes to practical institutional application for issuing, managing and verifying digital credentials, the use of BC is still limited.
- There is no use of the BC Technology and there was no awareness on the topic before the Micro-GEAR Project.

Co-funded by the European Union

CIMEA Micro-GEAR

Figure 4 Blockchain knowledge and deployment capacity

3. Workshop on blockchain and digital credentials

Within the frame of the Micro-GEAR Project, the workshop on blockchain technology and infrastructure[3] for granting digital credentials was held on December 15, 2025, in Madrid, Spain.

The event was hosted by the Universidad Carlos III de Madrid (UC3M) and the programme included expert presentations on blockchain-based digital credentials, with a special focus on legal aspects, reliability, governance and protection of rights as well as in-depth training on the CIMEA Diplome Chain for Institutions platform.

To fully understand the focus of the December 15 workshop, it is necessary to situate it within the evolving European Union policy landscape for micro-credentials. The EU has progressively built a comprehensive framework making micro-credentials an important element of its skills and education agenda.

The European Skills Agenda[4] announced in June 2020 identified micro-credentials first as a mechanism for up-skilling and re-skilling professionals, increasing the permeability and flexibility between different education sectors. The Digital Education Action Plan[5] 2021–2027 further positioned micro-credentials as tools to support the relevance, quality, and inclusiveness of European education and training at all levels.

The most significant policy milestone was the Council Recommendation of 16 June 2022[6] on European approach to micro-credentials for lifelong learning and employability. This recommendation established a common EU-level definition of micro-credentials and set out actions to create ecosystems for micro-credentials across member states and partner countries. The Recommendation defines a micro-credential as:

> *"...the record of the learning outcomes that a learner has acquired following a small volume of learning. These learning outcomes will have been assessed against transparent and clearly defined criteria. Learning experiences leading to micro-credentials are designed to provide the learner with specific knowledge, skills and competences that respond to societal, personal, cultural or labour market needs. Micro-credentials are owned by the learner, can be shared and are portable."*

Blockchain Technology

Blockchain technology, at its core, is a type of distributed ledger — a database shared and synchronized across a network of computers. Unlike conventional databases controlled by a single authority, a blockchain is maintained collectively by its participants. Entries (blocks) are cryptographically linked in sequence (a chain), making the record tamper-evident and effectively immutable without consensus from the network.

---

[3] https://microgear.org/Micro_GEAR_Workshop_on_Blockchain_and_Digital_Credentials_15_December_2025/en/.

[4] https://euroguidance.eu/new-skills-agenda

[5] https://education.ec.europa.eu/focus-topics/digital-education/actions

[6] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022H0627(03)

Key technical characteristics of blockchain that make it suitable for credentialing applications include:

- **Decentralization:** No single authority controls the ledger; records are replicated across multiple nodes, eliminating single points of failure.
- **Immutability:** Once data is written to the blockchain, it cannot be altered or deleted without detection, because each block contains a cryptographic hash of the previous block.
- **Transparency:** Transactions can be publicly auditable (in public blockchain configurations), allowing third parties to independently verify claims.
- **Smart Contracts:** Self-executing code deployed on blockchain platforms (most notably Ethereum) that automates credential issuance and verification logic without requiring intermediaries.
- **Cryptographic Security:** Public-private key cryptography ensures that only the authorized issuer can issue credentials, and only the holder can share them.

The Micro-GEAR project aligns with the European Council's Recommendation on micro-credentials for lifelong learning and employability, adopted in June 2022. The project's overarching goals include updating National Qualifications Frameworks in both Georgia and Armenia, establishing consensus on micro-credentialing principles, promoting educational activities for micro-credentials, and facilitating mutual recognition across borders.

The December 15 workshop focused specifically on the technological infrastructure underpinning modern micro-credentialing systems namely blockchain technology and digital credential frameworks.

The workshop was convened with the following core objectives:

- To introduce participants to the conceptual and technical foundations of blockchain technology as applied to digital credentials and micro-credentials.
- To examine existing platforms, standards, and tools for issuing, storing, and verifying digital credentials on distributed ledger systems.
- To explore how blockchain-based credentialing systems can support the implementation of micro-credentials in Georgian and Armenian higher education institutions.
- To present European and international standards — including W3C Verifiable Credentials and Open Badges — and discuss their relevance for the South Caucasus context.
- To enable participants to critically assess the benefits, limitations, and practical implementation challenges of blockchain-based credentialing.
- To position digital credential infrastructure within the broader policy framework established by the 2022 Council Recommendation on micro-credentials.

A critical dimension of the micro-credentials' ecosystem is the digital infrastructure required to issue, store, share, verify and stack credentials. Without robust, secure and interoperable digital systems, the policy ambitions around portability and mutual recognition of micro-credentials cannot be realized in practice.

This is where blockchain technology becomes directly relevant. As noted in the European Commission's work on the digitalization of credentials, digital systems support recognition by enabling portability, transparency and the reliable verification of authenticity. The December

15 workshop engaged directly with this challenge, exploring how distributed ledger technologies can serve as the backbone of a trustworthy credentialing ecosystem.

The Micro-GEAR workshop on blockchain and digital credentials delivered a substantive and well-structured training experience that successfully combined technical depth with policy relevance. The workshop's timing immediately preceding the broader methodology workshop of 16–17 December in Saarbrücken allowed participants to develop the specific digital infrastructure knowledge needed to fully engage with the methodological questions addressed in the following days.

The training was particularly effective in bridging the gap between the abstract policy language of EU Recommendations and the concrete technical realities of implementing blockchain-based credentialing systems. Participants left with a clear understanding of both the possibilities and the practical constraints of the technology.

The Micro-GEAR Workshop on blockchain and digital credentials has demonstrated that blockchain technology represents a mature and viable infrastructure for modern digital credentialing systems. While challenges remain particularly around standardization, cost and digital literacy the benefits for fraud prevention, portability and learner ownership are compelling.

Finally, the workshop on blockchain and digital credentials together with methodology workshop were made a valuable contribution to building the digital credentialing capacity of higher education stakeholders in Georgia and Armenia.

4. CIMEA Diplome Chain for Institutions

DiploMe is CIMEA's renewed platform for comparability and verification services developed using blockchain technology. Through the platform, users can provide foreign credentials digitally, apply for evaluation and/or verification, follow the status of the application, and receive alerts once a statement has been published. The primary purpose of the platform is to allow universities, certification bodies and partner organisations to notarise PDF documents on a dedicated blockchain infrastructure.

The platform is made available free of charge to Micro-GEAR partner institutions from Georgia and Armenia for the purpose of notarising the micro-credentials developed and issued within this project.

When a CIMEA Statement is issued, it is saved on blockchain, enabling access, download, and sharing from the platform in a secure and certified way. The platform also supports fast verification of metadata and document authenticity.

The webpage is organized in a highly functional and user-oriented manner. It begins with an introduction explaining the purpose of the platform, followed by detailed guidance on who can use the service. The platform is specifically intended for individuals holding officially recognized foreign qualifications, including upper-secondary diplomas that grant access to higher education as well as university-level degrees, up to doctoral qualifications.

Introduction to the platform

The CIMEA Diplome Chain for Institutions platform is a web application that enables universities, certification bodies and partner organisations to notarise PDF documents on the blockchain. Documents are notarised on CIMEA's proprietary blockchain infrastructure. Its purpose is to provide reliable and immutable proof of a file's existence at a specific point in time, ensuring that its content has not been altered. As such, the project represents a viable option for higher education institutions to ensure easy verification of the authenticity of any document issued as part of their procedures. The platform offers an open access area for verification of notarised documents as well. This section allows anyone to check if a given PDF has been notarised on the CIMEA Diplome Chain. This action is possible without needing to register on the platform.

Key features:

Timestamp and integrity - Each notarised PDF is associated with a cryptographic hash. The hash is a "digital fingerprint" of the content: if the file changes by even a single byte, the corresponding hash changes. By recording the hash on the blockchain, an immutable proof of the document's existence on that date is obtained.

Data confidentiality - The original document never leaves the uploader's device. The platform calculates the hash locally and sends this code to the blockchain, protecting the privacy of the content. Therefore, the CIMEA Diplome Chain for Institutions platform never saves the notarised document, ensuring maximum data protection and confidentiality.

UX/UI - The web interface is designed to be intuitive. To certify a file, simply log in to your account, select the PDFs and start the notarisation process. No specific technical skills are required.

Dedicated infrastructure – The blockchain on which the service is based, known as CIMEA Diplome Chain, is a permissioned blockchain managed by CIMEA. This model ensures high standards of security, reliability and scalability.

Roles and permissions for notarisation

To ensure the proper management of notarisation processes, the CIMEA Diplome Chain for Institutions platform introduces distinct roles that determine the actions permitted for each user:

Manager

This is the main user of the partner organisation. CIMEA is taking care of the creation of the Manager's profile, by inserting a name, surname, and email address previously provided. Once created, the system automatically sends an activation email to the provided address: via the link in the message, the new Manager sets his/her password and activates the account. Until the password is set, the Manager will not be able to log in. Manager has full control over the account and can:

- **Access the dashboard** to view the complete list of documents notarized by the organization and by individual users. The dashboard provides a clear overview of the notarized files, including information such as the document title, certification date (timestamp), and associated hash.
- **Upload and notarise documents**
- **View the list of documents already notarized**
- **Manage internal accounts** by creating new users or revoking access.

Users

These are the operators authorised by the manager to use the platform. All users within a specific organisation can:

- **Access the dashboard** to view the complete list of documents notarised by the organisation and by individual users.
- **Upload and notarise documents**
- **View the list of documents already notarised**

Back-office functionality

The back-office is the area reserved for authenticated users where the main operational activities take place. Its functions are organised into clear sections and allow the entire notarisation lifecycle to be managed.

The platform can be accessed via the login portal[7], where each user enters his/her email address and password.

Figure below shows the administrator/issuer dashboard of the CIMEA Diplome Chain for Institutions platform, including notarization statistics, credential management tools, and recent document activity.

[7] https://cimea-diplome-ntrz.it/login

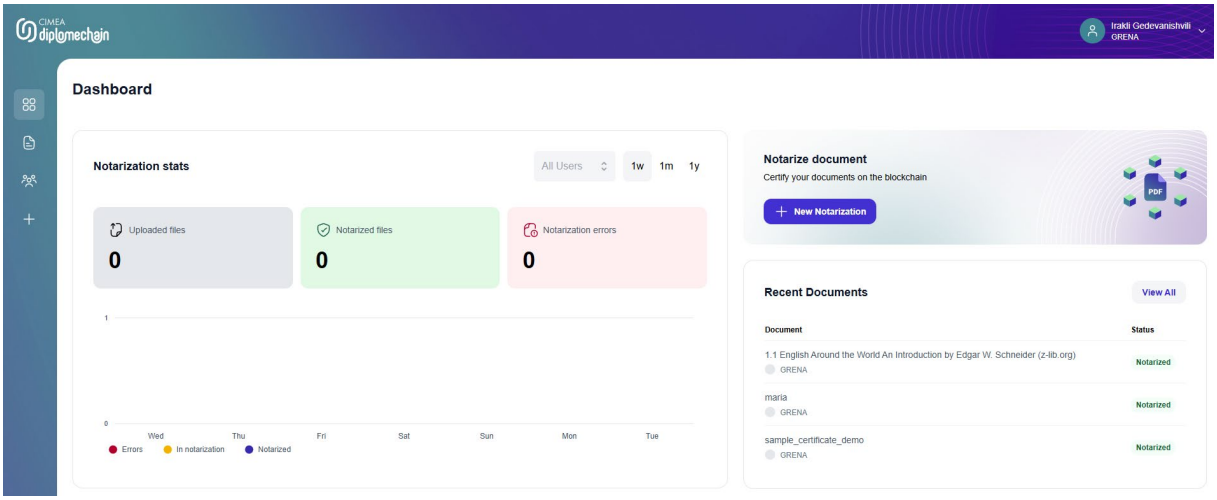


Figure 5 Administrator dashboard (issuer interface)

Notarisation process

The complete step-by-step procedure for notarising a document on the CIMEA Diplome Chain for Institutions platform is following:

Accessing the back-office - The Manager/User accesses the login page[8] and enters their credentials to access the back-office. After authentication, they are redirected to the main dashboard.

Navigating to the notarisation section - From the dashboard, select the 'New notarisation' option to start the process.

Uploading documents - The Manager/User can drag and drop PDFs into the upload area or select them manually. The maximum file size allowed for upload is 25 MB. It is advisable to check that the documents are in their final version, as any subsequent changes would alter the hash.

Filling in metadata - The Manager/User can manually enter certain information, including a "Metadata" field and a "Description" field. Please note that the information entered in the "Metadata" field will also be visible on the blockchain. It is advisable to fill in this information carefully to facilitate the searchability and traceability of notarised documents.

Hash generation. The system automatically calculates the hash of each file. The Manager/User can view these values and use them as a reference.

Confirmation of notarization - The request is sent with a single click: for each hash, a transaction is recorded on the blockchain certifying its existence. The system returns a summary with the certified hashes and corresponding timestamps.

Verification of registration - After notarisation, information about the documents appears in the Documents section. The Manager/User can access it at any time to verify the details or to provide others with the certified hash. If the notarisation process fails, the system will display

[8] https://cimeadiplome-ntrz.it/login

the label “failed” and, via a dedicated button, it will be possible to attempt the notarisation again.

Technical support related to the notarisation process can be obtained via techsupport-ntrz@cimea.it

One of the platform's most important features is its open-access verification area, available at CIMEA DiploMe without any need for registration or login. This public portal allows any person a prospective employer, another university, a government ministry, or any other third party to check whether a given PDF document has been notarised on the CIMEA Diplome Chain and whether it remains unaltered. The verification process is elegantly simple. The verifier visits the public portal and uploads the PDF they wish to check. The system immediately calculates the hash of that file locally, displaying it on screen. The verifier then clicks the "Verify file" button and the system searches the blockchain records for a matching hash. If a match is found, the document is confirmed as authentic: the portal displays the file name, the name of the organisation that notarised it, the document hash, the notarisation timestamp and any associated metadata. This outcome confirms that the document is intact and has not been changed since it was notarised. If no match is found, the system reports that the specific PDF is not present in the blockchain records meaning it was either never notarised on this platform, or it has been altered since notarisation, in either case warranting further inquiry with the issuing organisation. The public verification interface, where users can upload PDF documents to verify authenticity, integrity, and blockchain timestamping is presented on Figure 6.

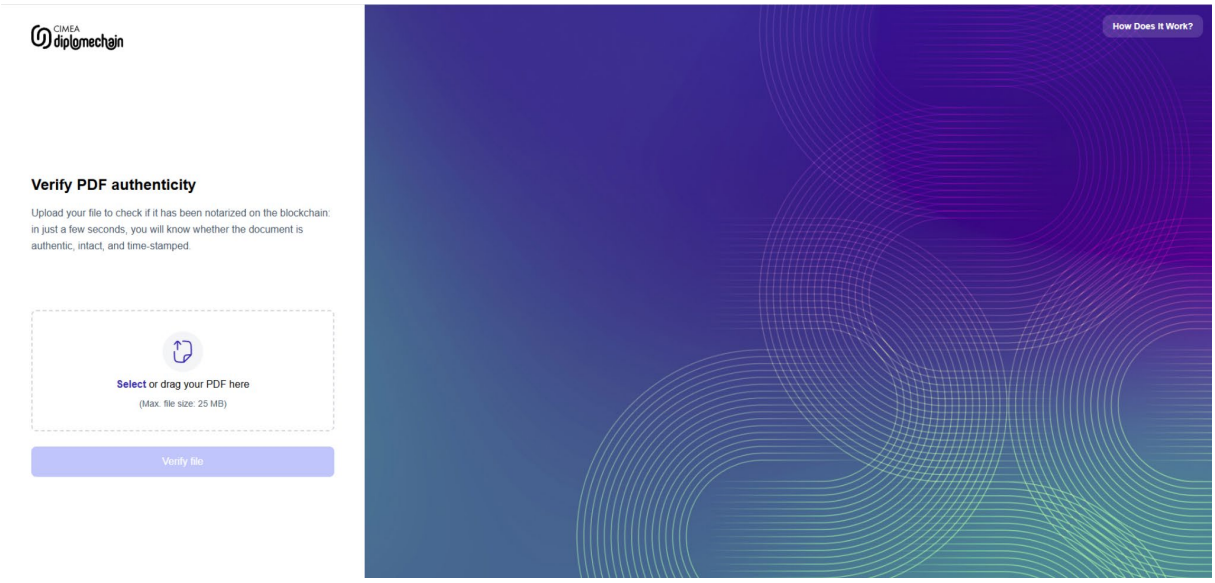


Figure 6 Public verification interface

5 Micro-GEAR Terms and Conditions for the use of CIMEA Diplome Chain for Institutions

Scope and parties

The Terms and Conditions of the CIMEA Diplome Chain for Institutions was developed to support project partners gain experience in notarisation of certification documents and governs the contractual relationship between Associazione CIMEA (acting as Service Provider) and each Micro-GEAR partner institution (referred to as the Partner). This section describes main conditions of the Terms and Conditions (signed full version is available at Associazione CIMEA and Partner institutions). The application is owned by CIMEA Diplome s.r.l., which has licensed it to Associazione CIMEA for use under this agreement. The service is provided entirely free of charge to Partner institutions for the full duration of the agreement, as part of the Micro-GEAR project.

Authorised use and partner obligations

The platform is provided exclusively to the Partner as a single institutional beneficiary. While the Partner may create multiple internal user accounts for its own staff, access credentials must not be shared with or transferred to external organisations or third parties. Any use of the platform by persons other than the Partner's own authorised personnel constitutes a material breach of the agreement.

By accepting the terms, the Partner warrants that:

- it has the legal authority to upload and notarise the documents in question;
- the documents do not infringe any third-party rights;
- the documents comply with applicable national and institutional laws and regulations;
- any personal data contained in uploaded documents is processed lawfully in compliance with the GDPR and relevant data protection rules.

The Partner is also expected to ensure the accuracy, completeness and integrity of all uploaded documents and to maintain the strict confidentiality of its access credentials. The partner remains fully responsible for all actions carried out under its accounts.

What is notarisation

The Terms and Conditions are explicit on a point that is essential for institutions to understand before using the platform: notarisation as provided by this service does not replace legal certification or official archiving obligations, and it does not constitute proof of authenticity recognised in all jurisdictions.

Technically, the service generates a cryptographic hash of the uploaded PDF and records it on a permissioned blockchain, creating a timestamped proof that the document existed in its current form at a specific point in time. The full document content is not stored on the blockchain only the hash or equivalent cryptographic representation is recorded. Any subsequent alteration of the document can be detected through cryptographic verification.

The legal weight and recognition of that record varies depending on the jurisdiction and the authority to which the document is presented. The Partner is responsible for verifying, before using the platform for a specific purpose, that notarised records will be accepted by the

relevant institutions or authorities. The Service Provider does not guarantee recognition of notarisation as legal proof in all jurisdictions.

Intellectual property

All intellectual property rights in the application remain with the Service Provider (via its Owner, CIMEA Diplome s.r.l.). The Partner retains full ownership of all documents it uploads. By using the application, the Partner grants the Service Provider a limited licence to process uploaded documents solely for the purpose of providing the notarisation service and for no other purpose.

Duration, renewal and termination

The agreement enters into force on the date the partner signs and returns it to CIMEA and remains valid for one year from that date. Upon expiry, access to the application is terminated unless CIMEA decides, at its sole discretion, to continue providing access — potentially under revised terms and conditions.

CIMEA may also suspend or terminate access at any time if the Partner breaches the agreement, if request volumes become excessively high, or for maintenance, technical, or other operational reasons at CIMEA's discretion.

A critical practical point: existing blockchain records are not affected when the agreement ends, as the immutable nature of the blockchain means those records remain permanently. However, the Partner's ability to access and consult those records through the platform's interface may cease once the agreement expires. Institutions should therefore maintain their own independent records of certified hashes and timestamps and must not rely solely on the platform for access to previously notarised documents.

Limitation of liability

The Service Provider's liability is limited to the fullest extent permitted by law. CIMEA is not liable for:

- indirect, incidental, or consequential damages;
- loss of data, reputation, or business opportunities;
- any reliance placed on notarised records beyond their technical function;
- consequences arising from the loss or disclosure of the Partner's access credentials.

The Service Provider is not obliged to ensure the service is suitable for any specific purpose the partner has in mind. Once the Partner begins using the application, it is presumed to have verified its suitability.

Governing law and jurisdiction

The agreement is governed by and construed in accordance with the laws of Italy. Any disputes arising from the agreement are subject to the exclusive jurisdiction of the courts of Rome, Italy, except where mandatory provisions of law require otherwise.

Amendments

The Service Provider reserves the right to amend this Agreement from time to time. The Partner will be notified of any significant changes through the designated communication channels. If any provision of this Agreement is deemed invalid, void, or for any reason

inapplicable, this condition will not in any case affect the validity and effectiveness of the other provisions.

Confidentiality

Both parties are obliged to keep confidential all non-public information received from the other party in connection with the agreement and to use such information solely for the purposes of performing their obligations. This confidentiality obligation survives the termination or expiry of the agreement for a period of three (3) years.

The obligation does not apply to information that: (i) is or becomes publicly available through no fault of the receiving party; (ii) was already known to the receiving party prior to disclosure; or (iii) is required to be disclosed by law or by order of a competent authority.

Assignment

The Partner may not assign, transfer, or sub-license any of its rights or obligations under this agreement to any third party without the prior written consent of the Service Provider. Any such assignment made without consent is null and void.

The Service Provider may assign the agreement, in whole or in part, to any entity it deems appropriate, provided this does not materially affect the Partner's rights. The Partner must be notified of any such assignment within thirty (30) days.

6 Pilot use of CIMEA Diplome Chain for Institutions platform for notarization of certificates

Within the frame of the Micro-GEAR project a series of micro-credential courses were developed and delivered by the partners in Georgia and Armenia to support learners in acquiring practical, up-to-date skills relevant to the evolving labour market. These short, flexible learning courses were designed to provide targeted knowledge and competencies that can be quickly applied in professional contexts.

The courses followed the micro-credential approach, meaning they focused on specific skill sets, were practice oriented and completed within a shorter period compared to traditional academic programs. All partners provided certificates to the students accomplished the courses. The next step was notarization of issued certificates. This is arranged using CIMEA Diplome Chain for Institutions platform described in sections 4 and 5.

Below notarization example of certificate issued by GRENA is presented. GRENA delivered the course: Network administration for small and medium sized organizations including Cisco and Juniper equipment and protocols. The duration of the course was two months. Upon completion of the course, participants received certificates, which were uploaded to the CIMEA Diplome Chain for Institutions platform for the notarization of MICRO-GEAR micro-credentials.

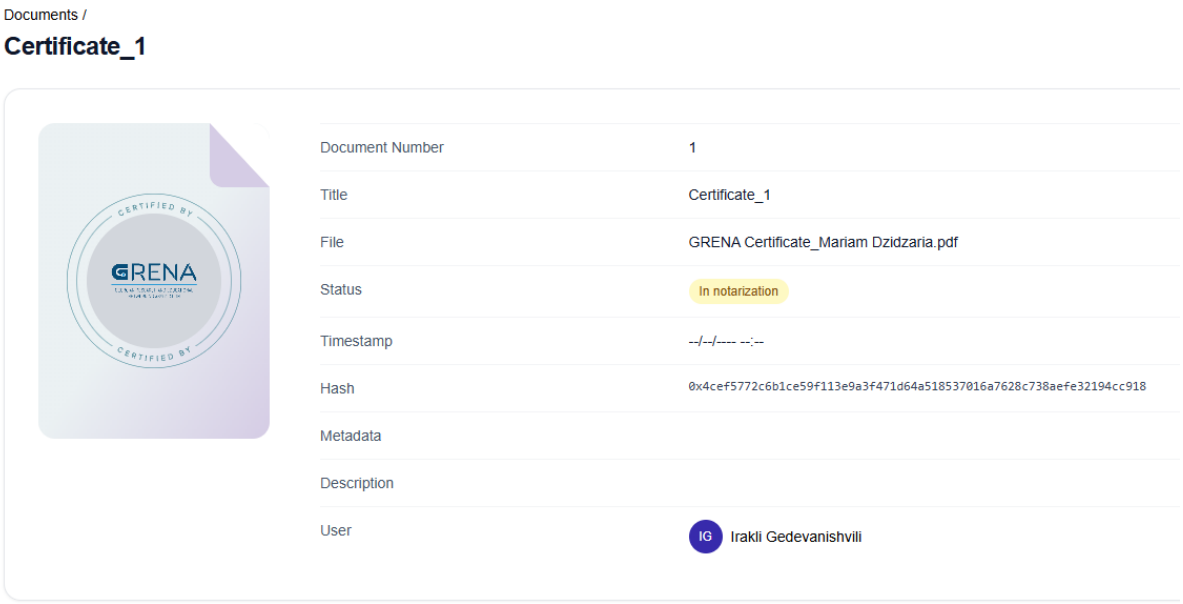


Figure 7 Screenshot of notarization of the certificate issued by GRENA

7 Conclusions

The aim of the Micro-GEAR project is to introduce and facilitate the broad proliferation of micro-credentials as a tool for improving relevance, quality and flexibility of Higher Education. Deliverable 3.2 presents work performed by the project partners to enhance technical capacity for the digital micro-credentialing in Georgia and Armenia. The main results are following:

1. Development of the survey by the Associazione CIMEA to measure the level of digitalization of the piloting partners in Georgia and Armenia. From each country two universities and one educational organization were participated. The survey results showed that participating institutions are still in the early stages of digital transformation and blockchain adoption, however there is institutional commitment to further development in this area. The findings demonstrated the need for continued technical training, institutional support, infrastructure development and policy alignment in order to establish secure and reliable digital credentialing systems.

2. Preparatory online meeting for the technical training on the use of Diplome-CHAIN was organized by Associazione CIMEA representatives on 13 November 2025. The following topics were discussed: introduction to WP3 and T3.2, results of survey and training topics for the Madrid workshop.

3. The study visit combined with face-to-face hands-on training workshop in Madrid was organized. The workshop programme introduced participants to European practices and technological solutions for digital credential issuance and verification, also blockchain and digital credentials: Legal aspects of reliability, governance and protection of rights were discussed by the representatives from Universidad Carlos III de Madrid and Universita Degli Studi. The second part of the event was devoted to practical training on CIMEA Diplome Chain for Institutions platform.

4. Micro-GEAR Terms and Conditions for the use of CIMEA Diplome Chain for partner institutions was developed and delivered by Associazione CIMEA. The pilot implementation of notarization of the developed by the project courses based on this platform is in progress.

Overall presented in this report activities significantly improved technical capacity of project partners in Georgia and Armenia to effectively design, develop, deliver and evaluate micro-credentials.

References

Analysis of Existing Micro-Cedential System Practices in Higher Education System of Georgia https://microgear.org/files/Analysis-of-Existing-Micro-Cedential-System-Practices-in-Higher-Education-System-of-Georgia.pdf

Analysis of Existing Micro-Credential Practices in Higher Education System of Armenia

Associazione CIMEA https://www.cimea.it/

CIMEA Diplome Chain for Institutions – Operational Manual

Education Management Information System https://emis.ge/

Higher Education and Science Committee https://www.hesc.am/en/

https://microgear.org/files/Analysis_of_Existing_Micro_Credential_Practices_in_HE_of_GEO_and_Armenia.pdf

Micro-GEAR TERMS and CONDITIONS for the use of CIMEA Diplome Chain

Micro-GEAR website https://microgear.org/

Minister of Education, Science, and Youth of Georgia https://mes.gov.ge/

Ministry of Education, Science, Culture and Sports of the Republic of Armenia https://escs.am/en

Glossary

D	Deliverable
EC	European Commission
ECTS	European Credit Transfer and Accumulation System
EU	European Union
GDPR	General Data Protection Regulation
HE	Higher Education
HEI	Higher Education Institution
QA	Quality Assurance
WP	Work Package
T	Task